The split prime μ-conjecture and further topics in Iwasawa theory

Dissertation
zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
"Doctor rerum naturalium"
der Georg-August-Universität Göttingen

im Promotionsprogramm Mathematical Sciences
der Georg-August University School of Science (GAUSS)

vorgelegt von
Vlad-Cristian Crişan
aus Baia Mare
Göttingen, 2019

Betreuungsausschuss

Prof. Dr. Preda Mihăilescu
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Jörg Brüdern
Mathematisches Institut, Georg-August-Universität Göttingen

Mitglieder der Prüfungskommission

Referent: Prof. Dr. Preda Mihăilescu
Mathematisches Institut, Georg-August-Universität Göttingen

Korreferent: Prof. Dr. Jörg Brüdern
Mathematisches Institut, Georg-August-Universität Göttingen

Weitere Mitglieder der Prüfungskommission:

Prof. Dr. Valentin Blomer
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Russell Luke
Institut für Numerische und Angewandte Mathematik,
Georg-August-Universität Göttingen

Prof. Dr. Viktor Pidstrygach
Mathematisches Institut, Georg-August-Universität Göttingen

Prof. Dr. Max Wardetzky
Institut für Numerische und Angewandte Mathematik,
Georg-August-Universität Göttingen

Tag der mündlichen Prüfung: 04.03.2019

To my parents

Acknowledgements

Throughout my Ph.D. studies I was fortunate enough to enjoy the support of many amazing people and I would like to take this opportunity to thank them for their contribution to my development as a mathematician and as a person.

I would like to thank my supervisor, Prof. Dr. Preda Mihăilescu for the hundreds of hours of mathematical discussions and for his endless enthusiasm for research. I am also very grateful for the flexibility he allowed me in exploring other areas of Mathematics outside those covered by my thesis. I would like to thank Prof. Dr. Jörg Brüdern, my second thesis supervisor, for his advice and active support with the various analytic number theory projects I worked on. I am thankful to Prof. Dr. John Coates for giving me the opportunity to complete the project covered in Chapter 1 of this thesis and for his tremendous help towards its publication. I would like to also express my gratitude towards several professors from the Department of Mathematics in Göttingen for their kind and helpful answers to numerous questions I contacted them with: Prof. Dr. Valentin Blomer, Prof. Dr. Harald Helfgott, Prof. Dr. Ulrich Stuhler, Prof. Dr. Evelina Viada.

I would like to thank all the people I worked with on various articles or books throughout my Ph.D. studies for the beautiful and fruitful collaboration we had: Prof. Dr. Titu Andreescu, Prof. Dr. Dorin Andrica, Katharina Müller, Dr. Dino Destefano, Prof. Dr. Paul Pollack, Marius Tiba, Dr. Francesco Veneziano, Prof. Dr. Evelina Viada.

I am extremely lucky to have an extended list of close people I am indebted to for their constant support. I would like to thank my parents for being the unconditional source of affection I could always rely on. I would like to thank my girlfriend for all her support throughout the ups and downs and for coloring my time in Göttingen in so many ways. From the friends I made in Göttingen, I am particularly indebted to Christoph, Mihai and Tomos for putting up with me on a daily basis and for all the wonderful moments we shared. I am grateful to Csaba, Deniz and Geoffrey for the fun stories we created during sport and outside. From the close friends outside Göttingen, I would like to specially thank Alin, Cătălin, Marius, Radu, and Raluca for their support, for all the beautiful memories and for the active efforts they made in keeping our friendship alive.

Contents

Introduction

Historical remarks

Fermat conjectured in the 17th century that the equation

$$x^n + y^n = z^n$$

has no solutions in positive integers for $n \geq 3$. This problem had famously preoccupied mathematicians for centuries until it was finally proved by Wiles in 1995 ([Wi 2]).

During the first decades of the 19th century there had been several flawed attempts to prove Fermat's conjecture that relied on factorising integers over rings containing the roots of unity. As it was pointed out by Kummer, the key problem with these attempts is that the ring $\mathbb{Z}[\zeta_n]$ (here ζ_n denotes a primitive nth root of unity) is not necessarily a unique factorization domain. Kummer showed in particular that $\mathbb{Z}[\zeta_{23}]$ is not a unique factorization domain (for a proof of this fact, see, for example, the discussion at the end of [Wa, Chapter 1]). After the development of the theory of ideals, it was shown that the failure to have unique factorization in the ring of integers of an algebraic number field can be encoded by the *ideal class group*, a finite abelian group that is trivial if and only if the ring of integers is a unique factorization domain. Kummer also proved the following remarkable connection between the ideal class group of $\mathbb{Q}(\zeta_p)$ and special values of the Riemann ζ-function, known as *Kummer's criterion*: if $p > 3$ is a prime and h_p denotes the size of the class group of $\mathbb{Q}(\zeta_p)$, then $p \mid h_p$ if and only if p divides at least one of the numerators of $\zeta(-1)$, $\zeta(-3)$, …, $\zeta(4-p)$ (see [Co-Su, Theorem 1.1.2]).

Kummer's criterion and the unique factorization property are just two of the early motivating results that led to an intensive study of the ideal class group of a number field. One question that arises is how the size of the class group grows if we pass from an extension of the rationals to a larger one. Iwasawa studied this question in a series of papers published in the second half of the 20th century, focusing on the following setting. For a number field $\mathbb{K}$ and a prime p, an algebraic extension $\mathbb{L}/\mathbb{K}$ is called a *$\mathbb{Z}_p$-extension* if $\mathbb{L}/\mathbb{K}$ is Galois and $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is isomorphic to $(\mathbb{Z}_p, +)$, the additive group of p-adic integers. For every $n \geq 0$, let $\mathbb{K} \subseteq \mathbb{K}_n \subset \mathbb{L}$ be the unique field defined by $[\mathbb{K}_n : \mathbb{K}] = p^n$. Iwasawa proved that if p^{e_n} denotes the exact power of p dividing the class number of $\mathbb{K}_n$, then for all sufficiently large n one has

$$e_n = \mu \cdot p^n + \lambda \cdot n + \nu, \tag{1}$$

for some constants μ, λ, ν that are independent of n. For a proof of this fact, see, for example, [Wa, Theorem 13.13].

One can readily foresee a series of questions that arise in this new theory founded by Iwasawa. For example, does a number field always have a $\mathbb{Z}_p$-extension? If so, how many? Also, can one say something more precise about the constants μ, λ, ν in (1)? We shall discuss these questions in the next section, where we also relate them to the structure of the present thesis. For now, we note only that there exists a $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$, obtained by taking $\mathbb{Q}_\infty$ to be the subfield of $\mathbb{Q}(\mu_{p^\infty})$ fixed by the torsion of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$. It also follows that every number field $\mathbb{K}$ has at least one $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/\mathbb{K}$, obtained by taking $\mathbb{K}_\infty = \mathbb{K} \cdot \mathbb{Q}_\infty$. This is called the *cyclotomic* $\mathbb{Z}_p$-extension of $\mathbb{K}$.

With his new approach, Iwasawa also sought to find an object that is the number fields analogue of the group of divisor classes of degree 0 of a curve defined over an algebraically closed field. To explain this in more detail, we shall follow the exposition from [KKS, Chapter 10]. Given a finite field $\mathbb{F}_q$ and a prime p different from its characteristic, for a curve X defined over $\mathbb{F}_q$, it is known that the p-part of $Cl^0\left(\overline{\mathbb{F}}_q(X)\right)$ (the group of divisor classes of degree 0 of $X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q$) is isomorphic to $\left(\mathbb{Q}_p/\mathbb{Z}_p\right)^{2g}$, where g is the curve's genus. Moreover, the action of the Frobenius on the aforementioned group induces an endomorphism of $\left(\mathbb{Q}_p/\mathbb{Z}_p\right)^{2g}$ and the congruence ζ-function of X can be expressed in terms of the characteristic polynomial of this endomorphism. Iwasawa suggested that if we start with $\mathbb{Q}$ as the base field and we are interested only in the p-parts of the class groups, the analogue for passing from $\mathbb{F}_q$ to $\overline{\mathbb{F}}_q$ should be played by the passage from $\mathbb{Q}$ to $\mathbb{Q}(\mu_{p^\infty})$. Let $A(\mathbb{Q}(\mu_{p^\infty}))$ be the p-part of the ideal class group of $\mathbb{Q}(\mu_{p^\infty})$. The *Iwasawa Main conjecture* (proved by Mazur and Wiles) shows that the action of the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ on $A(\mathbb{Q}(\mu_{p^\infty}))$ is intimately related to a p-adic analogue of the Riemann ζ-function. For the precise statement, we refer the reader to [KKS, Theorem 10.2]. Equivalent forms of the Iwasawa Main Conjecture are presented in [Wa, Section 15.4]. The proof was later generalized to arbitrary totally real fields by Wiles ([Wi 1]).

In 1970, Mazur developed a theory aimed at generalizing Iwasawa theory to abelian varieties and also formulated an analogous Main Conjecture for this new framework ([Ma]). A few years later, Coates and Wiles proposed in [Co-Wi 3] a Main Conjecture for CM elliptic curves, which we will discuss in greater detail in Chapter 1.

What we presented so far is just a modest glimpse into the history of Iwasawa theory and the motivation behind the problems it addresses. Ever since the early work conducted by Iwasawa during 1950's, the theory has been enriched and used in numerous areas of algebraic number theory. For a more detailed survey about the history and development of Iwasawa theory, we refer the reader to Greenberg's beautiful survey article [Gre 3] and its references.

Structure of this thesis

Chapter 1 of this thesis is dedicated to proving the following result, known as the *split prime μ-conjecture*. Let $\mathbb{K}$ be an imaginary quadratic field and let p be a prime that splits completely in $\mathbb{K}$ into two primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. By global class field theory, there exists a unique $\mathbb{Z}_p$-extension $\mathbb{K}_\infty$ of $\mathbb{K}$ in which only the prime $\mathfrak{p}$ (but not $\overline{\mathfrak{p}}$) ramifies. For an abelian extension $\mathbb{F}/\mathbb{K}$, the extension $\mathbb{F}_\infty/\mathbb{F}$ defined by $\mathbb{F}_\infty = \mathbb{F}\cdot\mathbb{K}_\infty$ is called a *split prime $\mathbb{Z}_p$-extension* of $\mathbb{F}$. If $\mathbb{F} \subset \mathbb{F}_n \subset \mathbb{F}_\infty$ satisfies $[\mathbb{F}_n : \mathbb{F}] = p^n$, then $\mathbb{F}_n/\mathbb{K}$ is a finite abelian extension and thus Leopoldt's conjecture holds for every $\mathbb{F}_n$. It follows that if $\mathbb{M}_\infty$ denotes the maximal p-abelian extension of $\mathbb{F}_\infty$ unramified outside the primes in $\mathbb{F}_\infty$ lying above $\mathfrak{p}$, then $\mathrm{Gal}(\mathbb{M}_\infty/\mathbb{F}_\infty)$ is a finitely generated Λ-torsion module, where $\Lambda \cong \mathbb{Z}_p[[T]]$ denotes the Iwasawa algebra of $\mathbb{F}_\infty/\mathbb{F}$. By the structure theorem of Λ-modules, it follows that the characteristic ideal of $\mathrm{Gal}(\mathbb{M}_\infty/\mathbb{F}_\infty)$ can be generated by $p^\mu f(T)$, for some nonnegative integer μ and a distinguished polynomial $f(T) \in \mathbb{Z}_p[T]$. The *split prime μ-conjecture* asserts that $\mu = 0$. This was proved independently by Gillard ([Gil 3]) and Schneps ([Sch]) for all primes $p \geq 5$. In Chapter 1 we extend the methods of Coates-Goldstein ([Co-Go]) and Schneps ([Sch]) to give an elementary and comprehensive proof for all primes.

In Chapter 2 we study the structure of the class groups and units along the cyclotomic $\mathbb{Z}_p$-extension of the field $\mathbb{K} = \mathbb{Q}(\zeta_p + \overline{\zeta_p})$, for an odd prime p. Let $\mathbb{K}_\infty$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ and for a positive integer n, we let $\mathbb{K} \subset \mathbb{K}_n \subset \mathbb{K}_\infty$ be the unique field defined by $[\mathbb{K}_n : \mathbb{K}] = p^n$. Greenberg's conjecture, which was stated more generally for arbitrary totally real fields (see [Gre 1]), predicts that the size of p-Sylow subgroup of the class group of $\mathbb{K}_n$ is uniformly bounded, independent of n. Using the class number formula and basic properties of the regulator, one can prove unconditionally that the size of the class group $\mathcal{C}(\mathbb{K}_n)$ of $\mathbb{K}_n$ is given by the formula

$$|\mathcal{C}(\mathbb{K}_n)| = |E_n/C_n|\,,$$

where E_n denotes the group of units of $\mathbb{K}_n$ and $C_n \subset E_n$ is the group of cyclotomic units of $\mathbb{K}_n$ (see [Wa, Theorem 8.2]). If we let A_n (resp. $(E_n/C_n)_p$) denote the p-Sylow subgroup of $\mathcal{C}(\mathbb{K}_n)$ (resp. of (E_n/C_n)), it follows that

$$|A_n| = \left|(E_n/C_n)_p\right|. \tag{2}$$

Let Λ denote the Iwasawa algebra of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$. The main result we prove in Chapter 2 is that whenever p is a prime such that Greenberg's conjecture holds for $\mathbb{K}$, the formula (2) can be improved for all sufficiently large n to an isomorphism of $\Lambda[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-modules

$$A_n \cong (E_n/C_n)_p\,.$$

In Chapter 3 we extend our analysis of class groups and units to a much more general setting and we use the tools we develop there to study a deep problem in Iwasawa theory concerning the number of linearly independent $\mathbb{Z}_p$-extension of a number field. For a number field $\mathbb{F}$, this number is given by the formula

$$r_2(\mathbb{F}) + \delta(\mathbb{F}) + 1,$$

where $r_2(\mathbb{F})$ represents the number of pairs of complex conjugate embeddings of $\mathbb{F}$ into $\mathbb{C}$ and $\delta(\mathbb{F})$ is a nonnegative integer. Leopoldt's conjecture predicts that $\delta(\mathbb{F})$ should always be 0, and for this reason $\delta(\mathbb{F})$ is referred to as *Leopoldt's defect.* Brumer proved in [Bru] that Leopoldt's conjecture is true whenever $\mathbb{F}$ is an abelian number field or an abelian extension of an imaginary quadratic field.

Beyond Brumer's result, not much is known in general. In Chapter 3 we study the Leopoldt defect and we focus on a certain class of totally real number fields. Let p be an odd prime, $\mathbb{K}$ be a CM field, $\mathbb{K}^+$ its maximal real subfield and let $\mathbb{K}_\infty$ (resp. $\mathbb{K}_\infty^+$) be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ (resp. of $\mathbb{K}^+$). We also let $\mathbb{H}_\infty$ denote the maximal p-abelian everywhere unramified extension of $\mathbb{K}_\infty$. Our main application to Leopoldt's conjecture shows that there exists a certain subgroup $A^-[T^*]$ of $\mathrm{Gal}(\mathbb{H}_\infty/\mathbb{K}_\infty)$ (which is explicitly described in Chapter 3) that encodes the Leopoldt defect. More precisely, we prove that $A^-[T^*]$ is a free $\mathbb{Z}_p$-module of rank $\delta(\mathbb{K}^+)$ and if in addition one has that $\mathbb{K}/\mathbb{Q}$ is Galois and $\mathbb{K}\cap\mathbb{Q}_\infty = \mathbb{Q}$, then $A^-[T^*]$ contains a finite index subgroup that is a cyclic $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-module. Our investigation of Leopoldt's conjecture led to the development of several complementary techniques in classical Iwasawa theory, which are used throughout Chapter 3 to identify projective limits of ideal class groups with projective radicals and Galois groups, respectively. Furthermore, we are able to use these techniques to provide a sufficient condition for when a group of ideal classes cannot be identified with an unramified extension of $\mathbb{K}_\infty$.

1. The vanishing of the μ-invariant for split prime $\mathbb{Z}_p$-extensions over imaginary quadratic fields

Acknowledgments. The present chapter comprises the article *The vanishing of the μ-invariant for split prime $\mathbb{Z}_p$-extensions over imaginary quadratic fields*, which was written in collaboration with Katharina Müller[1]. The manuscript has already been reviewed and approved by a referee for *The Asian Journal of Mathematics.* We are very grateful to Prof. John Coates for giving us this problem and for his support.

1.1 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 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 $\mathbb{L}_\infty$, which 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 Baker's 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 1.1. *The $\mathbb{Z}_p[[T]]$-module $X(\mathbb{L}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.*

Theorem 1.1 has been previously proved by L. Schneps ([Sch, Theorem III]) for $\mathbb{L} = \mathbb{K}$, $\mathbb{K}$ of class number 1, $p \geq 5$ and by R. Gillard ([Gil 3, Theorem I.2]) for any $\mathbb{L}$ abelian 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

[1] Mathematisches Institut, Georg-August-Universität Göttingen

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 3]. 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 1.1 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 1.1 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 1.1 for p-solvable extensions of $\mathbb{L}$, which are not necessarily abelian over $\mathbb{K}$.

Lemma 1.2. *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 ramification 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 1.2 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.

$$\begin{tikzcd}
 & & & & \mathbb{M}(\mathbb{L}_\infty) \\
\mathbb{K}_\infty \arrow[rrr, dash, "H"] \arrow[d, dash] \arrow[dd, dash, bend right=60, "\Gamma'"'] & & & \mathbb{L}_\infty = \mathbb{F}_\infty \arrow[ur, dash, "X(\mathbb{L}_\infty)"'] \arrow[d, dash, "\Gamma"] & \\
\mathbb{K}_t \arrow[r, dash] \arrow[d, dash] & \mathbb{H}(\mathbb{K}) \arrow[r, dash] & \mathbb{F} \arrow[r, dash] & \mathbb{L} & \\
\mathbb{K} \arrow[urr, dash, bend right, "G"] & & & &
\end{tikzcd}$$

We shall now summarize our strategy for proving Theorem 1.1. 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 1.1. 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 1.2. 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 $\mathfrak{p}$-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 $\mathfrak{p}$-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]).

1.2 Construction of the p-adic L-function

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 1.3. *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 χ as a map $\chi : \mathrm{Gal}(\mathbb{F}^{ab}/\mathbb{F}) \to Isom(E_0)$. A moment of 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 Lemma 9.2.5 from [Gr][2], 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 1.3 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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1.1}$$

for which the discriminant $\Delta(E)$ is coprime to any prime in $\mathbb{F}$ above $\mathfrak{p}$. We also take the model (1.1) to be minimal at all primes lying above $\mathfrak{p}$. The Neron differential attached to the above model is

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

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

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 $\mathbb{F}\left(E_{\mathfrak{p}^n}\right) = \mathbb{F}_n$.

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 (1.1) of E (resp. to ω). Since $\mathbb{F}(E_{tors})/\mathbb{K}$ is an abelian extension of $\mathbb{K}$, it follows that for any $\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})$, 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

$$\left(\wp_{\mathcal{L}_{\sigma_{\mathfrak{a}}}}(z) - \frac{(a_1^{\sigma_{\mathfrak{a}}})^2 + 4a_2^{\sigma_{\mathfrak{a}}}}{12}, \frac{1}{2}\left(\wp'_{\mathcal{L}_{\sigma_{\mathfrak{a}}}}(z) - a_1^{\sigma_{\mathfrak{a}}}\left(\wp_{\mathcal{L}_{\sigma_{\mathfrak{a}}}}(z) - \frac{(a_1^{\sigma_{\mathfrak{a}}})^2 + 4a_2^{\sigma_{\mathfrak{a}}}}{12}\right) - a_3^{\sigma_a}\right)\right),$$

where $\wp_{\mathcal{L}_{\sigma_{\mathfrak{a}}}}$ is the Weierstrass $\wp$-function associated with $\mathcal{L}_{\sigma_a}$.

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

$$\omega^{\sigma_{\mathfrak{a}}} \circ \eta(\mathfrak{a}) = \Lambda(\mathfrak{a})\omega, \tag{1.2}$$

which can also be written as

$$\eta(\mathfrak{a}) \circ \mathcal{M}(z, \mathcal{L}) = \mathcal{M}\left(\Lambda(\mathfrak{a})z, \mathcal{L}_{\sigma_{\mathfrak{a}}}\right). \tag{1.3}$$

Note that Λ satisfies the cocycle condition

$$\Lambda(\mathfrak{a}\mathfrak{b}) = \Lambda(\mathfrak{a})^{\sigma(\mathfrak{b})}\Lambda(\mathfrak{b}). \tag{1.4}$$

It follows that we can extend the definition of Λ to the set of all fractional ideals coprime to $\mathfrak{f}$ so that (1.4) 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

$$\Lambda(\mathfrak{a})\Omega_{\infty}\mathfrak{a}^{-1} = \mathcal{L}_{\sigma_{\mathfrak{a}}}. \tag{1.5}$$

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 1.4. *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 1.4 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 $\beta_{\mathfrak{a}}^v = \widehat{\eta(\mathfrak{a})} \circ \beta^v$ 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 $\beta_{\mathfrak{a}}^v(w)$. As proven for example in [Co-Go, Lemma 6], the relation between Ω_v and $\Omega_{\mathfrak{a},v}$ is given by

$$\Omega_{\mathfrak{a},v} = \Lambda(\mathfrak{a})\Omega_v. \tag{1.6}$$

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 $\widehat{\mathbf{G}}_a$:

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

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

$$\varphi_{\mathfrak{m}}(1)^{N(\mathfrak{a}) - \left(\frac{\mathbb{K}(\mathfrak{m})/\mathbb{K}}{\mathfrak{a}}\right)} = \left(\frac{\theta(1, \mathfrak{m})^{N(\mathfrak{a})}}{\theta(1, \mathfrak{a}^{-1}\mathfrak{m})}\right)^m. \tag{1.7}$$

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 1.5. *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*

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

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

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

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 1.20 in Section 1.4 for the precise statement). In view of these facts, our aim is to prove a $\mathfrak{p}$-adic analogue of Theorem 1.5. 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 (1.1). 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 in $\mathbb{F}$ of $\Delta(\alpha^{-1}\mathcal{L}_\sigma)/\Delta(\mathcal{L}_\sigma)^{N_{\mathbb{K}/\mathbb{Q}}(\alpha)}$ (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 (1.7)):

$$\xi_{\alpha,\sigma}(z)^{12} = \frac{\theta\left(z, \alpha^{-1}\mathcal{L}_\sigma\right)}{\theta\left(z, \mathcal{L}_\sigma\right)^{N(\alpha)}}. \tag{1.8}$$

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

$$\xi_{\alpha,\sigma\sigma_\mathfrak{b}}\left(\eta_\sigma(\mathfrak{b})(P_\sigma)\right) = \prod_{U \in E^\sigma_\mathfrak{b}} \xi_{\alpha,\sigma}(P_\sigma \oplus U), \tag{1.9}$$

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

It follows that

$$\xi_{\alpha,\sigma\sigma_\mathfrak{b},Q}\left(\eta_\sigma(\mathfrak{b})(P_\sigma)\right) = \prod_{U \in E^\sigma_\mathfrak{b}} \xi_{\alpha,\sigma,Q}\left(P_\sigma \oplus U\right). \tag{1.10}$$

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 $\mathcal{I}_\mathfrak{p}[\zeta_{p^n}]$. The point $\zeta_{p^n} - 1$ 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 (1.3), 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 $\mathrm{Gal}(\mathbb{M}/\mathbb{K})$ 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 1.6. *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 $\mathrm{Gal}(\mathbb{F}_n/\mathbb{K})$ 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 1.7. *We note that the definition of $\xi_{\alpha,\sigma,Q}(z)$ depends only on the restriction of σ to* $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$*, but that the point z_n does depend on the element $\sigma \in \mathrm{Gal}(\mathbb{F}_n/\mathbb{K})$ 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 (1.8), it follows that

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

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

$$\frac{d}{dz} \log \widetilde{\theta}(z + z_0, L) = \overline{z_0} A(L)^{-1} + \sum_{k=1}^{\infty} (-1)^{k-1} E_k^*(z_0, L) z^{k-1}. \tag{1.11}$$

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

$$\left(\frac{d}{dz} \right)^k \log \xi_{\alpha,\sigma,Q}(z)|_{z=z_n} = \left(\frac{d}{d\tilde{z}} \right)^k \log \xi_{\alpha,\sigma}(\tilde{z} + z_n + \Lambda(\mathfrak{a})\rho)|_{\tilde{z}=0}. \tag{1.12}$$

Combining (1.11) and (1.12), it follows that

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

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

$$E_k^*(\Lambda(\mathfrak{a})(w_n + \rho), \mathcal{L}_\sigma) = \left(\frac{\phi(\mathfrak{a}\mathfrak{q}_n)}{(w_n + \rho)\Lambda(\mathfrak{a})} \right)^k L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}\mathfrak{q}_n} \right), k \right), \tag{1.13}$$

and similarly

$$E_k^*(\alpha\Lambda(\mathfrak{a})(w_n + \rho), \mathcal{L}_\sigma) = \left(\frac{\phi(\mathfrak{a}\mathfrak{q}_n(\alpha))}{(\alpha)(w_n + \rho)\Lambda(\mathfrak{a})} \right)^k L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}\mathfrak{q}_n(\alpha)} \right), k \right). \tag{1.14}$$

Using (1.13) and (1.14), 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 (1.9), it follows that

$$\prod_{R \in E_{\mathfrak{p}}^{\sigma}} Y_{\alpha,\mathfrak{a}}\left(P_\sigma \oplus R\right) = 1. \tag{1.15}$$

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 1.8. *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* $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$. *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 already 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. □

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 a compact open subset O of $\mathbb{Z}_p$, 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

$$\nu|_{\mathbb{Z}_p^\times} \to F(w) - \frac{1}{p}\sum_{\zeta^p=1} F(\zeta(1+w)-1). \tag{1.16}$$

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

$$\nu \circ a|_O = \nu|_{aO} \circ a. \tag{1.17}$$

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

$$\nu \circ a \to F\left((1+w)^{-a} - 1\right). \tag{1.18}$$

We can now proceed to the construction of our measure. For every $\mathfrak{a} \in \mathfrak{C}_0$, we define $\mathcal{B}_{\alpha,\mathfrak{a}}(w) = h_{\alpha,\mathfrak{a}}\left(\beta_{\mathfrak{a}}^v(w)\right)$. By Lemma 1.8, 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 (1.15) 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 $\beta^v_{\mathfrak{a}}\left(\exp(z/\Omega_{\mathfrak{a},v})-1\right)=\mathcal{M}\left(\Lambda(\mathfrak{a})z,\mathcal{L}_{\sigma_{\mathfrak{a}}}\right)$, it follows that

$$D^k\,\mathcal{B}_{\alpha,\mathfrak{a}}(w)|_{w=w_1}=\Omega^k_{\mathfrak{a},v}\Lambda(\mathfrak{a})^{-k}\left(\frac{d}{dz}\right)^k\frac{1}{p}\log Y_{\alpha,\mathfrak{a}}\left(\mathcal{M}\left(\Lambda(\mathfrak{a})z,\mathcal{L}_{\sigma_{\mathfrak{a}}}\right)\right)|_{z=z_1}. \qquad (1.19)$$

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 Grössencharacter 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 1.9. *a) Let χ be a character of* $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$. *Then for every $k\geq 0$ one has*

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

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

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

Then for every $k\geq 0$ one has

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

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

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

It follows that

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

Reordering the sum

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

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 (1.6)), it follows that

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

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

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

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

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

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

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

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

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

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

$$\sum_{\sigma\in\mathrm{Gal}(\mathbb{F}_n/\mathbb{K}(\mathfrak{f}\mathfrak{p}^{n-1}))}\chi(\sigma) = 0.$$

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

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

Finally,

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

with $\tau(\chi)$ defined as in the statement. Using (1.19), part b) follows. □

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 1.10. *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*

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

Proof. When $n = 0$, by Proposition 1.6 and Lemma 1.9 a), it follows that

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

When $n \geq 1$, using Proposition 1.6 and Lemma 1.9 b), it follows that

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

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 1.11. *There exists a unique measure ν on $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$ 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*

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

with u_χ as defined in the proof of Theorem 1.10.

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 1.10 that

$$\nu_{\alpha_1}\left(N(\alpha_2)-\sigma_{(\alpha_2)}\right)=\nu_{\alpha_2}\left(N(\alpha_1)-\sigma_{(\alpha_1)}\right)\quad\text{(equality as measures)},\tag{1.20}$$

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 1.10 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 (1.20), 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 all $\theta(\sigma_{(\alpha)}-N(\alpha))\in\mathcal{D}_\mathfrak{p}[[X]]$ 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 $\theta(\sigma_{(\alpha_n)}-N(\alpha_n))$ approximates the element $\theta(g)(1+X)^a-u$, 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 $e_\theta=\frac{1}{m}\sum\limits_{g\in H}\theta(g)g^{-1}$ 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

$$\nu(\mathfrak{g}) := \nu(\mathfrak{f})|_{\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})} \prod_{\substack{\mathfrak{l} \mid \mathfrak{f} \\ \mathfrak{l} \nmid \mathfrak{g}}} \left(1 - \left(\sigma_{\mathfrak{l}}|_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)}\right)^{-1}\right)^{-1}, \tag{1.21}$$

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

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

where γ is a topological generator of Γ'.

Theorem 1.13. *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 1.12. Then one has

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

where u_χ and $G(\chi)$ are as in Theorem 1.10, 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 1.9, Theorem 1.11 and (1.7). 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

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

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

$$T_{\mathfrak{g}'}(\vartheta) = \prod_{\substack{\mathfrak{l} \mid \mathfrak{g}' \\ \mathfrak{l} \nmid \mathfrak{g}}} (1 - \chi(\mathfrak{l}))\, T_{\mathfrak{g}}(\vartheta). \tag{1.22}$$

The general case follows from our definition of $L_{\mathfrak{p},\mathfrak{m}}$, the relation (1.22) 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 1.14. *We recall that we fixed a decomposition*

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

where $\Gamma' \cong \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ *and* $H = \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K}_\infty)$. *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* $\mathfrak{p}$*-adic* L*-function of the character* χ *as*

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

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

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 1.14. 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 1.15. *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

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

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 1.10. 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

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

We note that by Theorem 1.11, 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 1.15, 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

$$\begin{aligned}\mathcal{R}_1&=\{\text{coset representatives of }\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{F})\text{ in }\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}_t)\};\\ \mathcal{R}_2&=\{\text{coset representatives of }\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}_t)\text{ in }\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K})\}.\end{aligned}$$

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

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

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

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

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 the fact 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

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

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

$$G(u^s-1,\chi)=\sum_{\sigma_2\in\mathcal{R}_2}\kappa^s(\sigma_2)\Gamma^{(i)}_{\sum\limits_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma}\left(p^t s\right). \tag{1.23}$$

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

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

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

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

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. □

By Lemma 1.16 and (1.23), it follows that

$$G(u^s-1,\chi)=\sum_{\sigma_2\in\mathcal{R}_2}\kappa^s(\sigma_2)\Gamma^{(i-1)}_{D\sum\limits_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma}\left(p^t s-1\right). \tag{1.24}$$

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 (1.24), it follows that

$$G(w,\chi)=\sum_{j=0}^{p^t-1}(1+w)^j G^{(i-1)}\left(\frac{(1+w)^{p^t}}{u^{p^t}}-1, D\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right). \tag{1.25}$$

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 (1.25) is zero. For this, we will use the following general lemma, which is also proved in [Gil 2, Lemma 2.10.2], but we redo the proof here for the convenience of the reader.

Lemma 1.17. *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 $\mu(f(w))\le\mu(f_j((1+w)^{p^t}-1))$, 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 power 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 $(1+w)^j f_j((1+w)^{p^t} - 1) = (1+w)^j G^{(i-1)}\left(\frac{(1+w)^{p^t}}{u^{p^t}} - 1, D\sum_{\sigma_1 \in \mathcal{R}_1} \chi^{-1}(\sigma_1)\nu_\alpha \circ \sigma\right)$, it follows from Lemma 1.17 and (1.25) that if for $\sigma_2 = 1$ one has

$$\mu\left(G^{(i-1)}\left(\frac{(1+w)^{p^t}}{u^{p^t}} - 1, D\sum_{\sigma_1 \in \mathcal{R}_1} \chi^{-1}(\sigma_1)\nu_\alpha \circ \sigma\right)\right) = 0, \tag{1.26}$$

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

To prove (1.26) 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 1.4.

Theorem 1.18. *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 1.15.

In view of (1.26), we note that

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

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 $P(\frac{(1+w)^{p^t}}{u^{p^t}} - 1)$ 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 1.18 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 1.15.

Proof of Theorem 1.15. By construction, $D\mathcal{B}_{\alpha,\mathfrak{a}}$ corresponds to the rational function on E given by

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

Since

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

it follows that

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

where

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

and

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

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 1.15. □

1.4 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 $\mathbb{L}_n$. 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:

$$\mathrm{ord}_p\left([\mathbb{M}(\mathbb{F}_n) : \mathbb{F}_\infty]\right) = p^{n+t}\mu + \lambda n + c, \tag{1.27}$$

where μ (resp. λ) is the μ-invariant (resp. λ-invariant) of $X(\mathbb{F}_\infty)$ as a $\mathbb{Z}_p[[\Gamma']]$-module, and c is a constant independent of n.

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

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

Since the extension $\mathbb{F}_\infty/\mathbb{F}_n$ is totally ramified above $\mathfrak{p}$, it follows that $\mathbb{H}(\mathbb{F}_n) \cap \mathbb{F}_\infty = \mathbb{F}_n$, 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 $d := \mathrm{ord}_p\left([\mathbb{F} : \mathbb{K}]\right)$. 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 1.19. *With the notations as above, one has*

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

Combining Proposition 1.19 with (1.27), one immediately deduces the following (see also [dS, Chapter III, Corollary 2.8]).

Corollary 1.20. *If $F\in\mathbb{Z}_p[[\Gamma']]$ is a characteristic power series for* $\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)$*, then for all sufficiently large n one has*

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

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 $\mathrm{level}(\rho)=m$ 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 1.21. *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 1.22. *For any ramified character ε of* $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{K})$*, 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* 1.10 *and we define $S_p(\varepsilon)$ by*

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

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

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

Let now χ be a character of H and recall that

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

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

We define $F(w,\chi)\in\mathcal{D}_{\mathfrak{p}}[[w]]$ to be the corresponding Iwasawa function. Then, using Theorem 1.13, for a character ρ of Γ' of sufficiently large finite order, one has

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

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

$$\prod_{\text{level}(\rho)=t+n} \rho(F) \sim p \prod_{\substack{\varepsilon=\chi\rho \\ \text{level}(\rho)=t+n}} G(\varepsilon) S_p(\varepsilon), \tag{1.28}$$

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

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

Proof of Theorem 1.1. Using (1.28), Corollary 1.20, Lemma 1.21 and Proposition 1.22, it follows that

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

In Theorem 1.15 we proved that $\mu\left(L_{\mathfrak{p}}(s, \chi)\right) = 0$. It follows that

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

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

1.5 Appendix: proof of Schneps' theorem

For the proof of Theorem 1.18, 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

$$\varepsilon_j = \sum_{i=1}^{n} a_{ij} \alpha_i, \quad 1 \le j \le m. \tag{1.29}$$

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

We can now state the aforementioned independence results.

Proposition 1.23. *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

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

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

Proposition 1.24. *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 $r \in \widetilde{D}$ and $r\left(\widetilde{[\alpha_i]}(t), \ldots, \widetilde{[\alpha_n]}(t)\right) = 0$ 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 1.25. *If C is any compact-open set in $\mathbb{Z}_p$, then for λ as in the statement of Theorem* 1.18 *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 1.18.

Proof of Theorem 1.18. 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 1.25, 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

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

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

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

It therefore suffices to prove that

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

First notice that if the power series associated with κ_i is divisible by π', then so is the power series associated with $\sum\limits_{\varepsilon \in V} \varepsilon^i \kappa_i \circ \varepsilon|_U$ (see (1.18)), hence $\Gamma^{(i)}_{\kappa_i}(s)$ is also divisible by π'.

Conversely, assume that π' divides the power series associated with the measure $\sum\limits_{\varepsilon \in V} \varepsilon^i \kappa_i \circ \varepsilon|_U$. By (1.17), 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 $\varepsilon_j^{-i}\ \kappa_i|_{(\varepsilon_j^{-1}U)}$. 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 (1.29). 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 1.24, it follows that $\sum\limits_{j=1}^{m}\widetilde{F_j}\circ\Phi_j$ is identically zero on $\widetilde{E}^n$, hence, by Proposition 1.23, 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 1.18 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 1.18 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. □

2. An isomorphism behind the class number formula

2.1 Introduction

Let $p > 3$ be an odd prime. For every $n \geq 1$, we let ζ_{p^n} be a primitive p^nth root of unity and consider the field $\mathbb{K}_n = \mathbb{Q}[\zeta_{p^n} + \overline{\zeta}_{p^n}]$, the maximal real subextension of $\mathbb{Q}(\zeta_{p^n})$. The field $\mathbb{K}_\infty = \bigcup_{n \geq 1} \mathbb{K}_n$ is the *cyclotomic* $\mathbb{Z}_p$-extension of $\mathbb{K}$ and it is a totally real field. Moreover, $\mathbb{K}_\infty$ is an abelian extension of $\mathbb{Q}$ and since the degree of $[\mathbb{K}_1 : \mathbb{Q}]$ is coprime to p, one has a direct product decomposition

$$\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{Q}) \cong \Gamma \times G,$$

where $\Gamma := \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ and $G_1 := \mathrm{Gal}(\mathbb{K}_1/\mathbb{Q})$. Similarly, if we denote $\Gamma_n = \mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_1)$ and $G_n = \mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})$, there is a decomposition

$$G_n \cong \Gamma_n \times G_1,$$

for all $n \geq 1$.

Let A_n be the p-Sylow subgroup of the ideal class group $\mathcal{C}(\mathbb{K}_n)$ of $\mathbb{K}_n$ and let $\underline{E}_n$ and $\underline{C}_n$ denote the global and the cyclotomic units of $\mathbb{K}_n$, respectively (we reserve the typical notations E_n and C_n for certain subgroups of $\underline{E}_n$ that will be of central interest in this chapter.) We recall that the group $\underline{C}_n$ is defined as the intersection between the group generated by $\{\pm\zeta_{p^n}, 1 - \zeta_{p^n}^a \mid 1 \leq a \leq n-1\}$ and $\underline{E}_n$. It is relatively easy to prove that the group $\underline{C}_n$ can be generated by -1 and the units

$$\xi_a := \zeta_{p^n}^{(1-a)/2} \frac{1 - \zeta_{p^n}^a}{1 - \zeta_{p^n}}, \quad 1 < a < \frac{1}{2}p^n, \gcd(a, p) = 1.$$

For a proof of this fact, see [Wa, Lemma 8.1]. This set of generators for $\underline{C}_n$ is useful because one can explicitly compute the regulator $R(\xi_a)$ of the units ξ_a, and it turns out that

$$R\left(\{\xi_a\}\right) = \pm \prod_{\substack{\chi \in \widehat{G_n} \\ \chi \neq 1}} -\frac{1}{2}\tau(\chi)L(1, \overline{\chi}), \tag{2.1}$$

where $\tau(\chi)$ is the Gauss sum

$$\tau(\chi) = \sum_{j=1}^{f_\chi} \chi(j) \exp\left(\frac{2\pi i j}{f_\chi}\right),$$

and $L(s, \chi)$ stands for the usual L-series attached to χ. The details behind the formula (2.1) can be found for example in [Wa, Theorem 8.2]. Using basic properties of Gauss sums and regulators together with the class number formula for $\mathbb{K}_n$, one deduces from (2.1) the following important relation

$$[\underline{E}_n : \underline{C}_n] = \left|\mathcal{C}(\mathbb{K}_n)\right|. \tag{2.2}$$

We refer the reader again to [Wa, Theorem 8.2] for details.

Because of the techniques employed in proving it, (2.2) is also sometimes referred to as the *class number formula*, which justifies the title of this chapter. From (2.2) it follows that

$$|A_n| = \left|(\underline{E}_n/\underline{C}_n)_p\right|. \tag{2.3}$$

Given the key role that cyclotomic fields play in classical algebraic Iwasawa theory (and in algebraic number theory in general), it is no surprise that the study of the group A_n led to a series of conjectures regarding its structure. The Kummer-Vandiver conjecture asserts that A_1 is trivial, and by a classical result in Iwasawa theory, this is equivalent to A_n being trivial for all $n \geq 1$ (see [Iwa 1]). The validity of the conjecture has been verified for $p \leq 163 \cdot 10^6$, but there seems to be some debate among specialists whether or not it should be true in general (see for example the exposition in [wiki 2]). After the second World War, possibly due to a raising scepticism in the validity of the Kummer-Vandiver Conjecture, Iwasawa and Leopoldt conjectured independently that $\mathcal{C}(\mathbb{Q}[\zeta_p])_p^-$ is a cyclic $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}]$-module, without excluding the possibility that $A_1 = \{1\}$ as in the Kummer-Vandiver Conjecture (for a more detailed discussion, see [Lang 1, Chapter 6, Section 4], particularly Theorem 4.2).

There is another conjecture due to Greenberg regarding the structure of A_n, which was formulated more generally for any totally real fields by Greenberg in his Ph.D. thesis (see also [Gre 1] for several results in favor of this conjecture). Greenberg's conjecture asserts that $|A_n|$ is uniformly bounded, independent of n. We will now formulate the result we proved in [Cri], assuming Greenberg's conjecture.

Let τ be a topological generator of $\Gamma = \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ and let

$$\Lambda := \varprojlim \mathbb{Z}_p[[\Gamma_n]]$$

be the Iwasawa algebra of Γ. We identify Λ with $\mathbb{Z}_p[[T]]$ by the means of the isomorphism which sends $\tau - 1$ to T. One can also define the Iwasawa algebra of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{Q})$ in the same manner, and using the decomposition $G_n \cong \Gamma_n \times G_1$, this is isomorphic to the group ring $\Lambda[G_1]$. The groups A_n, $\underline{E}_n$ and $\underline{C}_n$ are Λ-modules in the natural way and since G_1 can be viewed as a subgroup of G_n, they become modules over the group ring $\Lambda[G_1] \cong \varprojlim \mathbb{Z}_p[[G_n]]$. In [Cri] we proved that assuming Greenberg's conjecture as stated above, one has an isomorphism of $\Lambda[G_1]$-modules $(\underline{E}_n/\underline{C}_n)_p \cong A_n$ for all sufficiently large n. Here, we will choose a slightly different approach than the one we followed in [Cri], which will allow us to generalize this result (see Theorem 2.10 below) and we will also be able to highlight some important unconditional results about the structure of class groups and units in the cyclotomic tower $\mathbb{K}_\infty/\mathbb{K}_1$.

2.2 Unconditional preliminary results

Before we embark on showing how the equality (2.3) can be turned into an isomorphism of $\Lambda[G_1]$-modules, let us introduce some subgroups of $\underline{E}_n$ which will allow us to express the group $(\underline{E}_n/\underline{C}_n)_p$ more explicitly.

For every $n \geq 1$, let $\underline{e}_1, \ldots, \underline{e}_{r_n}$ (with the dependence on n being understood) be a fundamental system of units of $\underline{E}_n$, where $r_n = [\mathbb{K}_n : \mathbb{Q}] - 1$, as $\mathbb{K}_n$ is totally real. Then every element in $\underline{E}_n$ is of the form $\pm\underline{e}_1^{a_1} \cdots \underline{e}_{r_n}^{a_{r_n}}$, where $a_1, \ldots, a_{r_n} \in \mathbb{Z}$. Let $g \in \mathbb{Z}$ be a generator for $(\mathbb{Z}/p^2\mathbb{Z})^\times$ and hence also for $(\mathbb{Z}/p^n\mathbb{Z})^\times$ for any $n \geq 2$. Let $\eta_n = \frac{\zeta_{p^n}^g - \overline{\zeta}_{p^n}^g}{\zeta - \overline{\zeta}}$ and let $C_n = \eta_n^{\mathbb{Z}_p[G_n]}$ be the subgroup of $\underline{C}_n$ generated by η_n as a $\mathbb{Z}[G_n]$-module. Then one has the equality $C_n = \underline{C}_n/\{\pm 1\}$ ([Wa, Lemma 8.11]). Working with C_n instead of $\underline{C}_n$ is useful for us because the elements $(\eta_n)_{n\geq 1}$ form a norm-coherent sequence in the extension $\mathbb{K}_\infty/\mathbb{K}$. Since p is odd, it follows that

$$(\underline{E}_n/\underline{C}_n)_p = (\underline{E}_n/C_n)_p\,.$$

For each $j = 1, \ldots, r_n$, we write

$$q_j \cdot p^{\alpha_j} = \left|\underline{e}_j^{\mathbb{Z}}/\left(\underline{e}_j^{\mathbb{Z}} \cap C_n\right)\right|.$$

Now let $e_j = \underline{e}_j^{q_j}$ and let E_n be the subgroup of $\underline{E}_n$ generated by the elements $e_1, \ldots, e_{r_n}$ as a $\mathbb{Z}$-module. Notice that for each j we have $e_j \in (\underline{E}_n/C_n)_p$ and E_n/C_n is a subgroup of $\underline{E}_n/C_n$ with $|E_n/C_n| = \left|(\underline{E}_n/C_n)_p\right|$. As everything in sight is abelian, the p-Sylow subgroup is unique and thus

$$E_n/C_n \cong (\underline{E}_n/C_n)_p \,.$$

It follows that

$$|E_n/C_n| = |A_n|\,, \quad \text{for all} \quad n \geq 1. \tag{2.4}$$

We will also need for further reference the following standard notations from Iwasawa theory. For all $n \geq m \geq 1$ we define the elements

$$\omega_n = \tau^{p^{n-1}} - 1 = (T+1)^{p^{n-1}} - 1, \quad \text{and} \quad \nu_{n,m} = \omega_n/\omega_m,$$

and we let $N_{n,m}$ denote the norm map $N_{\mathbb{K}_n/\mathbb{K}_m}$. Notice that $N_{n,m}(\alpha_n^{\omega_m}) = 1$ for all $\alpha \in \mathbb{K}_n^\times$.

The first step in relating the structures of A_n and E_n/C_n is provided by the following result, whose proof can also be found in [Gre 1, Theorem 1]. We redo the proof for completeness.

Lemma 2.1. *For every $n \geq m \geq 1$, let $A_n[\omega_m]$ denote the subgroup of A_n consisting of all elements of A_n annihilated by ω_m and let $B_{n,m}$ be the subgroup of A_n consisting of classes which contain an ideal that is invariant under* $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$*. Then $B_{n,m} \subseteq A_n[\omega_m]$ and one has an isomorphism of $\Lambda[G_1]$-modules*

$$A_n[\omega_m]/B_{n,m} \cong E_m/N_{n,m}(E_n). \tag{2.5}$$

Proof. The assertion $B_{n,m} \subseteq A_n[\omega_m]$ is plain from the definitions, so we focus on constructing the isomorphism

$$A_n[\omega_m]/B_{n,m} \cong E_n/N_{n,m}(E_n).$$

Let $a_n \in A_n[\omega_m]$ and $\mathfrak{a}_n \in a_n$. Then by definition $\mathfrak{a}_n^{\omega_m} = (\alpha_n)$, for some $\alpha_n \in \mathbb{K}_n^\times$. It follows that $N_{n,m}(\alpha_n) = \varepsilon_m$, for some $\varepsilon_m \in \underline{E}_m$. We define the map $\phi : A_n[\omega_m] \to \underline{E}_m/N_{n,m}(\underline{E}_n)$ by $\phi(a_n) = \varepsilon_m \pmod{N_{n,m}(\underline{E}_n)}$. It is an easy check to show that ϕ is a well-defined homomorphism of groups. To see that it is in fact an isomorphism of $\Lambda[G_1]$-modules, note that for any element $g \in G_n$ we have the formal sequence of associations

$$a_n \to a_n^g \Rightarrow \mathfrak{a}_n \to \mathfrak{a}_n^g \Rightarrow (\alpha_n) \to (\alpha_n)^g \Rightarrow \epsilon_m \to \epsilon_m^g,$$

where we implicitly used the commutativity in the group ring $\mathbb{Z}_p[G_n]$.

It is also immediate that one has $B_{n,m} \subset \ker(\phi)$. For the converse, notice that if $\phi(a_n) = 1$, then it must be that $N_{n,m}(\alpha_n) = N_{n,m}(\varepsilon_n)$, for some $\varepsilon_n \in \underline{E}_n$. Then, by using Hilbert's Theorem 90 for the element α_n/ε_n, it follows that $\alpha_n/\varepsilon_n = \gamma_n^{\omega_m}$, for some $\gamma_n \in \mathbb{K}_n^\times$. It follows that the class a_n contains the invariant ideal $\mathfrak{a}_n \cdot (\gamma_n)^{-1}$ and thus $\ker(\phi) = B_{n,m}$.

We now prove that ϕ is surjective. Let $\varepsilon_m \in \underline{E}_m$. Let $\mathfrak{q}_m$ be any prime of $\mathbb{K}_m$. If $\mathfrak{q}_m$ is unramified in $\mathbb{K}_n$, then ε_m is a local norm from the completion of $\mathbb{K}_n$ at any prime of $\mathbb{K}_n$ lying over $\mathfrak{q}_m$. Since the only ramified prime in $\mathbb{K}_n/\mathbb{K}_m$ is the unique prime lying above p, it follows from Hasse's Norm Principle that ε_m is a norm from $\mathbb{K}_n$. It follows that $\varepsilon_m = N_{n,m}(\alpha_n)$, for some $\alpha_n \in \mathbb{K}_n^\times$. Using Hilbert's theorem 90 for ideals, it follows that $(\alpha_n) = \mathfrak{a}_n^{\omega_m}$, for some ideal $\mathfrak{a}_n$ of $\mathbb{K}_n$. Let d be the order of the ideal class containing $\mathfrak{a}_n$ and write $d = d' \cdot p^t$, where $\gcd(d,p) = 1$. Choose d'' a suitable multiple of d' such that $d'' \equiv 1 \pmod{p^{n-m}}$. Then the class a_n of $\mathfrak{a}_n^{d''}$ is an element of $A_n[\omega_m]$ and

$$\phi(a_n) = \varepsilon_m^{d''} \pmod{N_{n,m}(\underline{E}_n)} = \varepsilon_m \pmod{N_{n,m}(\underline{E}_n)},$$

since $\varepsilon_m^{p^{n-m}} \in N_{n,m}(\underline{E}_n)$.

Finally, since E_m is a $\mathbb{Z}_p[G_n]$-submodule of $\underline{E}_m$ of finite index coprime to p, by elementary facts in cohomology theory (for example the standard exact hexagon from algebraic number theory-[Jan, Chapter V, Lemma 1.2]) it follows that $H^0(\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m), \underline{E}_n) \cong H^0(\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m), E_n)$. Since by definition $H^0(\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m), \underline{E}_n) = \underline{E}_m/N_{n,m}(\underline{E}_n)$, our result follows. □

The plan for the rest of this chapter is to relate the groups in (2.5) to A_m and E_m/C_m, respectively. It will turn out that whenever Greenberg's conjecture holds for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}_1$, for every fixed $m \geq 1$ and all sufficiently large $n \geq m$ one has $A_n[\omega_m] = A_n$, $B_{n,m} = \{1\}$ and $N_{n,m}(E_n) = C_m$. We begin by describing $B_{n,m}$ with the aid of the following simple lemma (see also [Cri, Section 3]).

Lemma 2.2. *With the notations as above, if an ideal $\mathfrak{b}$ of $\mathbb{K}_n$ is invariant under* $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$ *and π_n does not occur in the factorization of $\mathfrak{b}$, then $\mathfrak{b}$ must be the lift of an ideal of $\mathbb{K}_m$. In particular, one has $B_{n,m} = \iota_{m,n}(A_m)$, where $\iota_{m,n}$ is the ideal classes lift map from $\mathbb{K}_m$ to $\mathbb{K}_n$.*

Proof. Let $\mathfrak{Q}$ be a prime dividing $\mathfrak{b}$ and let $\mathfrak{q} = \mathfrak{Q} \cap \mathbb{K}_m$. We know that all the primes above $\mathfrak{q}$ in $\mathbb{K}_n$ are conjugate under the action of $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$, so we can write

$$(\alpha) = \prod_j \mathfrak{Q}_j^{f_j(\omega_m)},$$

where $\mathfrak{Q}_j$ are primes in $\mathbb{K}_n$ and $f_j(\omega_m)$ are elements of $\mathbb{Z}[\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)]$. Since $\mathfrak{b}$ is invariant under $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)$, it follows that $N_{n,m}(\mathfrak{b}) = \mathfrak{b}^{p^{n-m}}$. In particular, for each j, one has

$$p^{n-m} \cdot f_j(\omega_m) = \mathrm{Tr}(f_j) \cdot N_{n,m},$$

where $\mathrm{Tr}(f_j)$ denotes the sum of the coefficients of f_j. This implies that all coefficients of f_j are equal, so f_j is a multiple of the norm $N_{n,m}$ for all j. This means precisely that $\mathfrak{b} = \iota_{m,n}(\mathfrak{a})$ for an ideal $\mathfrak{a}$ in $\mathbb{K}_m$.

Since the only ramified prime in the extension $\mathbb{K}_n/\mathbb{K}_m$ is principal, the equality $B_{n,m} = \iota_{m,n}(A_m)$ follows. □

We will now study the group $A_n[\omega_m]$. By the first isomorphism theorem one has $A_n/A_n[\omega_m] = A_n^{\omega_m}$. In particular, it follows that

$$|A_n[\omega_m]| = |A_n|/|A_n^{\omega_m}|.$$

It is plain that $A_n^{\omega_m} \subset \ker(N_{n,m} : A_n \to A_m)$. The following general result, which is of interest on its own, shows that in our case the converse also holds.

Lemma 2.3. *Let $\mathbb{L}/\mathbb{K}$ be a finite cyclic extension of number fields with* $\mathrm{Gal}(\mathbb{L}/\mathbb{K}) = \langle\sigma\rangle$ *and assume that at most one prime of $\mathbb{K}$ ramifies in $\mathbb{L}$. Then*

$$\ker\left(N_{\mathbb{L}/\mathbb{K}} : \mathcal{C}(\mathbb{L}) \to \mathcal{C}(\mathbb{K})\right) = \mathcal{C}(\mathbb{L})^{\sigma-1},$$

where $\mathcal{C}(\mathbb{L})$ and $\mathcal{C}(\mathbb{K})$ denote the class groups of $\mathbb{L}$ and $\mathbb{K}$, respectively. In particular, for the extension $\mathbb{K}_n/\mathbb{K}_m$ one has

$$\ker(N_{n,m} : A_n \to A_m) = A_n^{\omega_m}.$$

Proof. This result is proved in [Gre 4, Proposition 1.1.3], but since the cited manuscript has not been published, we will reproduce the proof here for completeness.

Let $\mathbb{H}(\mathbb{L})$ and $\mathbb{H}(\mathbb{K})$ denote the Hilbert class fields of $\mathbb{L}$ and $\mathbb{K}$, respectively. We have the following well-known commutative diagram from class field theory:

$$\begin{tikzcd}
\mathcal{C}(\mathbb{L}) \arrow[r] \arrow[d, "N_{\mathbb{L}/\mathbb{K}}"] & \mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{L}) \arrow[d, "\mathrm{Res}"] \\
\mathcal{C}(\mathbb{K}) \arrow[r] & \mathrm{Gal}(\mathbb{H}(\mathbb{K})/\mathbb{K}).
\end{tikzcd} \tag{2.6}$$

The kernel of the restriction map $\mathrm{Res} : \mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{L}) \to \mathrm{Gal}(\mathbb{H}(\mathbb{K})/\mathbb{K})$ is $\mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{H}(\mathbb{K}) \cdot \mathbb{L})$.

Let $\mathbb{F}$ be the maximal abelian extension of $\mathbb{K}$ contained in $\mathbb{H}(\mathbb{L})$. We begin by showing that under the hypotheses of the lemma, one has $\mathbb{F} = \mathbb{H}(\mathbb{K}) \cdot \mathbb{L}$.

First notice that the claim holds if no prime of $\mathbb{K}$ ramifies in $\mathbb{L}$, as we then have $\mathbb{F} = \mathbb{H}(\mathbb{K}) = \mathbb{H}(\mathbb{K}) \cdot \mathbb{L}$. Assume now that $\mathfrak{p}$ is the only prime of $\mathbb{K}$ which ramifies in $\mathbb{L}$. Let $I := I(\mathfrak{p})$ denote the inertia of the prime $\mathfrak{p}$ in $\mathrm{Gal}(\mathbb{F}/\mathbb{K})$. It follows that $I = \mathrm{Gal}(\mathbb{F}/\mathbb{H}(\mathbb{K}))$. Since $\mathbb{L} \subset \mathbb{F} \subset \mathbb{H}(\mathbb{L})$, the extension $\mathbb{F}/\mathbb{L}$ must be unramified. It follows that $I \cap \mathrm{Gal}(\mathbb{F}/\mathbb{L}) = \{1\}$, hence $\mathbb{F} = \mathbb{H}(\mathbb{K}) \cdot \mathbb{L}$, as claimed.

Note that by maximality, $\mathbb{H}(\mathbb{L})/\mathbb{K}$ is also a Galois extension. Let $\mathcal{G} = \mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{K})$ and let $N = \mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{L})$. We have a short exact sequence

$$1 \to N \to \mathcal{G} \to \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \to 1.$$

Let σ be a generator of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ and lift it to an element $\tilde{\sigma} \in \mathcal{G}$. Since, N is abelian, there is a well-defined action of σ on N via $h^\sigma = \tilde{\sigma} h \tilde{\sigma}^{-1}$, for all $h \in N$. Then $h^{\sigma-1} = \tilde{\sigma} h \tilde{\sigma}^{-1} h^{-1} \in [\mathcal{G}, \mathcal{G}]$, where $[\mathcal{G}, \mathcal{G}]$ is the commutator of the group $\mathcal{G}$. Hence $N^{\sigma-1} \subseteq [\mathcal{G}, \mathcal{G}]$.

We now show that we actually have $[\mathcal{G}, \mathcal{G}] = N^{\sigma-1}$. Indeed, $N^{\sigma-1}$ is a normal subgroup of $\mathcal{G}$ and one has the exact sequence

$$1 \to N/N^{\sigma-1} \to \mathcal{G}/N^{\sigma-1} \to \mathcal{G}/N \to 1.$$

Moreover, $N/N^{\sigma-1}$ is contained in the center of $\mathcal{G}/N^{\sigma-1}$ and we also know that $\mathcal{G}/N$ is a cyclic group. Therefore, $\mathcal{G}/N^{\sigma-1}$ is an abelian group, and by the definition of the commutator, we have $\mathcal{G}/N^{\sigma-1} \subseteq \mathcal{G}/[\mathcal{G}, \mathcal{G}]$, hence $[\mathcal{G}, \mathcal{G}] \subseteq N^{\sigma-1}$, which establishes our claim.

By definition, $\mathbb{F}$ is the field which corresponds to $[\mathcal{G}, \mathcal{G}]$ and by the above, this implies that $\mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{F}) = N^{\sigma-1} = \ker(\mathrm{Res} : \mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{L}) \to \mathrm{Gal}(\mathbb{H}(\mathbb{K})/\mathbb{K}))$. Since the isomorphism

$$\varphi : \mathcal{C}(\mathbb{L}) \to N$$

is $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$-equivariant, the commutative diagram (2.6) shows that $\ker\big(N_{\mathbb{L}/\mathbb{K}} : \mathcal{C}(\mathbb{L}) \to \mathcal{C}(\mathbb{K})\big) = \mathcal{C}(\mathbb{L})^{\sigma-1}$, as we wanted.

For the last part of the proof, notice that for any integers $n \geq m \geq 1$, the group A_n is a direct summand of $\mathcal{C}(\mathbb{K}_n)$ as $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)]$-modules, so it follows that

$$\ker(N_{n,m} : A_n \to A_m) = A_n^{\omega_m}. \tag{2.7}$$

□

Remark 2.4. *When $\mathbb{L}/\mathbb{K}$ is unramified, Lemma 2.3 is due to Furtwängler. A different proof of Lemma 2.3 was given by Tobias Bembom in his Ph.D. thesis (see [Bem, Theorem 2.3.2] and [Bem, Corollary 2.4.5]).*

This is perhaps a good moment to look at what we proved so far. Combining Lemma 2.1 and Lemma 2.2, it follows that

$$A_n[\omega_m]/\iota_{m,n}(A_m) \cong \underline{E}_m/N_{n,m}(\underline{E}_n) \cong E_m/N_{n,m}(E_n). \tag{2.8}$$

Moreover, from Lemma 2.3 it follows that $|A_n[\omega_m]| = |A_m|$. In particular, if we fix some $m \geq 1$, it follows from (2.8) that the quantity $H^0\left(\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m), \underline{E}_n\right)$ is uniformly bounded, independent of n. Furthermore, since $|A_m| = |E_m/C_m|$ and $C_m \subset N_{n,m}(E_n)$, it follows that $|\iota_{m,n}(A_m)| = |N_{n,m}(E_n)/C_m|$.

We recall that our goal is to relate $N_{n,m}(E_m)$ to C_m. For this, we will need the following result about cyclotomic units that we proved in [Cri].

Lemma 2.5. *For any $n \geq m \geq 1$, we have $C_n \cap \mathbb{K}_m = C_m$.*

Proof. We reproduce the proof we gave in [Cri]. We know that C_n is a cyclic $\mathbb{Z}[G_n]$ module and $N_{\mathbb{K}_n/\mathbb{Q}}(C_n) = \{1\}$. So there is a surjective homomorphism

$$\mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]) \to C_n \quad \text{given by} \quad \overline{\theta} \to \eta_n^\theta,$$

where $\overline{\theta}$ denotes the image of $\theta \in \mathbb{Z}[G_n]$ in $\mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n])$.

We know C_n has finite index in E_n, so it has the same $\mathbb{Z}$-rank as E_n, namely $[\mathbb{K}_n : \mathbb{Q}] - 1$ by Dirichlet's Unit Theorem. This is the same as the $\mathbb{Z}$-rank of $\mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n])$, so by Vasconcelos' Theorem (see [Mats, Theorem 2.4]), we know that the kernel of the above described map must be trivial. We have thus a short exact sequence

$$1 \longrightarrow \mathbb{Z}[G_n]/(N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]) \xrightarrow{\overline{\theta}\to\eta_n^{\theta}} C_n \longrightarrow 1. \tag{2.9}$$

The inclusion $C_m \subseteq C_n \cap \mathbb{K}_m$ is clear. Conversely, consider $e \in C_n \cap \mathbb{K}_m$. Then $e = \eta_{n+1}^{\theta}$, for some $\theta \in \mathbb{Z}[G_n]$. We have that $G_n = \Gamma_n \times \langle\sigma\rangle$, where $\langle\sigma\rangle$ is the cyclic group $G_1 = \mathrm{Gal}(\mathbb{K}_1/\mathbb{Q})$. Hence one has an isomorphism of $\mathbb{Z}$-algebras $\phi : \mathbb{Z}[G_n] \xrightarrow{\sim} \mathbb{Z}[\Gamma_n] \otimes_{\mathbb{Z}} \mathbb{Z}[G_1]$ given by

$$\phi\left(\sum_i a_i \cdot g_i\right) = \sum_i a_i h_i \otimes n_i,$$

where $a_i \in \mathbb{Z}$, $g_i \in G_n$, $h_i \in \Gamma_n$, $n_i \in G_1$ and $g_i = h_i \cdot n_i$.

By a slight abuse of notation, we shall write ω_m for the image of $\omega_m = \tau^{p^{m-1}} - 1 = (T+1)^{p^{m-1}} - 1$ in $\mathbb{Z}[\Gamma_n]$ and similarly for $\nu_{m,1}, T$, etc. For the rest of the proof, the notations ω_m, $\nu_{m,1}$, T, etc will always refer to elements in $\mathbb{Z}[\Gamma_n]$. Let $\widehat{\omega_m} = \phi^{-1}(\omega_m \otimes 1)$. Since $e \in \mathbb{K}_m$, we have $e^{\widehat{\omega_m}} = 1$, thus

$$\eta_n^{\widehat{\omega_m}\cdot\theta} = 1. \tag{2.10}$$

By (2.9), this implies that $\widehat{\omega_m} \cdot \theta \in N_{\mathbb{K}_n/\mathbb{Q}}\mathbb{Z}[G_n]$. Let $z \in \mathbb{Z}[G_n]$ be such that $\widehat{\omega_m} \cdot \theta = N_{\mathbb{K}_n/\mathbb{Q}} \cdot z$ and let us write $N_{\mathbb{K}_n/\mathbb{Q}} = \nu_{n,1} \cdot N_\sigma$, where N_σ is the norm map $N_{\mathbb{K}_1/\mathbb{Q}}$. Under the isomorphism $\mathbb{Z}[G_n] \cong \mathbb{Z}[\Gamma_n] \otimes_{\mathbb{Z}} \mathbb{Z}[G_1]$, the element $\widehat{\omega_m} \in \mathbb{Z}[G_n]$ is mapped to $\omega_m \otimes 1$ and $N_{\mathbb{K}_n/\mathbb{Q}}$ is mapped to $\nu_{n,1} \otimes N_\sigma$. Now let $\{g_i\}_{i=1}^{\frac{p-1}{2}}$ be a $\mathbb{Z}$-basis for $\mathbb{Z}[G_1]$. Then for all $i = 1, 2, \ldots, \frac{p-1}{2}$, there exist integers a_i, c_i and elements $\theta_i, \tilde{z}_i \in \mathbb{Z}[\Gamma_n]$ such that

$$\phi(\theta) = \sum_{i=1}^{(p-1)/2} a_i\theta_i \otimes g_i \quad \text{and} \quad \phi(z) = \sum_{i=1}^{(p-1)/2} c_i\tilde{z}_i \otimes g_i.$$

Then

$$\phi(\widehat{\omega_m} \cdot \theta) = \sum_i a_i\omega_m\theta_i \otimes g_i \quad \text{and} \quad \phi(N_{\mathbb{K}_n/\mathbb{Q}} \cdot z) = \sum_i c_i\nu_{n,1}\tilde{z}_i \otimes N_\sigma g_i.$$

We now rewrite the expression $\sum_i c_i\nu_{n,1}\tilde{z}_i \otimes N_\sigma g_i$ along the basis $\{g_i\}_{i=1}^{\frac{p-1}{2}}$, so that one has

$$\phi(N_{\mathbb{K}_n/\mathbb{Q}} \cdot z) = \sum_i b_i\nu_{n,1}z_i \otimes g_i,$$

for some $b_i \in \mathbb{Z}$ and $z_i \in \mathbb{Z}[\Gamma_n]$ which can be computed in terms of the c_i's and $\tilde{z}_i$'s, respectively.

From the equality $\omega_m \cdot \theta = N_{\mathbb{K}_n/\mathbb{Q}} \cdot z$ (inside $\mathbb{Z}[G_n]$), it follows that for all $i = 1, 2, \ldots, \frac{p-1}{2}$, the identity $a_i\omega_m\theta_i = b_i\nu_{n,1}z_i$ holds in $\mathbb{Z}[\Gamma_n]$.

We also know that $\omega_m = \nu_{m,1} \cdot T$. Plugging this into the equality $a_i\omega_m\theta_i = b_i\nu_{n,1}z_i$, we obtain $a_i\nu_{m,1}T\theta_i = b_i\nu_{n,1}z_i$.

Let $\kappa : \mathbb{Z}[\Gamma_n] \to \frac{\mathbb{Z}[X]}{(X^{p^{n-1}}-1)}$ be an explicit isomorphism with $\kappa(T) = X - 1$. Then one has $\kappa(\omega_m) = X^{p^{m-1}} - 1$ and $\kappa(\nu_{n,1}) = \frac{X^{p^{n-1}}-1}{X-1}$. From $a_i\omega_m\theta_i = b_i\nu_{n,1}z_i$, we obtain

$$a_i(X^{p^{m-1}} - 1)\kappa(\theta_i) = b_i\frac{X^{p^{n-1}} - 1}{X - 1}\kappa(z_i) \quad \text{in} \quad \frac{\mathbb{Z}[X]}{(X^{p^{n-1}} - 1)}.$$

It follows that there exists a polynomial $f_i(X) \in \mathbb{Z}[X]$ such that

$$a_i(X^{p^{m-1}} - 1)\kappa(\theta_i) + f_i(X)(X^{p^{n-1}} - 1) = b_i \frac{X^{p^{n-1}} - 1}{X - 1}\kappa(z_i) \quad \text{in} \quad \mathbb{Z}[X].$$

Dividing both sides by $\frac{X^{p^{m-1}}-1}{X-1}$, we get

$$a_i(X - 1)\kappa(\theta_i) + f_i(X)(X - 1)\frac{X^{p^{n-1}} - 1}{X^{p^{m-1}} - 1} = b_i \frac{X^{p^{n-1}} - 1}{X^{p^{m-1}} - 1}\kappa(z_i).$$

From this, one deduces that $\frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1} \mid a_i(X-1)\kappa(\theta_i)$ and since $\gcd((X-1), \frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1}) = 1$ with $\frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1}$ monic, we obtain $\frac{X^{p^{n-1}}-1}{X^{p^{m-1}}-1} \mid \kappa(\theta_i)$, as polynomials in $\mathbb{Z}[X]$. Hence there exists $g_i(X) \in \mathbb{Z}[X]$ such that $\kappa(\theta_i) = \kappa(\nu_{n,m}) \cdot g_i(X)$ as polynomials in $\frac{\mathbb{Z}[X]}{(X^{p^{n-1}}-1)}$. Thus $\theta_i = \nu_{n,m} \cdot s_i$, where $s_i = \kappa^{-1}(g_i(X)) \in \mathbb{Z}[\Gamma_n]$. Since this holds for all i, it implies via the isomorphism $\mathbb{Z}[G_n] \cong \mathbb{Z}[\Gamma_n] \otimes_{\mathbb{Z}} \mathbb{Z}[G_1]$ that one can write $\theta \in \mathbb{Z}[G_n]$ as $\widehat{\nu_{n,m}} \cdot s$, where $\widehat{\nu_{n,m}} = \phi^{-1}(\nu_{n,m} \otimes 1)$ and $s \in \mathbb{Z}[G_n]$. It is clear that $\eta_n^{\widehat{\nu_{n,m}}} = \eta_m$. Therefore, we obtain $e = \eta_n^{\widehat{\nu_{n,m}} \cdot s} = \eta_m^s$, which shows that $e \in C_m$, as required. □

2.3 Proof of the main theorem

So far, all the results we proved are unconditional and we managed to make good progress in understanding the structure of A_n, E_n and C_n using techniques from classical algebraic Iwasawa theory. To derive our main result, we will assume from now on that p is a prime for which Greenberg's conjecture holds for the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}_1$.

Let $A_\infty = \varprojlim_n A_n$ be the projective limit of the groups $(A_n)_{n \geq 1}$ with respect to the norm maps. For every $n \geq 1$, we let $\mathbb{H}(\mathbb{K}_n)$ be the Hilbert class field of $\mathbb{K}_n$. Then for any $n \geq m$ one has $\mathbb{K}_n \cap \mathbb{H}(\mathbb{K}_m) = \mathbb{K}_m$ because $\mathbb{K}_n/\mathbb{K}_m$ is totally ramified at p. It then follows from class field theory that the norms $N_{n,m} : A_n \to A_m$ are surjective for all $n \geq m \geq 1$ (see for example the Lemma after [Lang 1, Chapter 3 , Theorem 4.3].) It follows that the numbers $|A_n|$ form a non-decreasing sequence of positive integers. Assuming Greenberg's conjecture, this sequence is bounded above by the finite quantity $|A_\infty|$. Under this assumption, it follows that there must be an integer n_0 such that for any $n \geq m \geq n_0$, we have $|A_n| = |A_m| = |A_\infty|$ and the norm $N_{n,m}$ is in fact an isomorphism, so we have

$$A_n = A_m \cong A_\infty, \quad \forall n \geq m \geq n_0. \tag{2.11}$$

We now look at the ideal lift map $\iota_{m,n} : A_m \to A_n$ and its kernel (also referred to as the kernel of capitulation). When $|A_\infty|$ is finite, there exists $k' > 0$ such that $(A_\infty)^{p^{k'}} = 0$, and $n > n_0$. Since $N_{n,m} \circ \iota_{m,n} : A_m \to A_m$ is the p^{n-m} power map for $n > m \geq n_0$, by letting $n = m + k'$ we have

$$N_{n,m} \circ \iota_{m,n}(A_m) = (A_m)^{p^{k'}} = 0.$$

We have seen above that when $|A_\infty| < \infty$ the map $N_{n,m}$ is an isomorphism, so we get

$$\iota_{m,n}(A_m) \subset \ker(N_{n,m} : A_n \to A_m) = 0.$$

This argument also works for $1 \leq m < n_0$: let $k = k' + n_0$; then $\iota_{m,n} = \iota_{n_0,n} \circ \iota_{m,n_0}$ and since $\iota_{m,n_0}(A_m) \subset A_{n_0}$, $\iota_{n_0,n}(A_{n_0}) = \{1\}$, it follows that $\iota_{m,n}(A_m) = \{1\}$. We have proved the following.

Lemma 2.6. *Assuming Greenberg's conjecture, there exists a constant k such that for all $m \geq 1$ and $n \geq m + k$ we have*

$$A_n \cong A_\infty \quad \textit{and} \quad \iota_{m,n}(A_m) = 0.$$

Remark 2.7. *Greenberg also proved in [Gre 1, Proposition 2] that* $|A_\infty| < \infty$ *is equivalent to* $A_m = \bigcup\limits_{n \geq m} \ker(\iota_{m,n} : A_m \to A_n)$*, for all* $m \geq 1$.

We saw before that $|A_n[\omega_m]| = |A_m|$ and that under Greenberg's conjecture one has $|A_n| = |A_m|$ for all $n \geq m \geq n_0$. Combining these two pieces of information, we immediately deduce the following.

Lemma 2.8. *Assuming Greenberg's conjecture, there exists a positive integer* n_0 *such that for all* $n \geq m \geq n_0$ *one has*

$$A_n[\omega_m] = A_n \cong A_m,$$

where the last isomorphism is by means of the norm map $N_{n,m}$.

The last ingredient we need is to prove that $E_m/N_{n,m}(E_n) \cong E_m/C_m$ for all sufficiently large n. From Lemma 2.5 it follows that if $e \in \underline{E}_m \setminus C_m$ is a non-cyclotomic unit, then $e \notin C_n$ for any $n \geq m$. Notice also that $E_m \subseteq E_n$ for all $n \geq m \geq 1$. It follows that there exists an injection of $\Lambda[G_1]$-modules $E_m/C_m \hookrightarrow E_mC_n/C_n$. The analytic class number formula (relation (2.4)) together with Lemma 2.6 imply that under Greenberg's conjecture one has

$$|E_n/C_n| = |E_{n_0}/C_{n_0}| = |A_\infty|, \quad \text{for all} \quad n \geq n_0.$$

Since $E_mC_n \subseteq E_n = E_nC_n$ and E_m/C_m injects into $(E_mC_n)/C_n$ for $n > m$, we conclude that

$$E_n = E_mC_n, \qquad \text{for all } n \geq m \geq n_0. \tag{2.12}$$

We can now prove our last auxiliary result.

Lemma 2.9. *Assuming Greenberg's conjecture, for any positive integer* m *and all sufficiently large* $n \geq m$ *one has* $N_{n,m}(E_n) = C_m$.

Proof. Since $E_n = E_{n_0}C_n$ by (2.12), given $e \in E_n$ it follows that we can write $e = e_{n_0} \cdot c_n$, for some $e_{n_0} \in E_{n_0}$ and $c_n \in C_n$. If $m \geq n_0$, then $N_{n,m}(e) = N_{n,m}(e_{n_0}) \cdot N_{n,m}(c_n) = (e_{n_0}^{p^{n-m}}) \cdot N_{n,m}(c_n)$. For all sufficiently large n we have $e_{n_0}^{p^{n-m}} \in C_n$ and so $N_{n,m}(e) \in N_{n,m}(C_n) = C_m$. Similarly, if $m < n_0$, then $N_{n,m}(e) = N_{n_0,m}(N_{n,m}(e_{n_0})) \cdot N_{n,m}(c_n) = N_{n_0,m}((e_{n_0}^{p^{n-n_0}})) \cdot N_{n,m}(c_n)$ and $e_{n_0}^{p^{n-n_0}} \in C_{n_0}$, for all sufficiently large n. The conclusion follows. □

Putting everything together, we obtain the main result of this chapter.

Theorem 2.10. *If* p *is a prime for which Greenberg's conjecture holds for the cyclotomic* $\mathbb{Z}_p$*-extension of* $\mathbb{K}_1$*, then for any* $m \geq 1$ *and all sufficiently large* $n > m$ *one has an isomorphism of* $\Lambda[G_1]$*-modules*

$$A_n[\omega_m] \cong E_m/C_m.$$

In particular, there exists an integer n_0 *such that for all* $m \geq n_0$ *one obtains an isomorphism of* $\Lambda[G_1]$*-modules*

$$A_m \cong E_m/C_m.$$

Remark 2.11. *Theorem* 2.10 *sharpens the main result we previously proved in [Cri, Proposition 3.1], which asserts that one has an isomorphism of* $\Lambda[G_1]$*-modules* $E_m/C_m \cong A_m$*, for all* $m \geq n_0$.

Let us now look at some immediate consequences of our main result. In view of the Iwasawa-Leopoldt conjecture mentioned in introduction, it is natural to ask whether one can say something about the structure of A_1 over the group ring $\mathbb{Z}_p[G_1]$. To look at this into more detail, we need to introduce the following additional notations. For $0 \leq i \leq p-2$, consider the idempotents

$$\varepsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a) \sigma_a^{-1} \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}],$$

where $\omega : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ is the Teichmüller character and $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is given by $\sigma_a(\zeta_p) = \zeta_p^a$. We will also let $A(\mathbb{Q}(\zeta_p))$ stand for the p-Sylow subgroup of $\mathcal{C}(\mathbb{Q}(\zeta_p))$. The group A_1 can be identified with

$$A_1 = \bigoplus_{i \text{ even}} \varepsilon_i A(\mathbb{Q}(\zeta_p)),$$

and it is also well-known that $\varepsilon_0 A_1 = \{1\}$ (see for example [Wa, Proposition 6.16]). Furthermore, the reflection theorems (see [Wa, Theorem 10.9]) tell us that for i even, j odd with $i + j \equiv 1 \pmod{p-1}$, one has

$$p - \mathrm{rank}\,(\varepsilon_i A_1) \leq p - \mathrm{rank}\big(\varepsilon_j\,(A(\mathbb{Q}(\zeta_p)))\,\big) \leq 1 + p - \mathrm{rank}(\varepsilon_i A_1),$$

where $p - \mathrm{rank}(M)$ stands for the number of $\mathbb{Z}/p\mathbb{Z}$ summands in M/pM. Since $\mathcal{C}(\mathbb{Q}(\zeta_p))_p^-$ is defined by

$$A(\mathbb{Q}(\zeta_p))^- = \bigoplus_{j \text{ odd}} \varepsilon_j A(\mathbb{Q}(\zeta_p)),$$

it follows that if A_1 is $\mathbb{Z}_p[G_1]$-cyclic, then $A(\mathbb{Q}(\zeta_p))^-$ has at most two generators when regarded as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$-module (which would establish a weak form of the Iwasawa-Leopoldt conjecture). As consequence of the Main Conjecture, there is a sharper version of (2.3), namely for every even $2 \leq i \leq p-3$ one has

$$|\varepsilon_i A_1| = |\varepsilon_i E_1/C_1|\,.$$

A more elementary proof of this fact is given for example in [Wa, Theorem 15.7]. Furthermore, Washington shows in the discussion following [Wa, Proposition 8.13] that for the even values $2 \leq i \leq p-3$, $\varepsilon_i\,(E_1/C_1)$ is a cyclic group. It follows that E_1/C_1 is cyclic as a $\mathbb{Z}_p[G]$-module. The action of τ is trivial, so E_1/C_1 is cyclic as a $\Lambda[G_1]$-module. Using Theorem 2.10, we obtain the following.

Corollary 2.12. *For all n sufficiently large, $A_n[T]$ is a cyclic $\Lambda[G_1]$-module. In particular, for all even $2 \leq i \leq p-3$, $\varepsilon_i(A_n[T])$ is a cyclic $\mathbb{Z}_p$-module.*

Unfortunately, the above Corollary is not good enough for deducing that A_1 is $\mathbb{Z}_p[G_1]$-cyclic. For this, one would need to prove that the isomorphism $A_m \cong E_m/C_m$ holds for all $m \geq 1$, not just $m \geq n_0$, and the present methods seem to not be strong enough to achieve this.

3. Structure theorems for Iwasawa modules encoding classical conjectures

3.1 Introduction

The results we will present in this chapter emerged from the author's investigation of Leopoldt's conjecture for a pair $(\mathbb{F}, p)$ consisting of a totally real number field $\mathbb{F}$ and an odd prime p that splits completely in $\mathbb{F}$. This investigation led to an extended study of the modules that encode Leopoldt's conjecture and, more importantly, of the techniques one uses for studying these modules. Consequently, our primary goal in this chapter will be to develop some new tools in classical algebraic Iwasawa theory that allow one to gain more insight into longstanding classical conjectures, such as Leopoldt's conjecture. We will show how these new techniques can be used to refine some of the existing results and indicate the initial strategy for completing the conjecture in the aforementioned special case.

The central objects of study in classical algebraic Iwasawa theory are the abelian extensions and subextensions of a $\mathbb{Z}_p$-extension of a number field $\mathbb{K}$, and how the groups of units and of ideal classes vary with these extensions. In his seminal paper [Iwa73], Iwasawa used tools from class field theory, Kummer theory and commutative algebra in order to study these objects and proved a remarkable number of results regarding their structure. Here, we will restrict to a certain class of number fields $\mathbb{K}$ that are Galois extensions of $\mathbb{Q}$ and use the aforementioned tools to complement and refine some of the results available in the literature. *An important idea that will help us achieve our goal will be the study of the objects of interest not only as modules over the Iwasawa algebra* Λ, *but also as* $\Lambda[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$*-modules.* The other important feature of our work in this chapter is that in studying certain classical problems (such as Leopoldt's conjecture), one only has to consider extensions $\mathbb{M}$ of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{K}_\infty$ of $\mathbb{K}$ for which the Galois group $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a free $\mathbb{Z}_p$-module of finite rank, and by applying Leopoldt's reflection to this more restrictive setting, several standard results about class groups and units can be considerably refined.

Each of Section 3.2, 3.3 and 3.4 is of independent interest on its own, and can be read without referring to any of the others. As a result, each section starts with a rather general framework and progressively introduces further restrictions that allow us to develop the desired theory. As we develop our framework, we shall indicate appropriately which are the results of key interest in every section.

In order to state some of our main applications, we will need to first recall some background material on Leopoldt's conjecture and its equivalent forms for a certain class of number fields.

Let p be an odd prime and let $\mathbb{K}$ be a CM number field that contains the pth roots of unity. Let $\mathbb{K}^+$ denote the maximal totally real subextension of $\mathbb{K}$. It follows from the definition of a CM field that $[\mathbb{K} : \mathbb{K}^+] = 2$. Leopoldt's conjecture for the field $\mathbb{K}^+$ and the prime p asserts the non-vanishing of the p-adic regulator of $\mathbb{K}^+$. Iwasawa noted in [Iwa73, Section 2.3] that this conjecture is equivalent to the fact that the only $\mathbb{Z}_p$-extension of $\mathbb{K}^+$ is the cyclotomic one. Let $\mathbb{K}^+_\infty$ denote the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}^+$ and let $\Omega(\mathbb{K}^+)$ be the maximal p-abelian p-ramified extension of $\mathbb{K}^+$. It is a well-known fact, valid for arbitrary number fields, that the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{K}^+$ is a subfield of finite index in $\Omega(\mathbb{K}^+)$ (see for example [Lang 1, Chapter 5, Theorem 5.2]). It follows that Leopoldt's conjecture for the field $\mathbb{K}^+$ is equivalent to the assertion that $\mathbb{K}^+_\infty$ has finite index in $\Omega(\mathbb{K}^+)$.

Let $\mathbb{K}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ and let $\Omega(\mathbb{K})$ be the maximal p-abelian p-ramified extension of $\mathbb{K}$. Then the extensions $\Omega(\mathbb{K})/\mathbb{K}^+$ and $\mathbb{K}_\infty/\mathbb{K}^+$ are both Galois (see for example the discussion from [Iwa73, Section 11.3]). The diagram of fields is presented below.

$$\begin{tikzcd}
 & & & \Omega(\mathbb{K}) \\
 & \Omega(\mathbb{K}^+) \arrow[r, dash] & \Omega(\mathbb{K})^+ \arrow[ur, dash] & \\
\mathbb{K}^+_\infty \arrow[ur, dash] \arrow[r, dash] \arrow[d, dash] & \mathbb{K}_\infty \arrow[ur, dash] \arrow[d, dash] & & \\
\mathbb{K}^+ \arrow[r, dash] & \mathbb{K} & &
\end{tikzcd}$$

Let $\jmath \in \mathrm{Gal}(\mathbb{K}/\mathbb{K}^+)$ denote the complex conjugation automorphism. Since p is odd, it follows that there exists a direct sum decomposition

$$\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty) = (1+\jmath)\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty) \bigoplus (1-\jmath)\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty).$$

Let $\Omega(\mathbb{K})^+$ be the maximal abelian extension of $\mathbb{K}^+_\infty$ contained in $\Omega(\mathbb{K})$. Then $\mathbb{K}_\infty \subseteq \Omega(\mathbb{K})^+ \subseteq \Omega(\mathbb{K})$. Moreover, it was proved by Iwasawa in [Iwa73, Section 11.3] that

$$\mathrm{Gal}\left(\Omega(\mathbb{K}^+)/\mathbb{K}^+_\infty\right) \cong \mathrm{Gal}\left(\Omega(\mathbb{K})^+/\mathbb{K}_\infty\right) = (1+\jmath)\mathrm{Gal}\left(\Omega(\mathbb{K})/\mathbb{K}_\infty\right).$$

It follows that yet another equivalent formulation of Leopoldt's conjecture is the fact that $(1+\jmath)\mathrm{Gal}\left(\Omega(\mathbb{K})/\mathbb{K}_\infty\right)$ is a finite group. It will be this particular formulation that we will work with. Our task will be to use Kummer theory, Leopoldt's reflection, group theory and classical results from Iwasawa theory in order to prove that a certain group of ideal classes has exactly the same $\mathbb{Z}_p$-rank as $(1+\jmath)\mathrm{Gal}\left(\Omega(\mathbb{K})/\mathbb{K}_\infty\right)$, hence encoding Leopoldt's conjecture as well. To state precisely what this group is, we need to introduce some additional notation.

For every $n \geq 0$, we let $\mathbb{K}_n$ be the unique field $\mathbb{K} \subset \mathbb{K}_n \subset \mathbb{K}_\infty$ for which $[\mathbb{K}_n : \mathbb{K}] = p^n$. Let $\Gamma := \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$. We recall that the Iwasawa algebra of Γ is defined as

$$\Lambda := \varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_n/\mathbb{K})]$$

and that there exists a (non-canonical) isomorphism $\Lambda \cong \mathbb{Z}_p[[T]]$ obtained by mapping a topological generator γ_0 of Γ to $1+T$. Unless we specify it otherwise, we will always identify Λ with $\mathbb{Z}_p[[T]]$ by means of a fixed γ_0. Let χ be the canonical p-adic character of Γ for which

$$\zeta_{p^n}^{\gamma_0} = \zeta_{p^n}^{\chi(\gamma_0)},$$

for any $n \geq 0$ and any p^nth root of unity ζ_{p^n}. The Iwasawa involution

$$* : \Lambda \to \Lambda$$

is defined by $T^* = \frac{\chi(\gamma_0)}{1+T} - 1$ and extending it linearly to the whole Λ.

Let $\mathbb{H}_n$ be the maximal p-abelian everywhere unramified extension of $\mathbb{K}_n$ and $\mathbb{H}_\infty = \bigcup \mathbb{H}_n$, the maximal p-abelian everywhere unramified extension of $\mathbb{K}_\infty$. We also let A_n be the p-part of the class group of $\mathbb{K}_n$. For every $n \geq 0$, one has the Artin isomorphism

$$\mathrm{Gal}(\mathbb{H}_n/\mathbb{K}_n) \cong A_n,$$

and taking the limit with respect to the norm maps one obtains

$$\mathrm{Gal}(\mathbb{H}_\infty/\mathbb{K}_\infty) \cong \varprojlim_n A_n.$$

Let $A_\infty = \varprojlim_n A_n$. An important result of Iwasawa asserts that A_∞ is a noetherian torsion Λ-module (see [Iwa73, Theorem 5]). For a Λ-submodule B of A_∞, we let $B[T^*]$ denote the set of elements in B which are annihilated by T^*. Complex conjugation acts in a natural way on A_∞ and it induces a decomposition

$$A_\infty = A_\infty^+ \oplus A_\infty^-,$$

where

$$A_\infty^+ = \{a \in A_\infty : a^{1-\jmath} = 1\}, \quad A_\infty^- = \{a \in A_\infty : a^{1+\jmath} = 1\}.$$

We can now state an important application of the results we will develop in this chapter.

Theorem 3.1. *The Λ-module $A_\infty^-[T^*]$ is a finitely generated torsion-free $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-rank equal to the $\mathbb{Z}_p$-rank of $(1+\jmath)\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{K}_\infty)$. Furthermore, if $\mathbb{K}$ is a Galois extension of $\mathbb{Q}$ and $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$, then $A_\infty^-[T^*]$ becomes a pseudo-cyclic $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-module (i.e., there exists an element $a \in A_\infty^-[T^*]$ such that the $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-module generated by a has finite index in $A_\infty^-[T^*]$).*

The connection between Leopoldt's conjecture and various groups of ideal classes has been already noted in the literature. Greenberg proved in [Gre 1, Proposition 1] that if the $\mathbb{Z}_p$-rank of $(1+\jmath)\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{K}_\infty)$ is 0, then the subgroup $A_\infty^+(T)$ of A_∞, consisting of elements in A_∞^+ annihilated by positive integer powers of T, must be finite. As we will explain in Section 3.5, Greenberg's result also follows from the theorems we prove in this chapter. In [Ja], Jaulent used the construction of a certain unramified extension $\mathbb{F}/\mathbb{K}_\infty$ that encodes Leopoldt's conjecture to prove Leopoldt's conjecture for a family of number fields of small discriminant. We will also discuss this construction in Section 3.5 and show how it leads to a proof of the fact that $|A_\infty^-[T^*]| < \infty$ implies that Leopoldt's conjecture holds for $\mathbb{K}^+$ (which is a weaker form of Theorem 3.1).

Let us now explain how the condition $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$ in the second part of Theorem 3.1 arises. Assume $\mathbb{M}/\mathbb{K}_\infty$ is a Kummer extension with the property that $\mathbb{M}/\mathbb{Q}$ is a Galois extension, and thus we have an action of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{Q})$ on both $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ and its radical. Then the condition $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$ ensures that we have a decomposition

$$\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{K}/\mathbb{Q}), \tag{3.1}$$

and thus we can act with $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ on the radical of $\mathbb{M}/\mathbb{K}_\infty$ by identifying $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ with a subgroup of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{Q})$ using (3.1). In this setting, one can use the full Leopoldt reflection (which we introduce in Section 3.2) to study the objects of interest as $\Lambda[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-modules. In the general case when $\mathbb{K} \cap \mathbb{Q}_\infty \neq \mathbb{Q}$, the results become technically more difficult, but the core ideas are the same. It is also important to mention that within the framework developed for proving Theorem 3.1, after establishing several natural intermediate steps, one may conclude that the extension $\Omega(\mathbb{K}^+) \cdot \mathbb{K}_\infty \cap \mathbb{H}_\infty/\mathbb{K}_\infty$ is finite, which in particular establishes Leopoldt's conjecture for totally real fields in which the prime p splits completely. We indicate one of these intermediate results in Section 3.6. Unfortunately, due to the timeline of this thesis, we are not able to provide the full details of the remaining steps to the rigour we set for the rest of the thesis. However, the preliminary details worked out in this chapter are a solid basis for completing this project, towards the fulfillment of which I wish to contribute, alone or as part of a collaboration, in the near future. We also note that the results presented in this chapter serve as solid groundwork for other longstanding conjectures in Iwasawa theory.

An interesting class of pairs $(\mathbb{K}, p)$ with $\mathbb{K}$ a CM field and p an odd prime for which all the hypotheses of Theorem 3.1 are satisfied can be constructed as follows. Let $\mathbb{E}$ be a totally real number field and let $\mathbb{F}/\mathbb{E}$ be its Galois closure over $\mathbb{Q}$. It is a well-known fact in algebraic number theory that a prime p splits completely in $\mathbb{E}$ if and only if it splits completely in $\mathbb{F}$ (for a proof, see for example [Marcus, Theorem 31 and its Corollary] or [Cox, Exercises 8.13-8.15]). Let thus p be a prime that splits completely in $\mathbb{E}$ and let $\mathbb{Q}_\infty/\mathbb{Q}$ be the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Then p splits completely in $\mathbb{F}$ and since p is totally ramified in $\mathbb{Q}_\infty/\mathbb{Q}$, it follows that $\mathbb{F} \cap \mathbb{Q}_\infty = \mathbb{Q}$. Moreover, since $\mathbb{E}$ is totally real, so is $\mathbb{F}$. Consider now $\mathbb{K} = \mathbb{F}(\zeta_p)$. Then $\mathbb{K}$ is the compositum of $\mathbb{F}$ and $\mathbb{Q}(\zeta_p)$, hence a CM field that is Galois over $\mathbb{Q}$. Notice also that $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$ and thus the pair $(\mathbb{K}, p)$ satisfies all the hypotheses of Theorem 3.1. It is still an open problem whether Leopoldt's conjecture holds for a pair $(\mathbb{E}, p)$ with $\mathbb{E}$ a totally real field and p a prime that splits completely in $\mathbb{E}$, so in particular Theorem 3.1 addresses a non-trivial case of Leopoldt's conjecture.

Our strategy for proving Theorem 3.1 is as follows. In Section 3.2 we show how one can define an infinite projective radical for an extension $\mathbb{M}/\mathbb{K}_\infty$ whose Galois group is a free, finitely generated $\mathbb{Z}_p$-module and discuss some of its basic properties. In Section 3.3 we use class field theory to determine the structure of $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-module. In Section 3.4 we prove how one can construct a homomorphism from the projective radical of $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ to A_∞. When we restrict to the case when $\mathbb{M}$ is the compositum of all real $\mathbb{Z}_p$-extensions of $\mathbb{K}$ (which has finite index in $\Omega(\mathbb{K})^+$), we can show that this map is a pseudo-isomorphism into $A_\infty^-[T^*]$, by showing that it is injective and explicitly constructing an injective homomorphism from $A_\infty^-[T^*]$ to the radical, thus showing that the corresponding $\mathbb{Z}_p$-ranks must agree. In Section 3.5 we simply combine all the aforementioned facts to derive Theorem 3.1.

Two other important applications of our methods are Proposition 3.28 and Theorem 3.31, respectively. Proposition 3.28 has a similar flavor to Theorem 3.1, giving a pseudo-isomorphism between the radical of an extension of $\mathbb{K}_\infty$ and the subgroup A_∞^- of A_∞. In Theorem 3.31 we prove that certain ideal classes can never be radicals of unramified extension. This last result generalizes the proof behind Iwasawa's self-dual pairing from [Iwa73, Section 10], and it plays a crucial role in both our strategy for completing the proof of the aforementioned special case of Leopoldt's conjecture, as well as in other open problems in Iwasawa theory.

3.2 Infinite Kummer Theory over the cyclotomic $\mathbb{Z}_p$-extension

Let $\mathbb{K}$ be a number field that contains the pth roots of unity and let $\mathbb{K}_\infty = \mathbb{K}(\mu_{p^\infty})$ be its cyclotomic $\mathbb{Z}_p$-extension. Throughout this section, we regard all our fields as subfields of a fixed algebraic closure of $\mathbb{Q}$.

Let $\mathbb{M}$ be a p-abelian p-ramified extension of $\mathbb{K}_\infty$ with the property that the group $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a torsion-free, finitely generated $\mathbb{Z}_p$-module. For each $n \geq 1$, let $\mathbb{M}_n \subset \mathbb{M}$ be the maximal subextension of $\mathbb{M}$ with the property that $p^n\mathrm{Gal}(\mathbb{M}_n/\mathbb{K}) = \{1\}$. Since $\mu_{p^\infty} \subset \mathbb{K}_\infty$, it follows that for each $n \geq 1$ the extension $\mathbb{M}_n/\mathbb{K}_\infty$ is a finite Kummer extension and has a well-defined radical $\mathrm{Rad}(\mathbb{M}_n/\mathbb{K}_\infty) \subset \mathbb{K}_\infty^\times$ such that $(\mathbb{K}_\infty^\times)^{p^n} \subset \mathrm{Rad}(\mathbb{M}_n/\mathbb{K}_\infty)$ and $\mathbb{M}_n = \mathbb{K}_\infty(\mathrm{Rad}(\mathbb{M}_n/\mathbb{K}_\infty)^{1/p^n})$. Let $R_n = \mathrm{Rad}(\mathbb{M}_n/\mathbb{K}_\infty)/(\mathbb{K}_\infty^\times)^{p^n}$. Then R_n is a finite multiplicative group. Furthermore, if $\alpha_{n+1} \in \mathrm{Rad}(\mathbb{M}_{n+1}/\mathbb{K}_\infty)$, then $\mathbb{K}_\infty\left(\alpha_{n+1}^{1/p^{n+1}}\right) \subset \mathbb{M}_{n+1}$ and by the definition of $\mathbb{M}_n$, one also has $\mathbb{K}_\infty\left(\alpha_{n+1}^{1/p^n}\right) \subset \mathbb{M}_n$. It follows that there is a well-defined map

$$\begin{tikzcd} \mathrm{Rad}(\mathbb{M}_{n+1}/\mathbb{K}_\infty) \arrow[r] & \mathrm{Rad}(\mathbb{M}_n/\mathbb{K}_\infty) \\ \alpha_{n+1} \arrow[r] & \alpha_{n+1}, \end{tikzcd}$$

which induces a restriction map

$$\begin{tikzcd} R_{n+1} \arrow[r, "\mathrm{Res}"] & R_n \\ \alpha_{n+1} \pmod{(\mathbb{K}_\infty^\times)^{p^{n+1}}} \arrow[r] & \alpha_{n+1} \pmod{(\mathbb{K}_\infty^\times)^{p^n}}. \end{tikzcd}$$

To avoid overloading notation, we will use α_n to also denote the class of the element $\alpha_n \in \mathrm{Rad}(\mathbb{M}_n/\mathbb{K}_\infty)$ in R_n.

For each $n \geq 1$, finite Kummer theory gives a perfect pairing

$$\langle \cdot, \cdot \rangle : \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty) \times R_n \to \mu_{p^n}$$

defined as follows. For any $\sigma \in \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty)$ and any $\alpha \in R_n$ one has

$$\langle \sigma, \alpha \rangle = \frac{\sigma(\alpha^{1/p^n})}{\alpha^{1/p^n}}.$$

Moreover, for every $n \geq m \geq 1$ we have a compatible system of pairings

$$\begin{tikzcd} \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty) \arrow[d, "\mathrm{Res}"] & \times & R_n \arrow[d, "\mathrm{Res}"] \arrow[r] & \mu_{p^n} \arrow[d, "\cdot p^{n-m}"] \\ \mathrm{Gal}(\mathbb{M}_m/\mathbb{K}_\infty) & \times & R_m \arrow[r] & \mu_{p^m}, \end{tikzcd} \tag{3.2}$$

where, by a slight abuse of notation, Res denotes the restriction map both between the Galois groups and between the radicals.

Let R denote the projective limit $R = \varprojlim R_n$ with respect to the restriction maps. We call R the **radical** of the extension $\mathbb{M}/\mathbb{K}_\infty$. It follows that there exists a perfect pairing

$$\langle \cdot, \cdot \rangle : \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \times R \to \varprojlim_n \mu_{p^n},$$

which gives an isomorphism of $\mathbb{Z}_p$-modules

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \cong \mathrm{Hom}_{\mathbb{Z}_p}(R, \varprojlim_n \mu_{p^n}).$$

Fix once and for all an isomorphism $\varprojlim_n \mu_{p^n} \cong \mathbb{Z}_p$. It follows that there exists an isomorphism of $\mathbb{Z}_p$-modules

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \cong \mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p) =: \hat{R}, \tag{3.3}$$

where $\hat{R}$ denotes the dual module of the $\mathbb{Z}_p$-module R. It follows that $\hat{R}$ is a free $\mathbb{Z}_p$-module of rank r.

Similarly, one has an isomorphism of $\mathbb{Z}_p$-modules

$$R \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty), \mathbb{Z}_p). \tag{3.4}$$

It follows that R is also a free $\mathbb{Z}_p$-module of rank r.

We will now prove that whenever $\mathbb{M}$ is an extension as above and in addition $\mathbb{M}/\mathbb{K}$ is a Galois extension, there exists a positive constant k such that for all sufficiently large n, R_n can be generated by elements in $\mathbb{K}_{n+k}$, i.e., for every class in R_n we can choose a representative of that class which lies in $\mathbb{K}_{n+k}$. For this, we will need some preliminary facts from group theory and Iwasawa theory.

We first notice that whenever $\mathbb{M}/\mathbb{K}_\infty$ is a pro-p-extension and $\mathbb{M}/\mathbb{K}$ is Galois, since $\Gamma := \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ is isomorphic to $(\mathbb{Z}_p, +)$ and this is a free pro-p-group, it follows that there exists a semi-direct product decomposition

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}) \cong \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \rtimes \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}).$$

A proof of this fact is given for example in [Koch, Theorem 4.8]. In particular, Γ can be lifted to a subgroup of $\mathrm{Gal}(\mathbb{M}/\mathbb{K})$.

Let Λ stand for the Iwasawa algebra of the extension $\mathbb{K}_\infty/\mathbb{K}$ and we identify $\Lambda = \mathbb{Z}_p[[\Gamma]]$ with $\mathbb{Z}_p[[T]]$ by mapping a fixed topological generator τ of Γ to $T+1$. For $n \geq m \geq 0$, the elements ω_n and $\nu_{n,m}$ are defined as

$$\omega_n = (1+T)^{p^n} - 1, \quad \nu_{n,m} = \frac{\omega_n}{\omega_m}.$$

We recall that a polynomial $P(T) \in \mathbb{Z}_p[T]$ is called *distinguished* if it is of the form

$$P(T) = T^n + a_{n-1}T^{n-1} + a_{n-2}T^{n-2} + \ldots + a_1 T + a_0,$$

with $p \mid a_j$ for all $j = 0, \ldots, n-1$. Notice that for any $n \geq m \geq 0$, both ω_n and $\nu_{n,m}$ are distinguished polynomials.

We also recall that if $\mathbb{M}/\mathbb{K}_\infty$ is a pro-p abelian extension such that $\mathbb{M}/\mathbb{K}$ is Galois, then there is an action of $\Gamma = \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ on $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ defined as follows. For every $\tau \in \Gamma$, let $\tilde{\tau}$ be a lift of τ to $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$; then for an element $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ we define

$$\tau * \sigma = \tilde{\tau}\sigma\tilde{\tau}^{-1}.$$

Since the group $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is abelian, it follows that the action is independent of the chosen lift $\tilde{\tau}$ of τ (i.e., the right hand side in the above equality depends only on τ). Let now τ_0 be a topological generator of Γ. Since the action of Γ on $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is continuous, $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ admits a unique structure of Λ-module such that

$$(1+T)\sigma = \tau_0 * \sigma,$$

for any $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$.

Finally, we will need the following auxiliary result.

Lemma 3.2. *Let $f(T) \in \mathbb{Z}_p[T]$ be a distinguished polynomial of degree d. Then there exists a constant k which depends only on f such that for all sufficiently large n, one has*

$$\omega_{n+k} \in (p^n, f(T))\,\Lambda.$$

Proof. Let n_0 be a positive integer such that $\deg(\omega_{n_0}) > d$. By the division algorithm, we can write

$$\omega_{n_0} = f(T) \cdot q_1(T) + r_1(T),$$

for some $q(T), r(T) \in \mathbb{Z}_p[T]$, with $\deg(r(T)) < d$. Since both ω_{n_0} and f are distinguished polynomials, it follows that $p \mid r_1(T)$ in $\mathbb{Z}_p[T]$ (to see this, one can reduce the above equality modulo p and use that $\deg(\omega_{n_0}) > \deg(f) > \deg(r_1)$.) It follows that one can write

$$\omega_{n_0} = f(T) \cdot q_1(T) + p \cdot a(T),$$

for some $a(T) \in \mathbb{Z}_p[T]$. Multiplying both sides of the above equality by ν_{n_0+1,n_0} yields

$$\omega_{n_0+1} = f(T) \cdot q_1(T) \cdot \nu_{n_0+1,n_0} + p \cdot \nu_{n_0+1,n_0} \cdot a(T).$$

Since $\deg(\nu_{n_0+1,n_0}) \geq \deg \omega_{n_0} > d$ and ν_{n_0+1,n_0} is distinguished, it follows as before that we can write

$$\nu_{n_0+1,n_0} = f(T) \cdot Q(T) + p \cdot A(T),$$

for some $Q(T), A(T) \in \mathbb{Z}_p[T]$. It follows that

$$\omega_{n_0+1} = f(T) \cdot q_2(T) + p^2 \cdot r_2(T),$$

for some $q_2(T), r_2(T) \in \mathbb{Z}_p[T]$. Setting $k = n_0 - 1$, the result follows by induction.

□

We can now prove the following result, which we will use later in Section 3.4 to show how one can define a homomorphism from the radical of such an extension $\mathbb{M}/\mathbb{K}_\infty$ to ideal classes.

Proposition 3.3. *Let $\mathbb{K}$ be number field containing ζ_p and let $\mathbb{K}_\infty$ be its cyclotomic $\mathbb{Z}_p$-extension. Let $\mathbb{M}/\mathbb{K}$ be a Galois extension with the property that $\mathbb{K}_\infty \subset \mathbb{M}$ and $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a free $\mathbb{Z}_p$-module of finite rank. Then there exists a constant $k \geq 0$ such that for all sufficiently large n the extension $\mathbb{M}_n$ is abelian over $\mathbb{K}_{n+k}$. In particular, one can choose the generators of R_n to be elements of $\mathbb{K}_{n+k}$ for all sufficiently large n.*

Proof. Let R be the radical of $\mathbb{M}/\mathbb{K}_\infty$. We saw that under the given assumptions, R is a torsion-free $\mathbb{Z}_p$-module of rank r. Since $\mathbb{M}/\mathbb{K}$ is Galois, the group $\mathbb{M}/\mathbb{K}_\infty$ becomes a Λ-module as described above. Since it is a free $\mathbb{Z}_p$-module of finite rank, it follows that $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a Λ-torsion module and that its annihilator polynomial f is a distinguished polynomial. Furthermore, one has that

$$p - \mathrm{rank}(\mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty)) = \mathbb{Z}_p - \mathrm{rank}(\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)),$$

for all $n \geq 1$.

Let Ω_n denote the maximal p-abelian p-ramified extension of $\mathbb{K}_n$ and Ω_∞ be the maximal p-abelian p-ramified extension of $\mathbb{K}_\infty$. Then $\mathrm{Gal}(\Omega_\infty/\mathbb{K}_\infty)$ is a Λ-module and the above assumptions on $\mathbb{M}$ imply that for all $n \geq 1$,

$$\mathbb{M}_n \subset \Omega_\infty^{(p^n, f(T))},$$

where $(p^n, f(T))$ is the ideal of Λ generated by p^n and $f(T)$. By Lemma 3.2, there exists $k \geq 0$ such that $\omega_{n+k} \subset (p^n, f(T))$ for all $n \geq 0$. Since $\Omega_n = \Omega_\infty^{\omega_n}$, it follows that $\mathbb{M}_n \subset \Omega_{n+k}$ for all $n \geq 1$. Fix now a lift $\widetilde{\Gamma}$ of Γ to $\mathrm{Gal}(\mathbb{M}/\mathbb{K})$. Since $\mathbb{M}_n \subset \Omega_{n+k}$, it follows that $\mathbb{M}_n/\mathbb{K}_{n+k}$ is an abelian extension and thus one has an isomorphism

$$\mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_{n+k}) \cong \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty) \times \Gamma_{n+k},$$

where $\Gamma_n = \Gamma^{p^n}$. This isomorphism allows us to view Γ_{n+k} both as a subgroup and as a quotient of $\mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_{n+k})$.

For every $n \geq 1$, let $\widetilde{\mathbb{M}}_n = \mathbb{M}_n^{\Gamma_{n+k}}$. Then, since $\zeta_p \in \mathbb{K}$, one has that $\widetilde{\mathbb{M}}_n/\mathbb{K}_{n+k}$ is a Kummer extension and $\mathbb{M}_n = \mathbb{K}_\infty \cdot \widetilde{\mathbb{M}}_n$. This shows that the radical of $\mathbb{M}_n/\mathbb{K}_\infty$ can be defined by elements in $\mathbb{K}_{n+k}$ and completes our proof. □

The isomorphism (3.3) shows how the structure of the radical R can be related to the structure of $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ as $\mathbb{Z}_p$-modules. It turns out that whenever $\mathbb{M}/\mathbb{K}$ is Galois, the isomorphism (3.3) can be turned into a twisted isomorphism of Λ-modules and one can use this to relate the structure of $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ as a Λ-module to the one of R as a Λ-module. We first notice that if $\mathbb{M}/\mathbb{K}$ is Galois, then $\mathbb{M}_n/\mathbb{K}$ is also Galois for all $n \geq 1$ and there is thus an action of Γ on both $\mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty)$ and R_n. For $\gamma \in \Gamma$, $\sigma_n \in \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty)$ and $\alpha_n \in R_n$, we have

$$\langle \sigma_n, \alpha_n \rangle^\gamma = \langle \sigma_n^\gamma, \alpha_n^\gamma \rangle = \langle \sigma_n, \alpha_n \rangle^{\chi(\gamma)},$$

where $\chi : \Gamma \to \mathbb{Z}_p^\times$ is the cyclotomic character defined by

$$\zeta_{p^m}^\gamma = \zeta_{p^m}^{\chi(\gamma)}, \quad \text{for all } \gamma \in \Gamma \text{ and } m \geq 1.$$

It follows that

$$\langle \sigma^\gamma, \alpha \rangle = \langle \sigma, \alpha^{\gamma^*} \rangle,$$

where $\gamma^* := \chi(\gamma)\gamma^{-1}$. Notice that $* : \mathbb{Z}_p[\Gamma] \to \mathbb{Z}_p[\Gamma]$ is an involution (called *Iwasawa's involution*) and it can be extended to an involution of Λ by continuity. The action of Λ is compatible with the diagram (3.2) and in the projective limit we obtain

$$\langle \sigma^f, \alpha \rangle = \langle \sigma, \alpha^{f^*} \rangle,$$

for all $\sigma \in \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$, $\alpha \in R$ and $f \in \Lambda$.

The typical way in which one defines an action of Γ on $\mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)$ is via

$$\gamma\psi = \psi \circ \gamma^{-1} \quad \text{for all } \gamma \in \Gamma, \psi \in \mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p).$$

Let us define a new Γ-action on $\mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)$ by

$$\gamma\psi = \psi \circ \gamma^*,$$

and we extend it by linearity and continuity to an action of Λ. Following Iwasawa, we denote the resulting Λ-module by $\mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)^\bullet$, to distinguish it from the original one. One then obtains an isomorphism of Λ-modules

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \cong \mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)^\bullet. \tag{3.5}$$

Since $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a Λ-torsion module and a free $\mathbb{Z}_p$-module of finite rank, the structure theorem of Λ-modules ([Wa, Theorem 13.12]) implies that there exists an integer $k \geq 0$, positive integers $m_1, \ldots, m_k$, irreducible distinguished polynomials $f_1(T), \ldots, f_k(T)$, and an injective pseudo-isomorphism of Λ-modules

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \hookrightarrow \bigoplus_{i=1}^k \Lambda/\left(f_i^{m_i}\right).$$

The isomorphism (3.5) suggests that one might a have pseudo-isomorphism

$$R \hookrightarrow \bigoplus_{i=1}^k \Lambda/\left((f_i^*)^{m_i}\right),$$

where $* : \Lambda \to \Lambda$ denotes Iwasawa's involution. The following result shows that this is indeed the case.

Proposition 3.4. *Let p be an odd prime, let $\mathbb{K}$ be a number field containing ζ_p and let $\mathbb{K}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$. Let $\mathbb{M}/\mathbb{K}_\infty$ be an abelian p-extension with the property that* $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ *is a Λ-torsion module and a free $\mathbb{Z}_p$-module of finite rank, so that there exists an injective pseudo-isomorphism*

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \hookrightarrow \bigoplus_{i=1}^k \Lambda/\left(f_i^{m_i}\right),$$

for some positive integers k, $m_1, \ldots, m_k$ and some irreducible distinguished polynomials $f_1(T)$, $\cdots$, $f_k(T)$. Let R denote the radical of the extension $\mathbb{M}/\mathbb{K}_\infty$. Then there exists an injective pseudo-isomorphism of Λ-modules

$$R \hookrightarrow \bigoplus_{i=1}^{k} \Lambda / \left((f_i^*)^{m_i} \right).$$

Proof. Let $X = \mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$. If we denote

$$f_X(T) = \prod_{i=1}^{k} f_i(T)^{m_i}$$

and

$$\Lambda_X = \mathbb{Z}_p[T]/(f_X(T)),$$

it follows that $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ becomes a module over $\tilde{\Lambda}_X := \Lambda_X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. It also follows that

$$X \otimes \mathbb{Q}_p \cong \bigoplus_{i=1}^{k} \tilde{\Lambda}_X / \left(f_i^{m_i} \right).$$

Now let $x \in X \otimes \mathbb{Q}_p$ be such that $\tilde{\Lambda} x$ generates $\tilde{\Lambda} / \left(f_1^{m_1} \right)$ and

$$\tilde{\Lambda} x \cong \tilde{\Lambda} / \left(f_1^{m_1} \right).$$

Let $d = \deg(f_1^{m_1})$. Then a $\mathbb{Q}_p$-basis for $\tilde{\Lambda} x$ is given by

$$\mathcal{X} = \{\tau^i x : i = 0, \ldots, d-1\}.$$

We construct a dual basis $\mathcal{R}$ to $\mathcal{X}$ as follows. First, since we have a perfect bilinear pairing

$$\langle \cdot, \cdot \rangle : R \otimes \mathbb{Q}_p, X \otimes \mathbb{Q}_p \to \mathbb{Q}_p,$$

we can choose $\rho \in R \otimes \mathbb{Q}_p$ such that:

1) One has $\langle \rho, x \rangle = 1$ and
$$\langle \rho, \gamma^j x \rangle = 0 \text{ for all } j = 1, \ldots, d-1.$$

2) For every $y \in \bigoplus_{i=2}^{k} \tilde{\Lambda}_X / \left(f_i^{m_i} \right)$, one has
$$\langle \rho, y \rangle = 0.$$

Consider now the element $\gamma^\perp := (\gamma^*)^{-1}$. We claim that the set $\mathcal{R} := \{ \left(\gamma^\perp \right)^j \rho : j = 0, \ldots, d-1\}$ is a dual basis to $\mathcal{X}$. Indeed, from the properties of our pairing, it follows that for all $0 \leq j, k \leq d-1$ one has

$$\left\langle \left(\gamma^\perp \right)^j \rho, \gamma^k x \right\rangle = \langle \rho, \gamma^{k-j} x \rangle = \delta_{j,k}.$$

It follows by induction on k that there exists an isomorphism of $\tilde{\Lambda}_X$-modules

$$R \otimes \mathbb{Q}_p \cong \Lambda / (f_X^*) \otimes \mathbb{Q}_p.$$

Since R is free as a $\mathbb{Z}_p$-module, the conclusion follows. □

We conclude this section by studying a particular case that we will use for our application to Leopoldt's conjecture. Let $\mathbb{K}$ be a CM number field that is Galois over $\mathbb{Q}$ and contains the pth roots of unity. Assume in addition that $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$. As explained at the end of Section 3.1, an example of an infinite family of pairs $(\mathbb{K}, p)$ satisfying these conditions can be constructed by starting with a number field $\mathbb{E}$ and a prime p that splits completely in $\mathbb{E}$, taking $\mathbb{F}/\mathbb{E}$ to be its

Galois closure over $\mathbb{Q}$ and taking $\mathbb{K} = \mathbb{F}(\zeta_p)$. Let $\mathcal{Z}(\mathbb{K}^+)$ be the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{K}^+$ and consider the extension $\mathbb{M} = \mathcal{Z}(\mathbb{K}^+) \cdot \mathbb{K}_\infty$ of $\mathbb{K}_\infty$. Notice that the extension $\mathcal{Z}(\mathbb{K}^+)/\mathbb{Q}$ is Galois. Indeed, if $\sigma : \mathcal{Z}(\mathbb{K}^+) \hookrightarrow \overline{\mathbb{Q}}$ is an injective homomorphism fixing $\mathbb{Q}$, then $\sigma(\mathbb{K}^+) = \mathbb{K}^+$, since $\mathbb{K}^+/\mathbb{Q}$ is Galois. It follows that σ induces an isomorphism

$$\mathrm{Gal}(\mathcal{Z}(\mathbb{K}^+)/\mathbb{K}^+) \cong \mathrm{Gal}\left(\sigma\left(\mathcal{Z}(\mathbb{K}^+)\right)/\mathbb{K}^+\right).$$

Since $\mathcal{Z}(\mathbb{K}^+)$ is the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{K}^+$, it follows that $\sigma\left(\mathcal{Z}(\mathbb{K}^+)\right) = \mathcal{Z}(\mathbb{K}^+)$. Since σ was arbitrary, it follows that $\mathcal{Z}(\mathbb{K}^+)/\mathbb{Q}$ is a Galois extension, as claimed. It follows that $\mathbb{M} = \mathcal{Z}(\mathbb{K}^+) \cdot \mathbb{K}_\infty$ is the compositum of two Galois extensions of $\mathbb{Q}$, hence $\mathbb{M}/\mathbb{Q}$ is also Galois. The same argument as above shows that the extensions $\mathbb{M}_n/\mathbb{Q}$ are also Galois for all $n \geq 1$.

We can now discuss how we will use Leopoldt's reflection in our setting. Let $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ and $\mathcal{G} = \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{Q})$. Then $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$ implies that there exists a canonical isomorphism $\mathcal{G} \cong \Gamma \times G$, which allows us to view G both as a subgroup and as a quotient of $\mathcal{G}$. In what follows, G will be viewed as a subgroup of $\mathcal{G}$. Let $\chi : \mathcal{G} \to \mathbb{Z}_p^\times$ denote the cyclotomic character, defined as before by

$$\zeta_{p^m}^g = \zeta_{p^m}^{\chi(g)}, \quad \text{for all } g \in \mathcal{G}.$$

Moreover, since

$$\varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})] \cong \Lambda[G],$$

one can extend the action of $*$ to the whole group ring $\Lambda[G]$ and $*$ becomes an involution of $\Lambda[G]$ (also known as *Leopoldt's involution*). If we let $\mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)^\bullet$ be the $\Lambda[G]$-module on which $f \in \Lambda[G]$ acts by

$$f\psi = \psi \circ f^*,$$

then similarly as above, we obtain an isomorphism of $\Lambda[G]$-modules

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \cong \mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)^\bullet.$$

In particular, there exists an isomorphism of $\mathbb{Z}_p[G]$-modules

$$\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) \cong \mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)^\bullet. \tag{3.6}$$

Since the map $* : \mathbb{Z}_p[G] \to \mathbb{Z}_p[G]$ is an involution, it follows that for $X = \mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)$ or $X = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty), \mathbb{Z}_p)$, if X is a pseudo-cyclic $\mathbb{Z}_p[G]$-module, then $X^\bullet$ is also a pseudo-cyclic $\mathbb{Z}_p[G]$-module and vice-versa. In Section 3.3 we will prove that $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module. The following result shows that this implies that R is also a pseudo-cyclic $\mathbb{Z}_p[G]$-module.

Proposition 3.5. *If G is a finite group and N is a free $\mathbb{Z}_p$-module of finite rank with the property that N is a pseudo-cyclic $\mathbb{Z}_p[G]$-module, then the dual $\mathrm{Hom}_{\mathbb{Z}_p}(N, \mathbb{Z}_p)$ is also a pseudo-cyclic $\mathbb{Z}_p[G]$-module.*

To prove Proposition 3.5, we will need the following auxiliary lemma.

Lemma 3.6. *Let N be a finitely generated $\mathbb{Z}_p$-module and let G be a finite group which acts on N, so that N is also a $\mathbb{Z}_p[G]$-module. Then there exists an element $m \in N$ such that $m^{\mathbb{Z}_p[G]}$ has finite index N if and only if $N \otimes_{Z_p} \mathbb{Q}_p$ is a cyclic $\mathbb{Q}_p[G]$-module.*

Proof. Let $m_1, \ldots m_r$ be generators of N as a $\mathbb{Z}_p$-module. Then $\widetilde{m_j} = m_j \otimes_{\mathbb{Z}_p} 1$ are generators for $N \otimes \mathbb{Q}_p$ as a $\mathbb{Q}_p$-module.

The existence of an element $m \in N$ such that $m^{\mathbb{Z}_p[G]}$ has finite index N is equivalent to the existence of an element $a \in \mathbb{Z}$ such that $m_j^a \in m^{\mathbb{Z}_p[G]}$ for all $j = 1, \ldots, r$. This in turn is equivalent to the fact that $\widetilde{m} = m \otimes \frac{1}{a}$ generates $N \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as a $\mathbb{Q}_p[G]$-module.

□

Proof of Proposition 3.5. By Lemma 3.6, $N \otimes \mathbb{Q}_p$ is a cyclic $\mathbb{Q}_p[G]$-module. By Maschke's theorem, $N \otimes \mathbb{Q}_p$ is isomorphic to a direct summand of $\mathbb{Q}_p[G]$. It is well-known (see for example [Car, Theorem 2.5]) that there exists an isomorphism of $\mathbb{Q}_p[G]$-modules

$$\mathbb{Q}_p[G] \cong \mathrm{Hom}_{\mathbb{Q}_p}(\mathbb{Q}_p[G], \mathbb{Q}_p).$$

It follows that $\mathrm{Hom}_{\mathbb{Q}_p}(N \otimes \mathbb{Q}_p)$ is isomorphic to a direct summand of $\mathbb{Q}_p[G]$ and, therefore, the module $\mathrm{Hom}_{\mathbb{Q}_p}(N \otimes \mathbb{Q}_p)$ is $\mathbb{Q}_p[G]$-cyclic. Since there exists a canonical isomorphism of $\mathbb{Q}_p[G]$-modules

$$\mathrm{Hom}_{\mathbb{Q}_p}(N \otimes \mathbb{Q}_p) \cong \mathrm{Hom}_{\mathbb{Z}_p}(N, \mathbb{Z}_p) \otimes \mathbb{Q}_p,$$

it follows that $\mathrm{Hom}_{\mathbb{Z}_p}(N, \mathbb{Z}_p) \otimes \mathbb{Q}_p$ is a cyclic $\mathbb{Q}_p[G]$-module. By Lemma 3.6, it follows that $\mathrm{Hom}_{\mathbb{Z}_p}(N, \mathbb{Z}_p)$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module, as we wanted. □

3.3 Structure theorems for groups and quotients of local units

Let $\mathbb{K}$ be a number field that is Galois over $\mathbb{Q}$ with Galois group G and let p be an odd rational prime. We let s denote the number of primes in $\mathbb{K}$ lying above p and we denote these primes by $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$.

Let $\mathfrak{p} = \mathfrak{p}_1$, let $G_{\mathfrak{p}}$ denote the decomposition group of $\mathfrak{p}$ at p and let $\{g_1, \ldots, g_s\}$ be a set of left coset representatives of $G_{\mathfrak{p}}$ in G, such that

$$g_i(\mathfrak{p}) = \mathfrak{p}_i, \text{ for all } i = 1, \ldots, s.$$

For any $j = 1, \ldots, s$, we denote by $\mathbb{K}_{\mathfrak{p}_j}$ the completion of $\mathbb{K}$ at $\mathfrak{p}_j$, by $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}_j}}$ the usual discrete valuation subring of $\mathbb{K}_{\mathfrak{p}_j}$ and by $U_{1,\mathfrak{p}_j}$ the group of local units which are 1 modulo $\mathfrak{p}_j$. Since $\mathcal{O}_{\mathbb{K}_{\mathfrak{p}_j}} \cong \varprojlim_n \mathcal{O}_{\mathbb{K}}/\mathfrak{p}_j^n$, we can identify an element $u \in U_{1,\mathfrak{p}}$ with a sequence

$$u = (1, u_2, u_3, \ldots),$$

with $u_n \in \mathcal{O}_{\mathbb{K}}$ for all $n \geq 2$. It follows that

$$g_j(u) := (1, g_j(u_2), g_j(u_3), \ldots)$$

represents an element in $U_{1,\mathfrak{p}_j}$ and in this way g_j induces an isomorphism between $U_{1,\mathfrak{p}}$ and $U_{1,\mathfrak{p}_j}$.

It is an elementary check that $U_{1,\mathfrak{p}}$ is a $\mathbb{Z}_p[G_{\mathfrak{p}}]$-module. Consider now the group

$$U_1 := \prod_{i=1}^{s} U_{1,\mathfrak{p}_i} = \prod_{i=1}^{s} U_{1,g_i(\mathfrak{p})}.$$

The action of $G_{\mathfrak{p}}$ on $U_{1,\mathfrak{p}}$ induces an action of G on U_1 as follows.

For every $g \in G$ and every $i \in \{1, \ldots, s\}$, there exist elements $l(i) \in \{1, \ldots, s\}$ and $h \in G_{\mathfrak{p}}$ such that

$$g \cdot g_i = g_{l(i)} h,$$

which is just a rephrasing of the fact $\{g_1, \ldots, g_s\}$ is a complete set of coset representatives for $G_{\mathfrak{p}}$ in G. Now, given $u_i \in U_{g_i(\mathfrak{p})}$, it follows from the isomorphism induced by g_i that $u_i = g_i(u)$ for some $u \in U_{1,\mathfrak{p}}$. We define

$$g(1, \ldots, \underbrace{u_i}_{\substack{\uparrow \\ i\text{th entry}}}, 1, \ldots, 1) = (1, \ldots, \underbrace{g_{l(i)}\left(u^h\right)}_{\substack{\uparrow \\ l(i)\text{th entry}}}, 1, \ldots, 1),$$

and extend this multiplicatively for each coordinate i. A simple check shows that the result is independent of the choice of coset representatives. In this manner, we obtain a $\mathbb{Z}_p[G]$-representation of U_1 which is induced from the $\mathbb{Z}_p[G_{\mathfrak{p}}]$-representation of $U_{1,\mathfrak{p}}$.

The structure of $U_1(\mathbb{K})$ as a $\mathbb{Z}_p[G]$-module is described in the following result.

Lemma 3.7. *The module U_1 is a $\mathbb{Z}_p$-module of rank $|G|$ and also a pseudo-cyclic $\mathbb{Z}_p[G]$-module, i.e. there exists an element $u \in U_1$ such that*

$$[U_1 : u^{\mathbb{Z}_p[G]}] < \infty.$$

Proof. By the construction of U_1 as a $\mathbb{Z}_p[G]$-module, it suffices to prove that $U_{1,\mathfrak{p}}$ is pseudo-cyclic as a $\mathbb{Z}_p[G_{\mathfrak{p}}]$-module.

We denote by e and f the ramification degree and the residue field degree of $\mathfrak{p}$ at p, respectively. For $n \geq 1$, let $U_{n,\mathfrak{p}}$ denote the group of local units in $\mathbb{K}_{\mathfrak{p}}$ which are 1 modulo $\mathfrak{p}^n$. In view of the isomorphism $U_{n,\mathfrak{p}}/U_{n+1,\mathfrak{p}} \cong \left(\mathcal{O}_{\mathbb{K}_{\mathfrak{p}}}/\mathfrak{p}, +\right)$ (see [Neu 1, Chapter III, Proposition 1.1]) we then know that $|U_{n,\mathfrak{p}}/U_{n+1,\mathfrak{p}}| = p^f$. Moreover, for $n \geq e/(p-1)$, we have the isomorphisms of $\mathbb{Z}_p[G_{\mathfrak{p}}]$-modules

$$U_{n,\mathfrak{p}} \cong \mathfrak{p}^n \cong (\mathcal{O}(\mathbb{K}_{\mathfrak{p}}), +),$$

where the first isomorphism is given by the logarithmic map and has the exponential map as an inverse (see for example [Neu 1, Chapter III, Theorem 1.2]).

Therefore, it suffices to find an element $a \in \mathcal{O}(\mathbb{K}_{\mathfrak{p}})$ such that $\mathbb{Z}_p[G_{\mathfrak{p}}]a$ generates a subgroup of finite index in $(\mathcal{O}(\mathbb{K}_{\mathfrak{p}}), +)$. But this is now easy, since $\mathbb{K}_{\mathfrak{p}}$ is cyclic as a $\mathbb{Q}_p[G_{\mathfrak{p}}]$ module, so we can choose $\alpha \in \mathbb{K}_{\mathfrak{p}}$ such that $\{g\alpha : g \in G_{\mathfrak{p}}\}$ is a basis for $(\mathbb{K}_{\mathfrak{p}}, +)$ as a $\mathbb{Q}_p$-module. By multiplying α by a sufficiently large power of p if necessary, we can ensure that all $g\alpha$'s are in $\mathcal{O}(\mathbb{K}_{\mathfrak{p}})$. Then $\mathbb{Z}_p[G_{\mathfrak{p}}]\alpha$ has the same $\mathbb{Z}_p$-rank as $\mathcal{O}(\mathbb{K}_{\mathfrak{p}})$, so it generates a subgroup of finite index in $\mathcal{O}(\mathbb{K}_{\mathfrak{p}})$. This completes our proof. □

Remark 3.8. *i) Notice that the above result generalises the well-known result from class field theory which asserts that* $U_1 \cong (\text{finite}) \times \mathbb{Z}_p^{[\mathbb{K}:\mathbb{Q}]}$ *(see for example the discussion after [Wa, Lemma 13.5]). The local analysis can be generalised further to Galois extensions of local fields of characteristic* 0*, as illustrated for example in the first proof of [Ca-Fro, Chapter VI, Proposition 3].*

ii) We saw in the proof of Lemma 3.7 *that for any* $n \geq 1$*, the quotient* $U_{1,\mathfrak{p}}/U_{n,\mathfrak{p}}$ *is a finite group whose order is a power of* p*. Since for a sufficiently large* n *one has* $U_{n,\mathfrak{p}} \cong \mathbb{Z}_p^{e \cdot f}$*, using the fact that* $\mathbb{Z}_p$ *has no finite subgroups, it follows that the torsion subgroup of* $U_{1,\mathfrak{p}}$ *must consist only of* p*-power roots of unity.*

Let $E(\mathbb{K})$ denote the group of units in $\mathbb{K}$. For an element $\alpha \in \mathbb{K}$ and a non-archimedean prime $\mathfrak{q}$ of $\mathbb{K}$, we denote by $\alpha_{\mathfrak{q}}$ the image of α under the embedding $\mathbb{K} \hookrightarrow \mathbb{K}_{\mathfrak{q}}$. There exists a diagonal embedding of $E(\mathbb{K})$ into $\prod_{j=1}^{s} \mathcal{O}^*_{\mathbb{K}_{\mathfrak{p}_j}}$ given by

$$\varepsilon \to (\varepsilon_{\mathfrak{p}_1}, \varepsilon_{\mathfrak{p}_2}, \ldots, \varepsilon_{\mathfrak{p}_s}) .$$

Let E_1 denote the subgroup of $E(\mathbb{K})$ consisting of those units whose image under the above embedding lies in U_1. Notice that if $\varepsilon \in E$, then $\varepsilon_{\mathfrak{p}_i}^{N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{p}_i)-1} \in U_{1,\mathfrak{p}_i}$, hence E_1 has finite index in E (and in particular, the same $\mathbb{Z}$-rank). We denote by $\overline{E}_1$ the p-adic closure of the image of E_1 into U_1. The kernel of the embedding $E(\mathbb{K}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \to U_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p$, sometimes denoted $\Delta(\mathbb{K})$, is called the *Leopoldt kernel* and its $\mathbb{Z}_p$-rank, usually denoted by $\delta(\mathbb{K})$, is called the *Leopoldt defect.*

Let $\Omega(\mathbb{K})$ denote the maximal p-abelian p-ramified extension of $\mathbb{K}$ and let $\mathbb{H}(\mathbb{K})$ denote the p-part of the Hilbert class field of $\mathbb{K}$. An important application of global class field theory asserts that there exists an isomorphism of $\mathbb{Z}_p$-modules

$$U_1/\overline{E}_1 \cong \mathrm{Gal}\left(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K})\right) .$$

For a proof of this fact, see for example [Neu 1, Chapter IV, Theorem 7.8]. We will now explain why the above isomorphism is actually one of $\mathbb{Z}_p[G]$-modules, with $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ as before. In general, we know from class field theory that given a tower of extensions $\mathbb{M}/\mathbb{L}/\mathbb{F}$ with $\mathbb{M}/\mathbb{F}$ a Galois extension and $\mathbb{M}/\mathbb{L}$ an abelian extension, the group $\mathrm{Gal}(\mathbb{M}/\mathbb{F})$ is isomorphic to some corresponding group of ideles as $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$-modules as well. It thus suffices to show how the fact that $\mathbb{K}/\mathbb{Q}$ is a Galois extension implies that both $\mathbb{H}(\mathbb{K})/\mathbb{Q}$ and $\Omega(\mathbb{K})/\mathbb{Q}$ are Galois extensions. Such arguments are often referred to as *maximality arguments* in the literature, but because they are usually just stated or left as an exercise, we will give below an example of such an argument for completeness. We will only prove that $\Omega(\mathbb{K})/\mathbb{Q}$ is a Galois extension, since the proof for $\mathbb{H}(\mathbb{K})/\mathbb{K}$ is essentially the same (yet simpler, since we are dealing with a finite extension).

Lemma 3.9. *Let* $\mathbb{K}$ *be a finite Galois extension of* $\mathbb{Q}$ *and let* $\Omega(\mathbb{K})$ *be the maximal* p*-abelian,* p*-ramified extension of* $\mathbb{K}$*. Then* $\Omega(\mathbb{K})$ *is a Galois extension of* $\mathbb{Q}$*.*

Proof. The proof follows a similar strategy to the one we used for proving that $\mathcal{Z}(\mathbb{K}^+)/\mathbb{Q}$ is a Galois extension at the end of Section 3.2. We begin by fixing an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ for which $\Omega(\mathbb{K}) \subset \overline{\mathbb{Q}}$. Let now $\sigma : \Omega(\mathbb{K}) \hookrightarrow \overline{\mathbb{Q}}$ be an injection (which fixes $\mathbb{Q}$). Then $\sigma(\mathbb{K}) \subseteq \mathbb{K}$, since the extension $\mathbb{K}/\mathbb{Q}$ is Galois. So in fact we must have $\sigma(\mathbb{K}) = \mathbb{K}$. Therefore, σ induces an isomorphism $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}) \cong \mathrm{Gal}(\sigma\left(\Omega(\mathbb{K})\right)/\mathbb{K})$.

Moreover, the extension $\sigma(\Omega(\mathbb{K}))/\mathbb{K}$ is unramified outside p, because $\Omega(\mathbb{K})/\mathbb{K}$ is (if $\mathfrak{Q}$ is a prime in $\Omega(\mathbb{K})$ lying above a prime $\mathfrak{q}$ of $\mathbb{K}$, then $\sigma(\mathfrak{Q})$ lies above $\sigma(\mathfrak{q})$, and as an automorphism of $\mathbb{K}$, σ permutes the primes above a given rational prime). It follows that $\Omega(\mathbb{K})\sigma(\Omega(\mathbb{K}))$ (compositum inside $\overline{\mathbb{Q}}$) is a p-abelian Galois extension of $\mathbb{K}$ which is unramified outside p. Hence, by the maximality of $\Omega(\mathbb{K})$, this shows that $\sigma(\Omega(\mathbb{K})) = \Omega(\mathbb{K})$. As σ was an arbitrary $\mathbb{Q}$-injection, we conclude that $\Omega(\mathbb{K})$ is a Galois extension of $\mathbb{Q}$. □

Combining the above lemma with the observations preceding it, it follows that one has an isomorphism of $\mathbb{Z}_p[G]$-modules

$$U_1/\overline{E}_1 \cong \mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))\,. \tag{3.7}$$

The group G acts on $U_1/\overline{E}_1$ via its action on U_1 described above, while its action on the group $\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))$ is given by inner automorphisms.

Let $\mathbb{K}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$. Since $\mathbb{K}/\mathbb{Q}$ is a Galois extension, so is $\mathbb{K}_\infty/\mathbb{Q}$, since $\mathbb{K}_\infty$ is the compositum of $\mathbb{K}$ and $\mathbb{Q}_\infty$ (the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$), both of which are Galois over $\mathbb{Q}$. By the maximality of $\Omega(\mathbb{K})$, it also follows that $\mathbb{K}_\infty \subset \Omega(\mathbb{K})$. It follows that $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)$ is also a $\mathbb{Z}_p[G]$-module. In Lemma 3.7 we proved that U_1 is a pseudo-cyclic $\mathbb{Z}_p[G]$-module, which combined with the isomorphism (3.7) imply that $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module. From the Iwasawa-theoretic point of view, there are at least two natural questions that one can ask:

1) What can one say about the structure of $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)$ as a $\mathbb{Z}_p[G]$-module?

2) If we derive the equivalent of (3.7) at every finite level $\mathbb{K}_n$ in the cyclotomic tower, is there some compatibility between these isomorphisms? If so, what happens when we pass to the projective limit?

The rest of this section will be dedicated to answering these two questions. The answer to the first question will also play a key role in our application to Leopoldt's conjecture. We begin by addressing this one, since it is also significantly easier to handle.

We first notice that since U_1 is a finitely generated $\mathbb{Z}_p$-module, by (3.7), so is $\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))$. Since $\mathbb{Z}_p$ is a Principal Ideal Domain, the $\mathbb{Z}_p$-submodule $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty\cdot\mathbb{H}(\mathbb{K}))$ of $\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))$ must also be a finitely generated $\mathbb{Z}_p$-module. Moreover, since both $\mathbb{K}_\infty$ and $\mathbb{H}(\mathbb{K})$ are Galois extensions of $\mathbb{Q}$, it follows that $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty\cdot\mathbb{H}(\mathbb{K}))$ is also a $\mathbb{Z}_p[G]$-module. Since

$$|\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty) : \mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty\cdot\mathbb{H}(\mathbb{K}))| < \infty,$$

it follows that $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module if and only if $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty\cdot\mathbb{H}(\mathbb{K}))$ is.

The isomorphism (3.7) together with Lemma 3.7 show that $\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module. By Lemma 3.6, it follows that $\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))\otimes\mathbb{Q}_p$ is a cyclic $\mathbb{Q}_p[G]$-module. We also know that $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty\cdot\mathbb{H}(\mathbb{K}))\otimes\mathbb{Q}_p$ is a $\mathbb{Q}_p[G]$-submodule of $\mathrm{Gal}\,(\Omega(\mathbb{K})/\mathbb{H}(\mathbb{K}))\otimes\mathbb{Q}_p$. By Maschke's theorem, a submodule of $\mathbb{Q}_p[G]$ is a direct summand. It follows that the group $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty\cdot\mathbb{H}(\mathbb{K}))\otimes\mathbb{Q}_p$ is a cyclic $\mathbb{Q}_p[G]$-module. Using Lemma 3.6 again, we obtain the following result.

Proposition 3.10. *Let $\mathbb{K}$, $\mathbb{K}_\infty$, and $\Omega(\mathbb{K})$ be defined as above. Then the group* $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)$ *is a pseudo-cyclic $\mathbb{Z}_p[G]$-module.*

To answer our second question, we let

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_\infty$$

be the layers in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$. Since $\mathbb{K}/\mathbb{Q}$ is Galois, so are the extensions $\mathbb{K}_n/\mathbb{Q}$ (for any $n \geq 0$) and $\mathbb{K}_\infty/\mathbb{Q}$, respectively. For every $n \geq 0$ we let $G_n = \mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})$.

Note that the primes above p are totally ramified in the extension $\mathbb{K}_\infty/\mathbb{K}$. For every $n \geq 0$, we let $\mathfrak{p}_{n,1}, \dots, \mathfrak{p}_{n,s}$ denote the primes in $\mathbb{K}_n$ lying above p and for $1 \leq j \leq s$ we write $\mathbb{K}_{\mathfrak{p}_{n,j}}$ to denote the completion of $\mathbb{K}_n$ at $\mathfrak{p}_{n,j}$. We also define

$$U_1(\mathbb{K}_n) = \prod_{j=1}^{s} U_{n,j},$$

where for $1 \leq j \leq s$, $U_{n,j}$ denotes the group of units in $\mathbb{K}_{\mathfrak{p}_{n,j}}$ which are 1 modulo $\mathfrak{p}_{n,j}$.

For every $n \geq m \geq 0$, the global norm map $N_{\mathbb{K}_n/\mathbb{K}_m}$ induces a map between the groups of ideles $\mathbb{I}_{\mathbb{K}_n} \to \mathbb{I}_{\mathbb{K}_m}$ defined as follows. For a prime $\mathfrak{Q} \in \mathbb{K}_n$ lying above a prime $\mathfrak{q}$ of $\mathbb{K}_m$, there exists a norm map on the completions $N_{\mathfrak{Q}/\mathbb{Q}} : \mathbb{K}_{n,\mathfrak{Q}} \to \mathbb{K}_{m,\mathfrak{q}}$; for an element

$$x = (\dots, x_{\mathfrak{Q}}, \dots) \in \mathbb{I}_{\mathbb{K}_n},$$

one defines

$$N_{\mathbb{K}_n/\mathbb{K}_m}(x) = (\dots, y_{\mathfrak{q}}, \dots) \in \mathbb{I}_{\mathbb{K}_m},$$

where

$$y_{\mathfrak{q}} = \prod_{\mathfrak{Q}|\mathfrak{q}} N_{\mathfrak{Q}/\mathbb{Q}}(x_{\mathfrak{Q}}).$$

Since one can view $U_1(\mathbb{K}_n)$ as a subgroup of $\mathbb{I}_{\mathbb{K}_n}$ (just put 1 at all other places), it follows that one can define a norm map $N_{\mathbb{K}_n/\mathbb{K}_m} : U_1(\mathbb{K}_n) \to U_1(\mathbb{K}_m)$ by

$$N_{\mathbb{K}_n/\mathbb{K}_m}(u_{1,n}, \dots, u_{s,n}) = \left(N_{\mathbb{K}_{\mathfrak{p}_{n,1}}/\mathbb{K}_{\mathfrak{p}_{m,1}}}(u_{1,n}), \dots, N_{\mathbb{K}_{\mathfrak{p}_{n,s}}/\mathbb{K}_{\mathfrak{p}_{m,s}}}(u_{s,n}) \right).$$

We define

$$U_\infty^1 = \varprojlim_n U_1(\mathbb{K}_n) \text{ and } E_\infty^1 = \varprojlim_n \overline{E_1(\mathbb{K}_n)},$$

where the projective limits are taken with respect to the norm maps described above.

For every $n \geq 0$, we let Ω_n (resp. $\mathbb{H}_n$) denote the maximal p-abelian p-ramified (resp. everywhere unramified) extension of $\mathbb{K}_n$ and

$$\Omega_\infty = \bigcup_{n \geq 0} \Omega_n, \quad \mathbb{H}_\infty = \bigcup_{n \geq 0} \mathbb{H}_n.$$

We will need the following auxiliary result, which uses the full power of class field theory.

Lemma 3.11. *For every $n \geq m \geq 0$, one has a commutative diagram*

$$\begin{tikzcd}
U_1(\mathbb{K}_n)/\overline{E_1(\mathbb{K}_n)} \arrow[r, "\sim"] \arrow[d, "N_{n,m}"] & \mathrm{Gal}(\Omega_n/\mathbb{H}_n) \arrow[d, "\mathrm{Res}"] \\
U_1(\mathbb{K}_m)/\overline{E_1(\mathbb{K}_m)} \arrow[r, "\sim"] & \mathrm{Gal}(\Omega_m/\mathbb{H}_m).
\end{tikzcd}$$

The horizontal maps are isomorphisms of $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})]$-modules (resp. of $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_m/\mathbb{Q})]$-modules) induced by the Artin map, the first vertical map is the norm map $N_{n,m}$, while the second vertical map is the restriction between Galois groups.

Proof. The fact that the horizontal maps are isomorphisms of $\mathbb{Z}_p$-modules is a consequence of class field theory (see for example [Neu 1, Chapter IV, Theorem 7.8]). The fact that this isomorphism is compatible with the indicated group action follows from the equivariance of the Artin map, combined with the fact that for all $n \geq 0$, by a maximality argument like the one in Lemma 3.9, both Ω_n and $\mathbb{H}_n$ are Galois extensions of $\mathbb{Q}$.

The commutativity of the diagram when the objects are considered solely as $\mathbb{Z}_p$-modules is provided again by class field theory ([Neu 1, Chapter IV, Proposition 6.1]). Compatibility with the group action follows from the fact that for any $n \geq 0$, the subgroup $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K})$ is central in $\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})$ (and thus the norm map $N_{n,m}$ commutes with any element in $\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})$). The result follows. □

Let $\mathcal{G}$ denote the Galois group $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{Q})$. We define the Iwasawa algebra of $\mathcal{G}$ in the usual way as

$$\Lambda_{\mathcal{G}} = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})].$$

It is easy to see from the definition that if $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$, then

$$\Lambda_{\mathcal{G}} \cong \Lambda[G],$$

where Λ is the Iwasawa algebra of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$.

For the rest of this section, we assume that one has $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$. By Lemma 3.11, it follows that there is an isomorphism of $\Lambda[G]$-modules

$$U^1_\infty/E^1_\infty \cong \mathrm{Gal}(\Omega_\infty/\mathbb{H}_\infty), \tag{3.8}$$

where $\mathbb{H}_\infty$ is the maximal p-abelian everywhere unramified extension of $\mathbb{K}_\infty$.

The isomorphisms $\mathrm{Gal}(\Omega_n/\mathbb{H}_n) \cong U_1(\mathbb{K}_n)/\overline{E_1(\mathbb{K}_n)}$ and (3.8) show that in order to understand the structure of $\mathrm{Gal}(\Omega_n/\mathbb{H}_n)$ (resp. of $\mathrm{Gal}(\Omega_\infty/\mathbb{H}_\infty)$) as $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_n/\mathbb{Q})]$-module (resp. as $\Lambda[G]$-module), one can focus on understanding the structure of $U_1(\mathbb{K}_n)/\overline{E_1(\mathbb{K}_n)}$ (resp. of U^1_∞/E^1_∞).

In view of Lemma 3.7, we already know that $U_1(\mathbb{K}_n)$ is pseudo-cyclic as a $\mathbb{Z}_p[G_n]$-module. If we fix $u_n \in U_1(\mathbb{K}_n)$ such that $u_n^{\mathbb{Z}_p[G_n]}$ has finite index in $U_1(\mathbb{K}_n)$, one may wonder what happens with this index as we let n vary. The rest of this section is dedicated to addressing this question. The result we prove generalizes a classical theorem of Iwasawa theory which treats the case $\mathbb{K} = \mathbb{Q}(\zeta_p)$ (see [Wa, Theorem 13.54]). We also refer the reader to [Gil 1] and [Ich] for related results when $\mathbb{K}/\mathbb{Q}$ is an abelian extension.

We begin by proving a more precise result about the structure of $U_1(\mathbb{K}_n)$ as a $\mathbb{Z}_p[G_n]$-module. For this, we will need the following result, which is a direct application of Kummer theory and local class field theory. This result (Lemma 3.12 below) was already discussed in [MS] and the idea of the proof together with the references contained in the proof are taken from [MS].

Lemma 3.12. *Let $\mathbf{K}$ be a finite extension of $\mathbf{Q}_p$ containing the pth roots of unity. For every positive integer $n \geq 0$, we consider the field $\mathbf{K}_n = \mathbf{K}(\zeta_{p^{n+1}})$, where ζ_{p^n} is a primitive p^nth root of unity, and we let U_n denote the group of principal units in $\mathbf{K}_n$. If we define the subgroup U'_n of U_n by*

$$U'_n := \{u \in U_n : N_{\mathbf{K}_n/\mathbb{Q}_p}(u) = 1\},$$

then for every $n \geq m \geq 0$, the norm map

$$N_{\mathbf{K}_n,\mathbf{K}_m} : U'_n \to U'_m$$

is surjective.

Proof. For a fixed $m \geq 0$, let $\mathcal{N}_m := \bigcap_{n \geq m} N_{\mathbf{K}_n,\mathbf{K}_m}(\mathbf{K}^*_n)$ denote the subgroup of universal cyclotomic norms. It is known (see for example the proof of [Be-Pa, Proposition 2.1]) that an element $x \in \mathbf{K}^*_m$ satisfies $x \in \mathcal{N}_m$ if and only if $N_{\mathbf{K}_m/\mathbf{Q}_p}(x) \in p^{\mathbb{Z}}$. It follows that $U_m \cap \mathcal{N}_m = U'_m$.

We now prove that for any $n \geq m \geq 0$, the norm map

$$N_{\mathbf{K}_n,\mathbf{K}_m} : U'_n \to U'_m$$

is surjective. Let $x \in U'_m = \mathcal{N}_m \cap U_m$ be arbitrary and let $V = N^{-1}_{n,m}(x)$. Then V is a closed subset, and since for every $n \geq 0$ the set U_n is a compact space, it follows that the sequence of sets

$$V \cap N_{n+1,n}(U_{n+1}) \supset V \cap N_{n+2,n}(U_{n+2}) \supset \dots$$

is a nested sequence of closed subsets in a compact space. It follows that $V \cap \mathcal{N}_n$ is non-empty and thus

$$N_{\mathbf{K}_n,\mathbf{K}_m} : U'_n \to U'_m$$

is surjective. □

Remark 3.13. *The above result generalizes [Wa, Lemma 13.53], which treats only the case* $\mathbf{K} = \mathbf{Q}_p(\zeta_p)$.

Assume from now on that $\zeta_p \in \mathbb{K}$. For each $n \geq 0$ and for every $j = 1, \dots, s$, we define the group

$$U'_{n,j} = \{u \in U_{n,j} : N_{\mathbb{K}_{n,\mathfrak{p}_{n,j}}/\mathbb{Q}_p}(u) = 1\}.$$

From Lemma 3.12, it follows that

$$U^1_\infty = \prod_{j=1}^{s} \varprojlim_n U'_{n,j}. \tag{3.9}$$

We will now study the structure of $U'_{n,j}$ as a module over the group ring $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_{n,\mathfrak{p}_{n,j}}/\mathbb{Q}_p]$. Let $1 \leq j \leq s$ be arbitrary. We denote the Galois group $\mathrm{Gal}(\mathbb{K}_{n,\mathfrak{p}_{n,j}}/\mathbb{Q}_p)$ by $G_{n,j}$. We could prove that $U'_{n,j}$ is a pseudo-cyclic $\mathbb{Z}_p[G_{n,j}]$-module using the same strategy that we used in Proposition 3.10 for showing that $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module. However, we will use a more explicit approach here.

Let $N_n \in \mathbb{Z}_p[G_{n,j}]$ denote the norm element

$$N_n = \sum_{g \in G_{n,j}} g.$$

We denote the norm from $\mathbb{K}_{n,\mathfrak{p}_{n,j}}$ to $\mathbb{K}_{m,\mathfrak{p}_{m,j}}$ by $N_{n,m}$. We know from Lemma 3.7 that $U_{n,j}$ is a pseudo-cyclic $\mathbb{Z}_p[G_{n,j}]$-module. Let u_n be a pseudo-generator for $U_{n,j}$. The map

$$\mathbb{Z}_p[G_{n,j}] \to u_n^{\mathbb{Z}_p[G_{n,j}]}$$

is a surjective homomorphism of $\mathbb{Z}_p$-modules of the same rank, hence also injective. It follows that $u_n^f = 1$ for some $f \in \mathbb{Z}_p[G_{n,j}]$ if and only if $f = 0$.

Let $a_j = |G_{0,j}|$. Then $|G_{n,j}| = p^n a_j$. Notice that the element $u_n^{p^n a_j - N_n}$ lies in $U'_{n,j}$. The following result shows that it is even a pseudo-generator for $U'_{n,j}$.

Lemma 3.14. *The group* $U'_{n,j}$ *is a pseudo-cyclic* $\mathbb{Z}_p[G_{n,j}]$*-submodule of* $U_{n,j}$*, of* $\mathbb{Z}_p$*-rank equal to* $p^n a_j - 1$.

Proof. The fact that $U'_{n,j}$ is a $\mathbb{Z}_p[G_{n,j}]$-module of rank equal to $p^n a_j - 1$ follows from local class field theory. Indeed, there is an exact sequence of $\mathbb{Z}_p[G_{n,j}]$-modules

$$\begin{tikzcd} 1 \arrow[r] & U'_{n,j} \arrow[r] & U_{n,j} \arrow[r, "N_n"] & \mathbb{Z}_p^\times \arrow[r] & F \arrow[r] & 1, \end{tikzcd}$$

where F is a finite group. In particular,

$$\mathbb{Z}_p - \mathrm{rank}(U'_{n,j}) = \mathbb{Z}_p - \mathrm{rank}(U^{(n)}_{1,\mathfrak{p}_{n,j}}) - 1.$$

We choose a pseudo-generator u_n of $U_{n,j}$ and note as above that the element $v_n := u_n^{p^n a_j - N_n}$ lies in $U'_{n,j}$. Notice also that the elements

$$\{v_n^{1-g} : g \in G_{n,j},\, g \neq 1\}$$

are $\mathbb{Z}_p$-independent. Indeed, a simple computation shows that

$$v_n^{1-g} = u_n^{p^n a_j (1-g)}.$$

Since the elements $\{1 - g : g \in G_{n,j},\, g \neq 1\}$ are $\mathbb{Z}_p$-independent in the group ring $\mathbb{Z}_p[G_{n,j}]$ and $u_n^f = 1$ if and only if $f = 0$, the claim follows.

It follows that the elements $\{v_n^{1-g} : g \in G_{n,j},\, g \neq 1\}$ generate a $\mathbb{Z}_p$-submodule of $U'_{n,j}$ of the same rank as $U'_{n,j}$. It follows that v_n is a pseudo-generator, which completes the proof. □

If u_n is a pseudo-generator for $U_{n,j}$, it follows from the proof of Lemma 3.14 that there is a pseudo-isomorphism of $\mathbb{Z}_p[G_{n,j}]$-modules

$$U_{n,j} \sim u_n^{N_n} \oplus U'_{n,j}. \tag{3.10}$$

Let $u_n \in U'_{n,j}$ be such that $u_n^{\mathbb{Z}_p[G_{n,j}]}$ has finite index in $U'_{n,j}$. We have a surjective homomorphism of $\mathbb{Z}_p$-modules

$$\mathbb{Z}_p[G_{n,j}]/(N_n) \to u_n^{\mathbb{Z}_p[G_{n,j}]},$$

and since both $\mathbb{Z}_p[G_{n,j}]/(N_n)$ and $u_n^{\mathbb{Z}_p[G_{n,j}]}$ are $\mathbb{Z}_p$-modules of the same rank, it follows that the homomorphism is injective. This is a very useful property which allows us to deduce more precise results about the $\mathbb{Z}_p[G_{n,j}]$-module $u_n^{\mathbb{Z}_p[G_{n,j}]}$. As a warm-up application, we will prove that the group $u_n^{\mathbb{Z}_p[G_{n,j}]}$ is torsion-free. Indeed, if ζ was a torsion element in $u_n^{\mathbb{Z}_p[G_{n,j}]}$, then

$$\zeta = u_n^{f_\zeta},$$

for some $f_\zeta \in \mathbb{Z}_p[G_{n,j}]$ and since ζ is torsion, we obtain further that

$$u_n^{af_\zeta} = 1, \text{ for some } a \in \mathbb{Z}_p.$$

But then we must have that af_ζ is a multiple of the norm in $\mathbb{Z}_p[G_{n,j}]$, hence

$$af_\zeta = N_n \cdot g_\zeta = N_n Tr(g_\zeta),$$

where $g_\zeta \in \mathbb{Z}_p[G_{n,j}]$ and, as usual, $Tr(g_\zeta)$ denotes the sum of the coefficients of g_ζ. It follows that $a \mid Tr(g_\zeta)$, from where we deduce that f_ζ is a multiple of N_n, hence $u_n^{f_\zeta} = 1 = \zeta$.

Let $W_{n,j}$ denote the torsion subgroup of $U_{n,j}$. If $\zeta \in W_{n,j}$, then ζ is a principal unit and thus $N_{\mathbb{K}_{n,j}/\mathbb{Q}_p}(\zeta)$ lies in a subgroup of $\mathbb{Z}_p^\times$ of the form $1 + p^m\mathbb{Z}_p$ for some $m \geq 1$. Since such groups have no non-trivial finite subgroups, it follows that $\zeta^{N_n} = 1$ and hence $W_{n,j} \subset U'_{n,j}$ (alternatively, one can use Remark 3.8 ii)). It is also easy to see that $W_{n,j}$ is a $\mathbb{Z}_p[G_{n,j}]$-submodule.

The above analysis shows that if u_n is a pseudo-generator for $U'_{n,j}$, then $u_n^{\mathbb{Z}_p[G_{n,j}]} \cap W_{n,j} = \emptyset$, hence $W_{n,j} \times u_n^{\mathbb{Z}_p[G_{n,j}]}$ is a well-defined $\mathbb{Z}_p[G_{n,j}]$-submodule of $U'_{n,j}$.

The following result shows that if $n \geq m \geq 0$, $u_m \in U'_{m.j}$ is a pseudo-generator, then we can find $u_n \in U'_{n,j}$ is such that u_n is a pseudo-generator for $U'_{n,j}$ and $N_{n,m}(u_n) = u_m$.

Lemma 3.15. *Let u_n be a pseudo-generator of $U'_{n,j}$. Then there exists a pseudo-generator $u_{n+1} \in U'_{n+1,j}$ such that $N_{n+1,n}(u_{n+1}) = u_n$.*

Proof. Let $w_{n+1} \in U'_{n+1,j}$ be a pseudo-generator and let z be such that $N_{n+1,n}(z) = u_n$. Let γ be a generator of $\mathrm{Gal}(\mathbb{K}_{n+1,\mathfrak{p}_j}/\mathbb{K}_{n,\mathfrak{p}_j})$ and $u_{n+1} = zw_{n+1}^{\gamma-1}$. Clearly, one has $N_{n+1,n}(u_{n+1}) = u_n$. Since u_n is a pseudo-generator of $U'_{n,j}$, it follows that if we can show that $u_{n+1}^{\mathbb{Z}_p[G_{n+1,j}]}$ contains the kernel of $N_{n+1,n}$ up to finite index, then by a simple rank comparison we obtain immediately that u_{n+1} is a pseudo-generator. To ease the explanations, we will tensor everything with $\mathbb{Q}_p$.

The kernel of $N_{n+1,n} : U'_{n+1,j} \otimes \mathbb{Q}_p \to U'_{n.j} \otimes \mathbb{Q}_p$ is generated by $w_{n+1}^{\gamma-1} \otimes 1$. Notice that since $\gamma^p = 1$, one has that

$$(\gamma - 1)^p = p(\gamma - 1)u(\gamma),$$

for some unit $u(\gamma) \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_{n+1,\mathfrak{p}_j}/\mathbb{K}_{n,\mathfrak{p}_j})]$.

It follows that

$$\begin{aligned} u_{n+1}^{(\gamma-1)^{p-1}} \otimes 1 &= z^{(\gamma-1)^{p-1}} w_{n+1}^{-p(\gamma-1)u(\gamma)} \otimes 1 \\ &= w_{n+1}^{(\gamma-1)((\gamma-1)^{p-2}f_n - pu(\gamma))} \otimes 1, \end{aligned}$$

for some element $f_n \in \mathbb{Q}_p[G_{n,j}]$ and a unit $u(\gamma) \in \mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_{n+1,\mathfrak{p}_j}/\mathbb{K}_{n,\mathfrak{p}_j})]$. We are left to show that $(\gamma - 1)^{p-2}f_n - pu(\gamma)$ is a unit in $\mathbb{Q}_p[G_{n,j}]$. There exist natural homomorphisms

$$\mathbb{Q}_p[G_{n+1,j}] \to \mathbb{Q}_p[G_{n,j}]$$

$$\mathbb{Q}_p[G_{n+1,j}] \to \mathbb{Q}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_p)]$$

which give a homomorphism

$$\phi : \mathbb{Q}_p[G_{n+1,j}] \to \mathbb{Q}_p[G_{n,j}] \times \mathbb{Q}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^{n+1}})/\mathbb{Q}_p)].$$

This homomorphism is injective because it is injective on $G_{n+1,j}$. It is an easy verification that the image of ϕ consists of the elements of the form (a, b) such that a and b restrict to the same element in $\mathbb{Q}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)]$. Now notice that

$$\phi\left((\gamma-1)^{p-2}f_n - pu(\gamma)\right) = (-pu(\gamma), (\gamma-1)^{p-2}g_n - pu(\gamma)),$$

where g_n is the image of f_n under the homomorphism $\mathbb{Q}_p[G_{n+1,j}] \to \mathbb{Q}_p[G_{n,j}]$. Both components are units in the corresponding rings. As both components restrict to the same element in $\mathbb{Q}_p[\mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)]$, the same holds for their inverses. Hence, $(\gamma-1)^{p-2}f_n - pu(\gamma)$ is a unit in $\mathbb{Q}_p[G_{n,j}]$. The conclusion follows. □

Remark 3.16. *The "other direction" of Lemma* 3.15*, namely that if u_n is a pseudo-generator for $U'_{n,j}$ then $N_{n,m}(u_n)$ is a pseudo-generator for $U'_{m,j}$ is significantly easier. Indeed, by local class field theory, for any $n \geq m \geq 0$ one has $[U_{m,j} : N_{n,m}(U_{n,j})] \leq p^{n-m}$. Combining this with* (3.10)*, it follows that if u_n is a pseudo-generator for $U'_{n,j}$, then $N_{n,m}(u_n)$ is a pseudo-generator for $U'_{m,j}$ for any $n \geq m \geq 0$.*

We can prove the first important result regarding the structure of U^1_∞.

Theorem 3.17. *The Λ-module*

$$U'_{\infty,j} := \varprojlim_n U'_{n,j}$$

is a noetherian Λ-module and there exists a pseudo-isomorphism of Λ-modules

$$U'_{\infty,j} \sim \Lambda^{a_j} \oplus \Lambda/(T^*),$$

where $a_j = \frac{|G|}{s}$ and $* : \Lambda \to \Lambda$ is Iwasawa's involution.

Proof. We recall that a Λ-module X is noetherian if and only if $X/\mathfrak{m}X$ is finite, where $\mathfrak{m} = (p, T)$ is the unique maximal ideal of Λ. To see that $U'_{\infty,j}/\mathfrak{m}U'_{\infty,j}$ is finite, notice that for any $n \geq 0$ one has a natural isomorphism

$$U'_{n,j}/(p,T)U'_{n.j} \cong U'_{0,j}/pU'_{0,j}.$$

Since $U'_{0,j}$ is a finitely generated $\mathbb{Z}_p$-module, it follows that $U'_{n,j}/\mathfrak{m}U'_{n,j}$ is uniformly bounded, independent of n. It follows that $U'_{\infty,j}/\mathfrak{m}U'_{\infty,j}$ is finite.

The structure theorem of noetherian Λ-modules implies that there exists a non-negative integer $a \geq 0$ such that

$$U'_{\infty,j} \sim \Lambda^a \oplus \Lambda - \text{torsion}.$$

To prove that $a = a_j$, it suffices to show that

$$\mathbb{Z}_p - \text{rank}\left(U'_{\infty,j}/\nu_{m,0}U'_{\infty,j}\right) = (p^m - 1) \cdot a_j + O(1).$$

Since $N_{n+1,n}(U'_{n+1,j}) = U'_{n,j}$ it follows that

$$U'_{\infty,j}/\nu_{m,0}U'_{\infty,j} = \varprojlim_n U'_{n,j}/\nu_{m,0}U'_{n,j}.$$

Since $U'_{n,j}$ is pseudo-cyclic and for a pseudo-generator u_n one has $u_n^{\mathbb{Z}_p[G_{n,j}]} \cong \mathbb{Z}_p[G_{n,j}]/(N_n)$, it follows that

$$\mathbb{Z}_p - \text{rank}(U'_{n,j}/\nu_{m,0}U'_{n,j}) = \mathbb{Z}_p - \text{rank}(\mathbb{Z}_p[G_{n,j}]/\nu_{m,0}) = (p^m - 1)a_j,$$

for all sufficiently large n. Note that

$$\ker(N_{n,m}) = (\mathbb{K}^\times_{n,\mathfrak{p}_j})^{\omega_m} \subset (\mathbb{K}^\times_{n,\mathfrak{p}_j})^{T\nu_{m,0}} \subset (U'_{n,j})^{\nu_{m,0}}.$$

Thus, $N_{n,m}$ induces in fact an isomorphism $U'_{n,j}/\nu_{m,0}U'_{n,j} \to U'_{m,j}/\nu_{m,0}U'_{m,j}$. As the $\mathbb{Z}_p$-torsion has p-rank equal to 1 at every level it follows that $\mathbb{Z}_p - \operatorname{rank}(U'_{\infty,j}/\nu_{m,0}U'_{\infty,j}) = (p^m - 1)a_j + O(1)$.

We now prove that $U'_{\infty,j}$ contains no Λ-torsion of μ-type (i.e., no $\mathbb{Z}_p$-torsion). Assume the contrary, so that there exist a positive integer k and $u = (u_n)_{n\geq 0} \in U'_{\infty,j}$ such that $u^{p^k} = 1$. This would imply that $u_n^{p^k} = 1$ for all $n \geq 0$, and since the only torsion in $U'_{n.j}$ consists of the roots of unity, we obtain a contradiction.

Assume now that $f(T) \in \Lambda$ is the power of an irreducible distinguished polynomial and such that $u^{f(T)} = 1$, for some $u = (u_n)_{n\geq 1} \in U'_{\infty,j}$ with the property that u_n is not a root of unity for some (and hence for all sufficiently large) $n \geq 0$. First let us note that $f(T)$ must be coprime to ω_m for all $m \geq 0$. Indeed, since $f(T)$ is the power of some irreducible polynomial, if $\gcd(\omega_m, f(T)) \neq 1$, then it follows that there exists some element $\xi = (\xi_n) \in U'_{\infty,j}$ such that

$$\xi_n^{\omega_m} = 1, \quad \text{for all } n \geq 0.$$

But this implies that $\xi_n \in U'_{m,j}$ for all $n \geq m$, and such a sequence cannot be norm-coherent.

Now let v_n be a pseudo-generator of $\mathbb{Z}_p[G_{n,j}]$. It follows that there exists a non-negative integer l_n such that

$$u_n^{p^{l_n}} = v_n^{g_n},$$

for some $g_n \in \mathbb{Z}_p[G_{n,j}]$. Since u_n is not a root of unity, it follows that g_n has non-trivial image in $\mathbb{Z}_p[G_{n,j}]/(N_n)$. Since $f(T)$ annihilates u_n, it follows that

$$f(T)g_n = N_n h_n,$$

for some $h_n \in \mathbb{Z}_p[G_{n,j}]$. Since $N_n h_n = N_n c_n$, with $c_n = Tr(h_n)$, it follows that

$$f(T)g_n = N_n c_n,$$

for some $c_n \in \mathbb{Z}_p$.

Recall that by our assumption we have

$$\mathbb{Z}_p[G_{n,j}] \cong \mathbb{Z}_p[G_{0,j}] \otimes \mathbb{Z}_p[\Gamma_n].$$

We also identify $\mathbb{Z}_p[\Gamma_n]$ with $\mathbb{Z}_p[[T]]/(\omega_n)$ in the obvious way. Let

$$\sum_{\sigma \in G_{0,j}} \sigma \otimes g_{n,\sigma}(T)$$

be the image of g_n under the above isomorphism. It follows that for all $\sigma \in G_{0,j}$ one must have the following equality inside $\mathbb{Z}_p[\Gamma_n]$:

$$f(T)g_{n,\sigma}(T) = c_n \nu_{n,0}.$$

It follows that there exists $p_{n,\sigma}(T) \in \mathbb{Z}_p[[T]]$ such that the following equality holds in $\mathbb{Z}_p[[T]]$:

$$f(T)g_{n,\sigma}(T) + p_{n,\sigma}(T)\omega_n = c_n \nu_{n,0}.$$

Since $\nu_{n,0} \mid \omega_n$, it follows that $\nu_{n,0} \mid f(T)g_{n,\sigma}(T)$. We established above that $f(T)$ must be coprime to ω_n, hence $\nu_{n,0} \mid g_{n,\sigma}(T)$. But then the element

$$g_n = \sum_{\sigma \in G_{0,j}} \sigma \otimes g_{n,\sigma}(T)$$

is a multiple of $N_{n,0}$ in $\mathbb{Z}_p[G_{n,j}]$. In particular, it follows that $u_n^{p^{l_n}} \in U'_{0,j}$ for all sufficiently large n. But then for all sufficiently large n one has

$$u_n^{p^{l_n}T} = u_n^{f(T)} = 1.$$

Since $f(T)$ is coprime to ω_m, we have in particular that $f(T)$ is coprime to T. It follows that there exists some $j_n \in \mathbb{Z}_p$ such that

$$u_n^{p^{j_n}} = 1.$$

This contradicts our assumption that u_n is not a root of unity.

We are left to treat the case when the sequence $(u_n)_{n\geq 1}$ consists of roots of unity. In this case, by the definition of the cyclotomic character we have that

$$u_n^{T^*} = 1 \quad \text{for all } n \geq 0.$$

It follows that the only torsion in $U'_{\infty,j}$ consists of the T^*-torsion. Furthermore, since $\varprojlim W_{n,j} \cong \mathbb{Z}_p$ and $\Lambda/(T^*) \cong \mathbb{Z}_p$, it follows that

$$U'_{\infty,j} \sim \Lambda^a \oplus \Lambda/(T^*),$$

as desired. □

Let u_0 be a pseudo-generator of $U'_{0,j}$. For every $n \geq 0$, we let $u_{n+1} \in U'_{n+1,j}$ be a pseudo-generator such that $N_{n+1,n}(u_{n+1}) = u_n$ (such a construction is possible by Lemma 3.15). Furthermore, for every $n \geq 0$, we let w_n be a generator of $W_{n,j}$ such that $N_{n+1,n}(w_{n+1}) = w_n$. For every $n \geq 0$, we consider the submodule

$$V_{n,j} = W_{n,j} \times u_n^{\mathbb{Z}_p[G_{n,j}]} = w_n^{\mathbb{Z}_p[G_{n,j}]} \times u_n^{\mathbb{Z}_p[G_{n,j}]}$$

of $U'_{n,j}$. If we let $V_{\infty,j} = \varprojlim V_{n,j}$, then $V_{\infty,j}$ is a Λ-submodule of $U'_{n,j}$. Since

$$\mathbb{Z}_p - \operatorname{rank}(u_n^{\mathbb{Z}_p[G_{n,j}]}) = p^n a_j - 1$$

and

$$T^* \varprojlim W_{n,j} = \{1\},$$

it follows that

$$V_{\infty,j} \sim \Lambda^{a_j} \oplus \Lambda/(T^*).$$

We have shown that $U'_{\infty,j}/V_{\infty,j}$ is a Λ-torsion module.

Lemma 3.18. *The group $U'_{\infty,j}/V_{\infty,j}$ has uniformly bounded exponent.*

Proof. Assume the contrary. Then there exist a distinguished polynomial $f(T)$ and a norm-coherent sequence (v_n) such that $v_n^{f(T)} = u_n^{\sum_{\sigma\in G_j} g_\sigma(T)\sigma}$. As u_n is a pseudo-generator at level n, it follows that $f(T)$ is coprime to ω_n for all n. For every n, there exists a k_n such that $v^{p^{k_n}} = u_n^{\sum_{\sigma\in G_j} h_{\sigma,n}(T)\sigma}$ and such that not all the $h_{\sigma,n}(T)$ are divisible by p. It follows that

$$f(T)h_{\sigma,n}(T) - p^{k_n} g_\sigma(T) = a_n N_{n,0}. \tag{3.11}$$

Since $f(T)$ and $h_{\sigma,n}$ are not divisible by p, it follows that a_n is a unit and we can assume that $a_n = 1$. If we divide equation (3.11) by ω_{n-1} we obtain

$$f(T)h_{\sigma,n-1}(T) - p^{k_n} g_\sigma(T) = pN_{n-1,0}.$$

We know that $k_{n-1} + 1 = k_n$ for n large enough. It follows that $a_n = a_{n-1}$. Further,

$$f(T)h_{\sigma,n}(T) - p^{k_n} g_\sigma(T) = N_{n,0} = \nu_{n,n-1}(f(T)h_{\sigma,n-1}(T) - p^{k_{n-1}} g_\sigma(T)).$$

Note that $-\nu_{n,n-1} + p = u(\omega_{n-1})\omega_{n-1}^{p-1}$. Hence,

$$f(T)(h_{\sigma,n}(T) - \nu_{n,n-1}h_{\sigma,n-1}(T)) = g_\sigma(T)p^{k_n-1}u(\omega_{n-1})\omega_{n-1}^{p-1}.$$

Since $f(T)$ is coprime to ω_{n-1}, we obtain that $f(T) \mid g_\sigma(T)$. Using equation (3.11), we see that $f(T)$ divides $N_{n,0}$, yielding a contradiction. The conclusion follows. □

Let $w = (w_n)_{n\geq 0} \in \varprojlim W_{n,j}$ be a generator and let $u = (u_n)_{n\geq 0} \in U'_{n,j}$ be a norm-coherent sequence of pseudo-generators. By construction, w and u generate $V_{n,j}$ as a $\Lambda[G_{n,j}]$-module. From Lemma 3.18, it follows that w and u also generate $U'_{\infty,j}$ as a $\Lambda[G_{n,j}]$-module, up to a finite exponent. Since the structure of U^1_∞ as a $\Lambda[G]$-module is induced from the one of $U'_{\infty,j}$, we obtain the following important result.

Theorem 3.19. *Let $w, u \in U^1_\infty$ be as above. Then there exists a nonnegative integer k, such that for any $v \in U^1_\infty$ one has*

$$v^{p^k} \in w^{\Lambda[G]} \bigoplus u^{\Lambda[G]}.$$

The case $\mathbb{K} = \mathbb{Q}(\zeta_p)$ is a classical result from Iwasawa theory, proved for example in [Wa, Theorem 13.54]. Theorem 3.19 generalizes this to arbitrary number fields $\mathbb{K}$ for which $\zeta_p \in \mathbb{K}$ and $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$.

When $\mathbb{K} = \mathbb{Q}(\zeta_p)$, since $|G| = p-1$ and there is only one prime in $\mathbb{K}$, one can decompose the module U^1_∞ along the idempotents ε_i $(i = 0, \dots, p-2)$ of $\mathbb{Z}_p[G]$ and give an even more precise description of the modules $\varepsilon_i U^1_\infty$. When $i \neq 0, 1$, the structure of $\varepsilon_i U^1_\infty$ is given in the aforementioned result [Wa, Theorem 13.54]. We conclude this section by describing the structure of $\varepsilon_0 U_1(\mathbb{K}_n)$ and $\varepsilon_1 U_1(\mathbb{K}_n)$, respectively. The ideas from the proof of Proposition 3.20 below are used actively in the working group led by Prof. Mihăilescu for studying properties of Λ-modules in various contexts, one example being Prof. Mihăilescu's investigation of Vandiver's conjecture.

Proposition 3.20. *For every $n \geq 0$, we let $\mathbf{Q}_n$ be the localization of $\mathbb{Q}_n$ at the prime above p, we let $\pi_n = N_{\mathbb{K}_{\mathfrak{p}_{n,1}}/\mathbf{Q}_n}(1-\zeta_{p^{n+1}})$ be a uniformizer for $\mathbf{Q}_n$ and let $\Gamma_n = \mathrm{Gal}(\mathbb{K}_{\mathfrak{p}_{n,1}}/\mathbb{K}_{\mathfrak{p}_{0,1}})$. Then the following hold:*

a) One has

$$\varepsilon_0 U'(\mathbb{K}_{\mathfrak{p}_{n,1}}) = \left((\pi_n^T)^{\varepsilon_0}\right)^{\mathbb{Z}_p[\Gamma_n]}.$$

b) There exists $u_n \in U^1(\mathbb{K}_{\mathfrak{p}_{n,1}})$ such that

$$\varepsilon_1 U^1(\mathbb{K}_{\mathfrak{p}_{n,1}}) = \langle \zeta_{p^{n+1}} \rangle \times (u_n^{\varepsilon_1})^{\mathbb{Z}_p[\Gamma_n]},$$

and if $2 \leq i \leq p-2$, then $u_n^{\varepsilon_i}$ generates $\varepsilon_i U'(\mathbb{K}_{\mathfrak{p}_{n,1}})$ as a Λ-module. Furthermore, the elements $(u_n)_{n\geq 0}$ can be chosen to form a norm-coherent sequence.

Proof. Let $\Delta_n \in E(\mathbb{K}_n)$ denote the element which together with ± 1 generate the cyclotomic units $C(\mathbb{Q}_n)$ of $\mathbb{Q}_n$ under the action of $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$. It is well-known (see for example the proof of [Co-Su, Lemma 4.8.3]) that the p-part of the ideal class group of $\mathbb{Q}_n$ is trivial for all $n \geq 0$ and this combined with the Class Number Formula yield the fact that $(E(\mathbb{Q}_n)/C(\mathbb{Q}_n))_p = \{1\}$. It follows that

$$\overline{E^1(\mathbb{Q}_n)} = \overline{C(\mathbb{Q}_n)},$$

and both groups are $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$-cyclic, generated by Δ_n (we identified Δ_n with its image under the embedding $\mathbb{Q}_n \hookrightarrow \mathbf{Q}_n$). Notice also that by definition we have $\Delta_n = \pi_n^T$. We will prove that

$$\varepsilon_0 U'(\mathbb{K}_{n,\mathfrak{p}_{n,1}}) = U'(\mathbf{Q}_n) = \overline{E^1(\mathbb{Q}_n)} = \overline{C(\mathbb{Q}_n)},$$

which will finish the proof of part a).

The fact that $\varepsilon_0 U'(\mathbb{K}_{n,\mathfrak{p}_{n,1}}) = U'(\mathbf{Q}_n)$ is immediate from the definitions. To see that $U'(\mathbf{Q}_n) = \overline{E^1(\mathbb{Q}_n)}$, notice that by class field theory one has

$$U'(\mathbf{Q}_n)/\overline{E^1(\mathbb{Q}_n)} \cong \mathrm{Gal}(\Omega(\mathbb{Q}_n))/\mathbb{Q}_\infty,$$

and the extension $\Omega(\mathbb{Q}_n))/\mathbb{Q}_\infty$ is trivial because Leopoldt's conjecture holds for $\mathbb{Q}_n$.

For part b), we know from Lemma 13.36 from [Wa] that

$$\varepsilon_1 U^1(\mathbb{K}_{0,\mathfrak{p}_{n,1}}) \cong \langle \zeta_p \rangle \times \mathbb{Z}_p - \text{cyclic}.$$

Let v_0 be such that

$$\varepsilon_1 U^1(\mathbb{K}_{0,\mathfrak{p}_{n,1}}) = \langle \zeta_p \rangle \times v_0^{\mathbb{Z}_p}.$$

For $n \geq 0$, the only torsion in $\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ consists of $\langle \zeta_{p^{n+1}} \rangle$. By Lemma 3.12, there exists $v_n \in \varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ such that $N_{n,0}(v_n) = v_0$. We claim that

$$\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}}) = \left\langle \zeta_{p^{n+1}} \right\rangle \times v_n^{\Lambda}.$$

Assume the contrary. Then, by Nakayama's lemma, there exists $a_n \in \varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ which is not a root of unity such that v_n and a_n have distinct images in

$$\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})/(p,T)\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}}).$$

One has that

$$N_{n,0}(a_n) = \zeta_p^x \cdot u_0^y,$$

for some $x, y \in \mathbb{Z}_p$. Since modifying a_n by a root of unity does not change our setup, we can assume without loss of generality that $x = 0$. It follows that

$$N_{n,0}(v_n^y) = N_{n,0}(a_n),$$

hence, by Hilbert's Theorem 90, one has

$$v_n^y = a_n \cdot c_n^T,$$

for some $c_n \in \mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}$. The goal is to show that we can take $c_n \in \varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$. We will mimic the approach from [Wa, Theorem 13.54].

We know from class field theory that there is a decomposition as abelian groups

$$\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times} = \langle \mu_{p-1} \rangle \times \lambda_n^{\mathbb{Z}} \times U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}}),$$

where λ_n denotes a uniformizer for the unique maximal ideal of $\mathbb{K}_{n,\mathfrak{p}_{n,1}}$.

Notice that $\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}$ is not a $\mathbb{Z}_p[G_{\mathfrak{p}_1}]$-module (since it is not a $\mathbb{Z}_p$-module), so we cannot simply act with ε_1 on it. Instead, we look at the quotient $\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}/\left(\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}\right)^{p^N}$, which by above becomes

$$\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}/\left(\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}\right)^{p^N} = \lambda_n^{\mathbb{Z}/p^N\mathbb{Z}} \times U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})/\left(U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})\right)^{p^N}.$$

We now let ε_1 act on this space. The element $\varepsilon_1(\lambda_n) \pmod{\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{p^N}}$ is represented by a unit and since ε_1 is an idempotent, this unit must be an element of $\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$. Therefore,

$$\varepsilon_1 \mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}/\left(\mathbb{K}_{n,\mathfrak{p}_{n,1}}^{\times}\right)^{p^N} = \varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})/\left(U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})\right)^{p^N}.$$

In particular, we must have

$$\frac{v_n^y}{a_n} = \varepsilon_1 \frac{v_n^y}{a_n} = c_n^T \equiv \varepsilon_1 d_N^T \pmod{\left(K_{n,\mathfrak{p}_{n,1}}^{\times}\right)^{p^N}},$$

for some $d_N \in U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$. Since both $\frac{v_n^y}{a_n}$ and d_N are units, we obtain that

$$\varepsilon_i \frac{v_n^y}{a_n} \equiv \varepsilon_i d_N^T \pmod{U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})^{p^N}}.$$

As $U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ is compact, the sequence $\varepsilon_i d_N$ has a cluster point d in $\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ and it follows that $c_n^T = d^T$. Therefore, $v_n^y = a_n \cdot d^T$, for some $d \in \varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$. This yields the desired contradiction.

It follows that one has

$$\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}}) = \left\langle \zeta_{p^{n+1}} \right\rangle \times v_n^{\Lambda}.$$

We now fix an element v_0 as above and for every $n \geq 1$, we construct recursively $v_n \in \varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ such that $N_{n,n-1}(v_n) = v_{n-1}$. Then the sequence $(v_n)_{n\geq 0}$ is norm-coherent and by above, for every $n \geq 0$, one has that

$$\varepsilon_1 U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}}) = \left\langle \zeta_{p^{n+1}} \right\rangle \times v_n^{\Lambda}.$$

It follows that the Λ-module $\varepsilon_1 \varprojlim_n U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ is generated by $w = (w_n)_{n\geq 0}$ and $v = (v_n)_{n\geq 0}$, where w is a generator for $\varprojlim_n \langle \zeta_{p^n} \rangle$.

When $2 \leq i \leq p-2$, the existence of norm-coherent generators $\xi_i^{(n)}$ for $\varepsilon_i U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ is proved in Theorem 13.54 from [Wa].

For every $n \geq 0$, let $u_n \in U^1(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ be such that $u_n^{\varepsilon_1} = v_n$ and such that for $2 \leq i \leq p-2$ one has $u^{\varepsilon_i} = \xi_i^{(n)}$. Then the above analysis shows that the elements u_n and w_n generate $U'(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$ as a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{K}_{n,\mathfrak{p}_{n,1}}/\mathbb{Q}_p)]$-module and thus the elements $u = (u_n)_{n\geq 0}$ and $w = (w_n)_{n\geq 0}$ generate

$$U_1' := \varprojlim_n U'(\mathbb{K}_{n,\mathfrak{p}_{n,1}})$$

as a $\Lambda[G_{\mathfrak{p}_1}]$-module. □

3.4 Ideal classes as radicals

In Iwasawa theory, one typically studies the ideal classes in the cyclotomic tower by considering injective limits of finite radicals and linking them to the Pontrjagin dual $\mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim A_n, \mathbb{Q}_p/\mathbb{Z}_p)$ of $\varinjlim A_n$ (see for example [Lang 1, Chapter 6]). Iwasawa also proved in [Iwa73, Theorem 11] that there exists a pseudo-isomorphism of Λ-modules $\mathrm{Hom}_{\mathbb{Z}_p}(\varinjlim A_n, \mathbb{Q}_p/\mathbb{Z}_p) \sim \varprojlim A_n$. Here, we will instead work with projective limits of finite radicals (as introduced in Section 3.2) and we will link these to $\varprojlim A_n$ by an explicit homomorphism of $\Lambda[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-modules. As a result, we will be able to study subgroups of $A_\infty := \varprojlim A_n$ using the machinery of $\Lambda[\mathrm{Gal}(\mathbb{K}/\mathbb{Q})]$-modules devised in the previous sections. To achieve our objective, we first need some auxiliary results on the growth of quotients of Γ-modules and p-groups.

We start with the following general setting. Let $\mathbb{K}$ be a number field and let $\mathbb{L}/\mathbb{K}$ be a $\mathbb{Z}_p$-extension of $\mathbb{K}$ (not necessarily the cyclotomic one). We define the Iwasawa algebra Λ for the extension $\mathbb{L}/\mathbb{K}$ in the usual way and identify it with $\mathbb{Z}_p[[T]]$ as before. For $n \geq 0$, we let $\mathbb{K}_n$ be the subextension of $\mathbb{L}/\mathbb{K}$ defined by $[\mathbb{K}_n : \mathbb{K}] = p^n$ and we let A_n denote the p-Sylow subgroup of the class group of $\mathbb{K}_n$. We define $A_\infty = \varprojlim A_n$ with respect to the norm maps $N_{n,m} := N_{\mathbb{K}_n/\mathbb{K}_m}$ for $n \geq m \geq 0$. If we let $\mathbb{H}(\mathbb{L})$ stand for the maximal p-abelian everywhere unramified extension of $\mathbb{L}$, then the Artin map induces an isomorphism of Λ-modules

$$\mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{L}) \cong A_\infty.$$

As we already mentioned in Section 3.1, an important theorem of Iwasawa shows that A_∞ is a noetherian torsion Λ-module (see [Iwa73, Theorem 5]).

By the structure theorem of noetherian Λ-modules (see for example [Wa, Theorem 13.12]), it follows that whenever X is a noetherian torsion Λ-module, there exists an exact sequence of Λ-modules

$$1 \to K_1 \to X \to \bigoplus_{i=1}^{r} \Lambda/(p^{\mu_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}) \to K_2 \to 1,$$

where K_1 and K_2 are finite Λ-modules, r, t, μ_i, m_j are non-negative integers and $f_j(T)$ are irreducible distinguished polynomials. The quantities $\mu(X) := \sum_{i=1}^{r} \mu_i$ and $\lambda(X) := \sum_{j=1}^{t} m_j \cdot \deg(f_j(T))$ are referred to as the μ-invariant and the λ-invariant of X, respectively.

One typically studies the growth of the groups A_n using the ideal lift map $\iota_{m,n} : A_m \to A_n$ and the norm map $N_{n,m} : A_n \to A_m$. An elementary fact in Iwasawa theory shows that $\mathbb{L}/\mathbb{K}$ is unramified outside the primes lying above p and that there exists an integer $n_0 \geq 0$ such that the extension $\mathbb{L}/\mathbb{K}_{n_0}$ is totally ramified (see for example [Wa, Proposition 13.2] and [Wa, Lemma 13.3]). Hence, if $\mathbb{H}_n$ denotes the Hilbert class field of $\mathbb{K}_n$, it follows that for any $n \geq m \geq n_0$ one has $\mathbb{K}_n \cap \mathbb{H}_m = \mathbb{K}_m$. By class field theory, it follows that the norm map $N_{n,m}$ is surjective for any $n \geq m \geq n_0$ (see [Wa, Theorem 10.1]). The ideal lift map $\iota_{m,n}$ is not injective in general, but Iwasawa proved in [Iwa73, Theorem 10] that $|\ker(\iota_{n,n+1} : A_n \to A_{n+1})|$ is uniformly bounded (i.e., independent of n). In this section, we will use results from classical algebraic Iwasawa theory and group theory to derive more precise information about the maps $\iota_{m,n}$ and $N_{n,m}$ when one restricts his attention to certain subgroups of A_n.

The following result (Lemma 3.21 below) and its proof are taken from [Gre 4, Proposition 2.3.4]. Since the cited manuscript has not been published yet, we decided to reproduce the proof here for completeness.

Lemma 3.21. *Let X be a finitely generated, torsion Λ-module. Choose n_0 so that $X/\nu_{n,n_0}X$ is finite for all $n \geq n_0$. Assume that $\mu(X) = 0$. Then, for all $n \gg 0$, there is an isomorphism*

$$X/\nu_{n,n_0}X \cong \prod_{i=1}^{\lambda} \mathbb{Z}/p^{n+c_i}\mathbb{Z} \times C,$$

where $c_1, \ldots, c_\lambda$ are certain integers and C is isomorphic to the maximal, finite, Λ-submodule of X.

Proof. As a $\mathbb{Z}_p$-module, we have $X \cong U \times Z$, where $U \cong \mathbb{Z}_p^\lambda$. Here Z is a Λ-submodule of X, but U is just a $\mathbb{Z}_p$-submodule. Let t be such that $p^t Z = 0$. Then

$$p^t U = p^t X$$

is a Λ-submodule of X of finite index. Therefore, $\nu_{n,n_0} X \subset p^t U$ for all sufficiently large $n \geq n_0$. Note also that we have an isomorphism of $\mathbb{Z}_p$-modules

$$X/\nu_{n,n_0} X \cong U/\nu_{n,n_0} X \times Z.$$

The module $\nu_{n,n_0} X$ is a free $\mathbb{Z}_p$-module of rank λ. We will prove below that

$$\nu_{n+1,n_0} X = p \nu_{n,n_0} X,$$

whenever $n \geq n_1$, where n_1 will be chosen in a certain way (notice that this also shows that if $x \in X \setminus Z$, then the image of x in $X/\nu_{n,n_0} X$ has order p^{n+c} for all sufficiently large n, for some integer constant c). Thus, for all such n, if $U/\nu_{n,n_0} X$ is isomorphic to a direct product of cyclic groups of orders $p^{a_1}, \ldots, p^{a_\lambda}$, then $U/\nu_{n+1,n_0} X$ will be isomorphic to a direct product of cyclic groups of orders $p^{a_1+1}, \ldots, p^{a_\lambda+1}$. The result will then follow by induction.

First choose $n_0' \geq n_0$ so that $X' := \nu_{n_0',n_0} X \subset p^t U$. Then Γ acts continuously on the quotient group $X'/p^2 X'$. Choose $n_1 \geq n_0'$ so that the subgroup $\Gamma^{p^{n_1}}$ acts trivially on this quotient. If $i > n_1$, then

$$\phi_i := \sum_{j=0}^{p-1} \gamma_0^{jp^{i-1}}$$

acts on $X'/p^2 X'$ as the multiplication by p map. By Nakayama's lemma for $\mathbb{Z}_p$-modules, it follows that $\phi_i X' = pX'$. Let $n \geq n_1$. Then, taking $i = n+1$ and multiplying by ν_{n,n_0} gives the promised identity

$$\nu_{n+1,n_0} X = p \nu_{n,n_0} X.$$

This completes our proof. □

We can use Lemma 3.21 to retrieve information about the groups A_n at finite levels as follows.

Proposition 3.22. *There exists a constant c which depends only on $\mathbb{L}$ such that for any sufficiently large positive integer n one has an injective homomorphism of $\mathbb{Z}_p$-modules*

$$\phi_n : A_n^{p^c} \hookrightarrow \prod_{i=1}^{\lambda} \left(\mathbb{Z}/p^{n+c_i}\mathbb{Z}\right),$$

where $\lambda = \lambda(A_\infty)$ and c_i are integers independent of n. Furthermore, $|$ Coker $\phi_n|$ is uniformly bounded independent of n.

Proof. Let n_0 be such that $\mathbb{L}/\mathbb{K}_{n_0}$ is totally ramified at the primes above p. For every $n \geq 0$, let $\mathbb{H}_n$ be the Hilbert class field of $\mathbb{K}_n$ and $\mathbb{H}(\mathbb{L}) = \bigcup_{n \geq 0} \mathbb{H}_n$ as before. Let $X = \mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{L})$ and $Y = \mathrm{Gal}(\mathbb{H}(\mathbb{L})/\mathbb{H}_{n_0} \cdot \mathbb{L})$. Iwasawa proved in [Iwa73, Theorem 6] that there exists an isomorphism of Λ-modules

$$X/\nu_{n,n_0} Y \cong \mathrm{Gal}(\mathbb{H}_n/\mathbb{K}_n) \cong A_n. \tag{3.12}$$

Since X is a noetherian torsion Λ-module, it follows that there exists a homomorphism of Λ-modules with finite kernel and cokernel

$$X \to \bigoplus_{i=1}^{r} \Lambda/(p^{\mu_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(g_j(T)),$$

for some non-negative integers r, t, μ_i and some distinguished polynomials $g_j(T) \in \mathbb{Z}_p[[T]]$. Using this homomorphism together with the fact that Y has finite index in X, it follows that there exists a constant $c \geq 0$ such that $X^{p^c} \subseteq Y$ and such that there exists an injective homomorphism of Λ-modules with finite cokernel

$$X^{p^c} \hookrightarrow \bigoplus_{j=1}^{t} \Lambda/(g_j(T)).$$

With this choice of c we have $\mu(X^{p^c}) = 0$, $\lambda(X^{p^c}) = \lambda(X)$ and that X^{p^c} has no finite Λ-submodules. Applying Lemma 3.21 to the Λ-module X^{p^c}, it follows that

$$\frac{X^{p^c}}{\nu_{n,n_0}(X^{p^c})} \cong \prod_{i=1}^{\lambda(X)} \left(\mathbb{Z}/p^{n+c_i}\mathbb{Z}\right),$$

for some integers c_i depending on $\mathbb{L}$ and c.

To finish the problem, notice that (3.12) induces an isomorphism

$$\frac{X^{p^c}}{X^{p^c} \cap \nu_{n,n_0}(Y)} \cong A_n^{p^c}.$$

Notice also that if $x \in \nu_{n,n_0}(Y)$, then $x^{p^c} \in \nu_{n,n_0}(X^{p^c})$. Since X^{p^c} is a finitely generated $\mathbb{Z}_p$-module, it follows that there exists an injection of $\mathbb{Z}_p$-modules with finite cokernel (independent of n)

$$\frac{X^{p^c}}{\nu_{n,n_0}(Y) \cap X^{p^c}} \hookrightarrow \frac{X^{p^c}}{\nu_{n,n_0}(X^{p^c})}.$$

The result follows. □

For a finite p-abelian group G we let $p - \text{rank}(G)$ denote the number of copies of $\mathbb{Z}/p\mathbb{Z}$ in the decomposition of G/pG. Proposition 3.22 implies that for all sufficiently large $n \geq 0$ one has

$$p - \text{rank}(A_n^{p^c}) = p - \text{rank}(A_n^{p^{c+1}}) = \lambda(A_\infty). \tag{3.13}$$

The next two general results (Lemma 3.23 and Corollary 3.24 below), together with their proofs, were communicated to me by Prof. Mihăilescu. These are elementary results with multiple applications in the study of Λ-modules and had been previously used by the working group led by Prof. Mihăilescu in various contexts, such as Prof. Mihăilescu's work on Iwasawa's μ-conjecture for CM fields. In our present setting, we will use these results to show how one can deduce more precise information about the lift and the norm maps from relation (3.13), when we restrict to the subgroup $A_n^{p^c}$ of A_n.

Lemma 3.23. *Let A and B be finitely generated abelian $p-$groups denoted additively, such that*

$$p - \text{rank}(A) = p - \text{rank}(B) = p - \text{rank}(pA) = r. \tag{3.14}$$

The groups are endowed with two $\mathbb{Z}_p$-linear maps $N : B \to A$ and $\iota : A \to B$ such that $N \circ \iota : A \to A$ is the multiplication by p map and N is surjective. Then

a) We have $\iota(A) = pB$ and $\ker(N) = B[p] = \iota(A)[p]$.

b) For every $b \in B \setminus B[p]$, we have $\text{ord}(b) = p\text{ord}(\iota(N(b)))$.

Proof. Since A and B have the same p-rank and N is surjective, the induced map $\tilde{N} : B/pB \to A/pA$ is a surjective map between finite groups of equal cardinality, so it must be an isomorphism. Let $\tilde{\iota} : A/pA \to B/pB$ be the map induced from ι. Since $N \circ \iota = p$, it follows that $\tilde{N} \circ \tilde{\iota} = 0$ is the trivial map. But $\tilde{N}$ is an isomorphism, hence $\tilde{\iota} = 0$. Consequently $\iota(A) \subset pB$.

We have the following inequalities of p-ranks:

$$r = p - \text{rank}(B) \geq p - \text{rank}(pB) \geq p - \text{rank}(N(pB)) = p - \text{rank}(pA) = r.$$

Thus $p - \text{rank}(pB) = p - \text{rank}(B)$, and the map $\widehat{N} : pB/p^2B \to pA/p^2A$ induced by N is an isomorphism, too.

Let $\widehat{\iota} : A/pA \to pB/p^2B$ be the map induced by ι. Since $p - \text{rank}(A) = p - \text{rank}(pA) = p - \text{rank}(pA/p^2A)$, it follows that $\widehat{N} \circ \widehat{\iota} : A/pA \to pA/p^2A$ is an isomorphism, and hence so is $\widehat{\iota}$. As a consequence, we must have $\iota(A) = pB$.

We have established that $p - \text{rank}(pB) = p - \text{rank}(B)$. The definition of p-ranks yields

$$\begin{aligned} r = p - \text{rank}(B) &= p - \text{rank}(B[p]) = p - \text{rank}(pB) \\ &= p - \text{rank}(\iota(A)) = p - \text{rank}((\iota(A))[p]). \end{aligned}$$

Since $(\iota(A))[p] = (pB)[p] \subseteq B[p]$ and both are $\mathbb{F}_p$-vector spaces of equal dimension, it follows that

$$B[p] = (pB)[p] = (\iota(A))[p]).$$

Since $N \circ \iota = p$, we conclude that $B[p] \subseteq \ker(N)$.

Conversely, let $x \in \ker(N)$; if $x \in pB = \iota(A)$, then $Nx = px = 0$ so $x \in B[p]$. If x has non-trivial image in B/pB, the surjectivity of $\tilde{N}$ implies that $Nx \neq 0$; this confirms the fact that $\ker(N) = B[p]$ and completes the proof of part a).

For the proof of b), we consider the maps $\alpha : B \to \iota(A), x \mapsto px$ and $\beta = \iota \circ N$. Since $pB = \iota(A)$ and N is surjective, both maps are surjective and the kernels are $\ker(\alpha) = \ker(p) = B[p]$. Note that $B[p] \subseteq \ker(\beta)$, since for $x \in B[p]$ we have $N(x) = 0$ and thus $\iota \circ N(x) = 0$. We also have

$$|pB| = |\beta(B)| = |B|/|\ker(\beta)| = |B|/p^r = |B|/|B[p]|,$$

which implies that $|\ker(\beta)| = |B[p]|$, and since $\ker(\beta) \supseteq B[p]$, the two groups must be equal. Consequently, there is an isomorphism $\phi : pB \to pB$ such that $\phi \circ \beta = \alpha$. For $x \in B \setminus B[p]$ we have $\text{ord}(\phi(x)) = \text{ord}(x)$, since ϕ is an isomorphism, and

$$\text{ord}(\phi \circ \beta(x)) = \text{ord}(\beta(x)) = \text{ord}(\alpha(x)) = \text{ord}(px) = \text{ord}(x)/p,$$

so

$$\text{ord}(\alpha(x)) = \text{ord}(\iota(Nx)) = \text{ord}(x)/p.$$

Since the elements are equal, it follows that $\text{ord}(x) = p\text{ord}(\iota N(x))$, which is claim B. This completes the proof of the Lemma. □

In the case when there is a group acting on B, we have the following sharpening.

Corollary 3.24. *Let the groups A, B and the maps N, ι be like in Lemma 3.23 and assume that there is a cyclic group $G =< \tau >$ of order p acting on B, such that $\nu := \iota \circ N = \sum_{i=0}^{p-1} \tau^i$ and τ fixes $\iota(A)$. Then $\nu = p$ is the multiplication by p map and hence $\iota(N(x)) = px$ for all $x \in B$.*

Proof. Let $T = \tau - 1$, so $\nu = p + \binom{p}{2}T + O(T^2)$. From part a) of Lemma 3.23, we know that $\nu(x) \in \iota(A) = pB$, for all $x \in B$. Since τ fixes $\iota(A)$, it follows that $T\nu(x) = 0$; moreover, for arbitrary $y \in B$ we have $Tpy = 0 = p(Ty)$, so $Ty \in B[p]$. Consequently, $pTy = T^2y = 0$. We can now compute νx for arbitrary $x \in B$ explicitly, according to the previous expansion of ν:

$$\nu x = px + Tp\frac{p-1}{2}x + xO(T^2) = px,$$

where we used the facts established above, that $T^2x = pTx = 0$. This completes our proof. □

Proposition 3.22 tells us that there exists a constant c such that for all sufficiently large integers n, the p-ranks of $A_n^{p^c}$ and $A_{n+1}^{p^c}$ are the same. Then using Corollary 3.24, it follows that if $a_{n+1} \in A_{n+1}^{p^c}$ and $a_n = N_{n+1,n}(a_{n+1})$, then $\iota_{n,n+1}(a_n) = a_{n+1}^p$. Furthermore, Iwasawa's theorem tells us that

$$|\ker(\iota_{n,n+1} : A_n \to A_{n+1})|$$

is uniformly bounded independent of n, so by choosing c large enough, we obtain an injective map $\iota_{n,n+1} : A_n^{p^c} \to A_{n+1}^{p^c}$. Then iterating the result of Corollary 3.24, we obtain the following.

Proposition 3.25. *Let $\mathbb{K}$ be a number field and let $\mathbb{L}/\mathbb{K}$ be a $\mathbb{Z}_p$-extension. There exists a constant $c \geq 0$ such that for all $m \gg 0$ and $n > m$, the map $\iota_{m,n} : A_m^{p^c} \to A_n^{p^c}$ is injective, the map $N_{n,m} : A_n^{p^c} \to A_m^{p^c}$ is surjective and for any $a_n \in A_n^{p^c}$, one has*

$$\iota_{m,n}\left(N_{n,m}(a_n)\right) = a_n^{\nu_{n,m}} = a_n^{p^{n-m}}.$$

Proof. The first part of the statement is immediate from our previous observations, and so we only have to check the equalities

$$\iota_{m,n}\left(N_{n,m}(a_n)\right) = a_n^{\nu_{n,m}} = a_n^{p^{n-m}}.$$

We will prove this result by induction on $k = n - m \geq 1$. Notice first that for any m and any $k \geq 0$ we have $N_{m+k,m} \circ \iota_{m,m+k}(a_m) = a_m^{p^k}$, for any $a_m \in (A_m)^{p^c}$. In particular, for the base case $k = 1$, the result follows from Corollary 3.24, with $\mathrm{Gal}(\mathbb{K}_{m+1}/\mathbb{K}_m)$ playing the role of the group G. Assume now that the result holds for $k - 1$ ($k \geq 2$) and let us prove that it holds for k. By (3.13), it follows that for all sufficiently large m one has

$$p - \mathrm{rank}\left(A_{m+k-1}^{p^c}\right) = p - \mathrm{rank}\left(A_{m+k}^{p^c}\right) = p - \mathrm{rank}\left(p\left(A_{m+k-1}^{p^c}\right)\right).$$

Thus, by Corollary 3.24, $\iota_{m+k-1,m+k} \circ N_{m+k,m+k-1}(a_{m+k}) = a_{m+k}^p$. From the induction hypothesis, we have that $\iota_{m,m+k-1} \circ N_{m+k-1,m}(a_{m+k-1}) = a_{m+k-1}^{p^{k-1}}$. It follows that

$$\begin{aligned}\iota_{m,m+k}N_{m+k,m}(a_{m+k}) &= \iota_{m+k-1,m+k}(N_{m+k,m+k-1}(a_{m+k}^{p^{k-1}}))\\ &= \iota_{m+k-1,m+k}(N_{m+k,m+k-1}(a_{m+k}^{p^{k-1}}))\\ &= a_{m+k}^{p^k},\end{aligned}$$

which completes our proof. □

We will now use these refined results about the norm and the lift maps to show that when $\zeta_p \in \mathbb{K}$, $\mathbb{L}$ is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ and $\mathbb{M}$ is an extension of $\mathbb{L} = \mathbb{K}_\infty$ as in Section 3.2, one can create a map from the radical of $\mathbb{M}/\mathbb{K}_\infty$ to the group A_∞. Let thus $\mathbb{K}$ be a number field containing ζ_p, let $\mathbb{K}_\infty$ be its cyclotomic $\mathbb{Z}_p$-extension and let $\mathbb{M}/\mathbb{K}_\infty$ be a p-abelian extension, with the property that $\mathbb{M}/\mathbb{K}$ is Galois and $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a torsion-free $\mathbb{Z}_p$-module of finite rank r. For every $n \geq 0$, let $\mathbb{M}_n$ be the maximal extension of $\mathbb{K}_\infty$ contained in $\mathbb{M}$ with the property that $p^n\mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty) = 1$ and let R_n be its radical. Then, by Proposition 3.3, there exists a constant $k \geq 0$ depending on $\mathbb{M}$ such that for all $n \geq 0$, one has can choose the representatives for the generators of R_n to be elements of $\mathbb{K}_{n+k}$. We choose k to be large enough so that in addition, the extension $\mathbb{K}_\infty/\mathbb{K}_k$ is totally ramified at the primes above p.

Let

$$\tilde{\alpha}^{(1)} = (\alpha_1^{(1)}, \cdots); \quad \ldots \quad \tilde{\alpha}^{(r)} = (\alpha_1^{(r)}, \cdots)$$

be generators for $R := \varprojlim_n R_n$ with the property that $\alpha_n^{(j)} \in \mathbb{K}_{n+k}$ for all $n \geq 0$ and $j = 1, \ldots, r$.

Ultimately, we want to show how one can assign to an element $\tilde{\alpha} \in R$ a well-defined sequence in A_∞. We could not just choose a representative $\alpha_n \in \mathbb{K}_{n+k}$ for each class $[\alpha_n] \in R_n$ and then assign to it a class in A_{n+k}, since the map has to be independent of the choice of the class representative. To bypass this inconvenience, we will have to work with a slightly modified version of A_{n+k}, which is independent on the finite level we are working at. One thing we could try is to just lift A_{n+k} to $\mathbb{K}_\infty$ and show that no information is lost in this process. The following general result shows that this is indeed the case, provided that one restricts to a suitable subgroup of A_{n+k}.

Lemma 3.26. *Let $\mathbb{K}$ be a number field and let $\mathbb{L}/\mathbb{K}$ be a $\mathbb{Z}_p$-extension of $\mathbb{K}$. Let $A_\infty(\mathbb{L})$ be the p-primary component of the class group of $\mathbb{L}$. Then there exists a constant $c \geq 0$ such that for* *all sufficiently large n, the map $\iota_{n,\infty} : A_n^{p^c} \to A_\infty(\mathbb{L})$ is injective and one has an isomorphism of Λ-modules*

$$\varprojlim_n A_n^{p^c} \cong \varprojlim_n \iota_{n,\infty}(A_n^{p^c}),$$

where in the projective limit $\varprojlim_n \iota_{n,\infty}(A_n^{p^c})$, the transition maps

$$f_{n,m} : \iota_{n,\infty}(A_n^{p^c}) \to \iota_{m,\infty}(A_m^{p^c})$$

can be taken to be either $f_{n,m} = p^{n-m}$, or, equivalently, $f_{n,m} = \nu_{n,m}$.

Proof. Let c be as in Proposition 3.25. Then the injectivity of the map $\iota_{n,\infty} : A_n^{p^c} \to A_\infty(\mathbb{L})$ follows from Proposition 3.25.

Let $n_0 = n_0(\mathbb{L}/\mathbb{K})$ be such that for all $n \geq m \geq n_0$, the norm map $N_{n,m} : A_n \to A_m$ is surjective. Let $m \geq n_0$. We prove that the map

$$\iota_{m,\infty} : A_m^{p^c} \to \iota_{m,\infty}(A_m^{p^c})$$

is an isomorphism of Λ-modules. This is equivalent to showing that

$$\iota_{m,n} : A_m^{p^c} \to \iota_{m,n}(A_m^{p^c})$$

is an isomorphism of Λ-modules for every $n \geq m$. Let $a_m \in A_m^{p^c}$ be arbitrary and let $a_n \in A_n^{p^c}$ be such that $N_{n,m}(a_n) = a_m$. Then, since $N_{n,m} A_n^{p^c} \to A_m^{p^c}$ is a homomorphism of Λ-modules, it follows that $N_{n,m}(a_n^T) = a_m^T$. Therefore, by Proposition 3.25,

$$\begin{aligned} T\iota_{m,n}(a_m) &= Ta_n^{p^{n-m}} = Ta_n^{\nu_{n,m}} \\ &= \left(a_n^T\right)^{p^{n-m}} \\ &= \iota_{m,n}(a_m^T). \end{aligned}$$

It follows that $\iota_{m,\infty} : A_m^{p^c} \to \iota_{m,\infty}(A_m^{p^c})$ is an isomorphism of Λ-modules and also that for $a = (a_n)_{n\geq 0} \in \varprojlim_n A_n^{p^c}$ and any $n \geq m \geq n_0$ one has

$$\iota_{n,\infty}(a_n)^{\nu_{n,m}} = \iota_{n,\infty}(a_n)^{p^{n-m}} = \iota_{m,\infty}(a_m).$$

This completes our proof. □

For $\alpha \in \{\tilde{\alpha}^{(1)}, \dots, \tilde{\alpha}^{(r)}\}$, we let

$$\mathbb{K}_\infty\left(\alpha^{1/p^\infty}\right) := \bigcup_{n\geq 0} \mathbb{K}_\infty\left(\alpha_n^{1/p^n}\right),$$

which is a $\mathbb{Z}_p$-extension of $\mathbb{K}_\infty$.

For further reference, it will be useful to introduce the field Ω_E, defined by

$$\Omega_E = \bigcup_{n\geq 0} \mathbb{K}_n\left(E_n^{1/p^n}\right),$$

where E_n denotes the group of units in $\mathbb{K}_n$. Notice that if $\mathbb{K}_\infty\left(\alpha^{1/p^\infty}\right) \subset \Omega_E$, then for every $n \geq 0$ one must have that

$$\alpha_n \equiv e_n \pmod{\left(\mathbb{K}_\infty^\times\right)^{p^n}},$$

for some unit $e_n \in \mathbb{K}_\infty$.

In what follows, we prove that if $\alpha = (\alpha_n)_{n\geq 1}$ is an element of R as above, then there exists an element $a = (a_n)_{n\geq 0} \in \varprojlim_n \iota_{n,\infty}(A_n^{p^c})$ (with c as in Proposition 3.25) and a positive constant $t \geq 0$ such that for all sufficiently large n, one has

$$(\alpha_n) = \mathfrak{a}_n^{p^{n-t}},$$

and $[\mathfrak{a}_n] = a_n$.

Let $\widetilde{\mathbb{L}}_n = \mathbb{K}_{n+k}\left(\alpha_n^{1/p^n}\right)$. Since the extension $\widetilde{\mathbb{L}_n}/\mathbb{K}_{n+k}$ is p-ramified, the ideal (α_n) has in $\mathbb{K}_{n+k}$ a factorisation of the form

$$(\alpha_n) = \mathfrak{x}_n^{p^n} \cdot \mathfrak{b}_n,$$

where $\mathfrak{b}_n$ is p-primary and $\mathfrak{x}_n$ is coprime to p. Similarly, the ideal (α_{n+1}) has in $\mathbb{K}_{n+k+1}$ a factorisation of the form

$$(\alpha_{n+1}) = \mathfrak{x}_{n+1}^{p^{n+1}} \cdot \mathfrak{b}_{n+1}.$$

From the definition of α, we have that $\mathbb{K}_{n+k+1}(\alpha_n^{1/p^n}) = \mathbb{K}_{n+k+1}(\alpha_{n+1}^{1/p^n})$, so by Kummer theory one has

$$\alpha_{n+1} = v_n^{p^n} \cdot \alpha_n^c,$$

for some $v_n \in \mathbb{K}_{n+k+1}^\times$ and integer c coprime to p. Since α_n is the restriction of α_{n+1}, it follows that $c = 1$.

It follows that one has the following equality of ideals in $\mathbb{K}_{n+k+1}$:

$$\iota_{n+k,n+k+1}\left(\mathfrak{x}_n^{p^n} \cdot \mathfrak{b}_n\right) = (v_n^{-1})^{p^n} \mathfrak{x}_{n+1}^{p^{n+1}} \cdot \mathfrak{b}_{n+1}. \tag{3.15}$$

Since $\mathfrak{x}_n$ and $\mathfrak{x}_{n+1}$ are coprime to p and the primes above p are totally ramified in the extension $\mathbb{K}_{n+k+1}/\mathbb{K}_{n+k}$, it follows that $\mathfrak{b}_{n+1}$ is the pth power of some ideal. Using this recursively from $n = 1$, it follows that for any $n \geq 1$, one has the following equality of ideals in $\mathbb{K}_{n+k}$:

$$(\alpha_n) = \mathfrak{x}_n^{p^n} \cdot \mathfrak{B}_n^{p^{n-1}},$$

where $\mathfrak{a}_n$ is coprime to p and $\mathfrak{B}_n$ is p-primary.

Now let c be as in Proposition 3.25. It follows that for all $n \geq c+1$ one has

$$(\alpha_n) = \left((\mathfrak{x}_{\mathfrak{n}}{}^p \cdot \mathfrak{B}_n)^{p^c}\right)^{p^{n-c-1}}.$$

Let $\mathfrak{a}_n = (\mathfrak{x}_{\mathfrak{n}}{}^p \cdot \mathfrak{B}_n)^{p^c}$. Then $[\mathfrak{a}_n] \in A_{n+k}^{p^c}$ and by (3.15) it follows that

$$\iota_{n+k,n+k+1}\left([\mathfrak{a}_n]\right) = [\mathfrak{a}_{n+1}]^p.$$

Using the injectivity of the map $\iota_{n+k,n+k+1} : A_{n+k}^{p^c} \to A_{n+k+1}^{p^c}$, it follows from Proposition 3.25 that

$$N_{n+k+1,n+k}\left([\mathfrak{a}_{n+1}]\right) = [\mathfrak{a}_n]. \tag{3.16}$$

Let $\beta_n \in \mathbb{K}_\infty$ be another element representing the same class in R_n as α_n. Then by definition, one has

$$\alpha_n = \beta_n \cdot v^{p^n} \tag{3.17}$$

for some $v \in \mathbb{K}_\infty^\times$. Let $N \geq 0$ be minimal subject to $v \in \mathbb{K}_{n+k+N}$. Then we must also have $\beta_n \in \mathbb{K}_{n+k+N}$. The same analysis that was carried out for α_n shows that we can write

$$(\beta_n) = \mathfrak{a}_n'^{p^{n-c-1}},$$

for some ideal $\mathfrak{a}_n'$ whose class $[\mathfrak{a}_n']$ lies in $A_{n+k+N}^{p^c}$. From (3.17) it follows that

$$\iota_{n+k,n+k+N}\left([\mathfrak{a}_n]\right) = [\mathfrak{a}_n'].$$

It follows that

$$\iota_{n+k,\infty}\left([\mathfrak{a}_n]\right) = \iota_{n+k+N,\infty}\left([\mathfrak{a}_n']\right). \tag{3.18}$$

We conclude that there is a well-defined map $f : R \to \varprojlim_n \iota_{n,\infty}(A_n^{p^c})$ which sends the class of α_n to the class of the ideal $\mathfrak{a}_n$ defined by the relation $(\alpha_n) = \mathfrak{a}_n^{p^{n-c-1}}$. It is easy to see that f is in fact a homomorphism of $\mathbb{Z}_p$-modules and it is compatible with the action of $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ when $\mathbb{K}$ is disjoint from $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.

By construction, if $\alpha \in \ker(f)$, then the corresponding ideal $\mathfrak{a}_n$ must be principal for all n, say $\mathfrak{a}_n = (\delta_n)$. But this implies the equality of ideals

$$(\alpha_n) = (\delta_n)^{p^{n-c-1}}.$$

In particular, for every n there exists a unit $e_n \in \mathbb{K}_\infty$ such that $\alpha_n = e_n \delta_n^{p^{n-c-1}}$. But then

$$\alpha_n \equiv e_n \pmod{\left(K_\infty^\times\right)^{p^{n-c-1}}},$$

which implies that $\mathbb{K}_\infty\left(\alpha_{n-c-1}^{1/p^{n-c-1}}\right) \in \Omega_E$. Since this holds for all sufficiently large n, it follows that $\alpha \in \ker(f)$ implies $\mathbb{K}_\infty\left(\alpha^{1/p^\infty}\right) \subset \Omega_E$. The converse is immediate.

It is not hard to see that $Im(f)$ depends only on $\mathbb{M}$ and not on the choice of our basis for R as a $\mathbb{Z}_p$-module. Indeed, any other basis for R is related to our choice by an element $\phi \in GL_r(\mathbb{Z}_p)$, which, by the $\mathbb{Z}_p$-linearity of f, preserves $\mathrm{Im}(f)$.

If we specialize further to the setting where $\mathbb{K}$ is a CM field containing ζ_p, both $\mathbb{M}$ and $\mathbb{K}$ are Galois over $\mathbb{Q}$ and $\mathbb{K} \cap \mathbb{Q}_\infty = \mathbb{Q}$, then f becomes a homomorphism of $\Lambda[G]$-modules. Putting everything together, we obtain the following result.

Theorem 3.27. *Let $\mathbb{M}/\mathbb{K}_\infty$ be a p-abelian p-ramified extension such that $\mathbb{M}/\mathbb{K}$ is Galois and $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a torsion-free $\mathbb{Z}_p$-module of finite rank. Let R be the radical of the extension $\mathbb{M}/\mathbb{K}_\infty$. Then there exists a constant $c \geq 0$ which depends only on $\mathbb{K}$ and a homomorphism of $\mathbb{Z}_p$-modules*

$$f : R \to \varprojlim \iota_{n,\infty}(A_n^{p^c})$$

with the property that $\tilde{\alpha} \in \ker(f)$ if and only if $\mathbb{K}_\infty\left(\tilde{\alpha}^{1/p^\infty}\right) \subset \Omega_E$. If $\mathbb{K}/\mathbb{Q}$ is Galois with group G and both R and $\varprojlim \iota_{n,\infty}(A_n^{p^c})$ are $\Lambda[G]$-modules, then f becomes a homomorphism of $\Lambda[G]$-modules.

Theorem 3.27 shows how starting with a Galois extension $\mathbb{M}/\mathbb{K}$ with the property that the group $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a free $\mathbb{Z}_p$-module of finite rank, one can create a homomorphism from its radical to certain subgroups of $A_\infty = \varprojlim A_n$. Since we also have an explicit description of the kernel, we can use Theorem 3.27 to obtain lower bounds for the $\mathbb{Z}_p$-rank of various subgroups of A_∞. A natural question is when can one turn these rank inequalities into equalities, or at least provide 'good' lower and upper bounds. Our approach to answering this question will be to construct a homomorphism 'in the other other direction', i.e., from ideal classes to radicals and then combine the bounds we obtain with those from Theorem 3.27. It turns out that in one important case, both of these two homomorphisms are injective, so we even get equalities. It will be this particular case the one that also applies to Theorem 3.1.

For a homomorphism from ideal classes to radicals of extensions of $\mathbb{K}_\infty$, notice that if we start with an ideal class $a_n \in A_n$, choose $\mathfrak{a}_n \in a_n$ and

$$(\alpha_n) = \mathfrak{a}_n^{\mathrm{ord} a_n},$$

then, in order to create an extension of $\mathbb{K}_\infty$, we would have to choose a generator α_n of (α_n); but $\mathbb{K}_\infty(\alpha_n^{1/\mathrm{ord} a_n})$ is in general not independent of the generator we choose. However, when $\mathbb{K}$ is a CM field, there is a natural subgroup of A_n for which the above strategy works. More precisely, if we restrict to the subgroup A_n^- of A_n, since p is odd, for every element $a_n \in A_n^-$ there exists an element $b_n \in A_n^-$ such that

$$a_n = b_n/\overline{b_n}.$$

Notice also that $\mathrm{ord}(a_n) = \mathrm{ord}(b_n)$. Let $\mathfrak{b}_n \in b_n$ and $\mathfrak{a}_n = \mathfrak{b}_n/\overline{\mathfrak{b}_n} \in a_n$. If we let $(\beta_n) = \mathfrak{b}_n^{\mathrm{ord}(a_n)}$, it follows that

$$\mathfrak{a}_n^{\mathrm{ord}(a_n)} = \left(\beta_n/\overline{\beta_n}\right).$$

If we choose a different generator β'_n for $\mathfrak{b}_n^{\mathrm{ord}(a_n)}$, then

$$\beta_n/\overline{\beta_n} = e_n\beta'_n/\overline{\beta'_n},$$

for some unit e_n. It follows that $e_n^{1+\jmath} = 1$, and and since $\mathbb{K}$ is a CM field, all conjugates of e_n have norm one and thus e_n is a root of unity. Since $\mu_{p^\infty} \subset \mathbb{K}_\infty$, it follows that

$$\mathbb{K}_\infty\left(\left(\beta_n/\overline{\beta_n}\right)^{1/\mathrm{ord}a_n}\right) = \mathbb{K}_\infty\left(\left(\beta'_n/\overline{\beta'_n}\right)^{1/\mathrm{ord}a_n}\right).$$

Moreover, it is a straightforward check that if we start with a different ideal $\mathfrak{a}'_n \in a_n$, and define

$$\left(\mathfrak{a}'_n\right)^{\mathrm{ord}a_n} = \left(\alpha_n/\overline{\alpha_n}\right),$$

then $\alpha_n/\overline{\alpha_n}$ and $\beta_n/\overline{\beta_n}$ define the same class inside $\mathbb{K}_\infty^\times/\left(\mathbb{K}_\infty^\times\right)^{\mathrm{ord}(a_n)}$.

It follows that there is a well-defined map that sends a class $a_n \in A_n^-$ to an element in $\mathbb{K}_\infty^\times/\left(\mathbb{K}_\infty^\times\right)^{\mathrm{ord}(a_n)}$. Furthermore, if

$$\mathfrak{a}_n^{\mathrm{ord}(a_n)} = \left(\beta_n/\overline{\beta_n}\right),$$

then the extension $\mathbb{K}_\infty\left(\left(\beta_n/\overline{\beta_n}\right)^{1/\mathrm{ord}(\mathfrak{a}_n)}\right)/\mathbb{K}_\infty$ is unramified outside p (see for example [Wa, Exercise 9.1 b)]). We will simply write $\mathbb{K}\left(a_n^{1/\mathrm{ord}(a_n)}\right)$ for the extension $\mathbb{K}_\infty\left(\left(\beta_n/\overline{\beta_n}\right)^{1/\mathrm{ord}(a_n)}\right)$.

We will now use our results to characterize two important extensions of $\mathbb{K}_\infty$. Let thus p be an odd prime, let $\mathbb{K}$ be a CM field containing ζ_p and let $\mathbb{K}_\infty/\mathbb{K}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$. Consider the group

$$A^- = \varprojlim_n A_n^-.$$

By [Wa, Proposition 13.28], we know that there is an injective pseudo-isomorphism of Λ-modules

$$f : A^- \hookrightarrow \bigoplus_i \Lambda/(p^{k_i}) \oplus \bigoplus_j \Lambda/(g_j(T)), \tag{3.19}$$

where each $g_j(T)$ is a distinguished polynomial. Let A_λ^- be the Λ-submodule of A^- defined by

$$f^{-1}\left(\bigoplus_j \Lambda/(g_j(T))\right).$$

Then A_λ^- is a free $\mathbb{Z}_p$-module of finite rank equal to

$$\lambda^- := \sum_j \deg(g_j(T)).$$

Let Ω_∞ denote the maximal abelian p-extension of $\mathbb{K}_\infty$ unramified outside p and consider the decomposition

$$\Omega_\infty = \Omega_\infty^+ \oplus \Omega_\infty^-.$$

It is well-known that $\mathrm{Gal}(\Omega_\infty^+/\mathbb{K}_\infty)$ is a Λ-torsion module (see for example [Wa, Theorem 13.31]). Let $\mathrm{Gal}(\Omega_\infty^+/\mathbb{K}_\infty)^\circ$ denote the $\mathbb{Z}_p$-torsion submodule of $\mathrm{Gal}(\Omega_\infty^+/\mathbb{K}_\infty)$ and define the field

$$\Omega_\lambda^+ = \left(\Omega_\infty^+\right)^{\mathrm{Gal}(\Omega_\infty^+/\mathbb{K}_\infty)^\circ}.$$

It follows that $\mathrm{Gal}(\Omega_\lambda^+/\mathbb{K}_\infty)$ is a $\mathbb{Z}_p$-free module of finite rank. The extension $\Omega_\lambda^+/\mathbb{K}_\infty$ can be characterized as the compositum of all real $\mathbb{Z}_p$-extensions of $\mathbb{K}_\infty$ (i.e. the compositum of all $\mathbb{Z}_p$-extension of $\mathbb{K}_\infty$ whose Galois group is annihilated by $1-\jmath$).

Since $\jmath^* = -\jmath$ ($*$ denotes Iwasawa's involution), by Theorem 3.27, it follows that the radical $R(\Omega_\lambda^+/\mathbb{K}_\infty)$ of $\Omega_\lambda^+/\mathbb{K}_\infty$ must inject into A_λ^-. In particular, one has

$$\mathbb{Z}_p - \operatorname{rank}\left(R(\Omega_\lambda^+/\mathbb{K}_\infty)\right) \le \mathbb{Z}_p - \operatorname{rank}\left(A_\lambda^-\right). \tag{3.20}$$

On the other hand, Proposition 3.25 together with the above observations show that for an element $a = (a_n)_{n\ge 0} \in A_\lambda^-$, the extension

$$\mathbb{K}_\infty\left(a^{1/p^\infty}\right) := \bigcup_{n\ge 1} \mathbb{K}_\infty\left(a_n^{1/p^{\operatorname{ord}(a_n)}}\right)$$

is a $\mathbb{Z}_p$-extension of $\mathbb{K}_\infty$ unramified outside p, and

$$(1-\jmath)\mathrm{Gal}\left(\mathbb{K}_\infty\left(a^{1/p^\infty}\right)/\mathbb{K}_\infty\right) = \{1\}.$$

It follows that

$$\mathbb{K}_\infty\left(\left(A_\lambda^-\right)^{1/p^\infty}\right) := \bigcup_{a\in A_\lambda^-} \mathbb{K}_\infty\left(a^{1/p^\infty}\right)$$

is a subfield of Ω_∞^+ and, therefore, there exists an injective homomorphism of Λ-modules

$$A_\lambda^- \hookrightarrow R(\Omega_\infty^+/\mathbb{K}_\infty). \tag{3.21}$$

If in addition $\mathbb{K}$ is Galois over $\mathbb{Q}$ and $\mathbb{K}\cap\mathbb{Q}_\infty = \mathbb{Q}$, then (3.21) becomes a homomorphism of $\Lambda[G]$-modules.

Since both A_λ and $R(\Omega_\lambda^+/\mathbb{K}_\infty)$ are free $\mathbb{Z}_p$-modules of finite rank, it follows from (3.20) that the above injection (3.21) has finite cokernel. We obtain the following result.

Proposition 3.28. *With notations as above, one has the following pseudo-isomorphism of* Λ*-modules*

$$A_\lambda^- \sim R(\Omega_\infty^+/\mathbb{K}_\infty).$$

When $\mathbb{K}/\mathbb{Q}$ *is Galois and* $\mathbb{K}_\infty\cap\mathbb{Q}_\infty = \mathbb{Q}$*, the above pseudo-isomorphism becomes one of* $\Lambda[G]$*-modules.*

The second extension of $\mathbb{K}_\infty$ we look at is the one we considered at the end of Section 3.2 and also the one we will use for our application to Leopoldt's conjecture. We keep the same setup as above with $\mathbb{K}$ being a CM field containing ζ_p and we take $\mathbb{M} = \mathcal{Z}(\mathbb{K}^+)\cdot\mathbb{K}_\infty$, where $\mathcal{Z}(\mathbb{K}^+)$ denotes the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{K}^+$. By construction, one has

$$(1-\jmath)\,\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) = \{1\},$$

and moreover, since $\mathbb{M}/\mathbb{K}$ is an abelian extension, one also has

$$T\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty) = \{1\}.$$

If we let R denote the radical of $\mathbb{M}/\mathbb{K}_\infty$, it follows that

$$T^*R = (1+\jmath)R = 1. \tag{3.22}$$

Let $A^-[T^*]$ denote the submodule of A^- consisting of those elements annihilated by T^*. By (3.19), it follows that $A^-[T^*]$ is a free $\mathbb{Z}_p$-module of finite rank. Theorem 3.27 together with (3.22) show that there exists an injective homomorphism of Λ-modules

$$R \hookrightarrow A^-[T^*].$$

On the other hand, one can construct just like in (3.21) an injective homomorphism of Λ-modules

$$A^-[T^*] \hookrightarrow R. \tag{3.23}$$

Again, when $\mathbb{K}/\mathbb{Q}$ is Galois and $\mathbb{K}\cap\mathbb{Q}_\infty = \mathbb{Q}$, (3.23) becomes a homomorphism of $\Lambda[G]$-modules. We obtain the following result.

Proposition 3.29. *With notations as above, one has the following pseudo-isomorphism of* Λ*-modules*

$$A^-[T^*] \sim R.$$

When $\mathbb{K}/\mathbb{Q}$ *is Galois and* $\mathbb{K}_\infty\cap\mathbb{Q}_\infty = \mathbb{Q}$*, the above pseudo-isomorphism becomes one of* $\Lambda[G]$*-modules.*

3.5 Application to Leopoldt's conjecture

In this section we give the proof of Theorem 3.1 and compare our result to those of Greenberg and Jaulent that we already mentioned in Section 3.1.

Proof of Theorem 3.1. The fact that $A^-[T^*]$ is a free $\mathbb{Z}_p$-module of finite rank was established at the end of Section 3.4. To prove that $A^-[T^*]$ and $(1+\jmath)\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)$ have the same $\mathbb{Z}_p$-rank, we consider the field $\mathbb{M} = \mathbb{K}_\infty \cdot \mathcal{Z}(\mathbb{K}^+)$, where $\mathcal{Z}(\mathbb{K}^+)$ denotes the compositum of all $\mathbb{Z}_p$-extensions of $\mathbb{K}^+$. As we already noted in Section 3.1, the group $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ has finite index in $(1+\jmath)\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)$, so it suffices to show that $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ and $A^-[T^*]$ have the same $\mathbb{Z}_p$-rank. By Proposition 3.29, there exists a pseudo-isomorphism of Λ-modules

$$A^-[T^*] \sim R,$$

where R denotes the radical of $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$. Since R and $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ have the same $\mathbb{Z}_p$-rank, it follows that

$$\mathbb{Z}_p - \mathrm{rank}\left(A^-[T^*]\right) = \mathbb{Z}_p - \mathrm{rank}\left((1+\jmath)\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K}_\infty)\right). \tag{3.24}$$

If $\mathbb{K}/\mathbb{Q}$ is Galois, we know from Proposition 3.10 that $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K})$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module. Since $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a quotient of $\mathrm{Gal}(\Omega(\mathbb{K})/\mathbb{K})$, it follows that $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is also a pseudo-cyclic $\mathbb{Z}_p[G]$-module. If in addition $\mathbb{K}\cap\mathbb{Q}_\infty = \mathbb{Q}$, from the isomorphism (3.6) it follows that $\mathrm{Hom}_{\mathbb{Z}_p}(R, \mathbb{Z}_p)$ is a pseudo-cyclic $\mathbb{Z}_p[G]$-module. From Proposition 3.5 it follows that R is also a pseudo-cyclic $\mathbb{Z}_p[G]$-module. Using Proposition 3.29 again, it follows that $A^-[T^*]$ is pseudo-cyclic as a $\mathbb{Z}_p[G]$-module. This completes our proof. □

We will now explain how Theorem 3.1 relates to a construction used by Jaulent in [Ja]. Jaulent showed in [Ja] that if $\mathbb{F}$ is a number field with $\delta(\mathbb{F}) > 0$, then for each nontrivial element $e \in E(\mathbb{F})$ lying in the Leopoldt kernel, there exists a sequence $(e_n)_{n\geq 1}$ such that for all $n \geq 1$ one has $e_n \in E(\mathbb{F})$ and $\mathbb{F}_n(e_n^{1/p^n})/\mathbb{F}_n$ is an unramified extension of $\mathbb{F}_n$ in which all primes in $\mathbb{F}_n$ lying above p split completely. In our setting, this construction shows that if $\delta(\mathbb{K}^+) > 0$, then there exists a p-abelian extension $\mathbb{J}/\mathbb{K}_\infty$ with the following properties:

a) One has $\mathbb{J} \subset \mathbb{H}'_\infty$, where $\mathbb{H}'_\infty$ denotes the maximal unramified p-abelian extension of $\mathbb{K}_\infty$ in which all primes in $\mathbb{K}_\infty$ lying above p split completely.

b) The group $\mathrm{Gal}(\mathbb{J}/\mathbb{K}_\infty)$ is free of $\mathbb{Z}_p$-rank equal to $\delta(\mathbb{K}^+)$.

c) The radical of $\mathbb{J}/\mathbb{K}_\infty$ is annihilated by $1-\jmath$ and T.

Iwasawa proved in [Iwa73, Section 4.4] that

$$\mathrm{Gal}(\mathbb{H}'_\infty/\mathbb{K}_\infty) \cong A_\infty/B =: A'_\infty, \tag{3.25}$$

where $B \subset A_\infty$ denotes the Λ-submodule of A_∞ consisting of classes that contain a prime lying above p.

We will now prove that $A^-[T^*] \sim 0$ implies that $\mathbb{J}/\mathbb{K}_\infty$ is a trivial extension and thus $\delta(\mathbb{K}^+) = 0$. For this, we will create a suitable extension $\mathbb{F}$ of $\mathbb{K}_\infty$ with the property that $\mathbb{J} \subset \mathbb{F}$ and the radical of $\mathbb{F}/\mathbb{K}_\infty$ injects into $A^-[T^*]$.

Consider the decomposition

$$\mathbb{H}'_\infty = (1+\jmath)\mathbb{H}_\infty \bigoplus (1-\jmath)\mathbb{H}^-_\infty.$$

Let $\mathrm{Gal}((1+\jmath)\mathbb{H}'_\infty/\mathbb{K}_\infty)^\circ$ denote the $\mathbb{Z}_p$-torsion submodule of $\mathrm{Gal}((1+\jmath)\mathbb{H}'_\infty/\mathbb{K}_\infty)$ and consider the field

$$\left(\mathbb{H}'_\lambda\right)^+ := \left((1+\jmath)\mathbb{H}'_\infty\right)^{\mathrm{Gal}((1+\jmath)\mathbb{H}'_\infty/\mathbb{K}_\infty)^\circ}.$$

Then $\mathrm{Gal}(\left(\mathbb{H}'_\lambda\right)^+/\mathbb{K}_\infty)$ is a Λ-module and a free $\mathbb{Z}_p$-module of finite rank.

For a noetherian torsion Λ-module X and for a distinguished irreducible polynomial $f(T) \in \Lambda$, we denote by $X[f]$ the submodule of X consisting of elements that are annihilated by f and by $X(f)$ the submodule of X consisting of elements which are annihilated by powers of f. If X is a noetherian torsion Λ-module and in addition X has no finite $\mathbb{Z}_p$-torsion, then by the structure theorem of Λ modules there is an injection with finite cokernel

$$X \hookrightarrow \bigoplus \Lambda/(g_j(T)^{m_j}),$$

where $g_j(T)$ are distinguished irreducible polynomials. Let

$$h(T) = \prod_{\gcd(g_j(T), f(T))=1} g_j(T)^{m_j}.$$

Then $X[h(T)]$ is a Λ-submodule of X (it is the kernel of the map $h(T) : X \to X$) and moreover, one has an injective homomorphism with finite cokernel

$$X(f(T)) \sim X/X[h(T)].$$

Applying this procedure to $X = \mathrm{Gal}((\mathbb{H}'_\lambda)^+/\mathbb{K}_\infty)$, $f(T) = T$ and using (3.25), we obtain a field $\mathbb{F} \subset (\mathbb{H}'_\lambda)^+$ with the property that

$$\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty) \sim A'_\infty(T). \tag{3.26}$$

The field $\mathbb{F}$ can be characterized as the maximal subfield of $\mathbb{H}'_\infty$ with the property that $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$ is a free $\mathbb{Z}_p$-module annihilated by $1 - \jmath$ and whose annihilator polynomial as a Λ-module is a non-negative power of T. With this characterization it is then clear that $\mathbb{J} \subset \mathbb{F}$. Let $R_\mathbb{F}$ denote the radical of $\mathbb{F}/\mathbb{K}_\infty$. Using Theorem 3.27, it follows that there exists an injective homomorphism of Λ-modules

$$R_\mathbb{F} \hookrightarrow A^-[T^*].$$

In particular, since $\mathbb{J} \subset \mathbb{F}$, if $A^-[T^*]$ is trivial, then $\delta(\mathbb{K}^+) = 0$.

Let $\mathbb{H}_\infty$ denote the maximal p-abelian everywhere unramified extension of $\mathbb{K}_\infty$. In a similar manner as above, we can construct a subfield $\mathbb{L} \subset \mathbb{H}_\infty$ such that $\mathrm{Gal}(\mathbb{L}/\mathbb{K}_\infty)$ is a free $\mathbb{Z}_p$-module of finite rank and one has a pseudo-isomorphism of Λ-modules:

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}_\infty) \sim A^+_\infty(T).$$

Let $R_\mathbb{L}$ denote the radical of the extension $\mathbb{L}/\mathbb{K}_\infty$. By Theorem 3.27, there exists an injective homomorphism of Λ-modules

$$R_\mathbb{L} \hookrightarrow A^-_\infty(T^*).$$

In particular, if $\delta(\mathbb{K}^+) = 0$, then by Theorem 3.1, it follows that $A^-[T^*] = 0$, hence $A^-(T^*) = 0$, hence $A^+_\infty(T) = 0$. This gives a different proof of [Gre 1, Proposition 1].

3.6 Further developments

Let $\mathbb{K}$ be a CM field containing ζ_p, let $\mathbb{K}_\infty$ denote its cyclotomic $\mathbb{Z}_p$-extension and let $\mathbb{M}/\mathbb{K}_\infty$ be a Galois extension unramified outside p, with the property that $\mathrm{Gal}(\mathbb{M}/\mathbb{K}_\infty)$ is a free $\mathbb{Z}_p$-module of finite rank. Throughout this chapter, we have conducted an extensive investigation of the structure of such modules and their corresponding radicals. An important problem in Iwasawa theory is understanding how the radical of ramified or unramified extensions looks like. To state this question more precisely, we will need some additional notation.

Let $\mathbb{H}_\infty$ be the maximal p-abelian, everywhere unramified extension of $\mathbb{K}_\infty$. Using the same construction as at the end of the previous section, for an irreducible distinguished polynomial f, we can construct a subfield $\mathbb{F}$ of $\mathbb{H}_\infty$ with the property that $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$ is a noetherian Λ-module without $\mathbb{Z}_p$-torsion and one has a pseudo-isomorphism of Λ-modules

$$\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty) \sim A_\infty(f).$$

Then $\mathbb{F}$ can be described as the maximal $\mathbb{Z}_p$-free unramified extension of $\mathbb{K}_\infty$, with the property that $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$ is annihilated by positive integer powers of f. Let $R_{\mathbb{F}}$ denote the radical of $\mathbb{F}/\mathbb{K}_\infty$. By Theorem 3.27, we know that there exists a homomorphism of Λ-modules

$$\psi : R_{\mathbb{F}} \to A_\infty(f^*),$$

and the same result gives us a description of the kernel of ψ. The question we alluded to above is: can one give a useful description of the image of ψ?

In Proposition 3.29 and Proposition 3.28 we showed two important cases in which the map from the radical to the group of ideal classes is surjective, up to a finite index. However, the two radicals considered there were not restricted to unramified extensions, as in the above setup. Our goal for this section is to give a non-trivial description of the classes that are radicals of unramified extensions.

As before, we let $\mathbb{H}'_\infty$ denote the maximal unramified p-abelian extension of $\mathbb{K}_\infty$ in which all primes in $\mathbb{K}_\infty$ lying above p split completely. We define the field

$$\mathbb{H}'_{\infty,\lambda} = \mathbb{H}_\infty^{\mathrm{Gal}(\mathbb{H}'_\infty/\mathbb{K}_\infty)^\circ},$$

where $\mathrm{Gal}(\mathbb{H}'_\infty/\mathbb{K}_\infty)^\circ$ denotes the $\mathbb{Z}_p$-torsion submodule of $\mathrm{Gal}(\mathbb{H}'_\infty/\mathbb{K}_\infty)$. Then $\mathrm{Gal}(\mathbb{H}'_{\infty,\lambda}/\mathbb{K}_\infty)$ is a noetherian torsion Λ-module and a free $\mathbb{Z}_p$-module of finite rank. If we denote by R the radical of $\mathbb{H}'_{\infty,\lambda}/\mathbb{K}_\infty$, it follows from Theorem 3.27 that there exists a homomorphism of Λ-modules

$$\phi : R \to A_\infty.$$

We let $\mathcal{L}(\mathbb{K})$ denote the image of ϕ. In particular, $\mathcal{L}(\mathbb{K})$ is a Λ-submodule of A_∞.

In what follows, we will show that certain classes in A_∞ cannot be elements of $\mathcal{L}(\mathbb{K})$. To make this more precise, we first analyze a $\mathbb{Z}_p$-extension $\mathbb{L}/\mathbb{K}_\infty$ satisfying $\mathbb{L} \subset \mathbb{H}'_{\infty,\lambda}$. Let α be a generator for the radical of $\mathbb{L}/\mathbb{K}_\infty$. Since $\mathbb{L} \subset \mathbb{H}'_{\infty,\lambda}$, it follows from Proposition 3.3 that for every $n \geq 0$, we can choose $\alpha_n \in \mathbb{K}_{n+k}$ for some constant k independent of n. For all $n \geq 0$, we define the field $\tilde{L}_n$ by

$$\tilde{L}_n = \mathbb{K}_{n+k}(\alpha_n^{1/p^n}).$$

Then one has $\tilde{L}_n \subset \mathbb{H}'_\infty$. Therefore, by [Iwa73, Lemma 9], α_n is a local p^n power in $\mathbb{K}_{n+k}$ (i.e. a p^n power in $\mathbb{K}_{n+k,\mathfrak{p}}$ for every $\mathfrak{p}$ in $\mathbb{K}_{n+k}$ lying above p). In particular, for any positive integer N and any $n \geq 0$, there exists $\rho_n \in \mathbb{K}_{n+k}$ such that

$$\alpha_n \equiv \rho_n^{p^n} \pmod{p^N}.$$

Notice that modifying α_n by $\rho_n^{p^n}$ does not change the extension $\tilde{L}_n$ or the class in A_{n+k} that α_n gives rise to, so we can assume without loss of generality that $\alpha_n = 1 \pmod{p^N}$. It is important to note that in this process N can be as large as we want, i.e. we can make α_n as 'locally small' as we want. We will need this information shortly.

We are now ready to prove a sufficient condition for a class in A_∞ to not be in $\mathcal{L}(\mathbb{K})$. Since the constant k will play essentially no role in our subsequent analysis, we will take $k = 0$ to simplify our notations.

Proposition 3.30. *Let c be the absolute constant from Proposition 3.25 and let $b = (b_n)_{n\geq 0} \in A_\infty$ such that for all sufficiently large n, b_n is a non-trivial element in $A_n^{p^c}$. Assume that there is a cofinal sequence in $\mathbb{N}$ such that for all n in that sequence, there exists a $\mathbb{Z}_p$-extension $\mathbb{F}_n$ of $\mathbb{K}_n$ such that $\mathbb{F}_n \cap \mathbb{H}_n \neq \mathbb{K}_n$ and $\phi(b_n)$ generates the group $\mathrm{Gal}(\mathbb{F}_n \cap \mathbb{H}_n/\mathbb{K}_n)$. Then $b \notin \mathcal{L}(\mathbb{K})$.*

Proof. Assume the contrary. Then there exists a $\mathbb{Z}_p$-extension $\mathbb{L} \subset \mathbb{H}'_\infty$ which has finite intersection with Ω_E and $k \geq 0$ such that for all sufficiently large n, there exists an extension $\tilde{L}_n$ of $\mathbb{K}_{n+k}$ with $[\tilde{L}_n : \mathbb{K}_{n+k}] = p^n$ and $\tilde{L}_n \subset \mathbb{L}$. For $N > 0$, we let T_N be the p-part of the ray class field modulo the ray (p^N). Notice that $\bigcup\limits_{N\geq 1} T_N = \Omega(\mathbb{K}_n)$, so there exists some large enough N such that

$$[T_N \cap \mathbb{F}_n : \mathbb{K}_n] > p^n.$$

The discussion preceding Proposition 3.30 shows that we can take $\mathcal{B}_n \in b_n$ such that

$$\mathcal{B}_n^{p^n} = (\alpha_n) \quad \text{and } \alpha_n \equiv 1 \pmod{p^N}. \tag{3.27}$$

If we consider the Artin symbol of $\mathcal{B}_n$ in $T_N/\mathbb{K}_n$, by Chebotarev's theorem we can find a prime $\mathfrak{q}_n \in \mathbb{K}_n$ such that

$$\left(\frac{T_N/\mathbb{K}_n}{\mathfrak{q}_n}\right) = \left(\frac{T_N/\mathbb{K}_n}{\mathcal{B}_n}\right).$$

In particular, we must have that

$$\left(\frac{\mathbb{H}_n \cap \mathbb{F}_n}{\mathfrak{q}_n}\right) = \left(\frac{\mathbb{H}_n \cap \mathbb{F}_n}{b_n}\right).$$

By hypothesis, $\left(\frac{\mathbb{H}_n\cap\mathbb{F}_n}{b_n}\right)$ is a generator of $\mathrm{Gal}(\mathbb{H}_n \cap \mathbb{F}_n/\mathbb{K}_n)$, and therefore $\mathfrak{q}_n$ must be inert in $\mathbb{H}_n \cap \mathbb{F}_n$. Since $\mathfrak{q}_n$ is coprime to p, it follows that $\mathfrak{q}_n$ is inert in the $\mathbb{Z}_p$-extension $\mathbb{F}_n/\mathbb{K}_n$. On the other hand, by (3.27), it follows that

$$\left(\frac{T_N \cap \mathbb{F}_n/\mathbb{K}_n}{\mathfrak{q}_n^{p^n}}\right) = \left(\frac{T_N \cap \mathbb{F}_n/\mathbb{K}_n}{\mathcal{B}_n^{p^n}}\right) = \left(\frac{T_N \cap \mathbb{F}_n/\mathbb{K}_n}{(\alpha_n)}\right) = 1.$$

Since we considered N such that $[T_N \cap \mathbb{F}_n : \mathbb{K}_n] > p^n$, this contradicts the fact that $\mathfrak{q}_n$ is inert. The conclusion follows. □

Let $\mathbb{H}'_T := \Omega(\mathbb{K})^+ \cap \mathbb{H}'_\infty$. Essentially by the definition of the fields $\mathbb{H}'_\infty$ and $\Omega(\mathbb{K})^+$, one has that $\mathbb{H}'_T$ is a Galois extension of $\mathbb{K}_\infty$ for which the Artin map induces a pseudo-isomorphism of Λ-modules

$$\mathrm{Gal}\left(\mathbb{H}'_T/\mathbb{K}_\infty\right) \cong \frac{\left(A'(T)\right)^+}{T\left(A'(T)\right)^+}.$$

Now let $\mathbb{F} \subset \mathbb{H}'_T$ be a $\mathbb{Z}_p$-extension of $\mathbb{K}_\infty$ generated by an element $b = (b_n)_{n\geq 0}$ which has non-trivial image in $\frac{(A'(T))^+}{T(A'(T))^+}$. For all sufficiently large n, the unramified extension of $\mathbb{K}_n$ generated by b_n via the Artin map is $\mathbb{Z}_p$-extendable. Indeed, the $\mathbb{Z}_p$-extension of $\mathbb{K}_n$ is obtained by fixing a lift $\tilde{\Gamma}$ of Γ to $\mathrm{Gal}(\mathbb{H}'_T/\mathbb{K})$ and then considering the extension $\mathbb{F}^{\widetilde{\Gamma^n}}$, which will be a $\mathbb{Z}_p$-extension of $\mathbb{K}_n$. Hence, by Proposition 3.30, $b \notin \mathcal{L}(\mathbb{K})$.

We have the following important result.

Theorem 3.31. *Let $\mathbb{F}/\mathbb{K}_\infty$ be a $\mathbb{Z}_p$-extension with $\mathbb{F} \not\subset \Omega_E$ and let $a \in A_\infty$ be the image of the radical of $\mathbb{F}/\mathbb{K}_\infty$ under our standard homomorphism. If $a^{1-\jmath} = 1$ and the image of a in $\frac{(A'(T))^+}{T(A'(T))^+}$ under the natural projection has infinite order, then $\mathbb{F} \not\subset \mathbb{H}_\infty$.*

Proof. The discussion preceding the theorem shows that $\mathbb{F} \not\subset \mathbb{H}'_\infty$. To show the stronger statement that $\mathbb{F} \not\subset \mathbb{H}_\infty$, we proceed as follows.

Assume the contrary. Then, by duality, one necessarily has $\mathbb{F} \subset \mathbb{H}^-_{T^*}$, where $\mathbb{H}^-_{T^*}$ is the compositum of all unramified $\mathbb{Z}_p$-extensions of $\mathbb{K}_\infty$ whose radicals are annihilated by $1 - \jmath$ and positive integer powers of T. Moreover, one has

$$\mathrm{Gal}(\mathbb{H}^-_{T^*}/\mathbb{K}_\infty) \sim A^-(T^*).$$

Since $B^-(T^*)$ is finite, it follows that $A^-(T^*) \sim (A'(T^*))^-$. In particular, it follows that the group $\mathrm{Gal}(\mathbb{H}^-_{T^*}/\mathbb{H}^-_{T^*} \cap \mathbb{H}'_\infty)$ (and hence also its corresponding radical) is $\mathbb{Z}_p$-torsion. However, by our assumption the radical of $\mathbb{F}/\mathbb{K}_\infty$ gives an element of infinite order inside the radical of $\mathbb{H}^-_{T^*}/\mathbb{H}^-_{T^*} \cap \mathbb{H}'_\infty$, which is a contradiction. The conclusion follows. □

Bibliography

[Alp-Bell] Alperin, J.L, Bell, R.B. (1995). *Groups and Representations*: Springer.

[Art-Ta] Artin, E., Tate, J. (1967). *Class Field Theory*: AMS Chelsea Publishing.

[Bem] Bembom, T. (2012). *The Capitulation Problem in Class Field Theory*, Ph.D. thesis: `http://hdl.handle.net/11858/00-1735-0000-000D-F05F-8`.

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

[Be-Pa] Bertrandias, F., Payan, J-F. (1972). *Gamma extensions et invariants cyclotomiques*: Ann. Sci. ENS, 4, 5, pp. 517-543.

[BBM14] Bilu, Y., Bugeaud, Y., Mignotte, M. (2014). *The problem of Catalan*: Springer.

[Br] Brown, K.S. (1982). *Cohomology of groups*: Springer.

[Bru] Brumer, A. (1967). *On the units of algebraic number fields*: Mathematika, 14, pp. 121-124.

[Car] Carlson, J.F. (1996). *Modules and Group Algebras*: Birkhäuser Basel.

[Ca-Fro] Cassels, J.W.S, Frohlich, A. (1967). *Algebraic Number Theory*: Academic Press.

[C-K-L] Choi, J., Kezuka, Y., Li, Y. (2018). *Analogues of Iwasawas $\mu = 0$ conjecture and weak Leopoldt theorem for certain non-cyclotomic $\mathbb{Z}_2$-extensions*: arxiv:1711.01697v1.

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

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

[Co-Su] Coates, J., Sujatha, R. (2006). *Cyclotomic Fields and Zeta Values*: Springer.

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

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

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

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

[Cox] Cox, D. (2013). *Primes of the form $x^2 + ny^2$*, second edition: Wiley Press.

[Cri] Crişan, V. (2017). *On an isomorphism lying behind the class number formula*: Carpathian Journal of Mathematics Vol. 33, No. 1, pp. 43-48.

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

[Fe-Wa] Ferrero, B., Washington, L.C. (1979). *The Iwasawa invariant μ_p vanishes for abelian number fields*: Ann. of Math. (2) 109, no. 2, pp. 377-395.

[Gil 1] Gillard, R. (1979). *Unités cyclotomiqués, unités semi-locales et Z_l-extensions II*: Ann. Fourier Inst., 29, pp. 1-15.

[Gil 2] Gillard, R. (1985). *Fonctions L p-adiques des des corps quadratiques imaginaires et de leurs extensions abèliennes*: J. Reine Angew. Math. 358, pp. 76-91.

[Gil 3] Gillard, R. (1987). *Transformation de Mellin-Leopoldt des fonctions elliptiques*: J. Number Theory 25, no. 3, pp. 379-393.

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

[Gras] Gras, G. (2003). *Class Field Theory. From Theory to Practice*: Springer.

[Gre 1] Greenberg, R. (1976). *On the Iwasawa Invariants of Totally Real Number Fields*: American Journal of Mathematics, vol. 98, No. 1, pp. 263-284.

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

[Gre 3] Greenberg, R. (2001). *Iwasawa Theory - Past and Present*: Advanced Studies in Pure Mathematics 30, Class Field Theory - Its Centenary and Prospect, pp. 335-385.

[Gre 4] Greenberg, R. *Topics in Iwasawa Theory*, preprint: `https://www.math.washington.edu/~greenber/book.pdf`.

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

[Ich] Ichimura, H. (2015). *Semi-local units at p of a cyclotomic $\mathbb{Z}_p$-extension congruent to* 1 *modulo* $\zeta_p - 1$: Hokkaido Math. J., 44, no. 3, pp. 397-407.

[Iwa 1] Iwasawa, K. (1956). *A note on class numbers of algebraic number fields*: Abh. Math. Hamburg, 20, pp. 257-258.

[Iwa 2] Iwasawa, K. (1959). *On Γ-extensions of algebraic number fields*: Bulletin of the American Mathematical Society, 65, pp. 183-226.

[Iwa 3] Iwasawa, K. (1973). *On the μ-invariants of $\mathbb{Z}_l$-extensions*: Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Tokyo: Kinokuniya, pp. 1-11.

[Iwa73] Iwasawa, K. (1973). *On $\mathbb{Z}_l$-extensions of number fields*: Ann. Math. Second Series, 98, pp. 246-326.

[Jan] Janusz, G. (1973). *Algebraic Number fields*: Academic Press, New York.

[Ja] Jaulent, J. (2007). *Note sur la conjecture de Leopoldt*: hal-00198929.

[KKS] Kato, K., Kurokawa, N., Saito, T. (2012). *Number Theory 3. Iwasawa Theory and Modular Forms*: American Mathematical Society.

[Koch] Koch, H. (2002). *Galois Theory of p-Extensions*: Springer.

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

[Lang 1] Lang, S. (1990). *Cyclotomic fields I and II*: Springer-Verlag.

[Lang 2] Lang, S. (2002). *Algebra*: Springer-Verlag.

[Lu] Lubin, J. (1964). *One Parameter Formal Lie Groups over p-adic Integer Rings*: Annals of Mathematics, Second Series, Vol. 80, No. 3, pp. 464-484.

[Marcus] Marcus, D. (1977). *Number Fields*: Springer-Verlag, Berlin, Heidelberg, and New York.

[Mats] Matsumura, H. (1989). *Commutative Ring Theory*: Cambridge University Press.

[Ma] Mazur, B. (1972). *Rational points of abelian varieties with values in tower of number fields*: Inv. Math., 18, pp. 183-266.

[MO] `https://mathoverflow.net/questions/6928/how-do-we-study-iwasawa-theory`

[MS] `https://math.stackexchange.com/questions/2420504/roots-of-unity-wild-ramification-and-units-of-norm-one-in-local-fields`

[Neu 1] Neukirch, J. (1986). *Class Field Theory*: Springer Berlin Heidelberg.

[Neu 2] Neukirch, J. (1999). *Algebraic Number Theory*: Springer-Verlag Berlin Heidelberg.

[O-V] Oukhaba, H., Viguié, S. (2016). *On the μ-invariant of Katz p-adic L-functions attached to imaginary quadratic fields*: Forum Math. 28, no. 3, pp. 507-525.

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

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

[Sch] Schneps, L. (1987). *On the μ-invariant of p-adic L-functions attached to elliptic curves with complex multiplication*: J. Number Theory 25, no. 1, pp. 20-33.

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

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

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

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

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

[Wa] Washington, L.C. (1997). *Introduction to Cyclotomic fields, Second Edition*: Springer.

[We] Weil, A. (1955). *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.

[Wein] Weintraub, S.H. (2003). *Representation Theory of Finite Groups: Algebra and Arithmetic*: American Mathematical Society.

[wiki 1] `https://en.wikipedia.org/wiki/Fermat's_Last_Theorem`

[wiki 2] `https://en.wikipedia.org/wiki/Kummer-Vandiver_conjecture`

[Wi 1] Wiles, A. (1990). *The Iwasawa Conjecture for Totally Real Fields*: Annals of Mathematics, 131, pp. 493-540.

[Wi 2] Wiles, A. (1995). *Modular elliptic curves and Fermat's Last Theorem*: Annals of Mathematics, 141, pp. 443-551.