Asian J. Math.
Vol. 24, No. 2, pp. 267–302, April 2020

THE VANISHING OF THE μ-INVARIANT FOR SPLIT PRIME $\mathbb{Z}_P$-EXTENSIONS OVER IMAGINARY QUADRATIC FIELDS*

VLAD CRIŞAN† AND KATHARINA MÜLLER‡

Abstract. Let $\mathbb{K}$ be an imaginary quadratic field, p a rational prime which splits in $\mathbb{K}$ into two distinct primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, and $\mathbb{K}_\infty$ the unique $\mathbb{Z}_p$-extension of $\mathbb{K}$ unramified outside of $\mathfrak{p}$. For a finite abelian extension $\mathbb{L}$ of $\mathbb{K}$, we define $\mathbb{L}_\infty = \mathbb{L}\mathbb{K}_\infty$, and let $X(\mathbb{L}_\infty)$ be the Galois group of the maximal abelian p-extension of $\mathbb{L}_\infty$ which is unramified outside the primes of $\mathbb{L}_\infty$ lying above $\mathfrak{p}$. We use the Euler system of elliptic units and a suitable generalisation of Sinnott's method to give a rather elementary and completely self-contained proof that $X(\mathbb{L}_\infty)$ is always a finitely generated $\mathbb{Z}_p$-module. This is the analogue for this split prime $\mathbb{Z}_p$-extension of the Ferrero-Washington theorem for the cyclotomic $\mathbb{Z}_p$-extension. Our proof simplifies and clarifies earlier work by Schneps, Gillard, and Oukhaba-Viguié.

Key words. Iwasawa theory, p-adic L-functions, split prime μ-conjecture.

Mathematics Subject Classification. 11R23, 11G05.

1. Introduction. Let $\mathbb{K}$ be an imaginary quadratic field and p a rational prime which splits in $\mathbb{K}$ into two distinct primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$, respectively. By global class field theory, there exists a unique $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/\mathbb{K}$ that is unramified outside $\mathfrak{p}$. Let $\mathbb{L}$ be a finite abelian extension of $\mathbb{K}$. We call $\mathbb{L}_\infty := \mathbb{L}\cdot\mathbb{K}_\infty$ the *split prime* $\mathbb{Z}_p$-extension of $\mathbb{L}$ corresponding to $\mathfrak{p}$. It is an abelian extension of $\mathbb{K}$. We shall fix the prime $\mathfrak{p}$ once and for all and omit explicit reference to it whenever it is clear from the context. We regard all our number fields as subfields of an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$; we also fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$ which induces the prime $\mathfrak{p}$, respectively.

Let $\mathbb{M}_\infty$ be the maximal p-abelian extension of $\mathbb{L}_\infty$ that is unramified outside the primes in $\mathbb{L}_\infty$ lying above $\mathfrak{p}$. By a standard maximality argument, $\mathbb{M}_\infty/\mathbb{K}$ is a Galois extension. Hence, if we denote $\Gamma := \mathrm{Gal}(\mathbb{L}_\infty/\mathbb{L})$, then $X(\mathbb{L}_\infty) := \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{L}_\infty)$ becomes a $\mathbb{Z}_p[[\Gamma]]$-module in the natural way, and hence a module over $\mathbb{Z}_p[[T]]$ (the power series ring over $\mathbb{Z}_p$ with indeterminate T), under an isomorphism $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ obtained via a fixed topological generator for Γ. For every $n \geq 0$, we let $\mathbb{L}_n$ denote the unique extension of $\mathbb{L}$ of degree p^n with $\mathbb{L}_n \subset \mathbb{L}_\infty$. Then $\mathbb{L}_n$ is an abelian extension of the imaginary quadratic field $\mathbb{K}$, so, by the Baker-Brumer theorem, the $\mathfrak{p}$-adic Leopoldt conjecture holds for the intermediate fields $\mathbb{L}_n$. It follows that $X(\mathbb{L}_\infty)$ is a $\mathbb{Z}_p[[T]]$-torsion module and hence it has a well-defined (up to units in $\mathbb{Z}_p[[T]]$) characteristic polynomial of the form $p^\mu \cdot f(T)$ for some non-negative integer μ (called the μ-invariant of $X(\mathbb{L}_\infty)$) and some distinguished polynomial $f \in \mathbb{Z}_p[[T]]$.

In this article we shall prove the following result, which is equivalent to the assertion that the μ-invariant of $X(\mathbb{L}_\infty)$ is zero.

Theorem 1. *The $\mathbb{Z}_p[[T]]$-module $X(\mathbb{L}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.*

Theorem 1 was previously proved by Schneps ([Sch, Theorem III]) for $\mathbb{L} = \mathbb{K}$, $\mathbb{K}$ of class number 1, $p \geq 5$ and by Gillard ([Gil 2, Theorem I.2]) for any $\mathbb{L}$ abelian

*Received April 23, 2019; accepted for publication May 24, 2019.

†Mathematisches Institut, Georg-August-Universität Göttingen, Bunsenstraße 3-5, D-37073 Göttingen, Germany (vlad.crisan@mathematik.uni-goettingen.de).

‡Mathematisches Institut, Georg-August-Universität Göttingen, Bunsenstraße 3-5, D-37073 Göttingen, Germany (katharina.mueller@mathematik.uni-goettingen.de).

over $\mathbb{K}$, $p \geq 5$. Recently, Choi, Kezuka, Li ([C-K-L]) and Oukhaba, Viguié ([O-V]) have independently worked towards completing the proof of the theorem for the cases $p = 2$ and $p = 3$. In [C-K-L], the result is proved for $p = 2$, $\mathbb{K} = \mathbb{Q}(\sqrt{-q})$ with $q \equiv 7 \pmod 8$ and $\mathbb{L}$=Hilbert class field of $\mathbb{K}$, while in [O-V] the result is proved for $p = 2, 3$ and any $\mathbb{L}$, extending the methods in [Gil 2]. The purpose of this article is to give a comprehensive and rather elementary proof for all fields $\mathbb{L}$ abelian over $\mathbb{K}$ and all primes p.

Before we discuss our approach for proving Theorem 1 and the structure of the paper, we give a useful reduction step. For an integral ideal $\mathfrak{a}$ of $\mathbb{K}$, we let $\mathbb{K}(\mathfrak{a})$ denote the ray class field modulo $\mathfrak{a}$ and we let $\omega_{\mathfrak{a}}$ be the number of roots of unity in $\mathbb{K}$ which are 1 modulo $\mathfrak{a}$. We claim that it suffices to prove Theorem 1 when $\mathbb{L}$ is of the form $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p})$ (respectively $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p}^2)$ for $p = 2$), where $\mathfrak{f} = (f)$ is a principal integral ideal of $\mathcal{O}_{\mathbb{K}}$ coprime to $\mathfrak{p}$ with $\omega_{\mathfrak{f}} = 1$ (the last condition holds for any $\mathfrak{f} \neq (1)$ upon replacing $\mathfrak{f}$ by $\mathfrak{f}^m$ for a sufficiently large m). Indeed, first note that if $\mathbb{J}/\mathbb{L}$ is an arbitrary abelian extension and $\mathbb{J}_\infty = \mathbb{J} \cdot \mathbb{L}_\infty$, then $\mathbb{M}(\mathbb{L}_\infty) \cdot \mathbb{J}_\infty \subset \mathbb{M}(\mathbb{J}_\infty)$. In particular, if $X(\mathbb{J}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, so is $X(\mathbb{L}_\infty)$. This allows us to assume that $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p}^n)$ where $\mathfrak{f}$ is as above and n is a positive integer. By class field theory and Chinese remainder theorem, for every $n \geq 1$ one has

$$\mathrm{Gal}\left(\mathbb{K}(\mathfrak{f}\mathfrak{p}^n)/\mathbb{K}(\mathfrak{f})\right) \cong \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times .$$

The following simple application of Nakayama's lemma serves two purposes: firstly, it allows one to further reduce the exponent n of $\mathfrak{p}$ in the definition of $\mathbb{L}$; secondly, it shows that one can prove Theorem 1 for p-solvable extensions of $\mathbb{L}$, which are not necessarily abelian over $\mathbb{K}$.

Lemma 1. *Let $\mathbb{J}/\mathbb{L}$ be a finite Galois extension of order p and let $\mathbb{J}_\infty/\mathbb{J}$ and $\mathbb{L}_\infty/\mathbb{L}$ be the split prime $\mathbb{Z}_p$-extensions of $\mathbb{J}$ and $\mathbb{L}$, respectively, so that $\mathbb{J}_\infty = \mathbb{L}_\infty\mathbb{J}$. If $X(\mathbb{L}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, then $X(\mathbb{J}_\infty)$ is also a finitely generated $\mathbb{Z}_p$-module.*

Proof. Let σ denote a generator of the Galois group $\mathfrak{G} := \mathrm{Gal}(\mathbb{J}_\infty/\mathbb{L}_\infty)$. Then $X(\mathbb{J}_\infty)$ is a $\mathbb{Z}_p[\mathfrak{G}]$-module under the natural action. Let $\mathbb{F}$ be the maximal abelian extension of $\mathbb{L}_\infty$ contained in $\mathbb{M}(\mathbb{J}_\infty)$. Then

$$R := \mathrm{Gal}(\mathbb{F}/\mathbb{J}_\infty) \cong X(\mathbb{J}_\infty)/(\sigma - 1)X(\mathbb{J}_\infty).$$

By Nakayama's lemma, it suffices to prove that R is finitely generated. Define the set

$$S = \{\text{primes in } \mathbb{L}_\infty \text{ coprime to } \mathfrak{p} \text{ and ramified in } \mathbb{J}_\infty/\mathbb{L}_\infty\}.$$

We know a priori that S is finite. If $S = \emptyset$, we obtain $\mathbb{M}(\mathbb{L}_\infty) = \mathbb{F}$; in this case, R is finitely generated over $\mathbb{Z}_p$ since $X(\mathbb{L}_\infty)$ is.

If S is not empty, consider for every prime $\mathfrak{q} \in S$ its inertia group $I_{\mathfrak{q}}$ in $Gal(\mathbb{F}/\mathbb{L}_\infty)$. Since $\mathbb{F}/\mathbb{J}_\infty$ is unramified at each $\mathfrak{q} \in S$ it follows that $I_{\mathfrak{q}} \cap R = \{0\}$. Thus, $I_{\mathfrak{q}}$ is cyclic of order p. Let I be the group generated by all the $I_{\mathfrak{q}}$'s and let $\mathbb{F}' = \mathbb{F}^I$. Then $[\mathbb{F} : \mathbb{F}'] \leq p^{|S|}$. The field $\mathbb{F}'$ is contained in $\mathbb{M}(\mathbb{L}_\infty)$. It follows that $\mathrm{Gal}(\mathbb{F}'/\mathbb{L}_\infty)$ is finitely generated and hence so is R. □

Combining Lemma 1 with our previous observations, it follows that for any prime $\mathfrak{p}$, it suffices to consider fields $\mathbb{L}$ of the form $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p})$ (resp. $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p}^2)$ when $p = 2$), with $\mathfrak{f} = (f)$ as above.

We let $\mathbb{F} := \mathbb{K}(\mathfrak{f})$, and for any $n \geq 0$, we define

$$\mathbb{F}_n = \mathbb{K}(\mathfrak{f}\mathfrak{p}^n), \quad \mathbb{F}_\infty = \bigcup_{n \geq 0} \mathbb{F}_n.$$

Having reduced the problem to the case $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p})$ (resp. $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p}^2)$ when $p = 2$), one then has $\mathbb{L}_\infty = \mathbb{F}_\infty$, and we shall subsequently work with $\mathbb{F}_\infty$. We let $t \geq 0$ be such that

$$\mathbb{K}_t = \mathbb{H}(\mathbb{K}) \cap \mathbb{K}_\infty.$$

We also define the groups

$$G = \mathrm{Gal}(\mathbb{F}/\mathbb{K}), \quad H = \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}_\infty), \quad \mathcal{G} = \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}) \cong \mathbb{Z}_p^\times.$$

The diagram of fields and corresponding Galois groups is given below.

$$\begin{tikzcd}
 & & & & \mathbb{M}(\mathbb{L}_\infty) \\
\mathbb{K}_\infty \arrow[rrr, dash, "H"] \arrow[d, dash] \arrow[dd, dash, bend right, "\Gamma'"'] & & & \mathbb{L}_\infty = \mathbb{F}_\infty \arrow[d, dash, "\Gamma"] \arrow[ur, dash, "X(\mathbb{L}_\infty)"'] & \\
\mathbb{K}_t \arrow[r, dash] \arrow[d, dash] & \mathbb{H}(\mathbb{K}) \arrow[r, dash] & \mathbb{F} \arrow[r, dash] & \mathbb{L} & \\
\mathbb{K} \arrow[urr, dash, bend right, "G"] & & & &
\end{tikzcd}$$

We shall now summarize our strategy for proving Theorem 1. Firstly, notice that $\mathbb{M}(\mathbb{F}_\infty)/\mathbb{K}$ is a Galois extension. Secondly, since $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}) \cong \mathbb{Z}_p$, it follows that there exists an isomorphism

$$\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}) \cong H \times \Gamma', \quad \text{where} \quad \Gamma' = \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}).$$

We fix once and for all such an isomorphism, which allows us to identify Γ' with a subgroup of $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$. By abusing notation, we shall also call this subgroup Γ'. For each character χ of H one can consider the largest quotient of $\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)$ on which H acts through χ. We denote this quotient by $\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)_\chi$. The Main Conjecture for $X(\mathbb{F}_\infty)$, formulated by Coates and Wiles in [Co-Wi 3] predicts that for all characters χ of H, the characteristic ideal of $\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)_\chi$ can be generated by the power series corresponding to a p-adic L-function. Some cases of the Main Conjecture were proven by Rubin in [Ru]. In our general setting, even though we do not have the Main Conjecture, one can establish a correspondence between the μ-invariants of certain p-adic L-functions and the μ-invariant of $X(\mathbb{F}_\infty)$. More precisely, our method of proof will be to construct for every χ a p-adic L-function $L_{\mathfrak{p},\mathfrak{f}}(s, \chi)$ and show that the μ-invariant of each $L_{\mathfrak{p},\mathfrak{f}}(s, \chi)$ is zero; we will then show that the sum of all μ-invariants $\mu\left(L_{\mathfrak{p},\mathfrak{f}}(s,\chi)\right)$ is the same as the μ-invariant of $X(\mathbb{F}_\infty)$, which will establish Theorem 1. While some of the results that we prove have a correspondent (or even generalizations) in the aforementioned articles, our approach for constructing the p-adic L-functions uses only properties of certain rational functions on elliptic curves, which makes the exposition more elementary.

The construction of the p-adic L-functions $L_{\mathfrak{p},\mathfrak{f}}(s,\chi)$ is the first main building block of our article and is carried out in detail in Section 2. In [Co-Go], building on techniques previously developed in [Co-Wi 2] and [Co-Wi 3], Coates and Goldstein presented a recipe for constructing the p-adic L-functions, provided one has an elliptic curve defined over a number field $\mathbb{F}$ containing $\mathbb{K}$, which has complex multiplication by the ring of integers of $\mathbb{K}$ and for which $\mathbb{F}(E_{tors})/\mathbb{K}$ is an abelian extension. We shall follow closely this approach for constructing the p-adic L-functions, extending it to our general setting. The first step will thus be to prove that when $\mathbb{F}=\mathbb{K}(\mathfrak{f})$ with $\mathfrak{f}$ as above, one can construct a suitable elliptic curve $E/\mathbb{F}$.

For the vanishing of μ for the p-adic L-functions $L_{\mathfrak{p},\mathfrak{f}}(s,\chi)$, we will extend the argument given by Schneps in [Sch], where she uses the elliptic analogue of Sinnott's beautiful proof of $\mu=0$ for the cyclotomic $\mathbb{Z}_p$-extension of abelian number fields (earlier proved by Ferrero and Washington in [Fe-Wa]).

2. Construction of the p-adic L-function.

2.1. Existence of a suitable elliptic curve. As before, we let $\mathfrak{f}=(f)$ be an integral ideal of $\mathbb{K}$ coprime to $\mathfrak{p}$ and for which $\omega_{\mathfrak{f}}=1$. As above, we let $\mathbb{F}=\mathbb{K}(\mathfrak{f})$ and we let $G=\mathrm{Gal}(\mathbb{F}/\mathbb{K})$. For a number field $\mathbb{M}$, we let $\mathbb{I}_{\mathbb{M}}$ denote the group of ideles of $\mathbb{M}$. We begin by proving the following.

Lemma 2. *There exists an elliptic curve $E/\mathbb{F}$ which satisfies the following properties.*

a) *E has CM by the ring of integers $\mathcal{O}_{\mathbb{K}}$ of $\mathbb{K}$;*

b) *$\mathbb{F}(E_{tors})$ is an abelian extension of $\mathbb{K}$;*

c) *E has good reduction at primes in $\mathbb{F}$ lying above $\mathfrak{p}$.*

Proof. Let $\mathbb{H}=\mathbb{K}(1)$ be the Hilbert class field of $\mathbb{K}$. Every elliptic curve $A/\mathbb{H}$ has an associated j-invariant j_A and a Grössencharacter $\psi_{A/\mathbb{H}}:\mathbb{I}_{\mathbb{H}}\to\mathbb{K}^*$, where $\mathbb{K}^*$ denotes the multiplicative group of $\mathbb{K}$. The invariant j_A lies in a finite set J of possible candidates with $|J|=h$ (the class number of $\mathbb{K}$) and $\psi_{A/\mathbb{H}}$ is a continuous homomorphism whose restriction to $\mathbb{H}^*\subset\mathbb{I}_{\mathbb{H}}$ is the norm map. Gross proved in [Gr, Theorem 9.1.3] that given a pair (j,ψ) with $j\in J$ and $\psi:\mathbb{I}_{\mathbb{H}}\to\mathbb{K}^*$ a continuous homomorphism whose restriction to $\mathbb{H}^*$ is the norm, there exists an elliptic curve E_0 defined over $\mathbb{H}$, having complex multiplication by $\mathcal{O}_{\mathbb{K}}$, with $j(E_0)=j$ and whose Grössencharacter $\psi_{E_0/\mathbb{H}}$ is precisely ψ. Consider thus an element $j\in J$ and an elliptic curve E_0 defined over $\mathbb{H}$ with complex multiplication by $\mathcal{O}_{\mathbb{K}}$ with $j(E_0)=j$. Since $\mathbb{H}\subset\mathbb{F}$, we can regard our curve E_0 as defined over $\mathbb{F}$. We shall modify this elliptic curve $E_0/\mathbb{F}$ to satisfy all the required conditions. We begin by constructing an elliptic curve satisfying a) and b).

Let $\psi_{E_0/\mathbb{F}}$ be the associated Grössencharacter to $E_0/\mathbb{F}$. Shimura proved in [Shi, Theorem 7.44] that the existence of an elliptic curve $E/\mathbb{F}$ satisfying b) is equivalent to the existence of a Grössencharacter φ of $\mathbb{K}$ of infinity type $(1,0)$, for which

$$\psi_{E/\mathbb{F}}=\varphi\circ N_{\mathbb{F}/\mathbb{K}}.$$

Let φ be a Grössencharacter of $\mathbb{K}$ of infinity type $(1,0)$ and conductor $\mathfrak{f}$ (recall that $\omega_{\mathfrak{f}}=1$). Let $\psi=\varphi\circ N_{\mathbb{F}/\mathbb{K}}$. Then $\chi:=\frac{\psi}{\psi_{E_0/\mathbb{F}}}:\mathbb{I}_{\mathbb{F}}\to\mathbb{K}^*$ has the property that

$\chi(\mathbb{F}^*) = 1$. Therefore, under the reciprocity map of class field theory, we can regard χ as a homomorphism $\chi : \mathrm{Gal}(\mathbb{F}^{ab}/\mathbb{F}) \to \mathbb{K}^*$. Since the Galois group $\mathrm{Gal}(\mathbb{F}^{ab}/\mathbb{F})$ is compact, it follows that the image of χ must lie in the finite multiplicative group $\mathcal{O}_{\mathbb{K}}^{\times}$. In particular, χ is a character of finite order. Furthermore, $\mathcal{O}_{\mathbb{K}}^{*} \subset Isom(E_0)$, where $Isom(E_0)$ denotes the group of $\overline{\mathbb{Q}}$-automorphisms of E_0. Thus, we can view the character χ as a map $\chi : \mathrm{Gal}(\mathbb{F}^{ab}/\mathbb{F}) \to Isom(E_0)$. A moment's thought shows that χ is a 1-cocycle, hence it defines an isomorphism class of elliptic curves defined over $\mathbb{F}$ which has the same j-invariant as E_0 (see [Gr, Section 3.3]). It follows that the twist E_0^{χ} is an elliptic curve defined over $\mathbb{F}$, with the same j-invariant as E_0 and by [Gr, Lemma 9.2.5],[1] one has that

$$\psi_{E_0^{\chi}/\mathbb{F}} = \chi \cdot \psi_{E_0/\mathbb{F}} = \varphi \circ N_{\mathbb{F}/\mathbb{K}}.$$

It follows that if we set $E = E_0^{\chi}$, the curve E satisfies the properties a) and b).

Finally, once we have an elliptic curve satisfying conditions a) and b), part c) follows from the fact that $\mathfrak{f}$ is coprime to $\mathfrak{p}$ and the primes of bad reduction are precisely the primes dividing the conductor of $\psi_{E/\mathbb{F}}$. □

We now fix a Grössencharacter ϕ of $\mathbb{K}$ of conductor $\mathfrak{f}$ and infinity type $(1, 0)$ and let $E/\mathbb{F}$ be an elliptic curve satisfying the conditions in Lemma 2 for which its Grössencharacter $\psi_{E/\mathbb{F}}$ satisfies

$$\psi_{E/\mathbb{F}} = \phi \circ N_{\mathbb{F}/\mathbb{K}}.$$

Since E has good reduction at the primes in $\mathbb{F}$ lying above $\mathfrak{p}$, there exists a generalized Weierstrass model for E of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

for which the discriminant $\Delta(E)$ is coprime to any prime in $\mathbb{F}$ above $\mathfrak{p}$. We also take the model (1) to be minimal at all primes lying above $\mathfrak{p}$. The Neron differential attached to the above model is

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

We fix once and for all such a generalized model and differential ω for E. We also let $\mathcal{L}$ denote the period lattice determined by the pair (E, ω).

For an element $a \in \mathcal{O}_{\mathbb{K}}$, we identify a with the endomorphism of E whose differential is a and let E_a denote the kernel of this endomorphism; for an ideal $\mathfrak{a}$ of $\mathbb{K}$, we let $E_{\mathfrak{a}}$ denote

$$E_{\mathfrak{a}} = \bigcap_{a \in \mathfrak{a}} E_a.$$

With these notations, it is proved in [Co-Go, Lemma 3] that for any $n \geq 0$, one has $\mathbb{F}(E_{\mathfrak{p}^n}) = \mathbb{F}_n$.

For any $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, we will write E^{σ} (resp. ω^{σ}) for the curve (resp. the differential) obtained by applying σ to the equation (1) of E (resp. to ω). Since $\mathbb{F}(E_{tors})/\mathbb{K}$ is an abelian extension of $\mathbb{K}$, it follows that for any $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$,

[1] Gross only proves this when $\mathfrak{f} = 1$, but the result is true in general-see for example [Sil 2, Exercise II.2.25].

one has $\psi_{E^\sigma/\mathbb{F}} = \psi_{E/\mathbb{F}}$. Moreover, as the $\mathbb{F}$-isogeny class of $E/\mathbb{F}$ is determined by the Grössencharacter of $E/\mathbb{F}$, it follows that all the Galois conjugates of E are $\mathbb{F}$-isogeneous. Let $\mathfrak{a}$ be any ideal in $\mathcal{O}_\mathbb{K}$ coprime to $\mathfrak{f}$ and let $\sigma_\mathfrak{a}$ denote its Artin symbol in $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$. For an element $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, we let $\mathcal{L}_\sigma$ be the lattice associated with E^σ. The Weierstrass isomorphism $\mathcal{M}(z, \mathcal{L}_{\sigma_\mathfrak{a}}) : \mathbb{C}/\mathcal{L}_{\sigma_\mathfrak{a}} \to E^{\sigma_\mathfrak{a}}(\mathbb{C})$ is given by

$$z \to \left(\wp_{\mathcal{L}_{\sigma_\mathfrak{a}}}(z) - b_{\sigma_\mathfrak{a}}, \frac{1}{2}\left(\wp'_{\mathcal{L}_{\sigma_\mathfrak{a}}}(z) - a_1^{\sigma_\mathfrak{a}}\left(\wp_{\mathcal{L}_{\sigma_\mathfrak{a}}}(z) - b_{\sigma_\mathfrak{a}}\right) - a_3^{\sigma_\mathfrak{a}}\right)\right),$$

where $\wp_{\mathcal{L}_{\sigma_\mathfrak{a}}}$ is the Weierstrass $\wp$-function of $\mathcal{L}_{\sigma_\mathfrak{a}}$ and $b_{\sigma_\mathfrak{a}} = \frac{\left(a_1^{\sigma_\mathfrak{a}}\right)^2 + 4a_2^{\sigma_\mathfrak{a}}}{12}$.

By the main theorem of complex multiplication, for any such $\mathfrak{a}$ and any $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ there exists a unique isogeny $\eta_\sigma(\mathfrak{a}) : E^\sigma \to E^{\sigma\sigma_\mathfrak{a}}$ defined over $\mathbb{F}$, of degree $N(\mathfrak{a})$, which satisfies

$$\sigma_\mathfrak{a}(u) = \eta_\sigma(\mathfrak{a})(u),$$

for any $u \in E^\sigma[\mathfrak{g}]$, where $(\mathfrak{g}, \mathfrak{a}) = 1$. The kernel of this isogeny is precisely $E^\sigma_\mathfrak{a}$ (see [Co-Go, proof of Lemma 4]). From now on, we shall write $\eta(\mathfrak{p})$ and $\eta_\mathfrak{a}(\mathfrak{p})$ for the isogenies $\eta_e(\mathfrak{p}) : E \to E^{\sigma_\mathfrak{p}}$ and $\eta_{\sigma_\mathfrak{a}}(\mathfrak{p}) : E^{\sigma_\mathfrak{a}} \to E^{\sigma_\mathfrak{a}\sigma_\mathfrak{p}}$, respectively. As explained in [Co-Go, p. 341], there exists a unique $\Lambda(\mathfrak{a}) \in \mathbb{F}^*$ such that

$$\omega^{\sigma_\mathfrak{a}} \circ \eta(\mathfrak{a}) = \Lambda(\mathfrak{a})\omega, \tag{2}$$

which can also be written as

$$\eta(\mathfrak{a}) \circ \mathcal{M}(z, \mathcal{L}) = \mathcal{M}\left(\Lambda(\mathfrak{a})z, \mathcal{L}_{\sigma_\mathfrak{a}}\right). \tag{3}$$

Note that Λ satisfies the cocycle condition

$$\Lambda(\mathfrak{a}\mathfrak{b}) = \Lambda(\mathfrak{a})^{\sigma(\mathfrak{b})}\Lambda(\mathfrak{b}). \tag{4}$$

It follows that we can extend the definition of Λ to the set of all fractional ideals coprime to $\mathfrak{f}$ so that (4) remains valid. Moreover, when $\mathfrak{a}$ is integral with $\sigma_\mathfrak{a} = 1$, we obtain further that $\Lambda(\mathfrak{a}) = \phi(\mathfrak{a})$ (see [dS, p. 42] for details). The choice of the embedding of $\mathbb{F}$ in $\mathbb{C}$ gives a non-zero complex number $\Omega_\infty \in \mathbb{C}$ (which is well-defined up to multiplication by a root of unity in $\mathbb{K}$) such that $\mathcal{L} = \Omega_\infty \mathcal{O}_\mathbb{K}$ (see the discussion before relation (13) in [Co-Go]). Furthermore, it is proved in [Co-Go, p. 342], that for any integral ideal $\mathfrak{a}$ coprime to $\mathfrak{f}$ one has the relation

$$\Lambda(\mathfrak{a})\Omega_\infty \mathfrak{a}^{-1} = \mathcal{L}_{\sigma_\mathfrak{a}}. \tag{5}$$

Let v be the prime in $\mathbb{F}$ lying above $\mathfrak{p}$ which is induced by our fixed embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}_p$ and let $\mathfrak{m}_v$ denote the maximal ideal of $\mathcal{O}(\mathbb{F}_v)$. Let $\mathcal{I}_\mathfrak{p}$ be the ring of integers in the completion of the maximal unramified extension of $\mathbb{F}_v$. Let π be a generator of the prime ideal of $\mathcal{I}_\mathfrak{p}$. Then $\mathcal{I}_\mathfrak{p}/\pi\mathcal{I}_\mathfrak{p}$ has characteristic p and is algebraically closed. Lubin showed in [Lu, Corollary 4.3.3] that if the reduction at π of a formal group has height one, then it is isomorphic to the formal multiplicative group over $\mathcal{I}_\mathfrak{p}$. We recall that E has good reduction at every v above $\mathfrak{p}$. For each $\sigma \in G$, let $\widehat{E^{\sigma,v}}$ denote the formal group giving the kernel of reduction modulo v on the elliptic curve $E^\sigma/\mathbb{F}$ (see [Sil 1, Proposition V.2.2]). Note that $\widehat{E^{\sigma,v}}$ is a relative Lubin-Tate formal group in the sense of de Shalit ([dS, Chapter I] and [dS, Lemma II.1.10]). Since we chose a $\mathfrak{p}$-minimal model for E, a parameter for the formal group $\widehat{E^{\sigma,v}}$ is given by

$$t_\sigma = -x_\sigma / y_\sigma.$$

When σ is the identity, we shall simply write $\widehat{E^v}$, t, etc. Since p splits in $\mathbb{K}$ and $\mathfrak{p}$ is a prime of good reduction, the reduction of E modulo v is injective on the set $E_{\overline{\mathfrak{p}}}$. It follows that the reduction of E modulo v has to contain p-torsion points, which implies that the reduction of E modulo v has height 1 (see [Sil 1, Theorem V.3.1].) We obtain the following result.

Lemma 3. *There exists an isomorphism β^v between the formal multiplicative group $\widehat{\mathbf{G}}_m$ and the formal group $\widehat{E^v}$, which can be written as a power series $t = \beta^v(w) \in \mathcal{I}_\mathfrak{p}[[w]]$.*

As noted in [Co-Go], the isomorphism in Lemma 3 is unique up to composition with an automorphism of $\widehat{\mathbf{G}}_m$ over $\mathcal{I}_\mathfrak{p}$ and the group of automorphism of $\widehat{\mathbf{G}}_m$ over $\mathcal{I}_\mathfrak{p}$ can be identified with $\mathbb{Z}_p^\times$. We fix once and for all an isomorphism $\beta^v(w)$ and we let Ω_v denote the coefficient of w in $\beta^v(w)$. In particular, it follows that Ω_v is a unit in $\mathcal{I}_\mathfrak{p}$. For an integral ideal $\mathfrak{a}$ of $\mathbb{K}$ coprime to $\mathfrak{f}$, the isogeny $\eta(\mathfrak{a})$ induces a homomorphism

$$\widehat{\eta(\mathfrak{a})} : \widehat{E^v} \to \widehat{E^{\sigma_\mathfrak{a},v}},$$

which is defined over $\mathcal{O}(\mathbb{F}_v)$. When $\mathfrak{a}$ is coprime to $\mathfrak{f}\mathfrak{p}$, it becomes an isomorphism. It follows that one can construct an isomorphism $\beta^v_\mathfrak{a} = \widehat{\eta(\mathfrak{a})} \circ \beta^v$ between $\widehat{\mathbf{G}}_m$ and $\widehat{E^{\sigma_\mathfrak{a},v}}$. We also let $\Omega_{\mathfrak{a},v}$ be the coefficient of w in $\beta^v_\mathfrak{a}(w)$. As proven for example in [Co-Go, Lemma 6], the relation between Ω_v and $\Omega_{\mathfrak{a},v}$ is given by

$$\Omega_{\mathfrak{a},v} = \Lambda(\mathfrak{a})\Omega_v. \tag{6}$$

We also let $\widehat{\mathbf{G}}_a$ denote the formal additive group. One has the following commutative diagram of formal groups, in which we denoted by Log the isomorphism between $\widehat{\mathbf{G}}_m$ and $\widehat{\mathbf{G}}_a$:

$$\begin{tikzcd}
\widehat{\mathbf{G}}_m \arrow[r, "\beta^v"] \arrow[dr, "\mathrm{Log}"] & \widehat{E^v} \arrow[r, "\widehat{\eta(\mathfrak{a})}"] & \widehat{E^{v,\sigma_\mathfrak{a}}} \\
& \widehat{\mathbf{G}}_a \arrow[u, "\mathcal{M}"] \arrow[r, "\cdot\Lambda(\mathfrak{a})"] & \widehat{\mathbf{G}}_a \arrow[u, "\mathcal{M}_\mathfrak{a}"]
\end{tikzcd}$$

2.2. The basic rational functions. We will now introduce the basic rational functions for the elliptic curve $E/\mathbb{F}$, as given in [Co]. To motivate the choice of the rational functions we will introduce, we need some additional notations.

For any lattice L we define

$$s_2(L) = \lim_{s \searrow 0} \sum_{w \in L \setminus \{0\}} w^{-2} \cdot |w|^{-2s}, \quad A(L) = \frac{1}{\pi}\mathrm{Area}(\mathbb{C}/L),$$

and

$$\eta(z, L) = A(L)^{-1}\overline{z} + s_2(L)z.$$

With these notations, we define the θ-function for the lattice L by

$$\theta(z, L) = \Delta(L)\exp(-6\eta(z, L)z)\sigma(z, L)^{12},$$

where $\sigma(z, L)$ is the Weierstrass σ-function of L.

For every non-trivial ideal $\mathfrak{m}$ of $\mathbb{K}$ and any $\sigma \in \mathrm{Gal}(\mathbb{K}(\mathfrak{m})/\mathbb{K})$, the Robert's invariant is defined by $\varphi_{\mathfrak{m}}(\sigma) = \theta(1, \mathfrak{m}\mathfrak{c}^{-1})^m$, where m is the least positive integer in $\mathfrak{m} \cap \mathbb{Z}$ and $\sigma = \left(\frac{\mathbb{K}(\mathfrak{m})/\mathbb{K}}{\mathfrak{c}}\right)$. As proved for example in [dS, Chapter II Section 2.4], one has the identity

$$\varphi_{\mathfrak{m}}(1)^{N(\mathfrak{a}) - \left(\frac{\mathbb{K}(\mathfrak{m})/\mathbb{K}}{\mathfrak{a}}\right)} = \left(\frac{\theta(1, \mathfrak{m})^{N(\mathfrak{a})}}{\theta(1, \mathfrak{a}^{-1}\mathfrak{m})}\right)^m. \tag{7}$$

For an integral ideal $\mathfrak{m}$ of $\mathbb{K}$ and a character χ, we define the L-series of χ with modulus $\mathfrak{m}$ by

$$L_{\mathfrak{m}}(\chi, s) = \sum \chi(\mathfrak{a})N(\mathfrak{a})^{-s},$$

where the sum is over all integral ideals $\mathfrak{a}$ coprime to $\mathfrak{m}$. The following theorem proved in [Sie, Theorem 9] (see also [dS, Chapter II, Theorem 5.1]) gives a useful relation between global L-functions and logarithms of Robert-invariants.

Theorem 2. *Let $\mathfrak{m}$ be an non-trivial integral ideal of K and let χ be a character of finite order of conductor $\mathfrak{m}$. Let $L_{\infty,\mathfrak{m}}(\chi, s) = (2\pi)^{-s}\Gamma(s)L_{\mathfrak{m}}(\chi, s)$. Then*

$$L_{\infty,\mathfrak{m}}(\chi, 0) = \frac{-1}{12m\omega_{\mathfrak{m}}} \sum_{\sigma \in Gal(\mathbb{K}(\mathfrak{m})/\mathbb{K})} \chi(\sigma) \log|\varphi_{\mathfrak{m}}(\sigma)|^2,$$

where m is the smallest positive integer in $\mathfrak{m} \cap \mathbb{Z}$ and $\log$ *denotes the standard logarithm function on $\mathbb{R}$.*

In the same way in which in the class number formula the product $\prod_{\chi} L(\chi, 1)$ can be expressed in terms of the class number, the discriminant and the regulator of the field, it turns out that the product

$$\prod_{\chi} \frac{1}{12m\omega_{\mathfrak{m}}} \sum_{\sigma \in \mathrm{Gal}(\mathbb{K}(\mathfrak{m})/\mathbb{K})} \chi(\sigma) \log\varphi_{\mathfrak{m}}(\sigma) \quad \text{(p-adic logarithm here)}$$

can also be expressed in terms of the p-part of the class number, the $\mathfrak{p}$-adic regulator and the $\mathfrak{p}$-adic discriminant of the field. On the other hand, Coates and Wiles proved in [Co-Wi 1, Theorem 11] a relation between the μ-invariant of the Galois group $\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)$ and these p-adic quantities (see Corollary 1 in Section 4 for the precise statement). In view of these facts, our aim is to prove a $\mathfrak{p}$-adic analogue of Theorem 2. Since we construct our p-adic L-function using rational functions on the elliptic curve, we will need these rational functions to have a form closely related to the Robert's invariant.

We recall that $G = \mathrm{Gal}(\mathbb{F}/\mathbb{K})$. For $\sigma \in G$, we let P_σ denote a generic point on E^σ and let $x(P)$ denote its x-coordinate in the model (1). By abuse of notation, if u denotes a rational function on E^σ, we shall write $u(z)$ for $u \circ \mathcal{M}(z, \mathcal{L}_\sigma)$.

For any $\alpha \in \mathcal{O}_{\mathbb{K}}$ that is non-zero, coprime to 6 and not a unit, we define the rational function $\xi_{\alpha,\sigma}(P_\sigma)$ on E^σ by

$$\xi_{\alpha,\sigma}(P_\sigma) = c_\sigma(\alpha) \prod_{S \in V_{\alpha,\sigma}} \left(x(P_\sigma) - x(S)\right),$$

where $V_{\alpha,\sigma}$ is any set of representatives of the non-zero α-division points on E^σ modulo $\{\pm 1\}$ and $c_\sigma(\alpha)$ is a canonical 12th root $\mathbb{F}$ of the quotient $\Delta(\alpha^{-1}\mathcal{L}_\sigma)/\Delta(\mathcal{L}_\sigma)^{N_{\mathbb{K}/\mathbb{Q}}(\alpha)}$ (here Δ stands for the Ramanujan's Δ-function)-see [Co, Appendix, Proposition 1] and [Co, Appendix, Theorem 8].

The following identity, which is proved for example in [Go-Sch, Theorem 1.9], shows the connection between our rational function and the Theta function (compare with (7)):

$$\xi_{\alpha,\sigma}(z)^{12} = \frac{\theta\left(z, \alpha^{-1}\mathcal{L}_\sigma\right)}{\theta\left(z, \mathcal{L}_\sigma\right)^{N(\alpha)}}. \tag{8}$$

An important result about our rational functions is that their logarithmic derivatives can be related to special values of Hecke L-functions attached to ϕ^k. To state this result, we will need some additional definitions.

Let Q be the point on E given by the image of $\rho := \Omega_\infty/f$ under the Weierstrass isomorphism. Then Q becomes a primitive f-torsion point on E. Let $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$ be arbitrary and let $\mathfrak{a}$ be an integral ideal coprime to $\alpha\mathfrak{f}$ such that $\sigma_{\mathfrak{a}} = \sigma$. We define

$$\xi_{\alpha,\sigma,Q}(z) = \xi_{\alpha,\sigma}(z + \Lambda(\mathfrak{a})\rho),$$

and denote the corresponding rational function on E^σ by $\xi_{\alpha,\sigma,Q}(P_\sigma)$. Note that while $\Lambda(\mathfrak{a})$ does depend on the choice of the ideal $\mathfrak{a}$, the definition of $\xi_{\alpha,\sigma,Q}(z)$ depends only on the Artin symbol $\sigma_{\mathfrak{a}}$ and not on the choice of $\mathfrak{a}$. It is proved in [Co, Theorem 4] that for any integral ideal $\mathfrak{b}$ coprime to $\alpha\mathfrak{f}$ one has the identity

$$\xi_{\alpha,\sigma\sigma_{\mathfrak{b}}}\left(\eta_\sigma(\mathfrak{b})(P_\sigma)\right) = \prod_{U \in E^\sigma_{\mathfrak{b}}} \xi_{\alpha,\sigma}(P_\sigma \oplus U), \tag{9}$$

where $\oplus$ denotes the usual addition operation on the elliptic curve.

It follows that

$$\xi_{\alpha,\sigma\sigma_{\mathfrak{b}},Q}\left(\eta_\sigma(\mathfrak{b})(P_\sigma)\right) = \prod_{U \in E^\sigma_{\mathfrak{b}}} \xi_{\alpha,\sigma,Q}\left(P_\sigma \oplus U\right). \tag{10}$$

For every $n \geq 0$, we fix once and for all a primitive p^nth root of unity ζ_{p^n} such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. For a fixed $n \geq 0$, we can regard $\widehat{\mathbf{G}}_m$ as defined over $\mathcal{I}_{\mathfrak{p}}[\zeta_{p^n}]$. Then $\zeta_{p^n} - 1$ becomes a $\mathfrak{p}^n$-torsion point on $\widehat{\mathbf{G}}_m$ and for an integral ideal $\mathfrak{a}$ coprime to $\alpha\mathfrak{f}\mathfrak{p}$, $\beta^v_{\mathfrak{a}}$ maps $\zeta_{p^n} - 1$ to a $\mathfrak{p}^n$-torsion point on $\widehat{E^{\sigma_{\mathfrak{a}},v}}$. Let z_n be a corresponding $\mathfrak{p}^n$-torsion point for the lattice $\mathcal{L}_{\sigma_{\mathfrak{a}}}$. We define w_n similarly by starting with the map β^v instead. In particular, by (3), it follows that $z_n \equiv \Lambda(\mathfrak{a})w_n \pmod{\mathcal{L}_{\sigma_{\mathfrak{a}}}}$. Since w_n is a $\mathfrak{p}^n$-torsion point for $\mathcal{L}$ and ρ is an $\mathfrak{f}$-torsion point for $\mathcal{L}$, it follows that $w_n + \rho$ is a $\mathfrak{p}^n\mathfrak{f}$-torsion point for $\mathcal{L}$. In particular, we can write

$$\Omega_\infty^{-1}\left(w_n + \rho\right) = \mathfrak{q}_n/\mathfrak{p}^n\mathfrak{f},$$

for some integral ideal $\mathfrak{q}_n$ in $\mathcal{O}_{\mathbb{K}}$ coprime to $\mathfrak{p}\mathfrak{f}$.

For an arbitrary abelian extension $\mathbb{M}/\mathbb{K}$, if $\varphi : \mathbb{I}_{\mathbb{K}} \to \mathbb{C}$ is a Grössencharacter whose conductor divides the conductor of $\mathbb{M}/\mathbb{K}$, we let φ also denote the associated function on the group of ideals of $\mathbb{K}$ coprime to the conductor of $\mathbb{M}/\mathbb{K}$. Then for an ideal $\mathfrak{c}$ of $\mathbb{K}$, the partial Hecke L-function is defined by

$$L\left(\varphi, \left(\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{c}}\right), s\right) = \sum_{\mathfrak{a}} \varphi(\mathfrak{a})/N(\mathfrak{a})^s,$$

where $\left(\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{c}}\right)$ denotes the Artin symbol of $\mathfrak{c}$ in Gal$(\mathbb{M}/\mathbb{K})$ and the sum ranges over all integral ideals $\mathfrak{a}$ of $\mathbb{K}$ that are coprime to the conductor of $\mathbb{M}/\mathbb{K}$ and satisfy $\left(\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{a}}\right) = \left(\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{c}}\right)$.

We can now prove the promised connection between our rational functions and special values of L-functions. To simplify notations, for a character ϱ defined on ideals of $\mathbb{K}$, we will simply write $\varrho(\alpha)$ for $\varrho((\alpha))$, whenever $\alpha \in \mathbb{K}$. From now on, we will also view all Grössencharacters ϕ as functions on the ideals of $\mathbb{K}$.

Proposition 1. *Let ϕ denote the Grössencharacter of $\mathbb{K}$ for which $\psi_{E/\mathbb{F}} = \phi \circ N_{\mathbb{F}/\mathbb{K}}$. Let $n \geq 0$ be an integer and let $\mathfrak{q}_n$ and z_n be constructed as above. Let σ be an arbitrary element in Gal$(\mathbb{F}_n/\mathbb{K})$ and let $\mathfrak{a}$ be an integral ideal of $\mathbb{K}$ prime to $\mathfrak{f}$ such that $\left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}}\right) = \sigma$. Then for any α coprime to $\mathfrak{f}\mathfrak{p}$ and any positive integer k one has*

$$\left(\frac{d}{dz}\right)^k \log\left(\xi_{\alpha,\sigma,Q}(z)\right)\Big|_{z=z_n} = \left(-\frac{f\phi(\mathfrak{a}\mathfrak{p}^n)}{\Omega_\infty \Lambda(\mathfrak{a})}\right)^k (k-1)! \times$$
$$\left(N(\alpha) L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{q}_n \mathfrak{a}}\right), k\right) - \phi^k(\alpha) L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{q}_n \mathfrak{a}(\alpha)}\right), k\right)\right).$$

Remark 1. *We note that the definition of $\xi_{\alpha,\sigma,Q}(z)$ depends only on the restriction of σ to Gal$(\mathbb{F}/\mathbb{K})$, but that the point z_n does depend on the element $\sigma \in$ Gal$(\mathbb{F}_n/\mathbb{K})$ we choose. Also, the above relation implies directly that the right hand side is independent of the choice of the ideal $\mathfrak{a}$, since the left hand side is.*

Proof. When $n = 0$, this is [Co-Go, Theorem 5]. For the general case, we will follow a similar approach. Our main reference for the following definitions is [Go-Sch, Section 1]. For every positive integer k and every lattice L we define the function

$$H_k(z, s, L) = \sum_{\omega \in L} \frac{(\overline{z} + \overline{\omega})^k}{|z + \omega|^{2s}},$$

for any $Re(s) > k/2 + 1$. As noted in [Go-Sch], this function has an analytic continuation over the whole s-plane. We also let $E_k^*(z, L)$ be the value of $H_k(z, s, L)$ at $s = k$.

We define

$$\widetilde{\theta}(z, L) = \exp(-s_2(L) z^2/2) \sigma(z, L),$$

where $\sigma(z, L)$ is the Weierstrass σ-function of L.

Using (8), it follows that

$$\xi^2_{\alpha,\sigma}(z) = \left(c_\sigma(\alpha) \frac{\widetilde{\theta}(z, \alpha^{-1}\mathcal{L}_\sigma)}{\widetilde{\theta}(z, \mathcal{L}_\sigma)^{N(\alpha)}}\right)^2.$$

It is also proved in [Go-Sch, Corollary 1.7] that for any $z_0 \in \mathbb{C} \setminus L$ one has

$$\frac{d}{dz} \log \widetilde{\theta}(z + z_0, L) = \overline{z_0} A(L)^{-1} + \sum_{k=1}^{\infty} (-1)^{k-1} E_k^*(z_0, L) z^{k-1}. \tag{11}$$

If we let $z = \tilde{z} + z_n$, then one has

$$\left(\frac{d}{dz}\right)^k \log \xi_{\alpha,\sigma,Q}(z)\big|_{z=z_n} = \left(\frac{d}{d\tilde{z}}\right)^k \log \xi_{\alpha,\sigma}(\tilde{z} + z_n + \Lambda(\mathfrak{a})\rho)\big|_{\tilde{z}=0}. \tag{12}$$

Combining (11) and (12), it follows that

$$\begin{aligned}
&\left(\frac{d}{d\tilde{z}}\right)^k \log \xi_{\alpha,\sigma}(\tilde{z} + z_n + \Lambda(\mathfrak{a})\rho)\big|_{\tilde{z}=0} \\
&= \left(\frac{d}{d\tilde{z}}\right)^{k-1} \left(\sum_{j=1}^{\infty} (-\tilde{z})^{j-1} E_j^*(z_n + \Lambda(\mathfrak{a})\rho, \alpha^{-1}\mathcal{L}_\sigma)\right)\Bigg|_{\tilde{z}=0} \\
&- \left(\frac{d}{d\tilde{z}}\right)^{k-1} \left(\sum_{j=1}^{\infty} (-\tilde{z})^{j-1} N(\alpha) E_j^*(z_n + \Lambda(\mathfrak{a})\rho, \mathcal{L}_\sigma)\right)\Bigg|_{\tilde{z}=0} \\
&= (k-1)!(-1)^k \left(E_k^*\left(z_n + \Lambda(\mathfrak{a})\rho, \mathcal{L}_\sigma\right) \cdot N(\alpha) - \alpha^k E_k^*\left(\alpha(z_n + \Lambda(\mathfrak{a})\rho), \mathcal{L}_\sigma\right)\right).
\end{aligned}$$

The final ingredient that we need is the relation between $H_k(z, s, L)$ and the partial Hecke L-function. One can easily show (see for example [Go-Sch, Proposition 5.5] or [dS, Chapter II, Proposition 3.5]) that

$$E_k^*(\Lambda(\mathfrak{a})(w_n + \rho), \mathcal{L}_\sigma) = \left(\frac{\phi(\mathfrak{a}\mathfrak{q}_n)}{(w_n + \rho)\Lambda(\mathfrak{a})}\right)^k L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}\mathfrak{q}_n}\right), k\right), \tag{13}$$

and similarly

$$E_k^*(\alpha\Lambda(\mathfrak{a})(w_n + \rho), \mathcal{L}_\sigma) = \left(\frac{\phi(\mathfrak{a}\mathfrak{q}_n(\alpha))}{(\alpha)(w_n + \rho)\Lambda(\mathfrak{a})}\right)^k L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}\mathfrak{q}_n(\alpha)}\right), k\right). \tag{14}$$

Using (13) and (14), and noting that $\phi^k(\mathfrak{q}_n)(w_n + \rho)^{-k} = \phi^k(\mathfrak{p}^n)(f\Omega_\infty^{-1})^k$, our result follows. ☐

We now define the following sets of integral ideals of $\mathbb{K}$ that we will use throughout the rest of this article. For every $n \geq 0$, we let $\mathfrak{C}_n$ be a set of integral ideals $\mathfrak{a}$ of $\mathcal{O}_\mathbb{K}$ coprime to $\mathfrak{f}\mathfrak{p}$ with the property that as $\mathfrak{a}$ ranges over $\mathfrak{C}_n$, the set of Artin symbols $\left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}}\right)$ covers each element in $\mathrm{Gal}(\mathbb{F}_n/\mathbb{K})$ exactly once.

For each $\sigma \in G$, we let $\mathfrak{a} \in \mathfrak{C}_0$ be such that $\left(\frac{\mathbb{F}/\mathbb{K}}{\mathfrak{a}}\right) = \sigma$ and define

$$Y_{\alpha,\mathfrak{a}}(P_\sigma) = \frac{\xi_{\alpha,\sigma,Q}(P_\sigma)^p}{\xi_{\alpha,\sigma\sigma_\mathfrak{p},Q}(\eta_\sigma(\mathfrak{p})(P_\sigma))},$$

and we let $Y_{\alpha,\mathfrak{a}}(z)$ stand for the corresponding elliptic function for the lattice $\mathcal{L}_{\sigma_\mathfrak{a}}$. Using (9), it follows that

$$\prod_{R \in E_\mathfrak{p}^\sigma} Y_{\alpha,\mathfrak{a}}\left(P_\sigma \oplus R\right) = 1. \tag{15}$$

By a slight abuse of notation, we will also write $Y_{\alpha,\mathfrak{a}}(t_{\sigma_\mathfrak{a}})$ for the $t_{\sigma_\mathfrak{a}}$-expansion of $Y_{\alpha,\mathfrak{a}}(z)$. The following lemma is the key step in constructing a measure on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$ using our rational functions.

Lemma 4. *For an integral ideal $\mathfrak{a}$ of $\mathcal{O}_\mathbb{K}$ coprime to $\mathfrak{f}$, let $\sigma_\mathfrak{a}$ denote the Artin symbol of $\mathfrak{a}$ in Gal($\mathbb{F}/\mathbb{K}$). Then the series $Y_{\alpha,\mathfrak{a}}(t_{\sigma_\mathfrak{a}})$ lies in $1+\mathfrak{m}_v[[t_{\sigma_\mathfrak{a}}]]$ and the series $h_{\alpha,\mathfrak{a}}(t_{\sigma_\mathfrak{a}}) := \frac{1}{p}\log(Y_{\alpha,\mathfrak{a}}(t_{\sigma_\mathfrak{a}}))$ has coefficients in $\mathcal{O}(\mathbb{F}_v)$.*

Proof. The following proof is a straightforward extension of similar results proved in the literature (see for example [Co-Go, Lemma 9] or [Co-Wi 2, Lemma 23]). Let $\widehat{\eta_{\sigma_\mathfrak{a}}(\mathfrak{p})} : \widehat{E^{\sigma_\mathfrak{a},v}} \to \widehat{E^{\sigma_\mathfrak{a}\sigma_\mathfrak{p},v}}$ be the formal power series induced by $\eta_{\sigma_\mathfrak{a}}(\mathfrak{p})$. As p splits completely in $\mathbb{K}$, we have $N(\mathfrak{p}) = p$, hence

$$\widehat{\eta_{\sigma_\mathfrak{a}}(\mathfrak{p})}(t_{\sigma_\mathfrak{a}}) \equiv t_{\sigma_\mathfrak{a}}^p \pmod{\mathfrak{m}_v}.$$

Let $m_{\alpha,\sigma_\mathfrak{a}}(t_{\sigma_\mathfrak{a}})$ be the development of the rational function $\xi_{\alpha,\sigma_\mathfrak{a},Q}(P_{\sigma_\mathfrak{a}})$ as a power series in $t_{\sigma_\mathfrak{a}}$. Given

$$m_{\alpha,\sigma_\mathfrak{a}}(t_{\sigma_\mathfrak{a}}) = \sum_{n\geq 0} c_n t_{\sigma_\mathfrak{a}}^n,$$

it follows that

$$m_{\alpha,\sigma_\mathfrak{a}\sigma_\mathfrak{p}}\left(\widehat{\eta_{\sigma_\mathfrak{a}}(\mathfrak{p})}(t_{\sigma_\mathfrak{a}})\right) \equiv \sum_{n\geq 0} c_n^p t_{\sigma_\mathfrak{a}}^{pn} \equiv m_{\alpha,\sigma_\mathfrak{a}}^p \pmod{\mathfrak{m}_v}.$$

Since $m_{\alpha,\sigma_\mathfrak{a}}(t_{\sigma_\mathfrak{a}})$ is a unit (see for example the proof of [Co-Wi 2, Lemma 23]), it follows that $Y_{\alpha,\mathfrak{a}}(t_\sigma) \equiv 1 \pmod{\mathfrak{m}_v}$, which completes our proof. □

2.3. The p-adic L-function. We will now show how the results we obtained in the previous section can be used for constructing a measure on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$ with respect to which we define our p-adic L-function. We begin by recalling some basic definitions and properties of measures.

For any prime p, the group $\mathbb{Z}_p^\times$ has a decomposition

$$\mathbb{Z}_p^\times = V \times U,$$

where V is the group consisting of the $(p-1)$th roots of unity in $\mathbb{Z}_p$ (resp. $\{\pm 1\}$ when $p = 2$) and $U = 1 + p\mathbb{Z}_p$ (resp. $1 + 4\mathbb{Z}_2$ when $p = 2$). For an element $\alpha \in \mathbb{Z}_p^\times$, we denote by $\langle\alpha\rangle$ its projection onto the second factor. If we fix a topological generator u of U, then the map $x \to u^x$ gives an isomorphism of topological groups between $\mathbb{Z}_p$ and U.

Let $\mathfrak{G}$ be a profinite group and let A be the ring of integers of a complete subfield of the completion of the algebraic closure of $\mathbb{Q}_p$. We let $\Lambda_A(\mathfrak{G})$ denote the ring of A-valued measures defined on $\mathfrak{G}$, where the product is given by the usual convolution of measures. If $\mathfrak{G}$ is finite, there is an isomorphism $\Lambda_A(\mathfrak{G}) \cong A[\mathfrak{G}]$ given by

$$\nu \to \sum_{\sigma\in\mathfrak{G}} \nu(\{\sigma\})\sigma,$$

while for an infinite profinite group there is an isomorphism $\Lambda_A(\mathfrak{G}) \cong A[[\mathfrak{G}]]$ under the usual inverse limits taken over the normal subgroups of finite index:

$$\Lambda_A(\mathfrak{G}) = \varprojlim \Lambda_A(\mathfrak{G}/H) \cong \varprojlim A[\mathfrak{G}/H] = A[[\mathfrak{G}]].$$

For a general profinite abelian group $\mathfrak{G}$, following de Shalit, we define a *pseudo-measure* on $\mathfrak{G}$ to be any element in the localization of $\Lambda_A(\mathfrak{G})$ with respect to the set of non-zero divisors (see [dS, Section I.3.1]). Given a measure ν on $\mathfrak{G}$ and any compact subset O of $\mathfrak{G}$, we can define the measure $\nu|_O$ on $\mathfrak{G}$ by restricting ν to O and extending it by 0. Our main interests will be in the cases when $\mathfrak{G} = \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$ and $\mathfrak{G} = \mathbb{Z}_p$, respectively.

When $\mathfrak{G} = \mathbb{Z}_p$, there is an isomorphism $\Lambda_A(\mathbb{Z}_p) \cong A[[w]]$ due to Mahler, given by associating to a measure ν the element

$$\int_{\mathbb{Z}_p} (1+w)^x d\nu.$$

By our previous observation, for $O \subseteq \mathbb{Z}_p$ compact open, there is an inclusion $\Lambda_A(O) \hookrightarrow \Lambda_A(\mathbb{Z}_p)$. For the particular case when $O = \mathbb{Z}_p^\times$, if $F(w)$ is the power series associated with ν, we know by [Si, Lemma 1.1] that the power series associated with $\nu|_{\mathbb{Z}_p^\times}$ is

$$\nu|_{\mathbb{Z}_p^\times} \to F(w) - \frac{1}{p}\sum_{\zeta^p=1} F(\zeta(1+w)-1). \tag{16}$$

Throughout this article, we shall use ν^* to denote the measure $\nu|_{\mathbb{Z}_p^\times}$.

For a measure $\nu \in \Lambda_A(\mathbb{Z}_p)$ and $a \in \mathbb{Z}_p^\times$ we define the measure $\nu \circ a$ by $\nu \circ a(O) = \nu(aO)$ for any $O \subseteq \mathbb{Z}_p$ compact open. It then follows that

$$\nu \circ a|_O = \nu|_{aO} \circ a. \tag{17}$$

Moreover, if $F(w)$ is the power series associated with ν, then the power series associated with $\nu \circ a$ is

$$\nu \circ a \to F\left((1+w)^{-a} - 1\right). \tag{18}$$

We can now proceed to the construction of our measure. For every $\mathfrak{a} \in \mathfrak{C}_0$, we define $\mathcal{B}_{\alpha,\mathfrak{a}}(w) = h_{\alpha,\mathfrak{a}}(\beta^v_{\mathfrak{a}}(w))$. By Lemma 4, the series $\mathcal{B}_{\alpha,\mathfrak{a}}(w)$ lies in $\mathcal{I}_{\mathfrak{p}}[[w]]$, so it corresponds to a measure $\nu_{\alpha,\mathfrak{a}} \in \Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathbb{Z}_p)$. The identity (15) combined with the aforementioned lemma from [Si] implies that the measure $\nu_{\alpha,\mathfrak{a}}$ is actually supported on $\mathbb{Z}_p^\times$.

Let $\Psi_{\mathfrak{p}} : \mathcal{G} \to \mathbb{Z}_p^\times$ be the isomorphism giving the action of $\mathcal{G}$ on the $\mathfrak{p}$-power division points of E. Under this isomorphism, the measure $\nu_{\alpha,\mathfrak{a}}$ can be regarded as an element of $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathcal{G})$. Notice that for any $k \geq 0$, one has

$$\int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})} \Psi_{\mathfrak{p}}^k d\nu_{\alpha,\mathfrak{a}} = D^k \mathcal{B}_{\alpha,\mathfrak{a}}(w)|_{w=0},$$

where $D = (1+w)\frac{d}{dw}$. If we let exp denote the isomorphism $\widehat{\mathbf{G}}_a \to \widehat{\mathbf{G}}_m$, the substitution $w = \exp(z) - 1$ yields further

$$\begin{aligned}\int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})} \Psi_{\mathfrak{p}}(x)^k d\nu_{\alpha,\mathfrak{a}} &= \left(\frac{d}{dz}\right)^k \mathcal{B}_{\alpha,\mathfrak{a}}(\exp(z)-1)|_{z=0} \\ &= \Omega_{\mathfrak{a},v}^k \left(\frac{d}{dz}\right)^k \mathcal{B}_{\alpha,\mathfrak{a}}(\exp(z/\Omega_{\mathfrak{a},v})-1)|_{z=0}.\end{aligned}$$

More generally, if we are interested in evaluating $D^k\, \mathcal{B}_{\alpha,\mathfrak{a}}(w)|_{w=w_1}$, we can make the substitution $w_1 = \exp(z_1/\Omega_{\mathfrak{a},v}) - 1$, and noting that

$$\beta_{\mathfrak{a}}^v\left(\exp(z/\Omega_{\mathfrak{a},v}) - 1\right) = \mathcal{M}\left(\Lambda(\mathfrak{a})z, \mathcal{L}_{\sigma_{\mathfrak{a}}}\right),$$

it follows that

$$D^k\, \mathcal{B}_{\alpha,\mathfrak{a}}(w)|_{w=w_1} = \Omega_{\mathfrak{a},v}^k \Lambda(\mathfrak{a})^{-k} \left(\frac{d}{dz}\right)^k \frac{1}{p} \log Y_{\alpha,\mathfrak{a}}\left(\mathcal{M}\left(\Lambda(\mathfrak{a})z, \mathcal{L}_{\sigma_{\mathfrak{a}}}\right)\right)|_{z=z_1}. \quad (19)$$

For every $\mathfrak{a} \in \mathfrak{C}_0$, we constructed a measure $\nu_{\alpha,\mathfrak{a}} \in \Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathcal{G})$. For every such $\mathfrak{a}$, we let $\nu_{\alpha,\mathfrak{a}} \circ \sigma_{\mathfrak{a}}$ denote the pushforward measure on $\sigma_{\mathfrak{a}}^{-1}\mathcal{G}$ induced by $\sigma_{\mathfrak{a}}$, and we extend $\nu_{\alpha,\mathfrak{a}} \circ \sigma_{\mathfrak{a}}$ to a measure on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$ by 0. Consider now

$$\nu_\alpha := \sum_{\mathfrak{a} \in \mathfrak{C}_0} \nu_{\alpha,\mathfrak{a}} \circ \sigma_{\mathfrak{a}}.$$

Then ν_α becomes an $\mathcal{I}_{\mathfrak{p}}$-valued measure on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$.

Weil showed in [We] that, under our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, the character ϕ can be extended continuously to a character

$$\tilde{\phi} : \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}) \to \mathbb{C}_p^\times,$$

which satisfies the property that $\tilde{\phi}\left(\left(\frac{\mathbb{F}_\infty/\mathbb{K}}{\mathfrak{a}}\right)\right) = \phi(\mathfrak{a})$, for any ideal $\mathfrak{a}$ in $\mathbb{K}$ coprime to $\mathfrak{f}\mathfrak{p}$. Furthermore, for any $\sigma \in \mathcal{G}$ one has $\tilde{\phi}(\sigma) = \Psi_{\mathfrak{p}}(\sigma)$ (see [Co-Go, p. 352] for details). By a slight abuse of notation, we will simply write ϕ for $\tilde{\phi}$, since it will always be clear from the context what ϕ stands for.

The rest of the work we do in this section follows closely the exposition in [dS, Chapter II, Section 4].

Lemma 5. a) *Let χ be a character of Gal$(\mathbb{F}/\mathbb{K})$. Then for every $k \geq 0$ one has*

$$\int\limits_{Gal(\mathbb{F}_\infty/\mathbb{K})} \chi\phi^k\, d\nu_\alpha = \left(1 - \frac{\chi\phi^k(\mathfrak{p})}{p}\right) \sum_{\mathfrak{a} \in \mathfrak{C}_0} \Omega_{\mathfrak{a},v}^k \chi\phi^k(\sigma_{\mathfrak{a}}^{-1}) \left(\frac{d}{dz}\right)^k \log \xi_{\alpha,\sigma_{\mathfrak{a}},Q}(z)|_{z=0}.$$

b) *Let $n \geq 1$ be a positive integer and assume χ is a character of Gal$(\mathbb{F}_n/\mathbb{K})$ with the property that $\mathfrak{p}^n$ is the exact power of $\mathfrak{p}$ dividing its conductor. We define the Gauss sum*

$$\tau(\chi) = \frac{1}{p^n} \sum_{\gamma \in Gal(\mathbb{F}_n/\mathbb{F})} \chi(\gamma)\zeta_{p^n}^{-\Psi_{\mathfrak{p}}(\gamma)}.$$

Then for every $k \geq 0$ one has

$$\int\limits_{Gal(\mathbb{F}_\infty/\mathbb{K})} \chi\phi^k\, d\nu_\alpha$$
$$= \tau(\chi) \sum_{\mathfrak{a} \in \mathfrak{C}_n} \Omega_{\mathfrak{a},v}^k \chi\phi^k(\sigma_{\mathfrak{a}}^{-1}) \left(\frac{d}{dz}\right)^k \log\, \xi_{\alpha,\sigma_{\mathfrak{a}},Q}(z)|_{z=\mathcal{M}^{-1}\circ\beta_{\mathfrak{a}}^v(\zeta_{p^n}-1)}.$$

Proof. This result is the analogue of [dS, Chapter II, Theorem 4.7] and [dS, Chapter II, Theorem 4.8]. For part a), using the fact that ϕ and $\Psi_{\mathfrak{p}}$ coincide on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})$, it follows that

$$\begin{aligned}
&\int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})} \phi^k d\nu_\alpha \circ \sigma_{\mathfrak{a}}^{-1} \\
&= \Omega_{\mathfrak{a},v}^k \left(\frac{d}{dz}\right)^k \mathcal{B}_{\alpha,\mathfrak{a}}\left(\exp\left(\frac{z}{\Omega_{\mathfrak{a},v}}\right) - 1\right)\Bigg|_{z=0} \\
&= \Omega_{\mathfrak{a},v}^k \left(\frac{d}{d\tilde{z}}\right)^k \frac{1}{p}\log Y_{\alpha,\mathfrak{a}}(\tilde{z})|_{\tilde{z}=0} \\
&= \Omega_{\mathfrak{a},v}^k \left(\frac{d}{d\tilde{z}}\right)^k \left(\log \xi_{\alpha,\sigma_{\mathfrak{a}},Q}(\tilde{z}) - \frac{1}{p}\log \xi_{\alpha,\sigma_{\mathfrak{a}}\sigma_{\mathfrak{p}},Q}\left(\Lambda(\mathfrak{p})^{\sigma_{\mathfrak{a}}}\tilde{z}\right)\right)\Bigg|_{\tilde{z}=0}.
\end{aligned}$$

It follows that

$$\begin{aligned}
&\int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})} \chi\phi^k d\nu_\alpha \\
&= \sum_{\mathfrak{a}\in\mathfrak{C}_0} \chi\phi^k(\sigma_{\mathfrak{a}}^{-1})\Omega_{\mathfrak{a},v}^k \left(\frac{d}{d\tilde{z}}\right)^k \left(\log \xi_{\alpha,\sigma_{\mathfrak{a}},Q}(\tilde{z}) - \frac{1}{p}\log \xi_{\alpha,\sigma_{\mathfrak{a}}\sigma_{\mathfrak{p}},Q}\left(\Lambda(\mathfrak{p})^{\sigma_{\mathfrak{a}}}\tilde{z}\right)\right)\Bigg|_{\tilde{z}=0}.
\end{aligned}$$

Reordering the sum

$$S := \sum_{\mathfrak{a}\in\mathfrak{C}_0} \Omega_{\mathfrak{a},v}^k \chi\phi^k(\sigma_{\mathfrak{a}}^{-1}) \left(\frac{d}{d\tilde{z}}\right)^k \frac{1}{p}\log \xi_{\alpha,\sigma_{\mathfrak{a}}\sigma_{\mathfrak{p}},Q}\left(\Lambda(\mathfrak{p})^{\sigma_{\mathfrak{a}}}\tilde{z}\right)\Bigg|_{\tilde{z}=0}$$

according to $\mathfrak{a}' = \mathfrak{a}\mathfrak{p}$ and using the fact that $\Omega_{\mathfrak{a}\mathfrak{p},v}^k = \Omega_{\mathfrak{a},v}^k \left(\Lambda(\mathfrak{p})^{\sigma_{\mathfrak{a}}}\right)^k$ (see (6)), it follows that

$$S = \frac{\chi\phi^k(\mathfrak{p})}{p} \sum_{\mathfrak{a}\in\mathfrak{C}_0} \Omega_{\mathfrak{a},v}^k \chi\phi^k(\sigma_{\mathfrak{a}}^{-1}) \left(\frac{d}{dz}\right)^k \log \xi_{\alpha,\sigma_{\mathfrak{a}},Q}(z)|_{z=0}.$$

This completes the proof of part a).

For part b), we use a similar strategy. For $\mathfrak{b} \in \mathfrak{C}_n$, we let $\sigma_{\mathfrak{b}}$ denote the Artin symbol of $\mathfrak{b}$ in $\mathrm{Gal}(\mathbb{F}_n/\mathbb{K})$ and we define

$$B_{\alpha,\mathfrak{b}}(w) = h_{\alpha,\mathfrak{b}}\left(\beta_{\mathfrak{b}}^v(w)\right).$$

We will perform similar computations as above. For a character χ of $\mathrm{Gal}(\mathbb{F}_n/\mathbb{K})$ for which n is the exact power of $\mathfrak{p}$ dividing its conductor we have

$$\int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})} \chi\phi^k d\nu_\alpha = \sum_{\mathfrak{b}\in\mathfrak{C}_n} \chi\phi^k(\sigma_{\mathfrak{b}}^{-1}) \int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_n)} \phi^k d\nu_\alpha \circ \sigma_{\mathfrak{b}}^{-1}.$$

Again, using the fact that ϕ and $\Psi_{\mathfrak{p}}$ act in the same way on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})$, it follows that

$$\int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_n)} \phi^k d\nu_\alpha \circ \sigma_{\mathfrak{b}}^{-1} = \int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_n)} \Psi_{\mathfrak{p}}^k d\nu_\alpha \circ \sigma_{\mathfrak{b}}^{-1}.$$

Using the fact that the indicator function of $1+p^n\mathbb{Z}_p$ is $\frac{1}{p^n}\sum_{j=0}^{p^n-1}\zeta_{p^n}^{(x-1)j}$, it follows that

$$\int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_n)} \Psi_{\mathfrak{p}}^k d\nu_\alpha \circ \sigma_{\mathfrak{b}}^{-1} = \frac{1}{p^n}\sum_{j=0}^{p^n-1} D^k\, \mathcal{B}_{\alpha,\mathfrak{b}}(w)\big|_{w=\zeta_{p^n}^j-1}\,\zeta_{p^n}^{-j}.$$

To simplify the writing, we define

$$R_{\alpha,\mathfrak{b}}(w) := \log \xi_{\alpha,\,\sigma_{\mathfrak{b}}|_{\mathbb{F}},Q}(\beta_{\mathfrak{b}}^v(w)).$$

We recall that the measure associated with $\mathcal{B}_{\alpha,\mathfrak{b}}(w)$ is obtained by restricting the measure associated with $R_{\alpha,\mathfrak{b}}(w)$ to $\mathbb{Z}_p^\times$. In particular, if we restrict the measure associated with $\mathcal{B}_{\alpha,\mathfrak{b}}(w)$ to the subgroup $1+p^n\mathbb{Z}_p$ of $\mathbb{Z}_p^\times$, we obtain the restriction to $1+p^n\mathbb{Z}_p$ of the measure associated with $R_{\alpha,\mathfrak{b}}(w)$. Hence the quantity we are interested in computing is given by

$$\frac{1}{p^n}\sum_{j=0}^{p^n-1} D^k\, R_{\alpha,\mathfrak{b}}(w)\big|_{w=\zeta_{p^n}^j-1}\,\zeta_{p^n}^{-j},$$

which can be rewritten as

$$\frac{1}{p^n}\sum_{j:p\nmid j} D^k\, R_{\alpha,\mathfrak{b}}(w)\big|_{w=\zeta_{p^n}^j-1}\cdot\zeta_{p^n}^{-j} + \frac{1}{p^n}\sum_{j:p\mid j} D^k\, R_{\alpha,\mathfrak{b}}(w)\big|_{w=\zeta_{p^n}^j-1}\cdot\zeta_{p^n}^{-j}.$$

A simple check using the definitions shows that

$$D^k\, R_{\alpha,\mathfrak{b}}(w)\big|_{w=\zeta_{p^n}^j-1} = \Psi_{\mathfrak{p}}(\gamma)^{-k} D^k\, R_{\alpha,\mathfrak{b}_j}(w)\big|_{w=\zeta_{p^n}-1},$$

where $\gamma\in\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})$ is such that $\gamma(\zeta_{p^n})=\zeta_{p^n}^j$ (i.e. $\Psi_{\mathfrak{p}}(\gamma)\equiv j \pmod{p^n}$) and $\mathfrak{b}_j$ is the unique ideal in $\mathbb{K}$ with the property that $\left(\frac{\mathbb{F}_\infty/\mathbb{K}}{\mathfrak{b}_j}\right)=\left(\frac{\mathbb{F}_\infty/\mathbb{K}}{\mathfrak{b}}\right)\gamma$. It follows that

$$\frac{1}{p^n}\sum_{j:p\nmid j} D^k\, R_{\alpha,\mathfrak{b}}(w)\big|_{w=\zeta_{p^n}^j-1}\cdot\zeta_{p^n}^{-j} = \Psi_{\mathfrak{p}}(\gamma)^{-k}\frac{1}{p^n}\sum_{j:p\nmid j} D^k\, R_{\alpha,\mathfrak{b}_j}(w)\big|_{w=\zeta_{p^n}-1}\,\zeta_{p^n}^{-j}.$$

Moreover, when we consider the expression

$$\sum_{\mathfrak{b}\in\mathfrak{C}_n}\chi\phi^k(\sigma_{\mathfrak{b}}^{-1})\frac{1}{p^n}\sum_{p\mid j} D^k\, R_{\alpha,\mathfrak{b}}(w)\big|_{w=\zeta_{p^n}^j-1}\cdot\zeta_{p^n}^{-j},$$

notice that if $\mathfrak{c}\in\mathfrak{C}_n$ is such that $\sigma_{\mathfrak{c}}$ fixes $\mathbb{K}(\mathfrak{f}\mathfrak{p}^{n-1})$ (i.e. $\sigma_{\mathfrak{c}}$ defines an element in $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}(\mathfrak{f}\mathfrak{p}^{n-1}))$, then

$$D^k\, R_{\alpha,\mathfrak{a}\mathfrak{c}}(w)\big|_{w=\zeta_{p^{n-1}}^a-1} = \Psi_{\mathfrak{p}}(\mathfrak{c})^k D^k\, R_{\alpha,\mathfrak{a}}(w)\big|_{w=\zeta_{p^{n-1}}^a-1}.$$

Furthermore, since n is the exact power of $\mathfrak{p}$ dividing the conductor of χ, it follows that

$$\sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_n/\mathbb{F}_{n-1})}\chi(\sigma)=0.$$

If we partition the elements in $\mathfrak{C}_n$ according to cosets modulo the group $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}(\mathfrak{f}\mathfrak{p}^{n-1}))$, we get

$$\begin{aligned}
&\sum_{\mathfrak{b}\in\mathfrak{C}_n} \chi\phi^k(\sigma_{\mathfrak{b}}^{-1})\frac{1}{p^n}\sum_{p|j} D^k\ R_{\alpha,\mathfrak{b}}(w)|_{w=\zeta_{p^n}^j-1}\cdot\zeta_{p^n}^{-j}\\
&=\sum_{\mathfrak{b}\in\mathfrak{C}_n} \chi\phi^k(\sigma_{\mathfrak{b}}^{-1})\frac{1}{p^n}\sum_{a=0}^{p^{n-1}-1} D^k\ R_{\alpha,\mathfrak{b}}(w)|_{w=\zeta_{p^{n-1}}^a-1}\cdot\zeta_{p^{n-1}}^{-a}\\
&=\sum_{\mathfrak{c}\in\mathfrak{C}_{n-1}}\ \sum_{\substack{\mathfrak{d}\in\mathfrak{C}_n\\ \sigma_{\mathfrak{d}}\in\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}_{n-1})}}\chi\phi^k(\sigma_{\mathfrak{c}}^{-1}\sigma_{\mathfrak{d}}^{-1})\frac{1}{p^n}\sum_{a=0}^{p^{n-1}-1} D^k\ R_{\alpha,\mathfrak{c}\mathfrak{d}}(w)|_{w=\zeta_{p^{n-1}}^a-1}\cdot\zeta_{p^{n-1}}^{-a}\\
&=0.
\end{aligned}$$

Finally,

$$\begin{aligned}
&\sum_{\mathfrak{b}\in\mathfrak{C}_n} \chi\phi^k(\sigma_{\mathfrak{b}}^{-1})\frac{1}{p^n}\sum_{j:p\nmid j} D^k\ R_{\alpha,\mathfrak{b}_j}(w)|_{w=\zeta_{p^n}-1}\,\zeta_{p^n}^{-j}\Psi_{\mathfrak{p}}(\gamma)^{-k}\\
&=\sum_{\mathfrak{b}'\in\mathfrak{C}_n} D^k\ R_{\alpha,\mathfrak{b}'}(w)|_{w=\zeta_{p^n}-1}\,\frac{1}{p^n}\sum_{\mathfrak{b}'=\mathfrak{b}\gamma}\chi\phi^k(\sigma_{\mathfrak{b}}^{-1})\Psi_{\mathfrak{p}}(\gamma)^{-k}\zeta_{p^n}^{-\Psi_{\mathfrak{p}}(\gamma)}\\
&=\sum_{\mathfrak{b}'\in\mathfrak{C}_n} D^k\ R_{\alpha,\mathfrak{b}'}(w)|_{w=\zeta_{p^n}-1}\,\frac{1}{p^n}\chi\phi^k(\sigma_{\mathfrak{b}'}^{-1})\sum_{\gamma\in\mathrm{Gal}(\mathbb{F}_n/\mathbb{F})}\chi(\gamma)\zeta_{p^n}^{-\Psi_{\mathfrak{p}}(\gamma)}\\
&=\tau(\chi)\sum_{\mathfrak{b}\in\mathfrak{C}_n}\chi\phi^k(\sigma_{\mathfrak{b}}^{-1})D^k\ R_{\alpha,\mathfrak{b}}(w)|_{w=\zeta_{p^n}-1},
\end{aligned}$$

with $\tau(\chi)$ defined as in the statement. Using (19), part b) follows. $\square$

Let $n\geq 0$ be an integer and let χ be a character whose conductor divides $\mathfrak{f}\mathfrak{p}^n$ and with the property that n is the exact power of $\mathfrak{p}$ in its conductor. Consider the character $\varepsilon=\chi\phi^k$ and the set

$$S=\left\{\gamma\in\mathrm{Gal}\left(\mathbb{K}(\mathfrak{f}\mathfrak{p}^n\overline{\mathfrak{p}}^\infty)/\mathbb{K}\right):\gamma|_{\mathbb{K}(\mathfrak{f}\overline{\mathfrak{p}}^\infty)}=\left(\frac{\mathbb{K}(\mathfrak{f}\overline{\mathfrak{p}}^\infty)/\mathbb{K}}{\mathfrak{p}^n}\right)\right\}.$$

We define the sum $G(\varepsilon)$ as

$$G(\varepsilon)=\frac{\phi^k(\mathfrak{p}^n)}{p^n}\sum_{\gamma\in S}\chi(\gamma)\zeta_{p^n}^{-\gamma}.$$

We note that $G(\varepsilon)$ is well-defined, since $\zeta_{p^n}\in\mathbb{K}(\mathfrak{f}\mathfrak{p}^n\overline{\mathfrak{p}}^\infty)$. We also know (see for example [Go-Sch, Lemma 4.9]) that $G(\varepsilon)$ lies in a CM field and that $G(\varepsilon)\overline{G(\varepsilon)}=p^{n(k-1)}$.

THEOREM 3. *Let χ, ε and $G(\varepsilon)$ be defined as above. Then there exists a p-adic unit u_χ depending on χ such that for all $k\geq 1$ one has*

$$\int_{Gal(\mathbb{F}_\infty/\mathbb{K})}\varepsilon\,d\nu_\alpha=\frac{\Omega_v^k}{\Omega_\infty^k}(k-1)!(-1)^k f^k u_\chi G(\varepsilon)\left(1-\frac{\varepsilon(\mathfrak{p})}{p}\right)(N(\alpha)-\varepsilon(\alpha))\cdot L_{\mathfrak{f}}(\overline{\varepsilon},k).$$

Proof. When $n=0$, by Proposition 1 and Lemma 5 a), it follows that

$$\int\limits_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})} \chi\phi^k d\nu_\alpha = \frac{\Omega_v^k}{\Omega_\infty^k}(k-1)!(-1)^k f^k \left(1-\frac{\chi\phi^k(\mathfrak{p})}{p}\right)\times$$
$$\sum_{\mathfrak{a}\in\mathfrak{C}_0} \chi\phi^k(\sigma_{\mathfrak{a}}^{-1})\phi^k(\mathfrak{a})\left(N(\alpha)L(\overline{\phi},\sigma_{\mathfrak{a}},k)-\phi^k(\alpha)L(\overline{\phi}^k,\sigma_{\mathfrak{a}(\alpha)},k)\right).$$

The sum in the right hand side can be further rewritten as

$$\begin{aligned}&\sum_{\mathfrak{a}\in\mathfrak{C}_0} \chi\phi^k(\sigma_{\mathfrak{a}}^{-1})\phi^k(\mathfrak{a})(N(\alpha)-\chi\phi^k(\alpha))L\left(\overline{\phi}^k,\sigma_{\mathfrak{a}},k\right)\\ &=(N(\alpha)-\varepsilon(\alpha))L_{\mathfrak{f}}\left(\overline{\phi}^k\chi^{-1},k\right).\end{aligned}$$

When $n\geq 1$, using Proposition 1 and Lemma 5 b), it follows in a similar manner that

$$\begin{aligned}&\int\limits_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})} \chi\phi^k d\nu_\alpha\\ &=\left(\frac{-\Omega_v f}{\Omega_\infty}\right)^k (k-1)!\phi^k(\mathfrak{p}^n)\tau(\chi)\chi(\mathfrak{q}_n)(N(\alpha)-\varepsilon(\alpha))L_{\mathfrak{f}}(\overline{\phi}^k\chi^{-1},k).\end{aligned}$$

Let $\mathfrak{q}_n'$ be a prime in $\mathbb{K}$ with the property that

$$N(\mathfrak{q}_n')\equiv 1 \pmod{p^n} \quad\text{and}\quad \left(\frac{\mathbb{F}(\overline{\mathfrak{p}}^n)/\mathbb{K}}{\mathfrak{q}_n'}\right)=\left(\frac{\mathbb{F}(\overline{\mathfrak{p}}^n)/\mathbb{K}}{\mathfrak{p}^n}\right).$$

With this choice of $\mathfrak{q}_n'$, it is proved in [dS, p. 75] that $\chi(\mathfrak{q}_n')\phi^k(\mathfrak{p}^n)\tau(\chi)=G(\varepsilon)$. If we set $u_\chi=\chi(\mathfrak{q}_n)/\chi(\mathfrak{q}_n')$, then u_χ is clearly a p-adic unit and since $G(\varepsilon)=1$ for $n=0$, the result follows. □

We now have all the ingredients for proving the main theorem in the construction of the p-adic L-functions. We recall that $H=\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}_\infty)$. Let $m=|H|$ and let $\mathcal{D}_{\mathfrak{p}}=\mathcal{I}_{\mathfrak{p}}(\mu_m)$, the ring obtained by adjoining the mth roots of unity to $\mathcal{I}_{\mathfrak{p}}$.

Theorem 4. *There exists a unique measure ν on Gal$(\mathbb{F}_\infty/\mathbb{K})$ taking values in $\mathcal{D}_{\mathfrak{p}}$ such that for any $\varepsilon=\phi^k\chi$, with $k\geq 1$ and χ a character of conductor dividing $\mathfrak{f}\mathfrak{p}^n$ for some $n\geq 0$, one has*

$$\Omega_v^{-k}\int\limits_{Gal(\mathbb{F}_\infty/\mathbb{K})} \varepsilon\, d\nu=\Omega_\infty^{-k}(-1)^k(k-1)!f^k u_\chi G(\varepsilon)\left(1-\frac{\varepsilon(\mathfrak{p})}{p}\right)L_{\mathfrak{f}}(\overline{\varepsilon},k),$$

with u_χ as defined in the proof of Theorem 3.

Proof. The following proof is exactly the same argument as the one given in [dS, Chapter II, Theorem 4.12], but we redo it here for the convenience of the reader. We first note that for α_1 and α_2 coprime to $\mathfrak{p}\mathfrak{f}$, it follows from Theorem 3 that

$$\nu_{\alpha_1}\left(N(\alpha_2)-\sigma_{(\alpha_2)}\right)=\nu_{\alpha_2}\left(N(\alpha_1)-\sigma_{(\alpha_1)}\right) \quad \text{(equality as measures)}, \qquad (20)$$

where for an integral ideal $\mathfrak{a}$ of $\mathbb{K}$ coprime to $\mathfrak{f}\mathfrak{p}$, $\sigma_{\mathfrak{a}}$ stands for the Artin symbol of $\mathfrak{a}$ in $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$. Indeed, by Theorem 3 we know that the integrals of the two measures against any character of the form $\varepsilon = \phi\chi$ with χ a character of finite order are the same. Since the set of such characters $\phi\chi$ separates measures, it follows that the two measures are equal, as claimed.

We recall that we have a decomposition

$$\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}) = H \times \Gamma',$$

with $H = \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}_\infty)$ and $\Gamma' \cong \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$. One then has an isomorphism

$$\mathcal{D}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]] \cong \mathcal{D}[[\Gamma']][H] \cong \mathcal{D}[[X]][H].$$

Moreover, there exists an isomorphism

$$\mathbb{Q} \otimes \mathcal{D}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]] \cong \mathbb{Q} \otimes \mathcal{D}[[\Gamma']]^m,$$

given by sending element $1 \otimes \lambda \in \mathbb{Q} \otimes \mathcal{D}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]$ to $1 \otimes (\theta_1(\lambda), \dots \theta_m(\lambda))$, where $\theta_1, \dots, \theta_m$ are the characters of H.

For any character θ of H and $\alpha \in \mathcal{O}_\mathbb{K}$ non-unit and coprime to $6\mathfrak{f}\mathfrak{p}$, one has

$$\theta\left(\sigma_{(\alpha)} - N(\alpha)\right) = \theta\left(\sigma_{(\alpha)}\big|_H\right) \cdot \sigma_{(\alpha)}\big|_{\Gamma'} - N(\alpha).$$

Notice also that for any such α, the element $\sigma_{(\alpha)}\big|_{\Gamma'}$ is non-trivial and that $\theta\left(\sigma_{(\alpha)}\big|_H\right)$ is a root of unity. In particular, one has that $\theta\left(\sigma_{(\alpha)} - N(\alpha)\right)$ is a non-zero divisor in $\mathcal{D}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]$.

In view of (20), in order to prove that $\nu_\alpha/(N(\alpha) - \sigma_{(\alpha)})$ is an integral measure, it suffices to prove that as we range over the elements $\alpha \in \mathcal{O}_\mathbb{K}$ such that α is non-unit and coprime to $6\mathfrak{f}\mathfrak{p}$, one has that the gcd of the polynomials $\theta(\sigma_{(\alpha)} - N(\alpha)) \in \mathcal{D}_\mathfrak{p}[[X]]$ is 1. To this end, we let $m \geq 0$ be the exact power of $\overline{\mathfrak{p}}$ dividing $\mathfrak{f}$, so that $\zeta_{p^m} \in \mathbb{F}_\infty$, but $\zeta_{p^{m+1}} \notin \mathbb{F}_\infty$. Then, for any element $\gamma' \times g \in \Gamma' \times H$ fixing ζ_{p^m}, any $u \in 1 + p^m\mathbb{Z}_p$ and any $n \geq m$, one can find $\alpha_n \in \mathcal{O}_\mathbb{K}$ such that

$$\begin{cases} \sigma_{(\alpha_n)}\big|_{\mathbb{F}_n} = (\gamma' \times g)|_{\mathbb{F}_n} \\ N(\alpha_n) \equiv u \pmod{p^n}. \end{cases}$$

It follows that the sequence $\theta(\sigma_{(\alpha_n)} - N(\alpha_n))$ approximate $\theta(g)(1+X)^a - u$, for some $a \in p^m\mathbb{Z}_p$. It is now easy to see that as we range a and u, the series $\theta(g)(1+X)^a - u$ cannot have a common divisor, which shows that $\theta(\sigma_{(\alpha)} - N(\alpha)) \mid \theta(\nu_\alpha)$. In particular, there exists $\nu_\theta \in \mathcal{D}_\mathfrak{p}[[\Gamma']]$ such that

$$\theta\left(\sigma_{(\alpha)} - N(\alpha)\right) \cdot \nu_\theta = \theta(\nu_\alpha),$$

for any $\alpha \in \mathcal{O}_\mathbb{K}$ non-unit and coprime to $\mathfrak{f}\mathfrak{p}$.

Let $e_\theta = \frac{1}{m} \sum_{g \in H} \theta(g) g^{-1}$ and consider

$$\nu = \sum_{\theta \in \widehat{H}} \nu_\theta e_\theta.$$

Then $m\nu$ is a measure satisfying

$$\nu \cdot (\sigma_{(\alpha)} - N(\alpha)) = \nu_\alpha.$$

To finish, we argue that ν is itself a measure as follows. Assume by contradiction that this was not the case. Let $\mathcal{D}_{\mathfrak{p}}^{\circ}$ be the maximal ideal in $\mathcal{D}_{\mathfrak{p}}$. Choose an element $\mu \in \mathcal{D}_{\mathfrak{p}}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]$ such that $\mu \notin \mathcal{D}_{\mathfrak{p}}^{\circ}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]$ and

$$\mu = c\nu, \quad \text{but} \quad \mu\left(N(\alpha) - \sigma_{(\alpha)}\right) \in \mathcal{D}_{\mathfrak{p}}^{\circ}.$$

We decompose μ as

$$\mu = \sum_{g\in H} \mu_g \cdot g, \quad \mu_g \in \mathcal{D}_{\mathfrak{p}}[[\Gamma']].$$

Since $\mu \notin \mathcal{D}_{\mathfrak{p}}^{\circ}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]$, we can assume without loss of generality that $\mu_1 \notin \mathcal{D}_{\mathfrak{p}}^{\circ}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]$. Then

$$\left(\sigma_{(\alpha)} - N(\alpha)\right) \cdot \mu = \sum_{g\in H} \left(\mu_{hg}\sigma_{(\alpha)}\big|_{\Gamma'} - N(\alpha)\mu_g\right) g,$$

where $h = \left(\sigma_{(\alpha)}\big|_H\right)^{-1}$. It follows that

$$\mu_{hg} \equiv \mu_g N(\alpha)\left(\sigma_{(\alpha)}\big|_{\Gamma'}\right)^{-1} \pmod{\mathcal{D}_{\mathfrak{p}}^{\circ}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]}, \quad \text{for all} \quad g \in H.$$

If d is the order of h, it follows that

$$\mu_1\left(1 - \left(N(\alpha)\left(\sigma_{(\alpha)}\big|_{\Gamma'}\right)^{-1}\right)^d\right) \equiv 0 \pmod{\mathcal{D}_{\mathfrak{p}}^{\circ}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]}.$$

Since $\mu_1 \notin \mathcal{D}_{\mathfrak{p}}^{\circ}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]$, it follows that

$$N(\alpha)^d \equiv \left(\sigma_{(\alpha)}\big|_{\Gamma'}\right)^d \pmod{\mathcal{D}_{\mathfrak{p}}^{\circ}[[\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})]]},$$

which is a contradiction. The conclusion follows. □

So far, we constructed a measure ν on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$ with values in $\mathcal{D}_{\mathfrak{p}}$. There is an implicit dependence of ν on $\mathfrak{f}$, since $\mathbb{F}_\infty = \mathbb{K}(\mathfrak{f}\mathfrak{p}^\infty)$. For later purposes, we will need to be able to define measures (or pseudo-measures) for integral ideals $\mathfrak{g} \mid \mathfrak{f}$. For such an ideal $\mathfrak{g}$, we define the pseudo-measure $\nu(\mathfrak{g})$ on $\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})$ by

$$\nu(\mathfrak{g}) := \nu(\mathfrak{f})|_{\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})} \prod_{\substack{\mathfrak{l}\mid\mathfrak{f} \\ \mathfrak{l}\nmid\mathfrak{g}}} \left(1 - \left(\sigma_{\mathfrak{l}}|_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)}\right)^{-1}\right)^{-1}, \tag{21}$$

where $\nu(\mathfrak{f})|_{\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})}$ is the measure on $\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})$ induced from $\nu(\mathfrak{f})$. We note that whenever $\mathfrak{g}$ is such that $\omega_{\mathfrak{g}} = 1$, the $\nu(\mathfrak{g})$ we defined above is the same as the measure we would have obtained by constructing $\nu(\mathfrak{g})$ directly, using the same methods we used for constructing $\nu(\mathfrak{f})$ (compare also with the comments from [dS, Theorem II.4.12]). It follows that whenever $\mathfrak{g} \neq (1)$, $\nu(\mathfrak{g})$ is a measure, while for $\mathfrak{g} = 1$ we have that $\nu(1)$ is a pseudo-measure, but for any topological generator γ of Γ', $(1-\gamma)\nu(1)$ is also a measure.

Definition 1. *For any integral ideal $\mathfrak{g} \mid \mathfrak{f}$ and any character χ of the group Gal$(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})$, we define the p-adic L-function by*

$$L_{\mathfrak{p},\mathfrak{g}}(\chi) = \begin{cases} \displaystyle\int_{Gal(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})} \chi^{-1} d\nu(\mathfrak{g}) & \text{if } \mathfrak{g} \neq (1) \text{ or } \chi \neq 1 \\ \displaystyle\int_{Gal(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})} 1\, d\left((1-\gamma)\nu((1)\right) & \text{if } \mathfrak{g} = (1) \text{ and } \chi = 1, \end{cases}$$

where γ is a topological generator of Γ'.

THEOREM 5. *Let $\mathfrak{m}$ be a non-trivial integral ideal of $\mathbb{K}$ of the form $\mathfrak{m} = \mathfrak{h}\mathfrak{p}^n$, for some $\mathfrak{h} \mid \mathfrak{f}$ and a positive integer n with the property that for any prime ideal $\mathfrak{l}$ dividing $\mathfrak{f}$, the Artin symbol $\left(\frac{\mathbb{K}(\mathfrak{p}^n)/\mathbb{K}}{\mathfrak{l}}\right)$ is non-trivial. Let χ be a character of finite order whose conductor divides $\mathfrak{m}$ with the property that $\mathfrak{p}^n$ is the exact power of n dividing the conductor of χ. We define*

$$L_{\mathfrak{p},\mathfrak{m}}(\chi) = L_{\mathfrak{p},\mathfrak{h}}(\chi),$$

with $L_{\mathfrak{p},\mathfrak{h}}(\chi)$ as defined in Definition 1. Then one has

$$L_{\mathfrak{p},\mathfrak{m}}(\chi) = -\frac{1}{12h\omega_{\mathfrak{h}}} u_\chi G(\chi^{-1}) \sum_{\sigma \in Gal(\mathbb{K}(\mathfrak{m})/\mathbb{K})} \chi(\sigma) \log \varphi_{\mathfrak{m}}(\sigma),$$

where u_χ and $G(\chi)$ are as in Theorem 3, h is the smallest positive integer in $\mathfrak{h} \cap \mathbb{Z}$, and $\omega_{\mathfrak{h}}$ denotes the number of roots of unity in $\mathbb{K}$ which are 1 modulo $\mathfrak{h}$.

Proof. The case when $\mathfrak{m} = \mathfrak{f}\mathfrak{p}^n$ is an easy computation using Lemma 5, Theorem 4 and (7). For the general case, for an integral ideal $\mathfrak{g}$ of $\mathbb{K}$ and a character ϑ of $\mathrm{Gal}(\mathbb{K}(\mathfrak{g})/\mathbb{K})$, we define

$$T_{\mathfrak{g}}(\vartheta) = -\frac{1}{12g\omega_{\mathfrak{g}}} G(\vartheta^{-1}) \sum_{\sigma \in \mathrm{Gal}(\mathbb{K}(\mathfrak{g})/\mathbb{K})} \vartheta(\sigma) \log \varphi_{\mathfrak{g}}(\sigma).$$

It is proved in [Ku-La, Chapter 11, Theorem 2.1] that for two ideals $\mathfrak{g} \mid \mathfrak{g}'$, and ϑ a character of $\mathrm{Gal}(\mathbb{K}(\mathfrak{g})/\mathbb{K})$, one has

$$T_{\mathfrak{g}'}(\vartheta) = \prod_{\substack{\mathfrak{l} \mid \mathfrak{g}' \\ \mathfrak{l} \nmid \mathfrak{g}}} (1 - \chi(\mathfrak{l}))\, T_{\mathfrak{g}}(\vartheta). \tag{22}$$

The general case follows from our definition of $L_{\mathfrak{p},\mathfrak{m}}$, the relation (22) and the fact that the character χ acts non-trivially on each prime dividing $\mathfrak{f}$. ☐

We can now define the p-adic L-function associated with a character χ of H.

DEFINITION 2. *We recall that we fixed a decomposition*

$$Gal(\mathbb{F}_\infty/\mathbb{K}) = \Gamma' \times H,$$

where $\Gamma' \cong Gal(\mathbb{K}_\infty/\mathbb{K})$ and $H = Gal(\mathbb{F}_\infty/\mathbb{K}_\infty)$. We also fix a topological generator γ of Γ' and an isomorphism

$$\kappa : \Gamma' \to 1 + q\mathbb{Z}_p,$$

where $q = p$ if p is odd and $q = 4$ otherwise. Let χ be a character of H and let $\mathfrak{g}_\chi$ be the prime to $\mathfrak{p}$-part of its conductor. We define the p-adic L-function of the character χ as

$$L_{\mathfrak{p}}(s,\chi) = \int_{Gal(\mathbb{K}(\mathfrak{g}_\chi \mathfrak{p}^\infty)/\mathbb{K})} \chi^{-1}\kappa^s d\nu(\mathfrak{g}_\chi) \quad \textit{if } \chi \neq 1;$$

$$L_{\mathfrak{p}}(s,\chi) = \int_{Gal(\mathbb{K}(\mathfrak{p}^\infty)/\mathbb{K})} \chi^{-1}\kappa^s \; d\left((1-\gamma)\nu(1)\right) \quad \textit{if } \chi = 1.$$

3. Vanishing of the μ-invariant of the p-adic L-function. We recall that our strategy for proving that the Iwasawa's μ-invariant of $X(\mathbb{F}_\infty)$ is zero is to associate to each p-adic L-function $L_\mathfrak{p}(s,\chi)$ a certain invariant (called the μ-invariant of $L_\mathfrak{p}(s,\chi)$), prove that this invariant is zero for each χ, and then show that the sum over all $\mu(L_\mathfrak{p}(s,\chi))$ coincides with $\mu\left(X(\mathbb{F}_\infty)\right)$.

We will now define the μ-invariant of $L_\mathfrak{p}(s,\chi)$. Let $F(w)$ be an element in $\mathcal{D}_\mathfrak{p}[[w]]$. By Weierstrass preparation theorem, $F(w)$ can be written as $F(w) = U(w)\pi'^m g(w)$, where π' is a uniformizer of $\mathcal{D}_\mathfrak{p}$, $U(w)$ is a unit in $\mathcal{D}_\mathfrak{p}[[w]]$, $g(w)$ is a distinguished polynomial and m is a non-negative integer. Then one defines $\mu(F) = m$.

Fix now a character χ of H. It is well-known that $L_\mathfrak{p}(s,\chi)$ is an Iwasawa function, i.e. there exists $\tilde{G}(w,\chi) \in \mathcal{D}_\mathfrak{p}[[w]]$ such that

$$\tilde{G}(u^s - 1, \chi) = L_\mathfrak{p}(s,\chi),$$

where $u = \kappa(\gamma)$, with κ and γ as in Definition 2. We define

$$\mu\left(L_\mathfrak{p}(s,\chi)\right) = \mu\left(\tilde{G}(w,\chi)\right).$$

The main theorem of this section is the following.

THEOREM 6. *For every prime p, and for every character χ of H we have*

$$\mu\left(L_\mathfrak{p}(s,\chi)\right) = 0.$$

For our approach, it will be more convenient to work with the μ-invariant associated with the function

$$L_{\mathfrak{p},\mathfrak{f}}(s,\chi) := \int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})} \chi^{-1}\kappa^s d\nu.$$

We first notice that if $G_\mathfrak{f}(w,\chi)$ is the power series associated with $L_{\mathfrak{p},\mathfrak{f}}(s,\chi)$, then $\mu(G_\mathfrak{f}(w,\chi)) = 0$ implies $\mu(\tilde{G}(w,\chi)) = 0$. To show that $\mu\left(G_\mathfrak{f}(w,\chi)\right) = 0$ it will be in turn easier to use Theorem 3. To this end, we also fix some $\alpha \in \mathcal{O}_\mathbb{K}$ non-unit and coprime to $6\mathfrak{p}\mathfrak{f}$ and let $G(w,\chi) \in \mathcal{D}_\mathfrak{p}[[w]]$ be defined as

$$G(u^s - 1, \chi) = \int_{\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})} \chi^{-1}\kappa^s d\nu_\alpha.$$

We note that by Theorem 4, there exists a power series $h_\chi(w) \in \mathcal{D}_\mathfrak{p}[[w]]$ such that

$$h_\chi(w) G_\mathfrak{f}(w,\chi) = G(w,\chi).$$

Therefore, in order to prove Theorem 6, it suffices to show that $\mu\left(G(w,\chi)\right) = 0$.

We recall that $t \geq 0$ was chosen such that

$$\mathbb{H}(\mathbb{K}) \cap \mathbb{K}_\infty = \mathbb{K}_t,$$

where $\mathbb{H}(\mathbb{K})$ denotes the Hilbert class field of $\mathbb{K}$. We define the following sets

$\mathcal{R}_1 = \{$coset representatives of $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{F})$ in $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}_t)\}$;

$\mathcal{R}_2 = \{$coset representatives of $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}_t)$ in $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K})\}$.

Notice that we can choose the elements in $\mathcal{R}_1$ to lie in H and the elements in $\mathcal{R}_2$ to lie in the subgroup Γ' of $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K})$. We fix such a choice for both $\mathcal{R}_1$ and $\mathcal{R}_2$. Then the set

$$\mathcal{R} = \{\sigma_1\sigma_2 : \sigma_1 \in \mathcal{R}_1,\, \sigma_2 \in \mathcal{R}_2\}$$

is a complete set of coset representatives for $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{F})$ in $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K})$. We also let ω denote the Teichmüller character of $\mathbb{Z}_p$ and let $i \geq 0$ be such that χ^{-1} acts on $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ like ω^i. Then one has

$$\begin{aligned} G(u^s-1,\chi) &= \sum_{\sigma\in\mathcal{R}} \chi^{-1}\kappa^s(\sigma) \int_{\mathcal{G}} \chi^{-1}\kappa^s d\nu_\alpha \circ \sigma \\ &= \sum_{\sigma_1\in\mathcal{R}_1} \chi^{-1}(\sigma_1) \sum_{\sigma_2\in\mathcal{R}_2} \kappa^s(\sigma_2) \int_{\mathcal{G}} \omega^i\kappa^s d\nu_\alpha \circ \sigma. \end{aligned}$$

We will now introduce the notion of a Γ-transform. Let p be a prime and let μ be a measure on $\mathbb{Z}_p^\times$ taking values in $\mathcal{D}_\mathfrak{p}$. For $0 \leq i \leq p-2$ ($i = 0, 1$ when $p = 2$), we define the ith Γ-transform of the measure μ by

$$\Gamma_\mu^{(i)}(s) = \int_{\mathbb{Z}_p^\times} \omega^i(x)\langle x\rangle^s d\mu.$$

Let $G^{(i)}(w,\mu) \in \mathcal{D}_\mathfrak{p}[[w]]$ be the Iwasawa function corresponding to $\Gamma_\mu^{(i)}$.

Using the isomorphism $\mathcal{G} \cong \mathbb{Z}_p^\times$ and that $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}) = \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})^{p^t}$, it follows by the above computations that one has

$$G(u^s-1,\chi) = \sum_{\sigma_2\in\mathcal{R}_2} \kappa^s(\sigma_2) \sum_{\sigma_1\in\mathcal{R}_1} \chi^{-1}(\sigma_1)\Gamma^{(i)}_{\nu_\alpha\circ\sigma}(p^t s).$$

Since the quantities $\chi^{-1}(\sigma_1)$ are independent of s, we obtain further

$$G(u^s-1,\chi) = \sum_{\sigma_2\in\mathcal{R}_2} \kappa^s(\sigma_2)\Gamma^{(i)}_{\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma}\left(p^t s\right). \tag{23}$$

To be able to make further progress, we will need some further properties of Γ-transforms. For a $\mathcal{D}_\mathfrak{p}$-valued measure μ with corresponding power series $F_\mu(w) \in \mathcal{I}_\mathfrak{p}[[w]]$, we denote by $D\mu$ the measure corresponding to $DF_\mu(w)$, where we recall that $D = (1+w)\frac{d}{dw}$. Then one has the following result.

Lemma 6. *For any prime p and any i as above, one has*

$$\Gamma_\mu^{(i)}(s) = \Gamma_{D\mu}^{(i-1)}(s-1),$$

where the quantity $i-1$ should be read modulo $p-1$ (resp. modulo p for $p=2$).

Proof. The result is well-known for p odd. For $p = 2$, the proof is similar and we provide it below. For integers $s \equiv 1 \pmod 2$, one has

$$\begin{aligned}\int_{\mathbb{Z}_2^\times} \langle x\rangle^s d\mu &= \int_{\mathbb{Z}_2^\times} x^s \omega(x) d\mu \\ &= \int_{1+4\mathbb{Z}_2} x^s d\mu - \int_{-1+4\mathbb{Z}_2} x^s d\mu \\ &= \int_{1+4\mathbb{Z}_2} x^{s-1} d(D\mu) - \int_{-1+4\mathbb{Z}_2} x^{s-1} d(D\mu) \\ &= \int_{\mathbb{Z}_2^\times} x^{s-1}\omega(x) d(D\mu) \\ &= \int_{\mathbb{Z}_2^\times} \langle x\rangle^{s-1}\omega(x) d(D\mu).\end{aligned}$$

The cases when $s \equiv 0 \pmod 2$ and $i \neq 0$ are proved in a similar way. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_2$, the result follows by a simple continuity argument. $\square$

By Lemma 6 and (23), it follows that

$$G(u^s - 1, \chi) = \sum_{\sigma_2 \in \mathcal{R}_2} \kappa^s(\sigma_2) \Gamma^{(i-1)}_{D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma} \left(p^t s - 1\right). \tag{24}$$

Note that $\{\kappa^s(\sigma_2) : \sigma_2 \in \mathcal{R}_2\}$ corresponds to the set of power series $\{(1+w)^j : j = 0\dots, p^t - 1\}$. Using this, from (24), it follows that

$$G(w, \chi) = \sum_{j=0}^{p^t-1} (1+w)^j G^{(i-1)} \left(\frac{(1+w)^{p^t}}{u^{p^t}} - 1, D \sum_{\sigma_1 \in \mathcal{R}_1} \chi^{-1}(\sigma_1)\nu_\alpha \circ \sigma \right). \tag{25}$$

We will now explain how, in order to prove that $\mu(G(w,\chi)) = 0$, it suffices to show that the μ-invariant of any summand in the right hand side of (25) is zero. For this, we will use the following general lemma, which is also proved in [Gil 1, Lemma 2.10.2], but we redo the proof here for the convenience of the reader.

Lemma 7. *For every $j = 0, \dots, p^t - 1$, let $f_j(w) \in \mathcal{D}_{\mathfrak{p}}[[w]]$ be a power series and consider the series*

$$f(w) = \sum_{j=1}^{p^t-1} (1+w)^j f_j((1+w)^{p^t} - 1).$$

Then one has $\mu(f(w)) \leq \mu(f_j((1+w)^{p^t} - 1))$, for any $j = 0, \dots, p^t - 1$.

Proof. For every $j = 0, \dots, p^t - 1$, we let $\tilde{\nu}_j$ denote the measure associated with f_j and we also denote by $\tilde{\nu}$ the measure associated with f. We first notice that

$$\int_{\mathbb{Z}_p} (1+w)^{j+p^t x} d\tilde{\nu}_j(x) = (1+w)^j f_j((1+w)^{p^t} - 1).$$

On the other hand, there exists a bijection between $\mathbb{Z}_p$ and $j+p^t\mathbb{Z}_p$, and under this bijection, the measure $\tilde{\nu}_j$ corresponds to a measure $\overline{\nu}_j$ on $j+p^t\mathbb{Z}_p$. One then has the equality

$$\int_{\mathbb{Z}_p}(1+w)^{j+p^t x}d\tilde{\nu}_j(x)=\int_{j+p^t\mathbb{Z}_p}(1+w)^x d\overline{\nu}_j(x).$$

In particular, this shows that for every j, the series $(1+w)^j f_j((1+w)^{p^t}-1)$ corresponds to a measure supported on $j+p^t\mathbb{Z}_p$.

Moreover, we note that if π' divides the power series associated to the measure $\tilde{\nu}$, it must divide the power series associated to restriction of $\tilde{\nu}$ to $j+p^t\mathbb{Z}_p$ for any j, which by above is exactly $\overline{\nu}_j$. This completes our proof. □

By taking

$$f_j((1+w)^{p^t}-1)=G^{(i-1)}\left(\frac{(1+w)^{p^t}}{u^{p^t}}-1, D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right),$$

it follows from Lemma 7 and (25) that if for $\sigma_2=1$ one has

$$\mu\left(G^{(i-1)}\left(\frac{(1+w)^{p^t}}{u^{p^t}}-1, D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right)\right)=0, \tag{26}$$

then $\mu\left(G(w,\chi)\right)=0$.

To prove (26) for $\sigma_2=1$, we will need the following important result, which is essentially [Sch, Theorem I]. We recall that $\beta^v(w)\in\mathcal{I}_{\mathfrak{p}}[[w]]$ is the isomorphism $\beta^v:\widehat{\mathbf{G}}_m\to\hat{E}^v$ defined in Lemma 3.

Theorem 7. *Let $\lambda:\mathbb{Z}_p\to\mathcal{D}_{\mathfrak{p}}$ be a measure whose associated power series is of the form $R(\beta^v(w))$, for some rational function R on E with coefficients in a finite extension of $\mathcal{O}(\mathbb{F}_v)$. Let W be the group of roots of unity contained in $\mathbb{K}$. Then*

$$\mu\left(\Gamma_\lambda^{(i)}(s)\right)=\mu\left(\sum_{v\in W}\omega^i(v)\lambda^*\circ(v)\right),$$

where λ^* denotes the measure $\lambda|_{\mathbb{Z}_p^\times}$.

The work done by Schneps in [Sch] has a great degree of generality, which makes the arguments easy to adapt to our situation. For convenience of the reader, we will redo the main arguments from her proof (following the same notations as in [Sch] as much as possible) and also discuss the cases $p=2,3$ that are left out from her work, but can be easily included. Given that up to these minor modifications our proof is exactly the same as the one done in [Sch, Theorem I], we provide the details in the Appendix and we now proceed with the proof of Theorem 6.

In view of (26), we note that

$$\begin{aligned}&\mu\left(G^{(i-1)}\left(\frac{(1+w)^{p^t}}{u^{p^t}}-1, D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right)\right)\\&=\mu\left(G^{(i-1)}\left(w, D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right)\right).\end{aligned}$$

To see this, note that $\frac{(1+w)^{p^t}}{u^{p^t}} - 1$ is a distinguished polynomial because $u \equiv 1 \pmod p$. Thus, if we let $G^{(i-1)}\left(w, D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right) = \pi'^m P(w)U(w)$ for a distinguished polynomial $P(w)$ and a unit $U(w)$, it follows that the polynomial $P(\frac{(1+w)^{p^t}}{u^{p^t}} - 1)$ is again distinguished and $U(\frac{(1+w)^{p^t}}{u^{p^t}} - 1)$ is again a unit. Hence the two μ-invariants match.

Using Theorem 7 and the above observation, we are left to prove that

$$\mu\left(\sum_{v\in W}\omega^{(i-1)}(v)\lambda^*\circ(v)\right) = 0, \quad \text{where} \quad \lambda = D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma_1.$$

Let $\mathfrak{C}'\subset\mathfrak{C}_0$ be such that

$$\{\chi(\sigma_{\mathfrak{a}}) : \mathfrak{a}\in\mathfrak{C}'\} = \{\chi(\sigma_1) : \sigma_1\in\mathcal{R}_1\}.$$

Then, by the definition of ν_α, one has

$$\lambda = \sum_{\mathfrak{a}\in\mathfrak{C}'}\chi(\sigma_{\mathfrak{a}})D\nu_{\alpha,\mathfrak{a}}.$$

We now have all the ingredients required to prove Theorem 6.

Proof of Theorem 6. By construction, $D\mathcal{B}_{\alpha,\mathfrak{a}}$ corresponds to the rational function on E given by

$$\frac{1}{p}\Omega_v\frac{d}{dz}\log\left(\frac{\xi_{\alpha,\sigma_{\mathfrak{a}}}(\eta(\mathfrak{a})(P\oplus Q)^p}{\xi_{\alpha,\sigma_{\mathfrak{a}}\sigma_{\mathfrak{p}}}(\eta(\mathfrak{a}\mathfrak{p})(P\oplus Q))}\right).$$

Since

$$\xi_{\alpha,\sigma_{\mathfrak{a}}}(\eta(\mathfrak{a})(P\oplus Q)) = \prod_{R\in E_{\mathfrak{a}}}\xi_{\alpha,e}(P\oplus Q\oplus R),$$

it follows that

$$\frac{1}{p}\Omega_v\frac{d}{dz}\log\left(\frac{\xi_{\alpha,\sigma_{\mathfrak{a}}}(P\oplus Q)^p}{\xi_{\alpha,\sigma_{\mathfrak{a}}\sigma_{\mathfrak{p}}}(\eta(\mathfrak{a}\mathfrak{p})(P\oplus Q))}\right) = A(P) - B(P),$$

where

$$A(P) = \frac{1}{2p}\Omega_v p\left(\sum_{R\in E_{\mathfrak{a}}}\sum_{M\in E_\alpha\setminus\{0\}}\frac{x'(P\oplus Q\oplus R)}{x(P\oplus Q\oplus R) - x(M)}\right),$$

and

$$B(P) = \frac{1}{2p}\Omega_v\left(\sum_{R\in E_{\mathfrak{a}\mathfrak{p}}}\sum_{M\in E_\alpha\setminus\{0\}}\frac{x'(P\oplus Q\oplus R)}{x(P\oplus Q\oplus R) - x(M)}\right).$$

We first study the term $A(P)$. The possible poles are at points P satisfying

$$P\in\{M\ominus R\ominus Q : M\in E_\alpha, R\in E_{\mathfrak{a}}\},$$

where for two points S, T on the elliptic curve, we denoted by $S \ominus T$ the point $S \oplus (\ominus T)$, where $\ominus T$ denotes the inverse of T with respect to $\oplus$.

To compute the residues, we note that the t-expansions of x and y are

$$x = \frac{1}{t^2} - \frac{c_1}{t} - c_2 + O(t), \quad y = \frac{-1}{t^3} + \frac{d_1}{t^2} + \frac{d_2}{t} + d_3 + O(t),$$

for some constants c_1, c_2, d_1, d_2, d_3 (see [Sil 1, p. 113]). It follows that the residue at $P = \ominus Q \ominus R$ is equal to

$$\frac{1}{2p} \Omega_v \cdot p \left(N(\alpha) - 1 \right) (-2) = -\Omega_v \left(N(\alpha) - 1 \right).$$

When $p \mid N(\alpha) - 1$, which for example always happens for $p = 2$ due to the condition $(\alpha, 6) = 1$, this residue vanishes when reduced modulo π'. However, when $M \neq O$, the Laurent expansion of $\frac{x'(P \oplus Q \oplus R)}{x(P \oplus Q \oplus R) - x(M)}$ around $M \ominus Q \ominus R$ has leading coefficient 1. Using the symmetry of the x-function, it follows that the residue at a point of the form $M \ominus Q \ominus R$ with $M \neq O$ is Ω_v, and Ω_v is coprime to p, so this residue never vanishes modulo π'.

We now turn our attention to $B(P)$. We claim that this term does not have poles. To see this, note that $B(P)$ is obtained from a $\mathcal{D}_{\mathfrak{p}}$-valued measure supported on $q\mathbb{Z}_p$. Since all its possible poles have integral residues and every point in $E_{\mathfrak{p}}$ reduces to O, the restriction of these residues modulo π' vanishes, and the claim follows.

Let us now go back to the sum

$$\sum_{v \in W} \omega^{(i-1)}(v) \left(\sum_{\mathfrak{a} \in \mathfrak{C}'} \chi(\sigma_{\mathfrak{a}}) D\nu_{\alpha, \mathfrak{a}} \right) \circ (v).$$

We established that the set of poles of $D\nu_{\alpha,\mathfrak{a}}$ always contains the set

$$\mathcal{P}_{\mathfrak{a}} = \{ M \ominus Q \ominus R : \, M \in E_\alpha \setminus \{O\}, \, R \in E_{\mathfrak{a}} \}.$$

The key property that we will use is that the reduction modulo $\mathfrak{p}$ is injective on $\mathcal{P}_{\mathfrak{a}}$ for every $\mathfrak{a}$, and thus also on the set

$$\mathcal{P} := \bigcup_{\mathfrak{a} \in \mathfrak{C}'} \mathcal{P}_{\mathfrak{a}}.$$

Since W consists of the roots of unity in $\mathbb{K}$, a simple check shows that for any distinct $v_1, v_2 \in W$ one has

$$\{ v_1 \cdot P : \, P \in \mathcal{P} \} \cap \{ v_2 \cdot P : \, P \in \mathcal{P} \} = \emptyset.$$

Indeed, if

$$v_1 \left(M_1 \ominus Q \ominus R_1 \right) = v_2 \left(M_2 \ominus Q \ominus R_2 \right),$$

for some $M_1, M_2 \in E_\alpha, R_1 \in E_{\mathfrak{a}_1}, R_2 \in E_{\mathfrak{a}_2}$, then we can choose non-zero elements $\beta_1 \in \mathfrak{a}_1$ and $\beta_2 \in \mathfrak{a}_2$ such that

$$\beta_1 R_1 = \beta_2 R_2 = O.$$

It then follows that $v_1 \alpha \beta_1 \beta_2 Q = v_2 \alpha \beta_1 \beta_2 Q$. Since Q is a primitive f-torsion point and $(\alpha \beta_1 \beta_2, \mathfrak{f}) = 1$, it follows that $v_1 \equiv v_2 \pmod{\mathfrak{f}}$. But since $\omega_{\mathfrak{f}} = 1$, we deduce that $v_1 = v_2$.

We conclude that the expression $\sum_{v\in W}\omega^{(i-1)}(v)\left(\sum_{\mathfrak{a}\in\mathfrak{C}'}\chi(\sigma_{\mathfrak{a}})D\nu_{\alpha,\mathfrak{a}}\right)\circ(v)$ has poles at every point of the form $v\cdot P$ for $v\in W$, $P\in\mathcal{P}$. If P is of the form $P=M\ominus Q\ominus R$ with $M\neq O$ and $R\neq O$, then the residue at $v\cdot P$ is $\omega^{i-1}(v^{-1})\chi(\sigma_{\mathfrak{a}})\Omega_v$, for some $\mathfrak{a}\in\mathfrak{C}'$. Since the expression $\omega^{i-1}(v^{-1})\chi(\sigma_{\mathfrak{a}})\Omega_v$ is non-zero modulo π', it follows that our sum

$$\sum_{v\in W}\omega^{(i-1)}(v)\left(\sum_{\mathfrak{a}\in\mathfrak{C}'}\chi(\sigma_{\mathfrak{a}})D\nu_{\alpha,\mathfrak{a}}\right)\circ(v)$$

has non-trivial poles when it is reduced modulo π' and thus its μ-invariant must be 0. This completes the proof of the fact that

$$\mu\left(L_{\mathfrak{p},\mathfrak{f}}(s,\chi)\right)=0,$$

and hence, of Theorem 6. $\square$

4. Proof of the main theorem. For every $n\geq 2$, we let $\mathbb{M}(\mathbb{F}_n)$ denote the maximal p-abelian extension of $\mathbb{F}_n$ unramified outside the primes in $\mathbb{F}_n$ lying above $\mathfrak{p}$ and we denote by $\mathbb{H}(\mathbb{F}_n)$ the p-Hilbert class field of $\mathbb{F}_n$. Since $\mathbb{F}_n$ is an abelian extension of an imaginary quadratic field, Leopoldt's conjecture holds for the field $\mathbb{F}_n$ and thus $\mathbb{M}(\mathbb{F}_n)/\mathbb{F}_\infty$ is a finite extension. Since we fixed an isomorphism $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})\cong H\times\Gamma'$, we can regard $\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)$ as a module over $\mathbb{Z}_p[[\Gamma']]$. We also recall that $t\geq 0$ is defined by

$$\mathbb{H}(\mathbb{K})\cap\mathbb{K}_\infty=\mathbb{K}_t,$$

where $\mathbb{H}(\mathbb{K})$ stands for the Hilbert class field of $\mathbb{K}$. Then, if we denote $\Gamma:=\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{L})$, it follows that the image of Γ in Γ' under restriction to $\mathbb{K}_\infty$ is Γ'^{p^t}. With these notations, one has the following formula of Iwasawa, valid for all sufficiently large n:

$$\mathrm{ord}_p\left([\mathbb{M}(\mathbb{F}_n):\mathbb{F}_\infty]\right)=p^{n+t-e-1}\mu+(n-1-e)\lambda+c, \tag{27}$$

where μ (resp. λ) is the μ-invariant (resp. λ-invariant) of $X(\mathbb{F}_\infty)$ as a $\mathbb{Z}_p[[\Gamma']]$-module, c is a constant independent of n and e is equal to 1 if $p=2$ and $e=0$ otherwise.

For the purpose of the following result, we will work with some fixed $n\geq 2$. For a prime $\mathcal{P}$ in $\mathbb{F}_n$ lying above $\mathfrak{p}$, we let $U_{n,\mathcal{P}}$ denote the group of principal units in $\mathbb{F}_{n,\mathcal{P}}$, the localization of $\mathbb{F}_n$ at $\mathcal{P}$. We also let

$$U_n=\prod_{\mathcal{P}|\mathfrak{p}}U_{n,\mathcal{P}},\quad \Phi_n=\prod_{\mathcal{P}|\mathfrak{p}}\mathbb{F}_{n,\mathcal{P}}.$$

There exists a canonical embedding $\Psi:\mathbb{F}_n\hookrightarrow\Phi_n$. Let E_n denote group of units in $\mathbb{F}_n$ which are 1 modulo every prime $\mathcal{P}$ lying above $\mathfrak{p}$. Notice that if $e\in\mathcal{O}(\mathbb{F}_n)^\times$, then $e^{N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})-1}\in E_n$, so E_n has finite index in $\mathcal{O}(\mathbb{F}_n)$ and this index is coprime to p. Then $\Psi(E_n)\subset U_n$ and we let $\overline{E}_n$ denote the closure of E_n in U_n.

Since the prime $p=2$ plays a special role, we will use the same notations as before, letting $q=p$ when p is odd and $q=4$ when $p=2$. With this notation, we let D_n be the $\mathbb{Z}_p$-submodule of U_n generated by $\overline{E}_n$ and $(1+q)$. To compute $\mathrm{ord}_p\left([\mathbb{M}(\mathbb{F}_n):\mathbb{F}_\infty]\right)$, we will need several results from class field theory. Our main reference for the following exposition is [Co-Wi 1].

Let C_n denote the idéle class group of $\mathbb{F}_n$ and

$$Y_n := \bigcap_{m \geq n} N_{\mathbb{F}_m/\mathbb{F}_n}(C_m).$$

By class field theory, there exists an isomorphism of $\mathbb{Z}_p$-modules

$$(Y_n \cap U_n)/\overline{E}_n \cong \mathrm{Gal}\left(\mathbb{M}(\mathbb{F}_n)/\mathbb{H}(\mathbb{F}_n)\cdot\mathbb{F}_\infty\right).$$

Since the extension $\mathbb{F}_\infty/\mathbb{F}_n$ is totally ramified above $\mathfrak{p}$, it follows that the field $\mathbb{H}(\mathbb{F}_n) \cap \mathbb{F}_\infty = \mathbb{F}_n$, and therefore, in view of the above isomorphism, one obtains that

$$\mathrm{ord}_p\left([\mathbb{M}(\mathbb{F}_n) : \mathbb{F}_\infty]\right) = \mathrm{ord}_p\left(h(\mathbb{F}_n)\cdot\left[Y_n \cap U_n : \overline{E}_n\right]\right),$$

where $h(\mathbb{F}_n)$ denotes the class number of $\mathbb{F}_n$. It is proved in [Co-Wi 1, Lemma 5] that one has $Y_n \cap U_n = \ker\left(N_{\Phi_n/\mathbb{K}_\mathfrak{p}}\big|_{U_n}\right)$. It is also not difficult to show that $N_{\Phi_n/\mathbb{K}_\mathfrak{p}}(U_n) = 1 + qp^{n-1}\mathcal{O}(\mathbb{K}_\mathfrak{p})$ (see [Co-Wi 1, Lemma 6]). It follows that $N_{\Phi_n/\mathbb{K}_\mathfrak{p}}(\overline{E}_n) = 1$. Using this, it follows that $N_{\Phi_n/\mathbb{K}_\mathfrak{p}}(D_n) = 1 + qp^{n+d-1}\mathcal{O}(\mathbb{K}_\mathfrak{p})$, where $d := \mathrm{ord}_p([\mathbb{F} : \mathbb{K}])$. It follows that the diagram

$$\begin{tikzcd}
1 \arrow[r] & \overline{E}_n \arrow[r] \arrow[d] & D_n \arrow[r, "N_{\Phi_n/\mathbb{K}_\mathfrak{p}}"] \arrow[d] & 1 + qp^{n+d-1}\mathcal{O}(\mathbb{K}_\mathfrak{p}) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & Y_n \cap U_n \arrow[r] & U_n \arrow[r, "N_{\Phi_n/\mathbb{K}_\mathfrak{p}}"] & 1 + qp^{n-1}\mathcal{O}(\mathbb{K}_\mathfrak{p}) \arrow[r] & 1
\end{tikzcd}$$

has exact rows and the vertical maps are injective. It follows that

$$\left[Y_n \cap U_n : \overline{E}_n\right] = \frac{[U_n : D_n]}{p^d}.$$

Using the same methods as in the proof of [Co-Wi 1, Lemma 9], one can show that

$$\mathrm{ord}_p\left([U_n : D_n]\right) = \mathrm{ord}_p\left(\frac{qp^{n+d-1}R_\mathfrak{p}(\mathbb{F}_n)}{\omega(\mathbb{F}_n)\cdot\sqrt{\Delta_\mathfrak{p}(\mathbb{F}_n/\mathbb{K})}}\cdot\prod_{\mathcal{P}|\mathfrak{p}}\left(N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})\right)^{-1}\right),$$

where $\omega(\mathbb{F}_n)$ denotes the number of roots of unity in $\mathbb{F}_n$, $R_\mathfrak{p}(\mathbb{F}_n)$ is the $\mathfrak{p}$-adic regulator of $\mathbb{F}_n$ and $\Delta_\mathfrak{p}(\mathbb{F}_n/\mathbb{K})$ is the $\mathfrak{p}$-part of the relative discriminant of the extension $\mathbb{F}_n/\mathbb{K}$.

It will be convenient for further purposes to express the p-adic valuation of $\left(N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})\right)^{-1}$ in terms of the one of $1 - \frac{1}{N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})}$. But this is straightforward, since for any prime ideal $\mathcal{P}$ in $\mathbb{F}_n$ lying above $\mathfrak{p}$ one has that $N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P}) - 1$ is coprime to p, so the two valuations we are interested in are equal.

Putting everything together, we obtain the following result, which is a simple extension of [Co-Wi 1, Theorem 11].

Proposition 2. *With the notations as above, one has*

$$\mathrm{ord}_p\left([\mathbb{M}(\mathbb{F}_n) : \mathbb{F}_\infty]\right) = \mathrm{ord}_p\left(\frac{qp^{n-1}h(\mathbb{F}_n)R_\mathfrak{p}(\mathbb{F}_n)}{\omega(\mathbb{F}_n)\sqrt{\Delta_\mathfrak{p}(\mathbb{F}_n/\mathbb{K})}}\prod_{\mathcal{P}|\mathfrak{p}}\left(1 - \frac{1}{N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})}\right)\right).$$

Combining Proposition 2 with (27), one immediately deduces the following (see also [dS, Chapter III, Corollary 2.8]).

COROLLARY 1. *If $F \in \mathbb{Z}_p[[\Gamma']]$ is a characteristic power series for the Galois group Gal$(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)$, then for all sufficiently large n one has*

$$\begin{aligned}&\mu(F)p^{t+n-e-2}+\lambda(F)\\&=1+\operatorname{ord}_p\left[\frac{h\left(\mathbb{F}_n\right)R_{\mathfrak{p}}\left(\mathbb{F}_n\right)}{\omega\left(\mathbb{F}_n\right)\sqrt{\Delta_{\mathfrak{p}}\left(\mathbb{F}_n/\mathbb{K}\right)}}\Big/\frac{h\left(\mathbb{F}_{n-1}\right)R_{\mathfrak{p}}\left(\mathbb{F}_{n-1}\right)}{\omega\left(\mathbb{F}_{n-1}\right)\sqrt{\Delta_{\mathfrak{p}}\left(\mathbb{F}_{n-1}/\mathbb{K}\right)}}\right].\end{aligned}$$

The rest of this section is dedicated to showing how this formula relates to special values of our p-adic L-function. Consider the isomorphism $\mathcal{D}_{\mathfrak{p}}[[\Gamma']] \cong \mathcal{D}_{\mathfrak{p}}[[w]]$, and for ρ any character of Γ' of finite order, we write level$(\rho) = m$ if $\rho\left((\Gamma')^{p^m}\right) = 1$, but $\rho\left((\Gamma')^{p^{m-1}}\right) \neq 1$. We will need the following simple result, which is proved for example in [dS, Chapter III, Lemma 2.9].

LEMMA 8. *For any power series $F \in \mathcal{D}_{\mathfrak{p}}[[w]]$ and all sufficiently large n, one has*

$$\mu\left(F\right)p^{n+t-1}(p-1)+\lambda(F)=\operatorname{ord}_p\left\{\prod_{\mathrm{level}(\rho)=t+n}\rho(F)\right\},$$

where $\rho(F)$ means that the action of ρ is extended to $\mathcal{D}_{\mathfrak{p}}[[\Gamma']]$ by linearity and ord_p *is the valuation on $\mathbb{C}_p$ normalized by taking* $\operatorname{ord}_p(p) = 1$.

We will also need the following result, proved in [dS, Chapter III, Proposition 2.10].

PROPOSITION 3. *For any ramified character ε of Gal$(\mathbb{F}_\infty/\mathbb{K})$, we let $\mathfrak{g}$ be the conductor of ε and g the least positive integer in $\mathfrak{g}\cap\mathbb{Z}$. We define $G(\varepsilon)$ as in Theorem* 3 *and we define $S_p(\varepsilon)$ by*

$$S_p(\varepsilon)=-\frac{1}{12g\omega_{\mathfrak{g}}}\sum_{\sigma\in Gal(\mathbb{K}(\mathfrak{g})/\mathbb{K})}\varepsilon^{-1}(\sigma)\log\varphi_{\mathfrak{g}}(\sigma).$$

Let A_n be the collection of all ε for which n is the exact power of $\mathfrak{p}$ dividing their conductor. Then for all sufficiently large n one has

$$\begin{aligned}&\operatorname{ord}_p\left(\prod_{\varepsilon\in A_n}G(\varepsilon)S_p(\varepsilon)\right)\\&=\operatorname{ord}_p\left[\frac{h\left(\mathbb{F}_n\right)R_{\mathfrak{p}}\left(\mathbb{F}_n\right)}{\omega\left(\mathbb{F}_n\right)\sqrt{\Delta_{\mathfrak{p}}\left(\mathbb{F}_n/\mathbb{K}\right)}}\Big/\frac{h\left(\mathbb{F}_{n-1}\right)R_{\mathfrak{p}}\left(\mathbb{F}_{n-1}\right)}{\omega\left(\mathbb{F}_{n-1}\right)\sqrt{\Delta_{\mathfrak{p}}\left(\mathbb{F}_{n-1}/\mathbb{K}\right)}}\right].\end{aligned}$$

Let now χ be a character of H and recall that

$$L_{\mathfrak{p}}(s,\chi)=\int_{\mathrm{Gal}(\mathbb{K}(\mathfrak{g}_\chi\mathfrak{p}^\infty)/\mathbb{K})}\chi^{-1}\kappa^s d\nu(\mathfrak{g}_\chi)\quad\text{if }\chi\neq 1;$$

$$L_{\mathfrak{p}}(s,\chi)=\int_{\mathrm{Gal}(\mathbb{K}(\mathfrak{p}^\infty)/\mathbb{K})}\chi^{-1}\kappa^s(1-\gamma)d\nu(1)\quad\text{if }\chi=1.$$

We define $F(w,\chi) \in \mathcal{D}_{\mathfrak{p}}[[w]]$ to be the corresponding Iwasawa function. Then, using Theorem 5, for a character ρ of Γ' of sufficiently large finite order, one has

$$\rho(F(w,\chi^{-1})) \sim \begin{cases} G(\chi\rho)S_p(\chi\rho) & \text{if } \chi \neq 1; \\ (\rho(\gamma_0)-1)\, G(\chi\rho)S_p(\chi\rho) & \text{if } \chi = 1, \end{cases}$$

where $u \sim v$ denotes the fact that u/v is a $\mathfrak{p}$-adic unit. Let

$$F = \prod_{\chi\in\widehat{H}} F(w,\chi).$$

It follows that for all sufficiently large n one has

$$\prod_{\mathrm{level}(\rho)=t+n} \rho(F) \sim p \prod_{\substack{\varepsilon=\chi\rho \\ \mathrm{level}(\rho)=t+n}} G(\varepsilon)S_p(\varepsilon), \tag{28}$$

since in the product on the right hand side we range over all χ (including $\chi = 1$) and

$$\prod_{\mathrm{level}(\rho)=t+n} (\rho(\gamma_0)-1) = p.$$

Proof of Theorem 1. Using (28), Corollary 1, Lemma 8 and Proposition 3, it follows that

$$\mu(F) = \mu\left(\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)\right).$$

In Theorem 6 we proved that $\mu\left(L_{\mathfrak{p}}(s,\chi)\right) = 0$. It follows that

$$\mu\left(\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)\right) = 0,$$

which completes the proof of the main theorem of this article. □

Acknowledgements. This manuscript is part of the first author's (VC) Ph.D. thesis. We are very grateful to Prof. John Coates for giving us this problem and for his support.

5. Appendix: proof of Schneps' theorem. For the proof of Theorem 7, we will need two independence results (Theorem II and Theorem III in [Sch]). These two theorems are the 'hard work' in adapting Sinnott's independence result from the cyclotomic case (see Section 3 from [Si]). To state what these results are, we need in turn some additional notations.

We begin by noting that if $r = |W|$, then $r = 2$ except for $\mathbb{K} = \mathbb{Q}(i)$ and $\mathbb{K} = \mathbb{Q}(i\sqrt{3})$ when we have $r = 4$ and $r = 6$, respectively. Note that in the two exceptional cases we cannot have $p = 2$ or $p = 3$ since these primes do not split in either field.

For the proof, we will distinguish between the cases $p = 2$ and $p > 2$. The following notations are used for $p > 2$. Let $m = (p-1)/r$ and $\alpha_1, \ldots, \alpha_n$ be a basis for the $\mathcal{O}_{\mathbb{K}}$-module generated by the $(p-1)th$ roots of unity in $\mathbb{Z}_p$. For $1 \le j \le m$ we choose representatives ε_j for the $(p-1)$th roots of unity modulo W. It follows that there exist $a_{ij} \in \mathcal{O}_{\mathbb{K}}$ such that

$$\varepsilon_j = \sum_{i=1}^{n} a_{ij}\alpha_i, \quad 1 \le j \le m. \tag{29}$$

Let $\widetilde{\beta^v}(w) \in \overline{\mathbf{F}}_p$ be the reduction of $\beta^v(w)$ modulo π and we let $\hat{\varepsilon}$ be the formal group of $\widetilde{E}$, the reduction of E modulo π. We fix an indeterminate T and extend the field of definition of $\widetilde{E}$ to the field of fractions of $\mathbf{B} := \overline{\mathbf{F}}_p[[T]]$. From now on, we will also view $\mathbf{B}$ as the underlying set for $\widehat{\mathbf{G}}_m$ in characteristic p. With this setup, it follows that $\widetilde{\beta^v}$ converges to a value on $\hat{\varepsilon}$ whenever the image of w lies in (T), the maximal ideal of $\mathbf{B}$.

For every $\alpha \in \mathbb{Z}_p$ there exists a unique power series $[\alpha](t)$ such that $[\alpha](t) \equiv \alpha t \pmod{\deg 2}$ and $[\alpha](t)$ is an endomorphism of $\widehat{E}$ (see Proposition I.1.5 in [dS]). We will write $\widetilde{[\alpha]}(t)$ for the reduction of $[\alpha](t)$ modulo π.

With the positive integer n defined as above, we consider

$$E^n := \underbrace{E \times E \times \cdots \times E}_{n \text{ times } E}$$

and let $t_1, \ldots, t_n$ be the copies of the parameter t arising from the coordinate projections $E^n \to E$. Let $\mathbb{F}(E^n)$ be the field of rational functions on this abelian variety, written as Laurent expansions at $t_1, \ldots, t_n$, and define

$$D := \mathbb{F}(E^n) \cap \mathcal{D}_{\mathfrak{p}}[[t_1, \ldots, t_n]].$$

Analogously, we let $\widetilde{E}^n$ be the product of n copies of $\widetilde{E}$, and we also define $\widetilde{D} = \mathbb{F}(\widetilde{E}^n) \cap \mathbf{B}[[t_1, \ldots, t_n]]$.

We can now state the aforementioned independence results.

Proposition 4. *For $1 \leq j \leq m$, let $\Phi_j : \widetilde{E}^n \to \widetilde{E}$ be the map given by*

$$\Phi_j(P_1, \ldots, P_n) = \sum_{i=1}^{n} a_{ij} P_i,$$

and assume that $r_1, \ldots, r_m$ are rational functions on $\widetilde{E}$ with the property that

$$\sum_{j=1}^{m} r_j\left(\Phi_j(x)\right) = 0, \quad \text{for all} \quad x \in \widetilde{E}^n.$$

Then each r_j is a constant function on $\widetilde{E}$.

Proposition 5. *Let $\Theta : \mathbf{B}[[t_1, \ldots, t_n]] \to \mathbf{B}[[t]]$ be the map given by*

$$\Theta(t_i) = \widetilde{[\alpha_i]}(t).$$

Then the restriction of Θ to $\widetilde{D}$ is injective, i.e. if $r \in \widetilde{D}$ is such that

$$r\left(\widetilde{[\alpha_i]}(t), \ldots, \widetilde{[\alpha_n]}(t)\right) = 0,$$

then $r \equiv 0$.

We will also need the following auxiliary lemma, which is the content of the Proposition proved on page 25 in [Sch].

Lemma 9. *If C is any compact-open set in $\mathbb{Z}_p$, then for λ as in the statement of Theorem 7 one has that the power series associated with $\lambda|_C$ has the form $R_C\left(\beta^v(w)\right)$, where R_C is also a rational function on E.*

Armed with the above results, we can proceed to the proof of Theorem 7.

Proof of Theorem 7. We treat first the case $p \geq 3$. For every $0 \leq i \leq p-2$ we define a measure

$$\kappa_i = \sum_{\zeta \in W} \omega^i(\zeta)\lambda^* \circ (\zeta).$$

By Lemma 9, λ^* is associated with a rational function $R^*\left(\beta^v(w)\right)$, hence $\lambda^* \circ (\zeta)$ is associated with $R^*\left([\zeta^{-1}]\left(\beta^v(w)\right)\right)$. It follows that κ_i is associated with a rational function in $\beta^v(w)$ on E. Furthermore, one has

$$\begin{aligned}
\Gamma_{\kappa_i}^{(i)}(s) &= \sum_{\zeta \in W} \omega^i(\zeta) \int_{\mathbb{Z}_p^*} \langle x \rangle^s \omega^i(x) d\lambda^* \circ (\zeta) \\
&= \sum_{\zeta \in W} \omega^i(\zeta) \int_{\mathbb{Z}_p^*} \left\langle \zeta^{-1} x \right\rangle^s \omega^i\left(\zeta^{-1} x\right) d\lambda^* \\
&= \sum_{\zeta \in W} \omega^i(\zeta)\omega^i(\zeta^{-1}) \int_{\mathbb{Z}_p^*} \langle x \rangle^s \omega^i(x) d\lambda \\
&= r\Gamma_\lambda^{(i)}(s).
\end{aligned}$$

Since we are in the case $p \geq 3$ and $r \in \{2, 4, 6\}$, with $r \neq 6$ when $p = 3$, it follows that

$$\mu\left(\Gamma_\lambda^{(i)}(s)\right) = \mu\left(\Gamma_{\kappa_i}^{(i)}(s)\right).$$

It therefore suffices to prove that

$$\mu(\kappa_i) = \mu\left(\Gamma_{\kappa_i}^{(i)}(s)\right).$$

First notice that if the power series associated with κ_i is divisible by π', then so is the power series associated with $\sum_{\varepsilon \in V} \varepsilon^i \kappa_i \circ \varepsilon|_U$ (see (18)), hence $\Gamma_{\kappa_i}^{(i)}(s)$ is also divisible by π'.

Conversely, assume that π' divides the power series associated with the measure $\sum_{\varepsilon \in V} \varepsilon^i \kappa_i \circ \varepsilon|_U$. By (17), it follows that π' divides the power series associated with the measure

$$r \sum_{j=1}^{m} \varepsilon_j^{-i} \left.\kappa_i\right|_{(\varepsilon_j^{-1}U)} \circ \left(\varepsilon_j^{-1}\right).$$

Let $F_j(\beta^v(w))$ be the power series corresponding to the measure $\varepsilon_j^{-i} \left.\kappa_i\right|_{(\varepsilon_j^{-1}U)}$. It follows that

$$\sum_{j=1}^{m} F_j\left(\beta^v\left((1+w)^{\varepsilon_j} - 1\right)\right) \equiv 0 \pmod{\pi' \mathcal{D}_{\mathfrak{p}}[[w]]}.$$

If we let $\widetilde{F_j}$ be the reduction of F_j modulo π', it follows that

$$\sum_{j=1}^{m} \widetilde{F_j}\left(\widetilde{[\varepsilon_j]} \cdot \widetilde{\beta^v}(w)\right) = 0.$$

We now define the function $\Phi_j : \widetilde{E}^n \to \widetilde{E}$ by

$$\Phi_j(t_1, \ldots, t_n) = \sum_{i=1}^{n} \widetilde{[a_{ij}]}(t_i),$$

where $a_{ij} \in \mathcal{O}_{\mathbb{K}}$ are the quantities defined in (29). Then

$$\sum_{j=1}^{m} \widetilde{F_j}\left(\widetilde{[\varepsilon_j]} \cdot \widetilde{\beta^v}(w)\right) = \sum_{i=1}^{m} \widetilde{F_j}\left(\Phi_j\left(\widetilde{[\alpha_1]}(t), \ldots, \widetilde{[\alpha_n]}(t)\right)\right) = 0.$$

By Proposition 5, it follows that $\sum\limits_{j=1}^{m} \widetilde{F_j} \circ \Phi_j$ is identically zero on $\widetilde{E}^n$, hence, by Proposition 4, it follows that

$$\sum_{j=1}^{m} F_j \equiv 0 \pmod{\pi' \mathcal{D}_{\mathfrak{p}}[[w]]}.$$

By definition, $F_j(P)$ is the rational function on E corresponding to the measure $\varepsilon_j^{-i}\ \kappa_i|_{(\varepsilon_j^{-1}U)}$, so

$$\begin{aligned} \kappa_i &= \sum_{j=1}^{m} \sum_{\zeta \in W} \zeta^i\ \kappa_i|_{(\varepsilon_j^{-1}U)} \circ (\zeta) \\ &= \sum_{\zeta \in W} \left(\sum_{j=1}^{m} \varepsilon_j^i \zeta^i F_j(\zeta P) \right). \end{aligned}$$

It follows that π' divides κ_i.

We have thus established that the divisibility of κ_i by π' is equivalent to the divisibility of $\Gamma_{\kappa_i}^{(i)}(s)$ by π', which completes the proof in the case $p \geq 3$.

Finally, when $p = 2$, we saw that we cannot have $\mathbb{K} = \mathbb{Q}(i)$ or $\mathbb{K} = \mathbb{Q}(i\sqrt{3})$, hence $r = 2$. Following the trick from the proof of Theorem 1 in [Si], we note that it suffices to prove Theorem 7 when $\lambda = \lambda^*$ and $\omega^i(-1)\lambda \circ (-1) = \lambda$ (for, if λ corresponds to a rational function, then so does $\gamma := \lambda^* + \omega^i(-1)\lambda^* \circ (-1)$ and one has the identities $\gamma = \gamma^*$, $\gamma \circ (-1) = \omega^i(-1)\gamma$, $\Gamma_\gamma^{(i)}(s) = 2\Gamma_\lambda^{(i)}(s)$ and $\gamma^* + \omega^i(-1)\gamma^* \circ (-1) = 2(\lambda^* + \omega^i(-1)\lambda^* \circ (-1))$. We can also assume that λ is not divisible by π', since replacing λ by $\frac{1}{\pi'}\lambda$ (when π' divides λ) decreases both μ-invariants in the statement of Theorem 7 by 1. We are then left to prove that $\mu\left(\Gamma_\lambda^{(i)}(s)\right) = 1$, i.e. that $\mu\left(\mathcal{L}_{\lambda,i}(w)\right) = 1$, where

$$\mathcal{L}_{\lambda,i}(u^s - 1) = \int\limits_{\mathbb{Z}_p^\times} \omega^i(x)\langle x \rangle^s d\lambda.$$

We use the same strategy as in the case $p \geq 3$. Let $G(w)$ be the power series associated with $\lambda|_{1+4\mathbb{Z}_2}$. Using $\lambda = \lambda^*$ and $\omega^i(-1)\lambda \circ (-1) = \lambda$, it follows that

$$\int\limits_{\mathbb{Z}_p^\times} \omega^i(x)\langle x \rangle^s d\lambda = 2 \int\limits_{1+4\mathbb{Z}_2} \omega^i(x) x^s d\lambda = 2G(u^s - 1).$$

Assume by contradiction that $\mu(G(w)) > 0$. But then $\mu(G \circ (-1)) > 0$, and since $\lambda = \lambda^*$, it follows that $G \circ (-1)$ corresponds to $\lambda|_{-1+4\mathbb{Z}_2}$. Since

$$\lambda = \lambda^* = \lambda|_{1+4\mathbb{Z}_2} + \lambda|_{-1+4\mathbb{Z}_2} ,$$

it follows that $\mu(\lambda) > 0$, contradicting our previous assumption that $\mu(\lambda) = 0$. This completes the proof. □

REFERENCES

[B-G-S] D. Bernardi, C. Goldstein and N. Stephens, *Notes p-adiques sur les courbes elliptiques*, J. Reine Angew. Math., 351 (1984), pp. 129–170.

[C-K-L] J. Choi, Y. Kezuka and Y. Li, *Analogues of Iwasawas $\mu = 0$ conjecture and weak Leopoldt theorem for certain non-cyclotomic $\mathbb{Z}_2$-extensions*, Asian Journal of Mathematics, 23:3 (2019) pp. 383–400.

[Co] J. Coates, *Elliptic curves with complex multiplication and Iwasawa theory*, Bull. London Math. Soc., 23 (1991), pp. 321–350.

[Co-Go] J. Coates and C. Goldstein, *Some remarks on the main conjecture for elliptic curves with complex multiplication*, American J. of Mathematics, 105 (1983), pp. 337–366.

[Co-Wi 1] J. Coates and A. Wiles, *Kummer's criterion for Hurwitz numbers*, Algebraic number theory, Kyoto 1976, Japan Society for the Promotion of Science, pp. 9–23 (1977).

[Co-Wi 2] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math., 39 (1977), pp. 223–251.

[Co-Wi 3] J. Coates and A. Wiles, *On p-adic L-functions and elliptic units*, J. Australian Math. Soc., 26 (1978), pp. 1–25.

[Col79] R. Coleman, *Division values in local fields*, Invent. Math., 53 (1979), pp. 91–116.

[dS] E. de Shalit, *The Iwasawa theory of elliptic curves with complex multiplication*, Perspect. Math. Vol.3, (1987).

[Fe-Wa] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2), 109:2 (1979), pp. 377–395.

[Gil 1] R. Gillard, *Fonctions L p-adiques des des corps quadratiques imaginaires et de leurs extensions abèliennes*, J. Reine Angew. Math., 358 (1985), pp. 76–91.

[Gil 2] R. Gillard, *Transformation de Mellin-Leopoldt des fonctions elliptiques*, J. Number Theory, 25:3 (1987), pp. 379–393.

[Go-Sch] C. Goldstein and N. Schappacher, *Séries dEisenstein et fonctions L de courbes elliptiques à multiplication complexe*, Journal für die Reine und Angewandte Mathematik, 327 (1981), pp. 184–218 .

[Gre 2] R. Greenberg, *On the structure of certain Galois groups*, Invent. Math., 47 (1978), pp. 85–99.

[Gr] B. Gross, *Arithmetic on Elliptic curves with Complex Multiplication*, Springer-Verlag. (1980).

[Ku-La] D. S. Kubert and S. Lang, *Modular Units*, Grundelehren der mathematischen Wissenschaften 244: Springer (1981).

[Lu] J. Lubin, *One Parameter Formal Lie Groups over p-adic Integer Rings*, Annals of Mathematics, Second Series, 80:3 (1964), pp. 464–484.

[O-V] H. Oukhaba and S. Viguié, *On the μ-invariant of Katz p-adic L-functions attached to imaginary quadratic fields*, Forum Math., 28:3 (2016), pp. 507–525.

[Ro] G. Robert, *Unités elliptiques et formules pour le nombre de classes des extensions abéliennes d'un corps quadratique imaginaire*, Bulletin Sociente Mathematique de France, 36 (1973), pp. 5–77.

[Ru] K. Rubin, *The "main conjectures" of Iwasawa Theory for imaginary quadratic fields*, Invent. Math., 103 (1991), pp. 25–68.

[Sch] L. Schneps, *On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication*, J. Number Theory, 25:1 (1987), pp. 20–33.

[Shi] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Publications of the Mathematical Society of Japan (1971).

[Sie] C. L. Siegel, *Lectures on advanced analytic number theory*, Tata Institute of Fundamental Research (1961).

[Sil 1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106: Springer (1986).

[Sil 2] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer (1994).

[Si] W. Sinnott, *On the μ-invariant of the Γ-transform of a rational function*, Invent. Math., 75 (1984), pp. 273–282.

[We] A. Weil, *On a certain type of characters of the idèle class group of an algebraic number field*, Proc. Int. Symp. on Alg. Number Th. Tokyo, pp. 1–7 (1955).