Classical Conjectures in Iwasawa Theory for the split prime $\mathbb{Z}_p$-extension and the cyclotomic $\mathbb{Z}_p$-extension

Dissertation

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

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

vorgelegt von
Katharina Müller
aus Göttingen

Göttingen, Februar 2021

Betreuungsausschuss:

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

Prof. Dr. Harald Helfgott
Mathematisches Institut
Georg-August-Universität Göttingen

Mitglieder der Prüfungskommission:

Referent:

Prof. Dr. Preda Mihăilsecu
Mathematisches Institut
Georg-August-Universität Göttingen

Korreferent:

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

Weitere Mitglieder der Prüfungskommission:

Prof. Dr. Harald Helfgott
Mathematisches Institut
Georg-August-Universität Göttingen

Prof. Dr. Damaris Schindler
Mathematisches Institut
Georg-August-Universität Göttingen

Prof. Dr. Gerlind Plonka-Hoch
Institut für numerische und angewandte Mathematik
Georg-August-Universität Göttingen

Prof. Dr. Anja Sturm
Institut für mathematische Stochastik
Georg-August-Universität Göttingen

Tag der mündlichen Prüfung: 26.03.2021

Acknowledgments

I would like to thank all the people who supported me while writing this thesis. First of all my supervisor Prof. Dr. Preda Mihăilsecu for his guidance and many helpful discussions over the last years.

I would also like to thank Prof. Dr. Harald Helfgott and Prof. Dr. Jörg Brüdern for being always available to answer questions – both mathematically and non-mathematically.

I am especially grateful for the support by my coauthors: Vlad Crişan, Mohamed Mahmoud Chems-Eddin and Sören Kleine. Especially Sören was extremely supportive during the last year and helped me with many very useful remarks on my work.

I would also like to thank my parents and Björn, Hendrik, Hanna, Inge, Markus and Miriam for their emotional support during my PhD and for listening to all the small and big problems in the last years.

Contents

Chapter 1

Introduction

1.1 Historic overview

Throughout this thesis, let p be a prime and $\mathbb{Z}_p$ the ring of p-adic integers. In his seminal papers [Iw 1] and [Iw 2] Kenkichi Iwasawa introduced the theory of Galois extensions $\mathbb{K}_\infty$ of number fields $\mathbb{K}$ such that $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}) \cong \mathbb{Z}_p$ – so called $\mathbb{Z}_p$-extensions. In 1959, he intensively studied the structure of Γ-modules, where $\Gamma \cong \mathbb{Z}_p$ [Iw 1]. The main focus lay on discrete abelian modules. As discrete abelian modules are in Pontryagin's sense dual to compact abelian modules, he was able to derive results on compact abelian groups. In particular, he used his module theoretic results to derive an asymptotic formula for the size of the p-class group of the intermediate fields $\mathbb{K}_n$ of degree p^n of a $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/\mathbb{K}$.

Theorem. *[Iw 1] Let p^{e_n} be the order of the p-class group of $\mathbb{K}_n$. There are invariants μ, λ and ν such that*

$$e_n = \lambda n + p^n \mu + \nu \tag{1.1}$$

for all n large enough.

In the following years, Iwasawa developed his theory of $\mathbb{Z}_p$-extensions further [Iw 2]. One of the main results of his work is the description of the maximal p-abelian p-ramified extension $\mathbb{M}_\infty$ of a number field containing the p-th roots of unity (the 4-th roots if $p = 2$) in terms of Kummer-radicals and as a module over the ring of formal power series in one indeterminate and with coefficients in $\mathbb{Z}_p$.

In general the main interest of Iwasawa theory is to understand arithmetic and asymptotic properties along the different subfields of degree p^n in $\mathbb{Z}_p$-extensions $\mathbb{K}_\infty/\mathbb{K}$ for example class groups, certain Galois groups and units. More recent studies involve objects like Selmer groups of abelian varieties along $\mathbb{Z}_p$-extensions.

As already Iwasawa pointed out it is relatively easy to see that each number field has at least one $\mathbb{Z}_p$-extension. This so called *cyclotomic $\mathbb{Z}_p$-extension* is constructed as follows: Let $\mathbb{L}_\infty = \cup_{n\in\mathbb{N}}\mathbb{K}(\zeta_{p^n})$. Then $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}) \cong \mathbb{Z}_p^\times \cong W \times \mathbb{Z}_p$, where W denotes a finite abelian group. If we define $\mathbb{K}_\infty = \mathbb{L}_\infty^W$, we obtain a $\mathbb{Z}_p$-extension of $\mathbb{K}$. It is an interesting question how many $\mathbb{Z}_p$-extensions a fixed number field has. Leopoldt's conjecture predicts:

Conjecture (Leopoldt's Conjecture)**.** *An arbitrary number field has* $1 + r_2$ *linearly independent* $\mathbb{Z}_p$*-extensions, where* r_2 *is the number of pairs of complex conjugate embeddings of* $\mathbb{K}$*.*

It is well known that any number field admits at least $r_2 + 1$ independent $\mathbb{Z}_p$-extensions. So Leopoldt's conjecture can be formulated as the statement that there are not more than $r_2 + 1$ independnet $\mathbb{Z}_p$-extensions. Leopoldt's conjecture has been proved for abelian extensions of $\mathbb{Q}$ and abelian extensions of imaginary quadratic fields by works of Brumer [Br] and Ax [Ax] based on Baker's results on linear forms in logarithms. As a consequence, an imaginary quadratic field $\mathbb{K}$ has exactly two independent $\mathbb{Z}_p$-extensions. If p splits in $\mathbb{K}/\mathbb{Q}$ into two factors $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ then there exist exactly two independent $\mathbb{Z}_p$ extensions, one unramified outside $\mathfrak{p}$ and one unramified outside $\overline{\mathfrak{p}}$, respectively. We will refer to the extension unramfied outside $\mathfrak{p}$ as the *split prime* $\mathbb{Z}_p$*-extension.* In the bigger part of this thesis we will mainly consider the two $\mathbb{Z}_p$-extensions described above: The split prime $\mathbb{Z}_p$-extension and the cyclotomic one.

1.2 Notations and auxiliary results

We will always write τ for a topological generator of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ and define $T = \tau - 1$ as well as the ring of formal power series $\Lambda = \mathbb{Z}_p[[T]]$. Let S be the set of primes that ramify in $\mathbb{K}_\infty/\mathbb{K}$ and let $\mathbb{M}_n$ be the maximal p-abelian extension of $\mathbb{K}_n$ that is unramified outside S. We define $X_n = \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty)$. We define M_∞ as the maximal p-abelian extension of $\mathbb{K}_\infty$ that is unramified outside S. Clearly,

$$X_\infty := \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{K}_\infty) = \varprojlim_{\infty \leftarrow n} X_n.$$

Note that the fields $\mathbb{M}_n$ are Galois over $\mathbb{K}_n$ by maximality. Hence, there is a well defined action of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ on X_n, inducing an action of Λ on X_n. Thus, X_∞ is a Λ-module. Even though Iwasawa theory provides powerful tools to describe the Λ-module structure of X_∞ the most common context to use these tools is the one of class groups: Let A_n be the p-class group of $\mathbb{K}_n$ and $\mathbb{H}_n$ be the p-Hilbert class field of $\mathbb{K}_n$. By class field theory we obtain an isomorphism

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

as well as

$$A_\infty = \varprojlim_{\infty \leftarrow n} A_n \cong \mathrm{Gal}(\mathbb{H}_\infty/\mathbb{K}_\infty). \tag{1.2}$$

As before we can deduce that $\mathbb{H}_n$ is Galois over $\mathbb{K}$ and A_∞ is a Λ-module. In the Iwasawa theoretic description of A_∞ frequent use is made of the isomorphism (1.2). Apart from the class group, there are various other algebraic objects that have a Galois theoretic interpretation via class field theory, for example the global and local units, which we define as follows: Let s_n be the number of prime ideals in $\mathbb{K}_n$ that ramify in $\mathbb{K}_\infty/\mathbb{K}_n$. We denote these ramified primes by $\mathfrak{P}_{n,i}$ for $1 \leq i \leq s_n$. Consider the completions $\mathbb{K}_{n,i}$ of $\mathbb{K}_n$ at $\mathfrak{P}_{n,i}$. Then there exists a uniformizer $\pi_{n,i}$ in $\mathbb{K}_{n,i}$ generating the maximal ideal of the ring of integers $\mathcal{O}(\mathbb{K}_{n,i})$. Let $U_{n,i} \subset \mathbb{K}_{n,i}$ be the units that

are congruent to 1 modulo $\pi_{n,i}$ and let $V_{n,i} \subset \mathbb{K}_{n,i}$ be the subgroup of roots of unity whose order is coprime to p. Then we get a decomposition $\mathbb{K}_{n,i}^{\times} = \pi_{n,i}^{\mathbb{Z}} \cdot U_{n,i} \cdot V_{n,i}$. We define the local units U_n as the product $U_n = \prod_{i=1}^{s_n} U_{n,i}$. Let E_n be the group of units in $\mathcal{O}(\mathbb{K}_n)$ that are congruent to 1 modulo $\prod_{i=1}^{s_0} \mathfrak{P}_{0,i}$. We can embed E_n diagonally into U_n. Let $\overline{E}_n = \cap_{m\in\mathbb{N}} E_n U_n^{p^m}$ be the p-adic closure of E_n in U_n. By class field theory we have an Artin homomorphism

$$\phi_n \colon U_n \to Gal(\mathbb{M}_n/\mathbb{H}_n)$$

inducing an isomorphism

$$\phi_n \colon U_n/\overline{E}_n \to Gal(\mathbb{M}_n/\mathbb{H}_n).$$

We define $U_\infty = \lim_{\infty\leftarrow n} U_n$, $U_{\infty,i} = \lim_{\infty\leftarrow n} U_{n,i}$ and $\overline{E}_\infty = \lim_{\infty\leftarrow n} \overline{E}_n$, where the projective limit is taken with respect to the norms $N_{n,n-1} \colon \mathbb{K}_n \to \mathbb{K}_{n-1}$. Then we obtain an isomorphism

$$U_\infty/\overline{E}_\infty \cong \lim_{\infty\leftarrow n} U_n/\overline{E}_n.$$

As the norms $N_{n,n-1} \colon U_n \to U_{n-1}$ are compatible with the natural restrictions

$$\mathrm{Gal}(\mathbb{M}_n/\mathbb{H}_n) \to \mathrm{Gal}(\mathbb{M}_{n-1}/\mathbb{H}_{n-1})$$

this induces an Artin homomorphism

$$\phi \colon U_\infty \to \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{H}_\infty)$$

and an isomorphism

$$\phi \colon U_\infty/\overline{E}_\infty \to \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{H}_\infty).$$

To underline how powerful Artin's isomorphism is we will consider the following

Example 1.2.1. *Let $p > 2$ and $\mathbb{K}$ be an abelian extension of $\mathbb{Q}$ containing ζ_p such that $\mathbb{K}$ and $\mathbb{K}(\zeta_{p^2})$ are of class number 1 (e.g $p = 5$ and $\mathbb{K} = \mathbb{Q}(\zeta_5)$). Let $\mathbb{K}_n$ be the intermediate layers of the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/\mathbb{K}$ and assume that each $\mathbb{K}_n$ contains only one prime above p. It is easy to show that in this case the class number of $\mathbb{K}_n$ is coprime to p for all n. Hence, $U_n/\overline{E}_n \cong Gal(\mathbb{M}_n/\mathbb{K}_n)$. Let $e \in U_n^p \cap E$. Then $\mathbb{K}_n(e^{1/p})/\mathbb{K}_n$ is an unramifed Galois extension. As $|A_n|$ is coprime to p it follows that $e \in E^p$ and $U_n^p \cap \overline{E} = \overline{E}$. Therefore, $(U_n/\overline{E})^+ \cong \mathbb{Z}_p$ and $\mathbb{M}_\infty^+ = \mathbb{K}_\infty$.*

To study the structure of the groups X_∞ and A_∞ as Λ-modules in more generality we need the following

Definition 1.2.2. *Let $\mathfrak{h}_i$ be primes of height one in Λ. We call a Λ-module X elementary if there are indices e_i such that*

$$X \cong \Lambda^{e_0} \oplus \Lambda/\mathfrak{h}_1^{e_1} \oplus \cdots \oplus \Lambda/\mathfrak{h}_k^{e_k}.$$

Let X and Y be two Λ-modules. We call a Λ-homomorphism $f \colon X \to Y$ a pseudo isomorphism if the kernel and the cokernel are finite.

It is well known that every noetherian Λ-module is pseudo isomorphic to an elementary Λ-module. To verify that our Λ-modules of interest are noetherian we can use the following Lemma due to Nakayama [Wash, Lemma 13.16].

Lemma 1.2.3. *Let X be a compact Λ-module. Then the following are equivalent:*

i) X is a noetherian Λ-module.

ii) $X/(p,T)X$ is finite.

It is easy to verify that X_∞ and A_∞ satisfy *ii)*. As A_∞ is Λ-torsion we see that in this case $e_0 = 0$. In general the possible candidates for the $\mathfrak{h}_i$ are

1.) $\mathfrak{h} = (p)$

2.) $\mathfrak{h} = (f)$ is a distinguished polynomial.

If M is a noetherian Λ-torsion module and f_i is one of the distinguished polynomials occurring in the corresponding elementary Λ-module, then we denote by $M(f_i)$ the f_i rational part, i.e. the maximal submodule that is annihilated by a power of f_i.

Let E be any elementary Λ-module then we define the Iwasawa invariants associated to E as follows:

Definition 1.2.4. *Let $V_\lambda = \{i \mid \mathfrak{h}_i = (f)$ for a distinguished polynomial $f\}$ and $V_\mu = \{i \mid \mathfrak{h}_i = (p)\}$. Then we define*

$$\mu(E) = \sum_{i \in V_\mu} e_i$$
$$\lambda(E) = \sum_{i \in V_\lambda} \deg(\mathfrak{h}_i) e_i.$$

We define the characteristic ideal of E as the product $\prod_{i=1}^{k} \mathfrak{h}_i^{e_i}$.

As the elementary Λ-module associated to a Λ-torsion module X is unique, we define $\mu(X) = \mu(E)$ and $\lambda(X) = \lambda(E)$. Note that these invariants are precisely the ones that appeared in (1.1). If X_n is finite for all n it is easy to show that a formula similar to (1.1) holds for the size of X_n. One intermediate step in proving such identities is to write X_n and A_n as quotients of X_∞ and A_∞, respectively. To do so we define the polynomials

$$\omega_n(T) = (T+1)^{p^n} - 1$$
$$\nu_{n,m}(T) = \frac{\omega_n(T)}{\omega_m(T)} \text{ for } n \geq m \geq 0.$$

Recall that $T = \tau - 1$. Hence, we can rewrite ω_n as $\tau^{p^n} - 1$. The element τ^{p^n} is a topological generator for $\Gamma^{p^n} = \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}_n)$. So if we replace the base field $\mathbb{K}$ by $\mathbb{K}_n$ and define the Iwasawa algebra Λ' with respect to the $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/\mathbb{K}_n$, then

we obtain $\Lambda' \cong \mathbb{Z}_p[[\omega_n(T)]]$. It is easy to see that $\omega_n(T) = (\omega_m(T)+1)^{p^{n-m}} - 1$. Therefore,

$$\nu_{n,m}(T) = \sum_{k=0}^{p^{n-m}} (\tau^{p^m})^k$$

which is the norm $N_{n,m}\colon \mathbb{K}_n \to \mathbb{K}_m$ for $n \geq m$.

Note that $\mathbb{M}_n$ is the maximal abelian extension of $\mathbb{K}_n$ contained in $\mathbb{M}_\infty$. Hence,

$$X_n \cong \mathrm{Gal}(\mathbb{M}_n/\mathbb{K}_\infty) = X_\infty/\omega_n X_\infty$$

for all n large enough. If we want to derive a similar relation for A_∞ and A_n the situation is slightly more complicated. There is a submodule $Y \subset A_\infty$ and an index n_0 such that A_n is isomorphic to $A_\infty/\nu_{n,n_0}Y$ for all n large enough [Iw 2, Theorem 6]. We will use this result for example in Chapter 6. So in both cases the elementary Λ-module does not only determine the structure of the modules X_∞ and A_∞ but also provides information about the (finite) abelian groups X_n and A_n.

1.3 Structure of the thesis

In Chapters 2 and 3 we will study the split prime $\mathbb{Z}_p$-extension of an imaginary quadratic field $\mathbb{K}$ and a rational prime p which splits in $\mathbb{K}$ into two distinct primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. Recall that the split prime $\mathbb{Z}_p$-extension, denoted by $\mathbb{K}_\infty$, is unramified outside $\mathfrak{p}$. Let $\mathbb{L}$ be an arbitrary finite abelian extension of $\mathbb{K}$. Define $\mathbb{L}_\infty = \mathbb{K}_\infty\mathbb{L}$ and $\Gamma = \mathrm{Gal}(\mathbb{L}_\infty/\mathbb{L})$.

Let $\mathbb{M}_\infty$ be the maximal p-abelian extension of $\mathbb{L}_\infty$ that is unramified outside the primes in $\mathbb{L}_\infty$ lying above $\mathfrak{p}$. The module $X(\mathbb{L}_\infty) := \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{L}_\infty)$ becomes a $\mathbb{Z}_p[[\Gamma]]$-module under conjugation. Hence, we can view it as a module over $\mathbb{Z}_p[[T]]$ under a fixed isomorphism $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$. For every $n \geq 0$, we let $\mathbb{L}_n$ denote the unique extension of $\mathbb{L}$ of degree p^n with $\mathbb{L}_n \subset \mathbb{L}_\infty$. Then $\mathbb{L}_n$ is an abelian extension of the imaginary quadratic field $\mathbb{K}$, so, by the Baker-Brumer theorem [Ax, Br], the $\mathfrak{p}$-adic Leopoldt conjecture holds for the intermediate fields $\mathbb{L}_n$ – meaning that there is exactly one $\mathbb{Z}_p$-extension unramified outside $\mathfrak{p}$ above $\mathbb{L}_n$. It follows that $X(\mathbb{L}_\infty)$ is a $\mathbb{Z}_p[[T]]$-torsion module and hence it has a well-defined characteristic polynomial of the form $p^\mu \cdot f(T)$ for some non-negative integer μ and some distinguished polynomial $f \in \mathbb{Z}_p[[T]]$.

In Chapter 2 we shall generalize work of Leila Schneps [Sch] to prove a result which is equivalent to the assertion that the μ-invariant of $X(\mathbb{L}_\infty)$ is zero.

In Chapter 3 we specialize our focus to the case $p = 2$ and consider the Iwasawa Main Conjecture in the above setting.

In both chapters we will frequently use an elliptic curve E defined over a certain finite abelian extension of $\mathbb{K}$. But elliptic curves and more generally abelian varieties do not only play an important role in Iwasawa theory as a tool to prove results like Theorem 2.1.1, they are of their own independent interest. Greenberg and Vatsal introduced the study of the Iwasawa invariants of elliptic curves defined over $\mathbb{Q}$ with

good ordinary reduction at p [Gre-Vat] . They considered the p-primary part of the Selmer groups over $\mathbb{Q}_\infty$ (the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$) and proved that the μ-invariants of isogenous curves vanish simultaneously. In Chapter 4 we will prove an analogous result for general abelian varieties and their fine Selmer groups.

In the parts II and III of this thesis we will only consider the cyclotomic $\mathbb{Z}_p$-extension. This is the $\mathbb{Z}_p$-extension studied the most by Iwasawa himself. One of the main advantageous properties of this $\mathbb{Z}_p$-extension is the fact that it is – assuming that Leopoldt's conjecture holds – the only one that is a CM field – as long as the base field $\mathbb{K}$ is a CM field. Similar as for the split prime $\mathbb{Z}_p$-extension one expects the following behavior of the μ-invariants.

Conjecture. *The μ-invariant of the projective limit of the p-class groups of the intermediate fields $\mathbb{K}_n$, denoted by A_∞, vanishes (i.e. that the characteristic ideal of A_∞ is a distinguished polynomial).*

As for the split prime $\mathbb{Z}_p$-extension this is known for abelian extensions of $\mathbb{Q}$ ([Fe-Wa] or [Si]). In fact, the proof we give for Theorem 2.1.1 is a generalization of Sinnott's proof for the cyclotomic $\mathbb{Z}_p$-extension. Using cyclotomic units instead of elliptic units, one can formulate an Iwasawa Main conjecture – analogously to the one considered in Part I – relating characteristic ideals of class groups to the characteristic ideal of the quotient of the units modulo the cyclotomic units anlong the cyclotomic $\mathbb{Z}_p$-extension (see for example [Ru 3]).

In Chapter 6 we describe some consequences of the failure of the Leopoldt conjecture and the $\mu = 0$ conjecture for general CM fields. The ideas presented in Chapter 6 rely on analyzing certain Galois cohomology groups and radicals of finite Kummer extensions.

For any CM field $\mathbb{K}$ we let j denote the complex conjugation of $\mathbb{K}$. The homomorphism j acts naturally on the p-Sylow subgroup of the class group of $\mathbb{K}$, denoted by A, and if $p > 2$ it induces a decomposition $A = (1+j)A \oplus (1-j)A$. To abbreviate notation we will also write $A^+ = (1+j)A$ and $A^- = (1-j)A$. Let $\mathbb{K}_n$ be the intermediate fields of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ and denote by A_n the p-Sylow subgroup of the class group of $\mathbb{K}_n$. Greenberg stated in his thesis the following

Conjecture. *[Gre 1] Let $\mathbb{K}$ be a totally real field. Then the size of A_n^+ is uniformly bounded.*

Greenberg gave examples of infinite families of totally real quadratic fields satisfying this conjecture [Gre 3]. But the conjecture remains open in full generality.

In view of Greenberg's conjecture – but also independent of it – it is of particular interest to study the structure of A_n^- (here A_n denotes the p-Sylow subgroup of the class group of $\mathbb{K}_n$) and of $A_\infty^- = \lim_{\infty \leftarrow n} A_n^-$. In Chapter 5 we study the Gross and the Gross-Kuz'min conjecture. The Gross conjecture predicts that the maximal submodule of A_∞^- annihilated by T is finite. The Gross-Kuz'min conjecture is a generalization of the Gross Conjecture for number fields that are not CM.

We will give equivalent formulations of both conjectures in terms of class field theory and explain some applications of this equivalent formulation for CM fields.

In the last part of the thesis we turn our attention back to the CM number fields. For $p > 2$ one major advantage of minus parts of class groups is that they are complementable as Λ-modules and therefore induce a class field $\mathbb{H}_n^-$ such that $\mathrm{Gal}(\mathbb{H}_n^-/\mathbb{K}_n) \cong A_n^-$. So even without assuming Greenberg's conjecture it is relatively comfortable to work with the minus part of the class groups. Unfortunately, this complementability does not hold for $p = 2$. In Chapter 7 we will give an alternative definition for the minus part which allows us to define a corresponding class field even in the case $p = 2$. Consequently, we are able to derive several results, which are known for minus class groups for $p > 2$, for $p = 2$ as well. For example we show that the minus class group is capitulation free.

This result is one of the main ingredients to compute the 2-class groups for the cyclotmic $\mathbb{Z}_p$-extension of certain biquadratic number fields as we will do in Chapter 8.

Part I

Iwaswa Theory of ellipitc cuves and abelian varieties

Chapter 2

The split prime μ-conjecture

Acknowledgments

This Chapter is joint work with Vlad Crişan and also part of his Ph.D. thesis. This work was published in the Asian Journal of Mathematics [Cr-M]. We thank Prof. John Coates for giving us this problem and for his support.

2.1 General setup and statement of the split prime μ-conjecture

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

Let $\mathbb{M}_\infty$ be the maximal p-abelian extension of $\mathbb{L}_\infty$ that is unramified outside the primes in $\mathbb{L}_\infty$ lying above $\mathfrak{p}$. By a standard maximality argument, $\mathbb{M}_\infty/\mathbb{K}$ is a Galois extension. Hence, if we denote $\Gamma := \mathrm{Gal}(\mathbb{L}_\infty/\mathbb{L})$, then $X(\mathbb{L}_\infty) := \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{L}_\infty)$ becomes a $\mathbb{Z}_p[[\Gamma]]$-module in the natural way, and hence a module over $\mathbb{Z}_p[[T]]$ (the power series ring over $\mathbb{Z}_p$ with indeterminate T), under an isomorphism $\mathbb{Z}_p[[\Gamma]] \cong \mathbb{Z}_p[[T]]$ obtained via a fixed topological generator for Γ. For every $n \geq 0$, we let $\mathbb{L}_n$ denote the unique extension of $\mathbb{L}$ of degree p^n with $\mathbb{L}_n \subset \mathbb{L}_\infty$. Then $\mathbb{L}_n$ is an abelian extension of the imaginary quadratic field $\mathbb{K}$, so, by the Baker-Brumer theorem, the $\mathfrak{p}$-adic Leopoldt conjecture holds for the intermediate fields $\mathbb{L}_n$, i.e. $\mathbb{L}_n$ admits exactly one $\mathbb{Z}_p$-extension unramified outside $\mathfrak{p}$. 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 $f \in \mathbb{Z}_p[[T]]$. Note that

$X(\mathbb{L}_\infty)$ is finitely generated as a $\mathbb{Z}_p$-module if and only if $\mu = 0$. The aim of this chapter is to prove the following

Theorem 2.1.1. *The $\mathbb{Z}_p[[T]]$-module $X(\mathbb{L}_\infty)$ is a finitely generated $\mathbb{Z}_p$-module.*

Theorem 2.1.1 was previously proved by Schneps ([Sch, Theorem III]) for $\mathbb{L} = \mathbb{K}$, $\mathbb{K}$ of class number 1, $p \geq 5$ and by Gillard ([Gil 2, Theorem I.2]) for any $\mathbb{L}$ abelian over $\mathbb{K}$, $p \geq 5$. Recently, Choi, Kezuka, Li ([C-K-L]) and Oukhaba, Viguié ([O-V]) have independently worked towards completing the proof of the theorem for the cases $p = 2$ and $p = 3$. In [C-K-L], the result is proved for $p = 2$, $\mathbb{K} = \mathbb{Q}(\sqrt{-q})$ with $q \equiv 7 \pmod 8$ and $\mathbb{L}$=Hilbert class field of $\mathbb{K}$, while in [O-V] the result is proved for $p = 2, 3$ and any $\mathbb{L}$, extending the methods in [Gil 2]. The purpose of this chapter 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 2.1.1, we give a useful reduction step.

Lemma 2.1.2. *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 $\mathbb{M}(\mathbb{J}_\infty)$ (the maximal p-abelian extension of $\mathbb{J}_\infty$ unramified outside $\mathfrak{p}$). Then

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

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

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

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

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

□

Corollary 2.1.3. *Let $\mathbb{L}$ be a finite abelian extension of $\mathbb{K}$ and $\mathbb{J}/\mathbb{L}$ a finite p-solvable extension. Then $X(\mathbb{J}_\infty)$ is finitely generated as $\mathbb{Z}_p$-module.*

Proof. This is a direct consequence of Theorem 2.1.1 and Lemma 2.1.2. □

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 2.1.1 when $\mathbb{L}$ is of the form $\mathbb{L} = \mathbb{K}(\mathfrak{fp})$ (respectively $\mathbb{L} = \mathbb{K}(\mathfrak{fp}^2)$ 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 $\mathbb{L} = \mathbb{K}(\mathfrak{fp}^n)$ 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

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

Combining Lemma 2.1.2 with our previous observations, it follows that for any prime $\mathfrak{p}$, it suffices to consider fields $\mathbb{L}$ of the form $\mathbb{L} = \mathbb{K}(\mathfrak{fp})$ (resp. $\mathbb{L} = \mathbb{K}(\mathfrak{fp}^2)$ 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

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

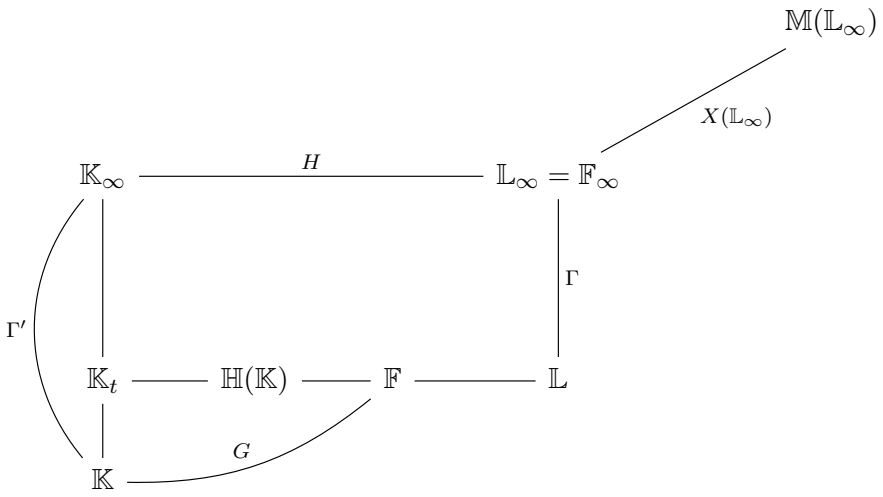
Having reduced the problem to the case $\mathbb{L} = \mathbb{K}(\mathfrak{fp})$ (resp. $\mathbb{L} = \mathbb{K}(\mathfrak{fp}^2)$ when $p = 2$), one then has $\mathbb{L}_\infty = \mathbb{F}_\infty$, and we shall subsequently work with $\mathbb{F}_\infty$. We let $\mathbb{H}(\mathbb{K})$ be the Hilbert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



We shall now summarize our strategy for proving Theorem 2.1.1. 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

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

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 $X(\mathbb{F}_\infty)$ on which H acts through χ. We denote this quotient by $X(\mathbb{F}_\infty)_\chi$. 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 $X(\mathbb{F}_\infty)_\chi$ can be generated by the power series corresponding to a p-adic L-function. We will discuss this formulation of the Main conjecture in more detail in Chapter 3. In the present chapter we are only interested in establishing 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 2.1.1. 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 in the proof of Theorem 2.1.1 and is carried out in detail in Section 2.2. In [Co-Go], building on techniques previously developed in [Co-Wi 2] and [Co-Wi 3], Coates and Goldstein presented a recipe for constructing the p-adic L-functions, provided one has an elliptic curve defined over a number field $\mathbb{F}$ containing $\mathbb{K}$, which has complex multiplication by the ring of integers of $\mathbb{K}$ and for which $\mathbb{F}(E_{tors})/\mathbb{K}$ is an abelian extension. We shall follow closely this approach for constructing the p-adic L-functions, extending it to our general setting. The first step will thus be to prove that when $\mathbb{F} = \mathbb{K}(\mathfrak{f})$ with $\mathfrak{f}$ as above, one can construct a suitable elliptic curve $E/\mathbb{F}$.

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

2.2 Construction of the p-adic L-function

2.2.1 Existence of a suitable elliptic curve

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

Lemma 2.2.1. *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 [Gro 02, Theorem 9.1.3] that given a pair (j, ψ) with $j \in J$ and $\psi : \mathbb{I}_{\mathbb{H}} \to \mathbb{K}^*$ a continuous homomorphism whose restriction to $\mathbb{H}^*$ is the norm, there exists an elliptic curve E_0 defined over $\mathbb{H}$, having complex multiplication by $\mathcal{O}_{\mathbb{K}}$, with $j(E_0) = j$ and whose Grössencharacter $\psi_{E_0/\mathbb{H}}$ is precisely ψ. Consider thus an element $j \in J$ and an elliptic curve E_0 defined over $\mathbb{H}$ with complex multiplication by $\mathcal{O}_{\mathbb{K}}$ with $j(E_0) = j$. Since $\mathbb{H} \subset \mathbb{F}$, we can regard our curve E_0 as defined over $\mathbb{F}$. We shall modify this elliptic curve $E_0/\mathbb{F}$ to satisfy all the required conditions. We begin by constructing an elliptic curve satisfying a) and b).

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

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

Let φ be a Grössencharacter of $\mathbb{K}$ of infinity type $(1, 0)$ and conductor $\mathfrak{f}$ (recall that $\omega_{\mathfrak{f}} = 1$). Let $\psi = \varphi \circ N_{\mathbb{F}/\mathbb{K}}$. Then $\chi := \frac{\psi}{\psi_{E_0/\mathbb{F}}} : \mathbb{I}_{\mathbb{F}} \to \mathbb{K}^*$ has the property that $\chi(\mathbb{F}^*) = 1$. Therefore, under the reciprocity map of class field theory, we can regard χ as a homomorphism $\chi : \mathrm{Gal}(\mathbb{F}^{ab}/\mathbb{F}) \to \mathbb{K}^*$. Since the Galois group $\mathrm{Gal}(\mathbb{F}^{ab}/\mathbb{F})$ is compact, it follows that the image of χ must lie in the finite multiplicative group $\mathcal{O}_{\mathbb{K}}^{\times}$. In particular, χ is a character of finite order. Furthermore, $\mathcal{O}_{\mathbb{K}}^* \subset Isom(E_0)$, where $Isom(E_0)$ denotes the group of $\overline{\mathbb{Q}}$-automorphisms of E_0. Thus, we can view the character χ as a map $\chi : \mathrm{Gal}(\mathbb{F}^{ab}/\mathbb{F}) \to Isom(E_0)$. A moment's thought shows that χ is a 1-cocycle, hence it defines an isomorphism class of elliptic curves defined over $\mathbb{F}$ which has the same j-invariant as E_0 (see [Gro 02, 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 [Gro 02, Lemma 9.2.5],[1] one has that

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

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

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

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

□

We now fix a Grössencharacter ϕ of $\mathbb{K}$ of conductor $\mathfrak{f}$ and infinity type $(1,0)$ and let $E/\mathbb{F}$ be an elliptic curve satisfying the conditions in Lemma 2.2.1 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 with $\mathfrak{p}$-integral coefficients in $\mathbb{F}$

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

for which the discriminant $\Delta(E)$ is coprime to any prime in $\mathbb{F}$ above $\mathfrak{p}$. Note that the model (2.1) is minimal at all primes lying above $\mathfrak{p}$. The Neron differential attached to the above model is

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

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

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

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

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

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 (2.1) 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

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

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

By the main theorem of complex multiplication, for any such $\mathfrak{a}$ and any σ 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 $\eta(\mathfrak{b})$ and $\eta_\mathfrak{a}(\mathfrak{b})$ for the isogenies $\eta_e(\mathfrak{b}) : E \to E^{\sigma_\mathfrak{b}}$ and $\eta_{\sigma_\mathfrak{a}}(\mathfrak{b}) : E^{\sigma_\mathfrak{a}} \to E^{\sigma_\mathfrak{a}\sigma_\mathfrak{b}}$, respectively. As explained in [Co-Go, p. 341], there exists a unique $\Lambda(\mathfrak{a}) \in \mathbb{F}^*$ such that

$$\omega^{\sigma_\mathfrak{a}} \circ \eta(\mathfrak{a}) = \Lambda(\mathfrak{a})\omega, \tag{2.2}$$

which can also be written as

$$\eta(\mathfrak{a}) \circ \mathcal{M}(z, \mathcal{L}) = \mathcal{M}\left(\Lambda(\mathfrak{a})z, \mathcal{L}_{\sigma_\mathfrak{a}}\right). \tag{2.3}$$

Note that Λ satisfies the cocycle condition

$$\Lambda(\mathfrak{a}\mathfrak{b}) = \Lambda(\mathfrak{a})^{\sigma(\mathfrak{b})}\Lambda(\mathfrak{b}). \tag{2.4}$$

It follows that we can extend the definition of Λ to the set of all fractional ideals coprime to $\mathfrak{f}$ so that (2.4) 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

$$\Lambda(\mathfrak{a})\Omega_\infty\mathfrak{a}^{-1} = \mathcal{L}_{\sigma_\mathfrak{a}}. \tag{2.5}$$

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 w above $\mathfrak{p}$. In particular, it has good reduction at v. 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 2.2.2. *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 2.2.2 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 $\mathfrak{fp}$, it becomes an isomorphism. It follows that one can construct an isomorphism $\beta^v_{\mathfrak{a}} = \widehat{\eta(\mathfrak{a})} \circ \beta^v$ between $\widehat{\mathbf{G}}_m$ and $\widehat{E^{\sigma_{\mathfrak{a}},v}}$. We also let $\Omega_{\mathfrak{a},v}$ be the coefficient of w in $\beta^v_{\mathfrak{a}}(w)$. As proven for example in [Co-Go, Lemma 6], the relation between Ω_v and $\Omega_{\mathfrak{a},v}$ is given by

$$\Omega_{\mathfrak{a},v} = \Lambda(\mathfrak{a})\Omega_v. \tag{2.6}$$

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

$$\begin{array}{ccccc}
\widehat{\mathbf{G}}_m & \xrightarrow{\beta^v} & \widehat{E^v} & \xrightarrow{\widehat{\eta(\mathfrak{a})}} & \widehat{E^{v,\sigma_{\mathfrak{a}}}} \\
& \searrow^{\mathrm{Log}} & \uparrow{\scriptstyle \mathcal{M}} & & \uparrow{\scriptstyle \mathcal{M}_{\mathfrak{a}}} \\
& & \widehat{\mathbf{G}}_a & \xrightarrow{\cdot\Lambda(\mathfrak{a})} & \widehat{\mathbf{G}}_a
\end{array}$$

2.2.2 The basic rational functions

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

For any 2-dimensional 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 $\sigma \in \mathrm{Gal}(\mathbb{K}(\mathfrak{m})/\mathbb{K})$, 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

$$\varphi_{\mathfrak{m}}(1)^{N(\mathfrak{a})-\left(\frac{\mathbb{K}(\mathfrak{m})/\mathbb{K}}{\mathfrak{a}}\right)} = \left(\frac{\theta(1,\mathfrak{m})^{N(\mathfrak{a})}}{\theta(1,\mathfrak{a}^{-1}\mathfrak{m})}\right)^m. \tag{2.7}$$

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

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

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

Theorem 2.2.3. *Let $\mathfrak{m}$ be an non-trivial integral ideal of K and let χ be a character of finite order of conductor $\mathfrak{m}$. Let $L_{\infty,\mathfrak{m}}(\chi, s) = (2\pi)^{-s}\Gamma(s)L_{\mathfrak{m}}(\chi, s)$. Then*

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

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

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

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

can also be expressed in terms of the p-part of the class number, the $\mathfrak{p}$-adic regulator and the $\mathfrak{p}$-adic discriminant of the field. On the other hand, Coates and Wiles proved in [Co-Wi 1, Theorem 11] a relation between the μ-invariant of the Galois group $\mathrm{Gal}(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)$ and these p-adic quantities (see Corollary 2.4.2 in Section 2.4 for the precise statement). In view of these facts, our aim is to prove a $\mathfrak{p}$-adic analogue of Theorem 2.2.3. 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 $x(P_\sigma)$ denote its x-coordinate in the model (2.1). 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 the quotient $\Delta(\alpha^{-1}\mathcal{L}_\sigma)/\Delta(\mathcal{L}_\sigma)^{N_{\mathbb{K}/\mathbb{Q}}(\alpha)}$ (here Δ stands for the Ramanujan's Δ-function)-see [Co, Appendix, Proposition 1] and [Co, Appendix, Theorem 8].

The following identity, which is proved for example in [Go-Sch, Theorem 1.9], shows the connection between our rational function and the Theta function (compare with (2.7)):

$$\xi_{\alpha,\sigma}(z)^{12} = \frac{\theta\left(z, \alpha^{-1}\mathcal{L}_\sigma\right)}{\theta\left(z, \mathcal{L}_\sigma\right)^{N(\alpha)}}. \tag{2.8}$$

An important result about the rational functions defined above 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

$$\xi_{\alpha,\sigma\sigma_\mathfrak{b}}\left(\eta_\sigma(\mathfrak{b})(P_\sigma)\right) = \prod_{U \in E^\sigma_\mathfrak{b}} \xi_{\alpha,\sigma}(P_\sigma \oplus U), \tag{2.9}$$

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

It follows that

$$\xi_{\alpha,\sigma\sigma_\mathfrak{b},Q}\left(\eta_\sigma(\mathfrak{b})(P_\sigma)\right) = \prod_{U \in E^\sigma_\mathfrak{b}} \xi_{\alpha,\sigma,Q}\left(P_\sigma \oplus U\right). \tag{2.10}$$

For every $n \geq 0$, we fix once and for all a primitive p^nth root of unity ζ_{p^n} such that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. For a fixed $n \geq 0$, we can regard $\widehat{\mathbf{G}}_m$ as defined over $\mathcal{I}_\mathfrak{p}[\zeta_{p^n}]$. Then $\zeta_{p^n} - 1$ becomes a 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 primitive $\mathfrak{p}^n$-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 (2.3), it follows that $z_n \equiv \Lambda(\mathfrak{a})w_n \pmod{\mathcal{L}_{\sigma_\mathfrak{a}}}$. Since w_n is a primitive $\mathfrak{p}^n$-torsion point for $\mathcal{L}$ and ρ is primitive 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

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

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

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

Remark 2.2.5. *We note that the definition of $\xi_{\alpha,\sigma,Q}(z)$ depends only on the restriction of σ to Gal$(\mathbb{F}/\mathbb{K})$, but that the point z_n does depend on the element σ in Gal$(\mathbb{F}_n/\mathbb{K})$ we choose. Also, the above relation implies directly that the right hand side is independent of the choice of the ideal $\mathfrak{a}$, since the left hand side is.*

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

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

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

We define

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

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

Using (2.8), it follows that

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

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

$$\frac{d}{dz} \log \widetilde{\theta}(z + z_0, L) = \overline{z_0} A(L)^{-1} + \sum_{k=1}^{\infty} (-1)^{k-1} E_k^*(z_0, L) z^{k-1}. \tag{2.11}$$

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

$$\left(\tfrac{d}{dz}\right)^k \log \xi_{\alpha,\sigma,Q}(z)|_{z=z_n} = \left(\tfrac{d}{d\tilde{z}}\right)^k \log \xi_{\alpha,\sigma}(\tilde{z} + z_n + \Lambda(\mathfrak{a})\rho)|_{\tilde{z}=0}. \tag{2.12}$$

Combining (2.11) and (2.12), it follows that

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

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

$$E_k^*(\Lambda(\mathfrak{a})(w_n + \rho), \mathcal{L}_\sigma) = \left(\frac{\phi(\mathfrak{a}\mathfrak{q}_n)}{(w_n + \rho)\Lambda(\mathfrak{a})} \right)^k L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}\mathfrak{q}_n} \right), k \right), \tag{2.13}$$

and similarly

$$E_k^*(\alpha\Lambda(\mathfrak{a})(w_n + \rho), \mathcal{L}_\sigma) = \left(\frac{\phi(\mathfrak{a}\mathfrak{q}_n(\alpha))}{(\alpha)(w_n + \rho)\Lambda(\mathfrak{a})} \right)^k L\left(\overline{\phi}^k, \left(\frac{\mathbb{F}_n/\mathbb{K}}{\mathfrak{a}\mathfrak{q}_n(\alpha)} \right), k \right) \tag{2.14}$$

Using (2.13) and (2.14), 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. $\square$

We now define the following sets of integral ideals of $\mathbb{K}$ that we will use throughout the rest of this chapter. 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 (2.9), it follows that

$$\prod_{R \in E_{\mathfrak{p}}^{\sigma}} Y_{\alpha,\mathfrak{a}}\left(P_\sigma \oplus R\right) = 1. \tag{2.15}$$

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

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

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

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

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

it follows that

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

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

2.2.3 The p-adic L-function

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

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

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

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

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

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

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

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

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

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

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

By our previous observation, for $O \subseteq \mathbb{Z}_p$ compact open, there is a natural 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

$$\nu|_{\mathbb{Z}_p^\times} \to F(w) - \frac{1}{p}\sum_{\zeta^p=1} F(\zeta(1+w)-1). \tag{2.16}$$

Throughout this chapter, 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

$$\nu \circ a|_O = \nu|_{aO} \circ a. \tag{2.17}$$

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

$$\nu \circ a \to F\left((1+w)^{-a} - 1\right). \tag{2.18}$$

We can now proceed to the construction of our measure. For every $\mathfrak{a} \in \mathfrak{C}_0$, we define $\mathcal{B}_{\alpha,\mathfrak{a}}(w) = h_{\alpha,\mathfrak{a}}(\beta_{\mathfrak{a}}^v(w))$. By Lemma 2.2.6, 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 (2.15) combined with the aforementioned lemma from [Si] implies that the measure $\nu_{\alpha,\mathfrak{a}}$ is actually supported on $\mathbb{Z}_p^\times$.

Let $\Psi_{\mathfrak{p}} : \mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F}) \to \mathbb{Z}_p^\times$ be the isomorphism giving the action of $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})$ 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 $\Lambda_{\mathcal{I}_{\mathfrak{p}}}(\mathrm{Gal}(\mathbb{F}_\infty/F))$. 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

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

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

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

it follows that under the substitution induced by multiplication by $\Lambda(\mathfrak{a})$

$$D^k\ \mathcal{B}_{\alpha,\mathfrak{a}}(w)|_{w=w_1} = \Omega_{\mathfrak{a},v}^k \Lambda(\mathfrak{a})^{-k} \left(\frac{d}{dz}\right)^k \frac{1}{p} \log Y_{\alpha,\mathfrak{a}}\left(\mathcal{M}\left(\Lambda(\mathfrak{a})z, \mathcal{L}_{\sigma_{\mathfrak{a}}}\right)\right)|_{z=\tilde{z}_1} \tag{2.19}$$

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

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

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

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

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

which satisfies the property that $\tilde{\phi}\left(\left(\frac{\mathbb{F}_\infty/\mathbb{K}}{\mathfrak{a}}\right)\right) = \phi(\mathfrak{a})$, for any ideal $\mathfrak{a}$ in $\mathbb{K}$ coprime to $\mathfrak{fp}$. 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 2.2.7. *a) Let χ be a character of Gal$(\mathbb{F}/\mathbb{K})$. Then for every $k \geq 0$ one has*

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

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

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

Then for every $k \geq 0$ one has

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

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

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

It follows that

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

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 (2.6)), it follows that

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

This completes the proof of part a).

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

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

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

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

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

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

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

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

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

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

which can be rewritten as

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

A simple check using the definitions shows that

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

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

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

Moreover, when we consider the expression

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

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

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

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

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

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

we get

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

Finally,

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

with $\tau(\chi)$ defined as in the statement. Using (2.19), 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 2.2.8. *Let χ, ε and $G(\varepsilon)$ be defined as above. Then there exists a p-adic unit u_χ depending on χ such that for all $k\geq 1$ one has*

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

Proof. When $n = 0$, by Proposition 2.2.4 and Lemma 2.2.7 a), it follows that

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

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

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

When $n \geq 1$, using Proposition 2.2.4 and Lemma 2.2.7 b), it follows in a similar manner that

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

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

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

with u_χ as defined in the proof of Theorem 2.2.8.

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 2.2.8 that

$$\nu_{\alpha_1}\left(N(\alpha_2) - \sigma_{(\alpha_2)}\right) = \nu_{\alpha_2}\left(N(\alpha_1) - \sigma_{(\alpha_1)}\right) \quad \text{(equality as measures)}, \tag{2.20}$$

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 2.2.8 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 (2.20), in order to prove that $\nu_\alpha/(N(\alpha) - \sigma_{(\alpha)})$ is an integral measure, it suffices to prove that as we range over the elements $\alpha \in \mathcal{O}_\mathbb{K}$ such that α is non-unit and coprime to $6\mathfrak{f}\mathfrak{p}$, one has that the gcd of the polynomials $\theta(\sigma_{(\alpha)} - N(\alpha)) \in \mathcal{D}_\mathfrak{p}[[X]]$ is 1. To this end, we let $m \geq 0$ be the unique integer, such 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 $\mathbb{H}(\zeta_{p^m})$, any $u \in 1 + p^m\mathbb{Z}_p$ and any $n \geq m$, one can find $\alpha_n \in \mathcal{O}_\mathbb{K}$ such that

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

It follows that the sequence $\theta(\sigma_{(\alpha_n)} - N(\alpha_n))$ approximate $\theta(g)(1+X)^a - u$, for some $a \in p^m\mathbb{Z}_p$. It is now easy to see that as we range a and u, the series $\theta(g)(1+X)^a - u$

cannot have a common divisor, which shows that $\theta(\sigma_{(\alpha)} - N(\alpha)) \mid \theta(\nu_\alpha)$. In particular, there exists $\nu_\theta \in \mathcal{D}_\mathfrak{p}[[\Gamma']]$ such that

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

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

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

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

Then $m\nu$ is a measure satisfying

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

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

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

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

$$\nu(\mathfrak{g}) := \nu(\mathfrak{f})|_{\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})} \prod_{\substack{\mathfrak{l}\mid\mathfrak{f}\\ \mathfrak{l}\nmid\mathfrak{g}}} \left(1 - \left(\sigma_\mathfrak{l}|_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)}\right)^{-1}\right)^{-1}, \tag{2.21}$$

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], the assumption that $\mathfrak{f}$ should be principal was mainly imposed to ease the computations). 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 2.2.10. *For any integral ideal $\mathfrak{g} \mid \mathfrak{f}$ and any character χ of the group $Gal(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})$, we define the p-adic L-function by*

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

where γ is a topological generator of Γ'.

Theorem 2.2.11. *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 2.2.10. Then one has

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

where u_χ and $G(\chi)$ are as in Theorem 2.2.8, m is the smallest positive integer in $\mathfrak{m} \cap \mathbb{Z}$, and $\omega_\mathfrak{m}$ denotes the number of roots of unity in $\mathbb{K}$ which are 1 modulo $\mathfrak{m}$.

Proof. The case when $\mathfrak{m} = \mathfrak{f}\mathfrak{p}^n$ is an easy computation using Lemma 2.2.7, Theorem 2.2.9 and (2.7). For the general case, for an integral ideal $\mathfrak{g}$ of $\mathbb{K}$ and a character ϑ of $\mathrm{Gal}(\mathbb{K}(\mathfrak{g})/\mathbb{K})$, we define

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

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

$$T_{\mathfrak{g}'}(\vartheta) = \prod_{\substack{\mathfrak{l} \mid \mathfrak{g}' \\ \mathfrak{l} \nmid \mathfrak{g}}} (1 - \chi(\mathfrak{l}))\, T_{\mathfrak{g}}(\vartheta). \tag{2.22}$$

The general case follows from our definition of $L_{\mathfrak{p},\mathfrak{m}}$, the relation (2.22) and the fact that the character χ acts non-trivially on each prime dividing $\mathfrak{f}$. □

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

Definition 2.2.12. *We recall that we fixed a decomposition*

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

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

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

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

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

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

2.3 The vanishing of the μ-invariant of the p-adic L-function

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

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

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

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

where $u = \kappa(\gamma)$, with κ and γ as in Definition 2.2.12. 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 2.3.1. *For every prime p, and for every character χ of H we have*

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

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

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

We first notice that if $G_{\mathfrak{f}}(w,\chi)$ is the power series associated with $L_{\mathfrak{p},\mathfrak{f}}(s,\chi)$, then $\mu(G_{\mathfrak{f}}(w,\chi)) = 0$ implies $\mu(\tilde{G}(w,\chi)) = 0$. To show that $\mu\left(G_{\mathfrak{f}}(w,\chi)\right) = 0$ it will be in turn easier to use Theorem 2.2.8. To this end, we also fix some $\alpha \in \mathcal{O}_{\mathbb{K}}$ non-unit and coprime to $6\mathfrak{p}\mathfrak{f}$ and let $G(w,\chi) \in \mathcal{D}_{\mathfrak{p}}[[w]]$ be defined as

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

We note that by Theorem 2.2.9, 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 2.3.1, 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 p-class field of $\mathbb{K}$. We define the following sets

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

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. Define χ_0 as the character that coincides with χ^{-1} on Γ. Note that χ_0 is of finite order and only non-trivial if $\Gamma'^{p^t} \neq \Gamma$. Then one has

$$\begin{aligned} G(u^s-1,\chi) &= \sum_{\sigma\in\mathcal{R}} \chi^{-1}\kappa^s(\sigma) \int_{\mathcal{G}} \chi^{-1}\kappa^s d\nu_\alpha \circ \sigma \\ &= \sum_{\sigma_1\in\mathcal{R}_1} \chi^{-1}(\sigma_1) \sum_{\sigma_2\in\mathcal{R}_2} \kappa^s(\sigma_2) \int_{\mathcal{G}} \omega^i\chi_0\kappa^s d\nu_\alpha \circ \sigma. \end{aligned}$$

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

$$G(u^s-1,\chi) = \sum_{\sigma_2\in\mathcal{R}_2} \kappa^s(\sigma_2) \int_{\mathcal{G}} \omega^i\chi_0\kappa^s d\left(\sum_{\sigma_1\in\mathcal{R}_1} \chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right). \tag{2.23}$$

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

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

Let $G^{(i)}(w,\mu) \in \mathcal{D}_{\mathfrak{p}}[[w]]$ be the Iwasawa function corresponding to $\Gamma_\mu^{(i)}$. Note that $\{\kappa^s(\sigma_2) : \sigma_2 \in \mathcal{R}_2\}$ corresponds to the set of power series $\{(1+w)^j : j = 0\ldots, p^t-1\}$. Using the isomorphism $\mathcal{G} \cong \mathbb{Z}_p^\times$ and that $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{L}) = \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})^{p^t}$, it follows by the above computations that one has

$$G(w,\chi) = \sum_{j=0}^{p^t-1} (1+w)^j G^{(i)}(\chi_0(\gamma_0')(1+w)^{p^t}-1, \sum_{\sigma_1\in\mathcal{R}_1} \chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma), \tag{2.24}$$

where γ_0' is a topological generator of Γ such that $\kappa(\gamma_0') = u^{p^t}$.

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 (2.24) is zero. For this, we will use the following general lemma, which is also proved in [Gil 1, Lemma 2.10.2], but we redo the proof here for the convenience of the reader.

Lemma 2.3.2. *For every $j = 0,\ldots,p^t-1$, let $f_j(w) \in \mathcal{D}_{\mathfrak{p}}[[w]]$ be a power series and consider the series*

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

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

Proof. For every $j = 0,\ldots,p^t-1$, 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

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

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

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

By taking

$$f_j((1+w)^{p^t}-1)=G^{(i)}\left(\chi_0(\gamma_0')(1+w)^{p^t}-1,\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma\right),$$

it follows from Lemma 2.3.2 that if for $\sigma_2=1$ one has

$$\mu\left(G^{(i)}\left(\chi_0(\gamma_0')(1+w)^{p^t}-1,\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma_1\right)\right)=0, \tag{2.25}$$

then $\mu\left(G(w,\chi)\right)=0$. In view of (2.25), we note that

$$\begin{aligned}&\mu\left(G^{(i)}\left(\chi_0(\gamma_0')(1+w)^{p^t}-1,\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma_1\right)\right)\\&=\mu\left(G^{(i)}\left(w,\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma_1\right)\right).\end{aligned}$$

To see this, note that $\chi_0(\gamma_0')$ is a p-power root of unity. Hence $\chi_0(\gamma_0')(1+w)^{p^t}-1$ is a distinguished polynomial. Thus, if we let $G^{(i)}\left(w,\sum_{\sigma_1\in\mathcal{R}_1}\chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma_1\right)=\pi'^mP(w)U(w)$ for a distinguished polynomial $P(w)$ and a unit $U(w)$, it follows that the polynomial $P(\chi_0(\gamma_0')(1+w)^{p^t}-1)$ is again distinguished and $U(\chi_0(\gamma_0')(1+w)^{p^t}-1)$ is again a unit. Hence the two μ-invariants match. 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 2.3.3. *For any prime p and any i as above, one has*

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

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

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

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

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

In view of Lemma Lemma 2.3.3 we obtain

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

The polynimial $\frac{w+1}{u} - 1$ is again distinguished, as $u \equiv 1 \mod p$. So we are left to prove that

$$\mu\left(G^{(i-1)}\left(w, D\sum_{\sigma_1\in\mathcal{R}_1} \chi^{-1}(\sigma_1)\nu_\alpha\circ\sigma_1\right)\right) = 0 \tag{2.26}$$

To prove (2.25), 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 2.2.2.

Theorem 2.3.4. *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. As the proof is up to minor modification exactly the same as in [Sch, Theorem I], the author decided to give it in an extra section at the end of this chapter and to proceed with the proof of Theorem 2.3.1 here.

Using Theorem 2.3.4 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 2.3.1.

Proof of Theorem 2.3.1. By construction, $D\mathcal{B}_{\alpha,\mathfrak{a}}$ corresponds to the rational function on E given by

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

Since

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

it follows that

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

where

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

and

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

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

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

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

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

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

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

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

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

We now turn our attention to $B(P)$. We claim that this term does not have poles. To see this, note that $B(P)$ is obtained from a $\mathcal{D}_{\mathfrak{p}}$-valued measure supported on $p\mathbb{Z}_p$. 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 2.3.1. □

2.4 Proof of the split prime μ-conjecture

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

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

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

$$\mathrm{ord}_p\left([\mathbb{M}(\mathbb{F}_n) : \mathbb{F}_\infty]\right) = p^{n+t-1-e}\mu + \lambda(n-1-e) + c, \tag{2.27}$$

where $e = 0$ if p is odd and $e = 1$ otherwise, 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 completion 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 the field $\mathbb{H}(\mathbb{F}_n) \cap \mathbb{F}_\infty = \mathbb{F}_n$, and therefore, in view of the above isomorphism, one obtains that

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

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

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \overline{E}_n & \longrightarrow & D_n & \xrightarrow{N_{\Phi_n/\mathbb{K}_\mathfrak{p}}} & 1 + qp^{n+d-1}\mathcal{O}(\mathbb{K}_\mathfrak{p}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & Y_n \cap U_n & \longrightarrow & U_n & \xrightarrow{N_{\Phi_n/\mathbb{K}_\mathfrak{p}}} & 1 + qp^{n-1}\mathcal{O}(\mathbb{K}_\mathfrak{p}) & \longrightarrow & 1
\end{array}$$

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

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

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

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

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

It will be convenient for further purposes to express the p-adic valuation of $\left(N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})\right)^{-1}$ in terms of the one of $1 - \frac{1}{N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})}$. But this is straightforward, since

for any prime ideal $\mathcal{P}$ in $\mathbb{F}_n$ lying above $\mathfrak{p}$ one has that $N_{\mathbb{F}_n/\mathbb{Q}}(\mathcal{P})-1$ is coprime to p, so the two valuations we are interested in are equal.

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

Proposition 2.4.1. *With the notations as above, one has*

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

Combining Proposition 2.4.1 with (2.27), one immediately deduces the following (see also [dS, Chapter III, Corollary 2.8]).

Corollary 2.4.2. *If $G\in\mathbb{Z}_p[[\Gamma']]$ is a characteristic power series for the Galois group $Gal(\mathbb{M}(\mathbb{F}_\infty)/\mathbb{F}_\infty)$, then for all sufficiently large n one has*

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

The rest of this section is dedicated to showing how this formula relates to special values of our p-adic L-function. Consider the isomorphism $\mathcal{D}_{\mathfrak{p}}[[\Gamma']]\cong\mathcal{D}_{\mathfrak{p}}[[w]]$, and for ρ any character of Γ' of finite order, we write $\mathrm{level}(\rho)=m$ 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 2.4.3. *For any power series $F\in\mathcal{D}_{\mathfrak{p}}[[w]]$ and all sufficiently large n, one has the following equality* [2]

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

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 $\mathrm{ord}_p(p)=1$.

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

Proposition 2.4.4. *For any ramified character ε of $Gal(\mathbb{F}_\infty/\mathbb{K})$, we let $\mathfrak{g}$ be the conductor of ε and g the least positive integer in $\mathfrak{g}\cap\mathbb{Z}$. We define $G(\varepsilon)$ as in Theorem 2.2.8 and we define $S_p(\varepsilon)$ by*

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

[2] Here the μ-invariant is normalized with respect to the absolute ramification index e' in $\mathcal{D}_{\mathfrak{p}}$.

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

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

Let now χ be a character of H and recall that

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

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

We define $F(w,\chi)\in\mathcal{D}_{\mathfrak{p}}[[w]]$ to be the corresponding Iwasawa function. Then, using Theorem 2.2.11, 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

$$\prod_{\mathrm{level}(\rho)=t+n}\rho(F)\sim p\prod_{\substack{\varepsilon=\chi\rho\\ \mathrm{level}(\rho)=t+n}}G(\varepsilon)S_p(\varepsilon),\tag{2.28}$$

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

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

Using (2.28), Corollary 2.4.2, Lemma 2.4.3 and Proposition 2.4.4, we have thus proved

Theorem 2.4.5. *$\lambda(F)=\lambda(G)$ and $\mu(F)=\mu(G)$*

From this we can deduce the main result of this chapter.

Proof of Theorem 2.1.1. From Theorem 2.4.5 it follows that

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

In Theorem 2.3.1 we proved that $\mu\left(L_{\mathfrak{p}}(s,\chi)\right)=0$. It follows that

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

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

2.5 Proof of Schneps' theorem

For the proof of Theorem 2.3.4, 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 $1 \leq j \leq m$ 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

$$\varepsilon_j = \sum_{i=1}^{n} a_{ij}\alpha_i, \quad 1 \leq j \leq m. \tag{2.29}$$

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

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

With the positive integer n defined as above, we consider

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

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

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

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

We can now state the aforementioned independence results.

Proposition 2.5.1. *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 2.5.2. *Let* $\Theta : \mathbf{B}[[t_1, \ldots, t_n]] \to \mathbf{B}[[t]]$ *be the map given by*

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

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

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

then $r \equiv 0$.

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

Lemma 2.5.3. *If* C *is any compact-open set in* $\mathbb{Z}_p$*, then for* λ *as in the statement of Theorem* 2.3.4 *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 2.3.4.

Proof of Theorem 2.3.4. 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 2.5.3, 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

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

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 $\sum_{\varepsilon\in V} \varepsilon^i \kappa_i \circ \varepsilon|_U$ (see (2.18)), hence $\Gamma^{(i)}_{\kappa_i}(s)$ is also divisible by π'.

Conversely, assume that π' divides the power series associated with the measure $\sum_{\varepsilon\in V} \varepsilon^i \kappa_i \circ \varepsilon|_U$. By (2.17), it follows that π' divides the power series associated with the measure

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

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 (2.29). 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 2.5.2, it follows that $\sum_{j=1}^{m} \widetilde{F_j}\circ\Phi_j$ is identically zero on $\widetilde{E}^n$, hence, by Proposition 2.5.1, 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 2.3.4 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 2.3.4 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

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

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

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

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. □

Chapter 3

The main conjecture for $p = 2$

3.1 Statement of the Main conjecture and reduction steps

We mentioned already in the previous chapter the Main conjecture that predicts that one can write the characteristic ideal of $X(\mathbb{L}_\infty)_\chi$ in terms of p-adic L-functions. We will give a precise statement of the conjecture below in Theorem 3.1.1 and reformulate it in terms of the L-functions we constructed in Chapter 2 in Theorem 3.1.3. The Main conjecture was stated by Coates and Wiles [Co-Wi 3] as on open question. In the following years the conjecture was subsequently proved for $p \geq 3$ by work of Rubin and Bley (see below for details). Therefore, we will restrict to the case $p = 2$ for the rest of this chapter.

As before $\mathbb{K}$ is an imaginary quadratic field in which $p = 2$ splits into two distinct primes $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ and $\mathbb{K}_\infty$ is the unique $\mathbb{Z}_2$-extension $\mathbb{K}_\infty/\mathbb{K}$ which is unramified outside $\mathfrak{p}$. Let $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p}^{\mathfrak{m}})$ for some m and as before $\mathbb{L}_\infty = \mathbb{K}_\infty\mathbb{L}$. We define $\mathbb{L}_n$ as the unique subextension such that $[\mathbb{L}_n : \mathbb{L}] = 2^n$. We will denote the Euler system of elliptic units in $\mathbb{L}_n$ by C_n.

Let $\mathfrak{f}$ be coprime to $\mathfrak{p}$ and $\mathbb{K} \subset \mathbb{L}' \subset \mathbb{L}$ be an abelian extension such that $\mathbb{L}$ is the smallest ray class field of the type $\mathbb{K}(\mathfrak{f}\mathfrak{p}^m)$ containing $\mathbb{L}'$. Analogous to $\mathbb{L}_\infty$ we let $\mathbb{L}'_\infty = \mathbb{K}_\infty\mathbb{L}'$ and $\mathbb{L}'_n$ be the intermediate fields. Let U_n be the local units congruent to 1 in $\mathbb{L}'_n$ modulo the primes above $\mathfrak{p}$ and $U_\infty = \lim_{\infty\leftarrow n} U_n$. We define the elliptic units in $\mathbb{L}'_n$ by $C_n(\mathbb{L}') = N_{\mathbb{L}_n/\mathbb{L}'_n}(C_n)$ (from a certain n on the conductor of $\mathbb{L}'_n$ will grow in p-steps as n tends to infinity). Let E_n be the units of $\mathbb{L}'_n$ congruent to 1 modulo $\mathfrak{p}$ and define $\overline{E}_\infty = \lim_{\infty\leftarrow n} \overline{E}_n$. We define further $\overline{C}_\infty = \lim_{\infty\leftarrow n} \overline{C}_n$, where the overline denotes in both cases the $\mathfrak{p}$-adic closure of the groups E_n and $C_n \cap U_n$, respectively (i.e. we embed the groups C and E in the local units and consider their topological closure). We denote by A_n the 2-part of the class group of $\mathbb{L}'_n$ and define $A_\infty = \lim_{\infty\leftarrow n} A_n$. Recall that $\mathbb{M}_\infty$ is the maximal 2-abelian $\mathfrak{p}$-ramified extension of $\mathbb{L}'_\infty$. We will use the notation $X := \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{L}'_\infty)$.

We fix a decomposition $\mathrm{Gal}(\mathbb{L}'_\infty/\mathbb{K}) \cong H \times \Gamma'$, where $H = \mathrm{Gal}(\mathbb{L}'_\infty/\mathbb{K}_\infty)$ and $\Gamma' \cong \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$. Let χ be a character of H and M an arbitrary $\Lambda := \mathbb{Z}_2[[\Gamma' \times H]]$-module[1]. Let $\mathbb{Z}_2(\chi)$ be the extension of $\mathbb{Z}_2$ generated by the values of χ and define

[1]Note that we defined Λ to be the ring of formal power series $\mathbb{Z}_p[[T]]$ in all other chapters. The

$M_\chi = M \otimes_{\mathbb{Z}_2[H]} \mathbb{Z}_2(\chi)$. So M_χ is the largest quotient on which H acts via χ. The modules M_χ are $\Lambda_\chi \cong \mathbb{Z}_2(\chi)[[T]]$-modules, where $T = \gamma - 1$ for a topological generator γ of Γ'. It is easy to verify that X, A_∞, $\overline{E}_\infty$ and $\overline{C}_\infty$ are Λ-modules. The main aim of this chapter is to understand their structure in more detail, i.e. to prove the following

Theorem 3.1.1 (Main conjecture)**.** *For any abelian extension $\mathbb{L}'/\mathbb{K}$ we have*

$$\mathrm{Char}(A_{\infty,\chi}) = \mathrm{Char}((\overline{E}_\infty/\overline{C}_\infty)_\chi) \text{ and } \mathrm{Char}(X_\chi) = \mathrm{Char}((U_\infty/\overline{C}_\infty)_\chi).$$

Choose an ideal $\mathfrak{f}$ coprime to $\mathfrak{p}$ such that $\mathbb{L}'_\infty \subset \mathbb{K}(\mathfrak{p}^\infty\mathfrak{f})$. Define the group $\widetilde{\Gamma} = \mathrm{Gal}(\mathbb{L}'_\infty/\mathbb{L}'_\infty \cap \mathbb{K}(\mathfrak{f}\mathfrak{p}^2)) \cong \mathbb{Z}_p$. If we consider the field $(\mathbb{L}'_\infty)^{\widetilde{\Gamma}}$, we obtain an abelian extension of $\mathbb{K}$ contained in $\mathbb{K}(\mathfrak{f}\mathfrak{p}^2)$. As the projective limit does not depend on the finite level we start with, we can without loss of generality assume that $\mathbb{L}' \subset \mathbb{K}(\mathfrak{f}\mathfrak{p}^2)$ for a suitable ideal $\mathfrak{f}$ being coprime to $\mathfrak{p}$. To prove the main result we will further need the following useful reduction step: Let $\mathfrak{f}'$ be a principal ideal coprime to $\mathfrak{p}$ in $\mathbb{K}$ such that $\omega_{\mathfrak{f}'} = 1$, where $\omega_{\mathfrak{f}'}$ denotes the number of roots of unity of $\mathbb{K}$ congruent to 1 mod $\mathfrak{f}'$.

Lemma 3.1.2. *If Theorem 3.1.1 holds for $\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty) := \cup_{n\in\mathbb{N}}\mathbb{K}(\mathfrak{f}'\mathfrak{p}^n)$, then it holds for every $\mathbb{L}'_\infty$.*

Note that $\mathrm{Char}((U_\infty/\overline{C}_\infty)_\chi)$ can be seen as the Iwasawa-function $F(w,\chi)$ associated to the $\mathfrak{p}$-adic L-function $L_\mathfrak{p}(s,\chi)$ defined as in the previous chapter (compare with Corollary 3.4.3). So we could reformulate the second statement of Theorem 3.1.1 for $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p}^2)$ as follows.

Theorem 3.1.3. *We have*

$$\mathrm{Char}(X_\chi) = F(w, \chi^{-1}).$$

Theorem 3.1.1 was addressed before by Rubin in [Ru 1] and [Ru 2] for $p \geq 3$ and $[\mathbb{L}' : \mathbb{K}]$ coprime to p. Bley proved the conjecture in [Bl] for $p \geq 3$ and general ray class fields $\mathbb{L}'$ under the assumption that the class number of $\mathbb{K}$ is coprime to p. Furthermore, there are various papers on the λ and μ-invariants and on divisor relations between $(\overline{E}_\infty/\overline{C}_\infty)_\chi$ and $A_{\infty,\chi}$ under different assumptions (for example [Ou] and [Vi-1]). Viguié actually proves the distribution relation we need in [Vi-2].The proof presented here is selfcontained and reduces everything to ray class fields of conductor $\mathfrak{f}\mathfrak{p}^2$. This makes some of the arguments easier. We will underline along the course of the present chapter where our proof differs from Viguié's.

The most recent work on this problem is due to Kezuka [Ke 2] for $\mathbb{K} = \mathbb{Q}(\sqrt{-q})$, where q is a prime congruent to 7 modulo 8. She proves the full Main conjecture, including the definition of the pseudo-measure necessary for the definition of the p-adic L-function, in the case $\mathbb{L}'$ is the Hilbert class field of $\mathbb{K}$ and for all primes p such that p is split in $\mathbb{K}$ and coprime to the class number of $\mathbb{K}$. Note that in Kezuka's case the definition of $\mathbb{K}$ ensures that $\mathbb{K}$ has odd class number - so her proof includes the

definition $\Lambda := \mathbb{Z}_2[[\Gamma' \times H]]$ will only be used in this particular chapter.

prime $p = 2$. In this chapter we drop the assumption that the class number has to be odd and allow $[\mathbb{L} : \mathbb{K}]$ to be even, i.e. we give a complete proof of the Main conjecture as stated in Theorem 3.1.1 for $p = 2$ and any finite abelian extension $\mathbb{L}/\mathbb{K}$.

Our proof will follow closely the methods developed by Rubin and generalized by Bley and Kezuka. Using properties of the Euler system of elliptic units developed by Rubin and Tchebotarev's Theorem we will prove that $\mathrm{Char}(A_{\infty,\chi})$ divides $\mathrm{Char}((\overline{E}_\infty/\overline{C}_\infty)_\chi)$. We will finish the proof by showing that they are generated by polynomials of the same degree and hence are equal.

An analoge of the relation between the Galois groups Γ' and $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K})$ explained in Section 3.3.2 holds for $p \geq 3$ as well. Thus, all results of Section 3.3.2 can be proven for general p and $\mathbb{L}$ as well. In fact most of them are in [Bl]. Combining the results from Section 3.3.2 with the analogous statements in Section 3.3.1 for $p \geq 3$ one can extend the proof given here to general ray class fields $\mathbb{L}$ and any prime p without the assumption that the class number of $\mathbb{K}$ has to be coprime to p. It is not stated here for the general case as it is given in [Bl] up to the slight modification in Section 3.3.2 and to avoid technical case distinctions for example in section 3.3.1, where the statements for $p \geq 3$ and $p = 2$ are actually different.

3.2 Proof of the reduction step

As a first step we will prove Lemma 3.1.2.

Proof of Lemma 3.1.2. Let $M \in \{A_\infty, U_\infty/\overline{C}_\infty, \overline{E}_\infty/\overline{C}_\infty, X\}$. We use the notation $M(\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty))$ to make the field we are working with clear. Let χ be a character of $\mathrm{Gal}(\mathbb{L}'_\infty/\mathbb{K}_\infty)$. By inflation χ is also a character of $\mathrm{Gal}(\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty)/\mathbb{K}_\infty)$. In particular, it is trivial on $\mathrm{Gal}(\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty)/\mathbb{L}'_\infty)$. As $\mathfrak{f}'$ is coprime to $\mathfrak{p}$ and none of the characteristic ideals is divisible by 2 (this follows from Theorem 3.1.1 for $\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty)$ and the fact that $\mathrm{Char}(X)$ and $\mathrm{Char}(A_\infty)$ are not divisible by 2 as shown in Theorem 2.1.1 and Corollary 3.3.22) $M(\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty))_\chi$ is pseudo isomorphic to the norm $N_{\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty)/\mathbb{L}'_\infty} M(\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty))_\chi$, which is pseudo isomorphic to $M(\mathbb{L}'_\infty)_\chi$. Thus, we obtain $\mathrm{Char}(M(\mathbb{L}'_\infty)_\chi) = \mathrm{Char}(M(\mathbb{K}(\mathfrak{f}'\mathfrak{p}^\infty)_\chi)$. □

So for the rest of the chapter we will only consider the case $\mathbb{L} = \mathbb{K}(\mathfrak{f}\mathfrak{p}^2)$ for $\mathfrak{f}$ being coprime to $\mathfrak{p}$, principal and such that $\omega_\mathfrak{f} = 1$. Define $\mathbb{F}_n = \mathbb{K}(\mathfrak{f}\mathfrak{p}^n)$ and note that $\mathbb{L}_n = \mathbb{F}_{n+2}$. We will use the notation $\mathbb{F}_0 = \mathbb{F} = \mathbb{K}(\mathfrak{f})$.

3.3 Elliptic units and Euler systems

Let E, σ and $\xi_{\alpha,\sigma}$ be the elliptic curve, the Galois elements and the rational functions defined in chapter 2. It is well known that for every $\mathfrak{m}$ torsion point $P^\sigma_\mathfrak{m}$ on E^σ the elements $\xi_{\alpha,\sigma}(P^\sigma_\mathfrak{m})$ are contained in $\mathbb{K}(\mathfrak{m})$ (see [dS, Proposition II 2.4] and the appendix of [Co]). The following proposition will be very useful in the course of our proof.

Proposition 3.3.1. *Let $\mathfrak{m}$ be an ideal coprime to α and $P \in E^\sigma_\mathfrak{m}$ a primitive $\mathfrak{m}$-division point. Let $\mathfrak{r}$ be a prime coprime to $\mathfrak{f}$ such that $\mathfrak{m} = \mathfrak{r}\mathfrak{m}'$ with $\omega_{\mathfrak{m}'} = 1$. Then*

$$N_{\mathbb{K}(\mathfrak{m})/\mathbb{K}(\mathfrak{m}')}\xi_{\alpha,\sigma}(P) = \begin{cases} \xi_{\alpha,\sigma\sigma_\mathfrak{r}}(\eta_\sigma(\mathfrak{r})P) & \mathfrak{r} \mid \mathfrak{m}' \\ \xi_{\alpha,\sigma\sigma_r}(\eta_\sigma(\mathfrak{r})P)^{1-\mathrm{Frob}_\mathfrak{r}^{-1}} & \mathfrak{r} \nmid \mathfrak{m}' \end{cases}.$$

Proof. This proof follows [Ke 1, Proposition 4.3.2]. The unit group $\mathcal{O}^\times = \mathcal{O}(\mathbb{K})^\times$ has exactly two elements. Hence, the map $\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{m}')^\times$ is injective. It follows that the kernel of the projection

$$\phi\colon (\mathcal{O}/\mathfrak{m})^\times/\mathcal{O}^\times \to (\mathcal{O}/\mathfrak{m}')^\times/\mathcal{O}^\times$$

is isomorphic to the kernel of

$$\phi'\colon (\mathcal{O}/\mathfrak{m})^\times \to (\mathcal{O}/\mathfrak{m}')^\times.$$

Hence,

$$[\mathbb{K}(\mathfrak{m}) : \mathbb{K}(\mathfrak{m}')] = \begin{cases} N\mathfrak{r} - 1 & \mathfrak{r} \nmid \mathfrak{m}' \\ N\mathfrak{r} & \mathfrak{r} \mid \mathfrak{m}' \end{cases}.$$

The conjugates of P under $\mathrm{Gal}(\mathbb{K}(\mathfrak{m})/\mathbb{K}(\mathfrak{m}'))$ are the set

$$\{P + Q \mid Q \in E^\sigma_\mathfrak{r} \text{ such that } P + Q \notin E^\sigma_{\mathfrak{m}'}\}$$

if $\mathfrak{r} \nmid \mathfrak{m}'$ and

$$\{P + Q \mid Q \in E^\sigma_\mathfrak{r}\}$$

if $\mathfrak{r} \mid \mathfrak{m}'$. In the first case there is exactly one $\mathfrak{r}$-torsion point Q_0 such that $P + Q_0$ is contained in $E^\sigma_{\mathfrak{m}'}$. We obtain

$$\xi_{\alpha,\sigma}(P + Q_0)N_{K(\mathfrak{m})/\mathbb{K}(\mathfrak{m}')}\xi_{\alpha,\sigma}(P) = \prod_{Q \in E^\sigma_\mathfrak{r}} \xi_{\alpha,\sigma}(P + Q) = \xi_{\alpha,\sigma\sigma_\mathfrak{r}}(\eta_\sigma(\mathfrak{r})P).$$

By the definition of η we obtain further that

$$\xi_{\alpha,\sigma}(P + Q_0)^{\mathrm{Frob}_\mathfrak{r}} = \xi_{\alpha,\sigma\sigma_\mathfrak{r}}(\eta_\sigma(\mathfrak{r})(P + Q_0)) = \xi_{\alpha,\sigma\sigma_\mathfrak{r}}(\eta_\sigma(\mathfrak{r})P),$$

which implies the claim in this case.

In the case $\mathfrak{r} \mid \mathfrak{m}$ we obtain the claim directly from

$$N_{K(\mathfrak{m})/\mathbb{K}(\mathfrak{m}')}\xi_{\alpha,\sigma}(P) = \prod_{Q \in E^\sigma_\mathfrak{r}} \xi_{\alpha,\sigma}(P + Q) = \xi_{\alpha,\sigma\sigma_\mathfrak{r}}(\eta_\sigma(\mathfrak{r})P).$$

□

Before we can define our Euler system we still need one further concept. Let $S_{n,l}$ be the set of square free ideals of $\mathcal{O}$ that are only divisible by prime ideals $\mathfrak{q}$ satisfying the following two conditions

i) $\mathfrak{q}$ is totally split in $\mathbb{L}_n = \mathbb{K}(\mathfrak{f}\mathfrak{p}^{n+2})$

ii) $N\mathfrak{q} \equiv 1 \mod 2^{l+1}$.

With these notations we can prove the following lemma.

Lemma 3.3.2. *Let $\mathbb{H}_n = \mathbb{K}(\mathfrak{p}^{n+2})$. Given a prime $\mathfrak{q}$ in $S_{n,l}$ there exists a cyclic extension $\mathbb{H}_n(\mathfrak{q})/\mathbb{H}_n$ of degree 2^l inside $\mathbb{H}_n\mathbb{K}(\mathfrak{q})$. Furthermore, $\mathbb{H}_n(\mathfrak{q})/\mathbb{H}_n$ is totally ramified at the primes above $\mathfrak{q}$ and unramified outside $\mathfrak{q}$. Let $\mathbb{V}$ be any subfield $\mathbb{H}_n \subset \mathbb{V} \subset \mathbb{L}_n$ and $\mathbb{V}(\mathfrak{q}) = \mathbb{H}_n(\mathfrak{q})\mathbb{V}$ then $Gal(\mathbb{V}(\mathfrak{q})/\mathbb{V}) \cong Gal(\mathbb{H}_n(\mathfrak{q})/\mathbb{H}_n)$ and the ramification behavior is the same.*

Note that from now on $\mathbb{K}(\mathfrak{q})$ denotes a ray class field of conductor $\mathfrak{q}$, while we denote for any $\mathbb{V} \neq \mathbb{K}$ the field constructed in Lemma 3.3.2 by $\mathbb{V}(\mathfrak{q})$.

Proof. As $\mathfrak{q}$ is unramified in $\mathbb{H}_n/\mathbb{K}$ it follows that $\mathbb{K}(\mathfrak{q}) \cap \mathbb{H}_n = \mathbb{K}(1) \cap \mathbb{H}_n = \mathbb{K}(1)$. Hence, $\mathrm{Gal}(\mathbb{H}_n\mathbb{K}(\mathfrak{q})/\mathbb{H}_n) = \mathrm{Gal}(\mathbb{K}(\mathfrak{q})/\mathbb{K}(1)) \cong (\mathcal{O}/\mathfrak{q})^\times/\mathcal{O}^\times$. As $|\mathcal{O}^\times| = 2$ and $N\mathfrak{q} \equiv 1 \mod 2^{l+1}$ we can extract a cyclic extension of degree 2^l over $\mathbb{H}_n$. By definition $\mathfrak{q}$ is totally ramified in $\mathbb{H}_n(\mathfrak{q})/\mathbb{H}_n$ and the extension is unramified outside $\mathfrak{q}$. The rest of the claim is an immediate consequence of the fact that $\mathfrak{q}$ is unramified in $\mathbb{L}_n$. □

If $\mathfrak{r} = \prod \mathfrak{q}_i$ with $\mathfrak{q}_i$ distinct primes in $S_{n,l}$ then we define $\mathbb{V}(\mathfrak{r})$ as the compositum of the $\mathbb{V}(\mathfrak{q}_i)$.

Having this in place we can define Euler systems.

Definition 3.3.3. *Let α be a non-trivial principal ideal in $\mathbb{K}$ coprime to $6\mathfrak{f}$ and let $S_{n,l,\alpha}$ be the set of ideals in $S_{n,l}$ that are coprime to α. An Euler system is a set of global elements*

$$\{\alpha^\sigma(n,\mathfrak{r}) \mid n \geq 0, \mathfrak{r} \in S_{n,l,\alpha}, \sigma \in Gal(\mathbb{K}(\mathfrak{f}\mathfrak{p}^2)/\mathbb{K})\}$$

satisfying

i) $\alpha^\sigma(n,\mathfrak{r}) \in \mathbb{L}_n(\mathfrak{r})^\times$ is a global unit in $\mathbb{L}_n(\mathfrak{r})$ for $\mathfrak{r} \neq (1)$.

ii) If $\mathfrak{q}$ is a prime such that $\mathfrak{q}\mathfrak{r} \in S_{n,l,\alpha}$, then

$$N_{\mathbb{L}_n(\mathfrak{r}\mathfrak{q})/\mathbb{L}_n(\mathfrak{r})}(\alpha^\sigma(n,\mathfrak{r}\mathfrak{q})) = \alpha^\sigma(n,\mathfrak{r})^{\mathrm{Frob}_\mathfrak{q}-1}.$$

iii) $\alpha^\sigma(n,\mathfrak{r}\mathfrak{q}) \equiv \alpha^\sigma(n,\mathfrak{r})^{(N\mathfrak{q}-1)/2^l} \mod \lambda$ for every prime λ above $\mathfrak{q}$.

Note that if we fix σ and n and let only $\mathfrak{r}$ vary we obtain an Euler system in the sense of [Ru 2] for the field $\mathbb{L}_n$. So in Rubin's language our Euler-System is a system of Euler systems indexed by the pairs (σ, n).

We now give a precise definition of the elliptic units.

Definition 3.3.4. *Let $\mathfrak{g} \mid \mathfrak{f}$ be a non-trivial ideal. We define the elliptic units $C_{\mathfrak{g},n}$ in $\mathbb{L}_n$ as the group of units (they are units by [dS, Chapter II Proposition 2.4 iii)]) generated by all the $\xi_{\alpha,\sigma,Q_\mathfrak{g}}(P^\sigma_{n+2})$, where $Q_\mathfrak{g}$ is a primitive $\mathfrak{g}$ division point and P^σ_n is a $\mathfrak{p}^n$-torsion point on E^σ. If $\mathfrak{g} = (1)$, we define $C_{(1),n}$ as the group generated by all the units of the form $\prod_{i=1}^s \xi_{\alpha_i,\sigma}(P^\sigma_{n+2})^{m_i}$ with $\sum_{i=1}^s m_i(N\alpha_i - 1) = 0$ (they are units by [dS, Chapter II Exercise 2.4]) and by all elements $\xi_{\alpha,\sigma}(P^\sigma_{n+2})^{\tau-1}$, where τ lies in $Gal(\mathbb{L}_n/\mathbb{K})$ (they are units due to [dS, Chapter II Exercise 2.4 and Proposition 2.4 i)]. We define further the group $C_{\mathfrak{g},\infty} = \lim_{\infty\leftarrow n} C_{\mathfrak{g},n}$ and the group $C_\infty(\mathfrak{g}) = \prod_{\mathfrak{h}\mid\mathfrak{g}} C_{\mathfrak{h},\infty}$. We will also use the notation C_n and C_∞ instead of $C_n(\mathfrak{g})$ and $C_\infty(\mathfrak{g})$ if the conductor is clear form the context.*

This allows us to prove the following Lemma.

Lemma 3.3.5. *For every $u \in C_{\mathfrak{g},n}$ there exists an Euler system such that $\alpha^\sigma(n,1) = u$.*

Proof. As the properties defining an Euler-system are multiplicative it suffices to consider the case of u being one of the generators, i.e. $u = \xi_{\alpha,\sigma}(P^\sigma_{n+2} + Q_\mathfrak{g})$. Assume first that $\mathfrak{g} \neq (1)$ and let $\mathbb{V}_n = \mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2})$. Define

$$\alpha^\sigma(n,\mathfrak{r}) = N_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r})/\mathbb{V}_n(\mathfrak{r})}\xi_{\alpha,\sigma}(P^\sigma_{n+2} + Q_\mathfrak{g} + \sum_{\mathfrak{l}\mid\mathfrak{r}} Q_\mathfrak{l}),$$

where $\mathfrak{l}$ denotes primes in $S_{l,n,\alpha}$. Then $\alpha^\sigma(n,1) = u$. It remains to show that α generates an Euler system. Using that $\sigma_\mathfrak{q} = 1$ and that $\mathrm{Gal}(\mathbb{L}_n(\mathfrak{r}\mathfrak{q})/\mathbb{L}_n(\mathfrak{r})) = Gal(\mathbb{V}_n(\mathfrak{r}\mathfrak{q})/\mathbb{V}_n(\mathfrak{r}))$ we obtain by Proposition 3.3.1:

$$\begin{aligned}
N_{\mathbb{L}_n(\mathfrak{r}\mathfrak{q})/\mathbb{L}_n(\mathfrak{r})}(\alpha^\sigma(n,\mathfrak{r}\mathfrak{q})) &= N_{\mathbb{V}_n(\mathfrak{r}\mathfrak{q})/\mathbb{V}_n(\mathfrak{r})} N_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r}\mathfrak{q})/\mathbb{V}_n(\mathfrak{r}\mathfrak{q})}\xi_{\alpha,\sigma}(P^\sigma_{n+2} + Q_\mathfrak{g} + \sum_{\mathfrak{l}\mid\mathfrak{r}\mathfrak{q}} Q_\mathfrak{l}) \\
&= N_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r})/\mathbb{V}_n(\mathfrak{r})} N_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r}\mathfrak{q})/\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r})}\xi_{\alpha,\sigma}(P^\sigma_{n+2} + Q_\mathfrak{g} + \sum_{\mathfrak{l}\mid\mathfrak{r}\mathfrak{q}} Q_\mathfrak{l}) \\
&= N_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r})/\mathbb{V}_n(\mathfrak{r})}\xi_{\alpha,\sigma\sigma_\mathfrak{q}}(\eta_\sigma(\mathfrak{q})(P^\sigma_{n+2} + Q_\mathfrak{g} + \sum_{\mathfrak{l}\mid\mathfrak{r}\mathfrak{q}} Q_\mathfrak{l}))^{1-\mathrm{Frob}_\mathfrak{q}^{-1}} \\
&= N_{\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r})/\mathbb{V}_n(\mathfrak{r})}\xi_{\alpha,\sigma}(P^\sigma_{n+2} + Q_\mathfrak{g} + \sum_{\mathfrak{l}\mid\mathfrak{r}} Q_\mathfrak{l})^{\mathrm{Frob}_\mathfrak{q}(1-\mathrm{Frob}_\mathfrak{q}^{-1})} \\
&= (\alpha^\sigma(n,\mathfrak{r}))^{\mathrm{Frob}_\mathfrak{q}-1}.
\end{aligned}$$

It remains to check property iii): The group $\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r}\mathfrak{q})/\mathbb{V}_n(\mathfrak{r}\mathfrak{q})\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r}))$ acts only on the $\mathfrak{q}$-torsion points. By definition we obtain that

$$|\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r}\mathfrak{q})/\mathbb{V}_n(\mathfrak{r}\mathfrak{q})\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r}))| = (N\mathfrak{q} - 1)/2^l$$

due to the fact that $\mathbb{K}(\mathfrak{p}^{n+2}\mathfrak{g}) \neq \mathbb{K}$ is non-trivial. Using the fact that $\mathfrak{q}$-torsion points reduce to zero modulo λ and that $\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r}\mathfrak{q})/\mathbb{V}_n(\mathfrak{r}\mathfrak{q}))$ restricts surjectively to $\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^{n+2}\mathfrak{r})/\mathbb{V}_n(\mathfrak{r}))$ the claim is an easy consequence of the definitions.

If $\mathfrak{g} = (1)$, let $\mathbb{V}_n = \mathbb{K}(\mathfrak{p}^{n+2})$ and choose $\alpha^\sigma(n,\mathfrak{r}) = N_{\mathbb{K}(\mathfrak{p}^{n+2}\mathfrak{r})/\mathbb{V}_n(\mathfrak{r})}(\prod_{i=1}^s \xi_{\alpha_i,\sigma}(P^\sigma_{n+2} + \sum_{\mathfrak{l}\mid\mathfrak{r}} Q_\mathfrak{l})^{m_i})$ or $\alpha^\sigma(n,\mathfrak{r}) = N_{\mathbb{K}(\mathfrak{p}^{n+2}\mathfrak{r})/\mathbb{V}_n(\mathfrak{r})}\xi_{\alpha,\sigma}(P^\sigma_{n+2} + \sum_{\mathfrak{l}\mid\mathfrak{r}} Q_\mathfrak{l}))^{\tau-1}$ and proceed as above. □

For every prime $\mathfrak{q} \in S_{n,l}$ we fix a generator $\tau_\mathfrak{q}$ of $G_\mathfrak{q} = \mathrm{Gal}(\mathbb{L}_n(\mathfrak{q})/\mathbb{L}_n)$ and define the following group ring elements

$$N_\mathfrak{q} = \sum_{i=0}^{2^l-1} \tau_\mathfrak{q}^i \quad D_\mathfrak{q} = \sum_{i=0}^{2^l-1} i\tau_\mathfrak{q}^i.$$

For $\mathfrak{r} = \prod_{k=1}^s \mathfrak{q}_k$ we define $D_\mathfrak{r} = \sum_{k=1}^s D_{\mathfrak{q}_k} \in \mathbb{Z}[\mathrm{Gal}(\mathbb{L}_n(\mathfrak{r})/\mathbb{L}_n)]$.

With these definitions we have the following

Lemma 3.3.6. *[Ru 2, Proposition 2.2] For every Euler system $\alpha^\sigma(n,\mathfrak{r})$ there exists a canonical map*

$$\kappa\colon S_{n,l,\alpha} \to \mathbb{L}_n^\times/(\mathbb{L}_n^\times)^{2^l}$$

such that $\kappa(\mathfrak{r}) = (\alpha^\sigma(n,\mathfrak{r}))^{D_\mathfrak{r}} \mod (\mathbb{L}_n(\mathfrak{r}))^{2^l}$.

For every prime ideal $\mathfrak{q} \in S_{n,l}$ of $\mathbb{K}$ we define the free group of ideals in $\mathbb{L}_n$

$$I_\mathfrak{q} = \oplus_{\mathfrak{Q}|\mathfrak{q}}\mathbb{Z}\mathfrak{Q} = \mathbb{Z}[\mathrm{Gal}(\mathbb{L}_n/\mathbb{K})]\mathfrak{Q}.$$

For every $y \in \mathbb{L}_n^\times$ denote by $[y]_\mathfrak{q}$ the coset of the principal ideal (y) in $I_\mathfrak{q}/2^l I_\mathfrak{q}$. Let $\tilde{\mathfrak{Q}}$ be a prime above $\mathfrak{Q}$ in $\mathbb{L}_n(\mathfrak{q})$ and note that for every $x \in \mathbb{L}_n(\mathfrak{q})^\times$ the element $x^{1-\tau_\mathfrak{q}}$ lies in $(\mathcal{O}(\mathbb{L}_n(\mathfrak{q}))/\tilde{\mathfrak{Q}})^\times$. As $\mathcal{O}(\mathbb{L}_n(\mathfrak{q}))/\tilde{\mathfrak{Q}} \cong \mathcal{O}(\mathbb{L}_n)/\mathfrak{Q}$ there is a well defined image $\overline{x^{1-\tau_\mathfrak{q}}}$ in $(\mathcal{O}(\mathbb{L}_n)/\mathfrak{Q})^\times$. Thus, we can define a map

$$\mathbb{L}_n(\mathfrak{q})^\times \to (\mathcal{O}(\mathbb{L}_n)/\mathfrak{Q})^\times/((\mathcal{O}(\mathbb{L}_n)/\mathfrak{Q})^\times)^{2^l} \quad x \mapsto (\overline{x^{1-\tau_\mathfrak{q}}})^{1/d},$$

where $d = (N\mathfrak{q}-1)/2^l$. This map is surjective and the kernel of this map consists precisely of the elements whose $\tilde{\mathfrak{Q}}$ valuation is divisible by 2^l. Let now w be an element in $(\mathcal{O}(\mathbb{L}_n)/\mathfrak{Q})^\times/((\mathcal{O}(\mathbb{L}_n)/\mathfrak{Q})^\times)^{2^l}$ and let x be a preimage. Define

$$l_\mathfrak{Q}(w) = \mathrm{ord}_{\tilde{\mathfrak{Q}}}(x) \mod 2^l \in \mathbb{Z}/2^l\mathbb{Z}.$$

Note that $l_\mathfrak{Q}$ is a well defined isomorphism. Thus, we can define

$$\varphi_\mathfrak{q} : (\mathcal{O}(\mathbb{L}_n)/\mathfrak{q})^\times/((\mathcal{O}(\mathbb{L}_n)/\mathfrak{q})^\times)^{2^l} \to I_\mathfrak{q}/I_\mathfrak{q}^{2^l} \quad w \mapsto \sum_{\mathfrak{Q}|\mathfrak{q}} l_\mathfrak{Q}(w)\mathfrak{Q}.$$

With these notations we have the following

Proposition 3.3.7. *[Ru 2, Proposition 2.4] Let $\alpha^\sigma(n,\mathfrak{r})$ be an Euler system and κ be the map defined in Lemma 3.3.6. Let $\mathfrak{r} \neq (1)$ be an ideal in $S_{n,l,\alpha}$ and $\mathfrak{q}$ be a prime in $\mathbb{K}$. Then*

i) If $q \nmid \mathfrak{r}$, then $[\kappa(\mathfrak{r})]_\mathfrak{q} = 0$.

ii) Assume that $\mathfrak{q} \mid \mathfrak{r}$ and $\mathfrak{r}/\mathfrak{q} \neq (1)$. Then $[\kappa(\mathfrak{r})]_\mathfrak{q} = \varphi_\mathfrak{q}(\kappa(\mathfrak{r}/\mathfrak{q}))$

iii) Assume that $\mathfrak{r} = \mathfrak{q}$ and that the $\mathfrak{Q}$-valuation of $(\alpha^\sigma(n,(1)))$ is divisible by 2^l for all $\mathfrak{Q}$ above $\mathfrak{q}$ in $\mathbb{L}_n$. Then $[\kappa(\mathfrak{r})]_\mathfrak{q} = \varphi_\mathfrak{q}(\kappa(\mathfrak{r}/\mathfrak{q}))$.

Note that Rubin does not distinguish between the cases ii) and iii). But as Bley [Bl, Proposition 3.3] points out, the extra assumption in iii) is necessary.

Let y be any element in the kernel of $[\cdot]_{\mathfrak{q}}$. Then $y = \mathfrak{B}^{2^l}\mathfrak{C}$, where $\mathfrak{B}$ is an ideal only divisible by primes above $\mathfrak{q}$ and $\mathfrak{C}$ is coprime to $\mathfrak{q}$. Let $(\beta) = \mathfrak{B}\mathfrak{D}$ for some ideal $\mathfrak{D}$ coprime to $\mathfrak{q}$. Then $y = \beta^{2^l}u$ and u is coprime to $\mathfrak{q}$. In particular, u is a unit at all ideals above $\mathfrak{q}$. Thus, $\varphi_{\mathfrak{q}}(u)$ is well defined and we can extend $\varphi_{\mathfrak{q}}$ on $\ker([\cdot]_{\mathfrak{q}})$.

3.3.1 An application of Tchebotarev's theorem

This section follows ideas of Bley in [Bl] and of Greither in [Gr]. The main goal of this section is to prove the following Theorem.

Theorem 3.3.8. *Let $\mathbb{M} = \mathbb{L}_n$ for some n and write $G = Gal(\mathbb{M}/\mathbb{K})$. Assume that $\overline{\mathfrak{p}}^c$ is the precise power of $\overline{\mathfrak{p}}$ dividing the conductor of the extension $\mathbb{M}/\mathbb{K}$. Let $M = 2^l$ for some l and let $W \subset \mathbb{M}^\times/(\mathbb{M}^\times)^M$ be a finite $\mathbb{Z}[G]$-module. Assume that there is a $\mathbb{Z}[G]$- homomorphism $\psi\colon W \to \mathbb{Z}/M\mathbb{Z}[G]$. Let $C \in A(\mathbb{M})$ be an arbitrary ideal class. Then there are infinitely many primes $\mathfrak{Q}$ in $\mathbb{M}$ satisfying:*

i) $[\mathfrak{Q}] = 2^{3c+4}C$.

ii) If $\mathfrak{q} = \mathfrak{Q} \cap \mathbb{K}$, *then* $N\mathfrak{q} \equiv 1 \mod 2M$ *and* $\mathfrak{q}$ *is totally split in* $\mathbb{M}$.

iii) For all $w \in W$ *one has* $[w]_{\mathfrak{q}} = 0$ *and there exists a unit* u *in* $\mathbb{Z}/M\mathbb{Z}$ *such that* $\varphi_{\mathfrak{q}}(w) = 2^{3c+4}u\psi(w)\mathfrak{Q}$.

A similar result was also proved by Viguié in [Vi-2] including the case $p = 2$. As our result is slightly different from Viguié's and to underline the technical differences for the case $p = 2$ in more detail we give a complete proof here. The proof of Theorem 3.3.8 relies on several lemmas which we will prove in the following. We fix the following notation: Let $\mathbb{H}$ be the Hilbert class field of $\mathbb{M}$ and define $\mathbb{M}' = \mathbb{M}(\zeta_{2M})$ and $\mathbb{M}'' = \mathbb{M}'(W^{1/M})$.

Lemma 3.3.9. $[\mathbb{H} \cap \mathbb{M}' : \mathbb{M}] \leq 2^{c-1}$ *if* $c \geq 1$. *The extension* $\mathbb{H} \cap \mathbb{M}'/\mathbb{M}$ *is trivial if* $c = 0$.

Proof. As 2 is totally split in $\mathbb{K}/\mathbb{Q}$ the ideal $\overline{\mathfrak{p}}$ is totally ramified in $\mathbb{K}(\zeta_{2M})/\mathbb{K}$ and the ramification index is M. If $c = 0$, then $\mathbb{M}/\mathbb{K}$ is unramified at $\overline{\mathfrak{p}}$ and $\mathbb{M}'/\mathbb{M}$ is totally ramified at all primes above $\overline{\mathfrak{p}}$. Hence, $\mathbb{M}' \cap \mathbb{H} = \mathbb{M}$ and the claim follows in this case. Assume now that $c \geq 1$, then the ramification index of $\overline{\mathfrak{p}}$ in $\mathbb{M}/\mathbb{K}$ is at most $|(\mathcal{O}(\mathbb{K})/\overline{\mathfrak{p}}^c)^\times|$. Hence, the ramification index of every divisor of $\overline{\mathfrak{p}}$ in $\mathbb{M}'/\mathbb{M}$ is at least $M/2^{c-1}$. In particular, $[\mathbb{M}' : \mathbb{M}' \cap \mathbb{H}] \geq M/2^{c-1}$. Using that $[\mathbb{M}' : \mathbb{M}] \leq M$ it follows that $[\mathbb{H} \cap \mathbb{M}' : \mathbb{M}] \leq 2^{c-1}$. □

Lemma 3.3.10. *If* $c = 0$, *then the group* $Gal(\mathbb{M}'' \cap \mathbb{H}/\mathbb{M})$ *is annihilated by* 4. *If* $c \geq 1$, *then* $Gal(\mathbb{M}'' \cap \mathbb{H}/\mathbb{M})$ *is annihilated by* 2^{2c}. *In both cases it is annihilated by* 2^{2c+2}.

Proof. By definition we have $[\mathbb{K}(\zeta_{2M}) : \mathbb{M} \cap \mathbb{K}(\zeta_{2M})] \geq \min(M, M/2^{c-1})$. Consider first the case $c \geq 1$. As $\mathrm{Gal}(\mathbb{K}(\zeta_{2M})/\mathbb{K}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/(M/2)\mathbb{Z}$ we can choose an element j in $\mathrm{Gal}(\mathbb{K}(\zeta_{2M})/\mathbb{M} \cap \mathbb{K}(\zeta_{2M}))$ of order $M/2^c$. Choose $r \in \mathbb{Z}$ such that $j(\zeta_{2M}) = \zeta_{2M}^r$. It follows that $r^{M/2^c} \equiv 1 \mod 2M$ and $r^b \not\equiv 1 \mod 2M$ for every $0 < b < M/2^c$. The element j has a lift to $\mathrm{Gal}(\mathbb{M}'/\mathbb{M})$ of the same order. Let $W' \subset \mathbb{M}'^{\times}/(\mathbb{M}'^{\times})^M$ be the Kummer-radical of $\mathbb{M}''/\mathbb{M}'$. Let σ be an element in $\mathrm{Gal}(\mathbb{M}''/\mathbb{M}')$ and α in $\mathbb{M}''$ such that $\alpha^M = w$ for some representative $w \in \mathbb{M}$ of a class $\overline{w} \in W'$. By Kummer-theory there exists an even integer t_w such that $\sigma(\alpha) = \zeta_{2M}^{t_w}\alpha$. We have a well defined non-degenerate Kummer pairing

$$\langle \cdot, \cdot \rangle \colon W' \times \mathrm{Gal}(\mathbb{M}''/\mathbb{M}') \to \langle \zeta_{2M} \rangle, \quad \langle w, \sigma \rangle \mapsto \frac{\sigma(w^{1/M})}{w^{1/M}}.$$

By definition $h(W') = W'$ for every $h \in \mathrm{Gal}(\mathbb{M}'/\mathbb{M})$. For every element h in $\mathrm{Gal}(\mathbb{M}'/\mathbb{M})$ we have $\langle h(w), h\sigma h^{-1} \rangle = h\langle w, \sigma \rangle$ [Gu, Theorem 1.26]. Recall from the definitions that $\zeta_{2M}^{t_w} = \langle w, \sigma \rangle$. Clearly, every class in W' has a representative in $\mathbb{M}$. In particular, $\mathrm{Gal}(\mathbb{M}'/\mathbb{M})$ acts trivially on W'. We obtain

$$\zeta_{2M}^{rt_w} = j(\zeta_{2M}^{t_w}) = j\langle w, \sigma \rangle = \langle jw, j\sigma j^{-1} \rangle = \langle w, j\sigma j^{-1} \rangle.$$

This implies that $j\sigma j^{-1}(\alpha) = \zeta_{2M}^{rt_w}\alpha$. As we can do this argument for every element $w \in W'$, we obtain

$$j\sigma j^{-1} = \sigma^r. \tag{3.1}$$

The extension $(\mathbb{M}'' \cap \mathbb{H}\mathbb{M}')/\mathbb{M}$ is clearly abelian. Hence $\mathrm{Gal}(\mathbb{M}'/\mathbb{M})$ acts trivially on the group $H = \mathrm{Gal}(\mathbb{M}'' \cap \mathbb{H}\mathbb{M}'/\mathbb{M}')$. Together with (3.1) this implies that H is annihilated by $r - 1$. On the other hand it is a Kummer extension of exponent at most M. Therefore, H is annihilated by $2^d = \gcd(M, r-1)$. Then $r \equiv 1 \mod 2^d$. Assume now that $r^{2^{v-d}} \equiv 1 \mod 2^v$ for some $v \geq d$. Then $r^{2^{v+1-d}} \equiv 1 \mod 2^{v+1}$. This shows that $r^{2^{l+1-d}} \equiv 1 \mod 2^{l+1}$. Recall that $M = 2^l$ and that $r^b \not\equiv 1 \mod 2M$ for all $0 < b < M/2^c$. It follows that $M/2^c \mid 2M/2^d$ and $c \geq d - 1$. Therefore 2^{c+1} annihilates H. There is a natural surjective projection

$$H \to \mathrm{Gal}(\mathbb{M}'' \cap \mathbb{H}/\mathbb{M}' \cap \mathbb{H}).$$

Using Lemma 3.3.9 this gives the claim in the case $c \neq 0$.

In the case $c = 0$ we choose j of order $M/2$. Then $r^{M/2} \equiv 1 \mod 2M$ and $r^b \not\equiv 1 \mod 2M$ for all $0 < b < M/2$. Using the same arguments as above but this time for $c = 1$ we obtain that the extension $\mathbb{M}'' \cap \mathbb{H}\mathbb{M}'/\mathbb{M}'$ is annihilated by 4. This implies the claim in the case $c = 0$. □

Using the Kummer pairing we see that there is a homomorphism

$$F : \mathrm{Gal}(\mathbb{M}''/\mathbb{M}') \to \mathrm{Hom}(W, \zeta_M)$$

given by $F(\sigma)(w) = \sigma(w^{1/M})/w^{1/M}$.

Lemma 3.3.11. 2^{c+2} *annihilates the cokernel of* F.

For every finite abelian group G' and every G'-module Z we denote by $H^1(G', Z)$ the usual group cohomology, i.e. the quotient of cocycles by coboundaries. If G' is cyclic we will define the Tate cohomology groups $\widehat{H}^0(G', Z) = Z^{G'}/Z^{\sum_{g\in G'} g}$ and $\widehat{H}^1(G', Z) = \ker(\sum_{g\in G'} g \mid_Z)/Z^{g_0-1}$, where g_0 is a generator of G'. Note that $\widehat{H}^1(G', Z) \cong H^1(G', Z)$ for cyclic groups G'. To avoid using two different notations for the same object we will always use the notation $H^1(G', Z)$ as it can be used for non-cyclic groups as well.

Proof. Let W' be the image of W in $\mathbb{M}'/(\mathbb{M}')^M$. By Kummer duality we have $\mathrm{Hom}(W', \langle\zeta_M\rangle) \cong \mathrm{Gal}(\mathbb{M}''/\mathbb{M}')$. Let $f\colon (\mathbb{M}^\times)/(\mathbb{M}^\times)^M \to (\mathbb{M}'^\times)/(\mathbb{M}'^\times)^M$ be the natural map. Using the exact sequence

$$0 \to \ker(f) \to W \to W' \to 0$$

we obtain a second exact sequence

$$\mathrm{Hom}(W', \langle\zeta_M\rangle) \to \mathrm{Hom}(W, \langle\zeta_M\rangle) \to \mathrm{Hom}(\ker(f), \langle\zeta_M\rangle).$$

Hence, to prove the lemma it suffices to prove that the kernel of f is annihilated by 2^{c+2}. Let $u \in \ker(f)$ and choose an element $v \in \mathbb{M}'$ such that $u = v^M$. We define $\delta_v : \mathrm{Gal}(\mathbb{M}'/\mathbb{M}) \to \langle\zeta_M\rangle$ by $\delta_v(g) = g(v)/v$. As

$$\delta_v(gh) = gh(v)/g(v) \cdot g(v)/v = \delta_v(g) \cdot g\delta_v(h),$$

it follows that δ_v is a cocycle. Note that v is unique up to M-th roots of unity. If we choose $v' = v\zeta_M^c$, we obtain $\delta_{v'}(g) = g(v)/v \cdot g(\zeta_M^c)/\zeta_M^c$. Hence, δ_v is uniquely defined up to coboundaries and δ_v has a well defined image in $H^1(\mathrm{Gal}(\mathbb{M}'/\mathbb{M}), \langle\zeta_M\rangle)$. Thus, we have an injective map $\ker(f) \hookrightarrow H^1(\mathrm{Gal}(\mathbb{M}'/\mathbb{M}), \langle\zeta_M\rangle)$. Therefore, it suffices to bound $H^1(\mathrm{Gal}(\mathbb{M}'/\mathbb{M}), \langle\zeta_M\rangle)$. If the group $\mathrm{Gal}(\mathbb{M}'/\mathbb{M})$ is cyclic, we see that $\langle\zeta_M\rangle$ has a trivial Herbrandt quotient. So it suffices to consider

$$|\widehat{H}^0(\mathrm{Gal}(\mathbb{M}'/\mathbb{M}), \langle\zeta_M\rangle)| \leq |\langle\zeta_M\rangle \cap \mathbb{M}| \leq 2^{c+1}.$$

If $\mathrm{Gal}(\mathbb{M}'/\mathbb{M})$ is not cyclic then it is isomorphic to $\Delta \times C_r$ where C_r is cyclic and $\Delta \cong \mathbb{Z}/2\mathbb{Z}$. Consider the exact sequence

$$H^1(\Delta, \langle\zeta_M^{C_r}\rangle) \to H^1(\mathrm{Gal}(\mathbb{M}'/\mathbb{M}), \langle\zeta_M\rangle) \to H^1(C_r, \langle\zeta_M\rangle).$$

The last term is annihilated by 2^{c+1}, while the first one is annihilated by 2. Thus, we obtain that the middle term is annihilated by 2^{c+2} proving the lemma. □

Now we have all ingredients to prove Theorem 3.3.8.

of Theorem 3.3.8. Consider the map $\iota : (\mathbb{Z}/M\mathbb{Z})[G] \to \langle\zeta_M\rangle$ defined by $\sum a_\sigma\sigma \to \zeta_M^{a_1}$. Then $\iota \circ \psi \in \mathrm{Hom}(W, \langle\zeta_M\rangle)$. Using Lemma 3.3.11 we see that $2^{c+2}(\iota \circ \psi)$ has a preimage γ in $\mathrm{Gal}(\mathbb{M}''/\mathbb{M}')$. Let $\gamma_1 = 2^{c+2}\left(\frac{C}{\mathbb{H}/\mathbb{M}}\right)$ and choose $\delta \in \mathrm{Gal}(\mathbb{M}''\mathbb{H}/\mathbb{M})$ such that $\delta \mid_{\mathbb{H}} = 2^{2c+2}\gamma_1$ and $\delta \mid_{\mathbb{M}''} = 2^{2c+2}\gamma$. Note that this is possible as $\mathrm{Gal}(\mathbb{M}'' \cap \mathbb{H}/\mathbb{M})$

is annihilated by 2^{2c+2} due to Lemma 3.3.10. Using Tchebotarev's Theorem we can find infinitely many primes $\mathfrak{Q} \in \mathbb{M}$ of degree 1 such that

$$\left(\frac{\mathfrak{Q}}{\mathbb{M}''\mathbb{H}/\mathbb{M}}\right) = \text{conjugacy class of } \delta.$$

As $\delta\mid_{\mathbb{M}'} = 2^{2c+2}\gamma\mid_{\mathbb{M}'} = \mathrm{id}$ we see that $\mathfrak{Q}$ is totally split in $\mathbb{M}'/\mathbb{M}$. Let $\mathfrak{q} = \mathfrak{Q} \cap \mathbb{K}$. Then $\mathfrak{q}$ is totally split in $\mathbb{M}'/\mathbb{K}$ and $N\mathfrak{q} \equiv 1 \mod 2M$. Further $\delta\mid_{\mathbb{H}} = 2^{2c+2}\gamma_1\mid_{\mathbb{H}} = 2^{3c+4}\left(\frac{C}{\mathbb{H}/\mathbb{M}}\right)$. It follows that $[\mathfrak{Q}] = 2^{3c+4}C$. It remains to prove point iii) of the Theorem. To do so we note that

$$\mathrm{ord}_{\mathfrak{Q}}(2^{3c+4}\psi(w)\mathfrak{Q}) \equiv 0 \mod M \Leftrightarrow 2^{3c+4}\iota \circ \psi(w) = 1.$$

Using that γ is the preimage of $2^{c+2}\iota \circ \psi$ we see that

$$2^{3c+4}\iota \circ \psi(w) = 1 \Leftrightarrow (2^{2c+2}\gamma)w^{1/M}/w^{1/M} = 1.$$

As one of the ideals above $\mathfrak{Q}$ in $\mathbb{M}''$ has $2^{2c+2}\gamma \in \mathrm{Gal}(\mathbb{M}''/\mathbb{M})$ as Frobenius homomorphism, we see that

$$\mathrm{ord}_{\mathfrak{Q}}(2^{3c+4}\psi(w)\mathfrak{Q}) \equiv 0 \mod M \Leftrightarrow w \text{ is an } M\text{-th power modulo } \mathfrak{Q}.$$

w is an M-th power in $\mathbb{M}''$ and $\mathfrak{Q}$ is not ramified in $\mathbb{M}''/\mathbb{M}$. Therefore, $[(w)]_{\mathfrak{q}} = 0$. By definition $\mathrm{ord}_{\mathfrak{Q}}(\varphi_{\mathfrak{q}}(w)) = 0 \Leftrightarrow w$ is an M-th power modulo $\mathfrak{Q}$. It follows that $\mathrm{ord}_{\mathfrak{Q}}(2^{3c+4}\psi(w)\mathfrak{Q}) = u'\mathrm{ord}_{\mathfrak{Q}}(\varphi_{\mathfrak{q}}(w))$ for some unit u'. From this the claim follows as in [Ru 3, page 403]. □

3.3.2 The χ-components on the class group and on E/C

Recall that we fixed a decomposition $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}) \cong \Gamma' \times H$ with $H = \mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}_\infty)$. Let γ' be a topological generator of Γ'. To simplify notation we will use the notation γ'_n for the element γ'^{2^n}. Let $\Gamma = \mathrm{Gal}(\mathbb{L}_\infty/\mathbb{L})$. There exists a power of 2 such that Γ'^{2^m} is contained in $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{L})$. In particular $\mathbb{L}_\infty/\mathbb{L}_\infty^{\Gamma'^{2^m}}$ is totally ramified at all primes above $\mathfrak{p}$ and $\Gamma'^{2^{m+n}} = \Gamma^{2^{m'+n}}$ for some $m' \leq m$ independent of n. Recall that A_n denotes the class group of $\mathbb{L}_n$, i. e. $\gamma'^{2^{m+n-m'}}$ acts trivial on A_n and $\mathbb{L}_n$ for $n \geq m'$. We fixed the notations $\Lambda = \lim_{\infty\leftarrow n}\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{L}_n/\mathbb{K})]]$ and $A_\infty = \lim_{\infty\leftarrow n} A_n$. Let χ be a character of H. Then $A_{\infty,\chi}$ and $(\overline{E}_\infty/\overline{C}_\infty)_\chi$ are Λ_χ-modules. Let $\Lambda_{\chi,n}$ be the quotient of Λ_χ by $1-\gamma'_n$. In particular, there are polynomials g_i in Λ_χ (powers of irreducible polynomials) and a pseudo isomorphism

$$A_{\infty,\chi} \sim \bigoplus_{i=1}^{k} \Lambda_\chi/g_i, \tag{3.2}$$

with finite kernel and cokernel.

Lemma 3.3.12. *The kernel of the multiplication of $(1-\gamma'_n)$ on A_∞ is finite for every n.*

Proof. This follows directly from the fact that all finite subextensions of $\mathbb{L}_\infty/\mathbb{K}$ are abelian over $\mathbb{K}$ and that the $\mathfrak{p}$-adic Leopoldt conjecture holds for any abelian extension of $\mathbb{K}$. In particular, the $\mathfrak{p}$-adic Leopoldt conjecture holds for every field $\mathbb{L}_n$ (see [Ru 1, page 705] for more details). □

Lemma 3.3.13. *Let χ be a character of H and $n \geq m'$. Then there is a $\Lambda_{\chi,n}$ homomorphism*

$$A_{\chi,n} \to \bigoplus_{i=1}^{k} \Lambda_{\chi,m+n-m'}/(\overline{g}_i),$$

with uniformly bounded cokernel. Here, $\overline{g_i}$ is the restriction of g_i to level n.

Proof. This proof is very similar to [Gr, Lemma 3.10]: By [Wash, page 281] the module A_n is isomorphic to $A_\infty/\nu_{m+n-m',m}Y$ for some submodule Y. Consider the map

$$\phi_n \colon A_\infty/(1-\gamma'_{m+n-m'})A_\infty \to A_n.$$

By definition, the kernel is isomorphic to $\nu_{m+n-m',m}Y/(1-\gamma'_{m+n-m'})A_\infty$, which is bounded by the size of $Y/(1-\gamma'_m)A_\infty \leq A_\infty/(1-\gamma'_m)A_\infty$. By Lemma 3.3.12 this quotient is finite and the kernel of ϕ_n is uniformly bounded. Thus, the kernel of the natural projections

$$A_{\infty,\chi}/(1-\gamma'_{m+n-m'})A_{\infty,\chi} \to A_{\chi,n}$$

is uniformly bounded and we can deduce the claim from (3.2). □

Let $\Gamma'_{n_2,n_1} = \Gamma'^{2^{n_1}}/\Gamma'^{2^{n_2}}$ for $n_2 > n_1$. Recall that Γ'^{2^n} fixes the field $\mathbb{L}_{m'+n-m}$ for $n > m$. Hence $\mathrm{Gal}(\mathbb{L}_{n_2-m+m'}/\mathbb{L}_{n_1-m+m'}) = \Gamma'_{n_2,n_1}$.

Lemma 3.3.14. *Let $E'_{m'+n_2-m}$ be the $\mathfrak{p}$-units in $\mathbb{L}_{m'+n_2-m}$. Then we have that $|H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})|$ is uniformly bounded for $n_2 \geq n_1 \geq m$.*

Iwasawa [Iw 2, page 267] proves the same result for the group of the p-units instead of the $\mathfrak{p}$-units.

Proof. Let $A'_n = A_n/B_n$ where B_n is the group generated by the ideal classes of the ideals above $\mathfrak{p}$ for all n. Then the capitulation kernel C_{n_2,n_1} of the natural homomorphism

$$A'_{n_1+m'-m} \to A'_{n_2+m'-m}$$

is uniformly bounded for all $n_2 \geq n_1 \geq m$. This can be seen as in [Iw 2, Theorem 10] using the corresponding definition of A'_n. If we can show that

$$C_{n_2,n_1} \cong H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})$$

we are done. Let $a \in C_{n_2,n_1}$ and $a = cB_{n_1+m'-m}$. Let $\mathfrak{a}$ be an ideal in c. Then there is some $\gamma \in \mathbb{L}_{n_2-m+m'}$ such that $(\gamma) = \mathfrak{A}\mathfrak{B}$, where $\mathfrak{B}$ is only divisible by ideals above $\mathfrak{p}$. Recall that $\tau = \gamma'^{2^{n_1}}$ is a generator for Γ'_{n_2,n_1}. Thus, $\gamma^{\tau-1} \in E'_{n_2+m'-m}$. Note that the image of $\gamma^{\tau-1}$ in $H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})$ is independent of the choice of c, $\mathfrak{A}$

and γ. If $\gamma^{\tau-1} \in {E'}^{\tau-1}_{n_2+m'-m}$, then $\gamma = \eta\alpha$ with $\alpha \in \mathbb{L}_{n_1+m'-m}$ and $\eta \in E'_{n_2+m'-m}$. We obtain that a is trivial. Hence, we have an injective homomorphism

$$C_{n_2,n_1} \to H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m}).$$

It remains to show that it is surjective. Let $e \in E'_{m'+n_2-m}$ lie in the kernel of the norm $N\colon \mathbb{L}_{n_2+m'-m} \to \mathbb{L}_{n_1+m'-m}$. Then there is some element $\gamma \in \mathbb{L}_{n_2+m'-m}$ such that $e = \gamma^{1-\tau}$. As ideal we see that $(\gamma) = \mathfrak{A}\mathfrak{B}$ for some ideal $\mathfrak{A}$ that is a lift from $\mathbb{L}_{n_1+m'-m}$ and some ramified ideal $\mathfrak{B}$. Let $c = [\mathfrak{A}]$ and $a = cB_{n_1+m'-m}$. Then $a \in C_{n_2,n_1}$ and a is a preimage of the image of e in $H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})$. □

As a consequence we obtain:

Lemma 3.3.15. *There is a constant k such that*

$$|(1-\gamma'_m)H^1(\Gamma'_{n_2,n_1}, E_{m'+n_2-m})| \le 2^k \text{ and } |(1-\gamma'_m)\widehat{H}^0(\Gamma'_{n_2,n_1}, E_{m'+n_2-m})| \le 2^k$$

for any pair (n_1, n_2) with $n_2 > n_1 \ge m$.

Proof. The proof follows the ideas of [Ru 1, Lemma 1.2]. But it is restated here as we use weaker assumptions. Let $\mathcal{E}_{m'+n_2-m}$ be the units of $\mathbb{L}_{m'+n_2-m}$ and $R_{m'+n_2-m}$ be the $\mathbb{Z}$-free group defined by the exact sequence

$$0 \to \mathcal{E}_{m'+n_2-m} \to E'_{m'+n_2-m} \to R_{m'+n_2-m} \to 0.$$

As $\mathbb{L}_\infty/\mathbb{L}_{m'}$ is totally ramified we see that Γ'^{m} acts trivially on $R_{m'+n_2-m}$. We know from Lemma 3.3.14 that $|H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})|$ is uniformly bounded. Further, we have the exact sequence

$$\widehat{H}^0(\Gamma'_{n_2,n_1}, R_{m'+n_2-m}) \to H^1(\Gamma'_{n_2,n_1}, \mathcal{E}_{m'+n_2-m}) \to H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m}).$$

The first term is annihilated by $1-\gamma'_m$ and the last term is uniformly bounded. It follows that $(1-\gamma'_m)H^1(\Gamma'_{n_2,n_1}, \mathcal{E}_{m'+n_2-m})$ is uniformly bounded.

It is an immediate consequence from [Ja, V Theorem 2.5] that $q(E'_{m'+n_2-m}) = 2^{(n_2-n_1)(1-s)}$, where s is the number of primes above $\mathfrak{p}$. Thus,

$$2^{(n_2-n_1)(s-1)}|H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})| = |\widehat{H}^0(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})|.$$

Consider the surjective map $\widehat{H}^0(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m}) \to N_{n_1,m}E'_{m'+n_1-m}/N_{n_2,m}E'_{m'+n_2-m}$ induced by $N_{n_1,m} = (\gamma'_{n_1}-1)/(\gamma'_m-1)$. Using that $N_{n_1,m}(1-\gamma'_m) = (1-\gamma'_{n_1})$ and that $\Gamma'^{2^{n_1}}$ is precisely the group fixing $\mathbb{L}_{m'+n_1-m}$ we see that the subgroup

$$((1-\gamma'_m)E'_{m'+n_1-m} + N_{n_2,n_1}E'_{m'+n_2-m})/N_{n_2,n_1}E'_{m'+n_2-m}$$

is certainly contained in the kernel. Note that $N_{n_1,m}E'_{m'+n_1-m}/N_{n_2,m}E'_{m'+n_2-m}$ is the kernel of the natural map $\widehat{H}^0(\Gamma'_{n_2,m}, E'_{m'+n_2-m}) \to \widehat{H}^0(\Gamma'_{n_1,m}, E'_{m'+n_1-m})$. Thus, we obtain:

$$\begin{aligned}|(1-\gamma'_m)\widehat{H}^0(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})| &\le \frac{|\widehat{H}^0(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})||\widehat{H}^0(\Gamma'_{n_1,m}, E'_{m'+n_1-m})|}{|\widehat{H}^0(\Gamma'_{n_2,m}, E'_{m'+n_2-m})|} \\ &\le \frac{2^{(n_2-n_1)(s-1)+k}2^{(n_1-m)(s-1)+k}}{2^{(n_2-m)(s-1)}} = 2^{2k},\end{aligned}$$

where 2^k is the uniform bound on $H^1(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})$. It is easy to verify that the natural map $\widehat{H}^0(\Gamma'_{n_2,n_1}, \mathcal{E}_{m'+n_2-m}) \to \widehat{H}^0(\Gamma'_{n_2,n_1}, E'_{m'+n_2-m})$ is an injection. As $|(\mathcal{O}(\mathbb{L}_n)/\mathfrak{P})^\times|$ is coprime to 2 for every prime ideal $\mathfrak{P}$ above $\mathfrak{p}$, the claim follows. □

Lemma 3.3.16. *Let $n \geq m'$ and consider the projection*

$$\pi_n \colon \overline{E}_\infty/(1-\gamma'_{m+n-m'})\overline{E}_\infty \to \overline{E}_n.$$

There exists an integer k such that $2^k(1-\gamma'_m)$ annihilates the kernel and the cokernel of π_n for all $n \geq m'$.

Proof. We have an exact sequence

$$\begin{aligned}&\varprojlim_{\infty \leftarrow n'} H^1(\Gamma'_{m+n'-m',m+n-m'}, \overline{E}_{n'}) \to \\ \to &\overline{E}_\infty/(1-\gamma'_{m+n-m'})\overline{E}_\infty \to \overline{E}_n \to \varprojlim_{\infty \leftarrow n'} \widehat{H}^0(\Gamma'_{m+n'-m',m+n-m'}, \overline{E}_n).\end{aligned}$$

Then the first and the last term of the above sequence are annihilated by $2^k(1-\gamma'_m)$ due to Lemma 3.3.15. □

Lemma 3.3.17. *Let U_∞ be defined as in the introduction. Then we have*

i) $U_\infty \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ *and*

ii) $U_{\infty,\chi} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Proof. Claim i) follows as in [Bl, Lemma 3.5 Claim 2]. Bley gives two references for this proof. Note that the second one is only stated for $p > 2$ but the proof works for $p = 2$ as well (we will actually give the details in Lemma 3.4.1).

Claim ii) can be proved as follows:

$$U_\infty \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Let $I_\chi \subset \mathbb{Z}(\chi)[H]$ be the module generated by $\sigma - \chi(\sigma)$ for $\sigma \in H$. It is an easy verification that

$$\begin{aligned}&U_\infty \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/I_\chi(U_\infty \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \\ \cong\ &\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/I_\chi(\Lambda \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p).\end{aligned}$$

It is proved in [Ts, Lemma 2.1] that $M_\chi \cong (M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi))/I_\chi(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi))$. Further, for any module M we see that

$$\begin{aligned}&M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/I_\chi(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \\ &= (M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi)/I(\chi)(M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi))) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = M_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.\end{aligned}$$

Using this for U_∞ and Λ the second claim follows. □

Lemma 3.3.18. *Let h_χ be the characteristic ideal of $(\overline{E}_\infty/\overline{C}_\infty)_\chi$ and $n \geq m$. Then there exist constants n_0, c_1 and c_2 independent of n, a divisor h'_χ of h_χ and a $Gal(\mathbb{L}_{m'+n-m}/\mathbb{K})$-homomorphism*

$$\vartheta_{m'+n-m} : \overline{E}_{m'+n-m,\chi} \to \Lambda_{n,\chi}$$

such that

i) h'_χ is prime to $1-\gamma'_v$ for all v,

ii) $(\gamma'_{n_0}-1)^{c_1}2^{c_2}h'_\chi\Lambda_{n,\chi} \subset \vartheta_{m'+n-m}(im(\overline{C}_{m'+n-m,\chi}))$, where $im(\overline{C}_{m'+n-m,\chi})$ denotes the image of $\overline{C}_{m'+n-m,\chi}$ in $\overline{E}_{m'+n-m,\chi}$.

Proof. From the second claim of Lemma 3.3.17 and the fact that $\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is a principal ideal domain we obtain that the submodule $\overline{E}_{\infty,\chi} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is free cyclic over the ring $\Lambda_\chi \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We obtain a pseudo isomorphism $f\colon \overline{E}_{\infty,\chi} \to \Lambda_\chi \oplus \mathcal{M}$, where $\mathcal{M}$ is an elementary Λ_χ-module of finite exponent. Let p denote the natural projection of $\Lambda_\chi \oplus \mathcal{M} \to \Lambda_\chi$. Let $\alpha = p \circ f$. Consider the following diagram

$$\begin{array}{ccccccccc} & & 0 & \longrightarrow & \overline{E}_{\infty,\chi} & \longrightarrow & \overline{E}_{\infty,\chi} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \alpha} & & \\ 0 & \longrightarrow & \mathcal{M} & \longrightarrow & \Lambda_\chi \bigoplus \mathcal{M} & \xrightarrow{p} & \Lambda_\chi & \longrightarrow & 0 \end{array}$$

It is immediate that the kernel of α is annihilated by some power of 2 and that the cokernel of α is finite.

Consider the map

$$\pi'_n : \overline{E}_\infty/(1-\gamma'_n) \to \overline{E}_{m'+n-m}.$$

Note that $\pi'_n = \pi_{n+m'-m}$. The rest of the proof is exactly the same as [Bl, Lemma 3.5]; we just have to substitute E_n by $E_{m'+n-m}$ due to the index shift we defined at the beginning of the present section. Further, we have to write $(1-\gamma'_m)$ instead of $(1-\gamma')$ in all computations due to the fact that Lemma 3.3.16 is weaker than the corresponding claim in Bley's case, meaning that $m=0$ in his setting. We still give a complete proof below for the convenience of the reader.

Let $W_{m'+n-m}$ be the image of π'_n in $\overline{E}_{m'+n-m}$ and define

$$\mathcal{T} = \mathrm{Tor}_{\mathbb{Z}_p[H]}(\text{ Coker }(\pi'_n), \mathbb{Z}_p(\chi)).$$

Then we obtain the following two exact sequences:

$$\begin{array}{ccccccccc} & & & & \mathcal{T} & \longrightarrow & W_{m'+n-m,\chi} & \longrightarrow & \overline{E}_{m'+n-m,\chi} \longrightarrow \text{ Coker }(\pi'_n)_\chi \longrightarrow 0 \\ & & & & & & {\scriptstyle =}\uparrow & & \\ \ker(\pi'_n)_\chi & \longrightarrow & \overline{E}_{\infty,\chi}/(1-\gamma'_n)\overline{E}_{\infty,\chi} & \xrightarrow{\pi'_n} & W_{m'+n-m,\chi} & \longrightarrow & 0 & & \end{array}.$$

Let $\pi'_{n,\chi}$ be the compositum of π'_n and $\beta\colon W_{m'+n-m,\chi} \to \overline{E}_{m'+n-m,\chi}$. Then we obtain

$$0 \to \ker(\pi'_{n,\chi}) \to \overline{E}_{\infty,\chi}/(1-\gamma'_n)\overline{E}_{\infty,\chi} \to \overline{E}_{m'+n-m,\chi} \to \text{ Coker } (\pi'_n)_\chi \to 0$$

It is immediate from Lemma 3.3.16 that the cokernel of $\pi'_{n,\chi}$ is annihilated by $2^k(1-\gamma'_m)$. In the next step we also want to bound the size of $\ker(\pi'_{n,\chi})$. Let therefore $e \in \ker(\pi'_{n,\chi})$. Then $\pi'_n(e)$ lies in the image of $\mathcal{T}$ and $\pi'_n((1-\gamma'_m)2^k e) = 0$. Hence, $(1-\gamma'_m)2^k e$ lies in the image of $\ker(\pi'_n)_\chi$ in $\overline{E}_{\infty,\chi}/(1-\gamma'_n)\overline{E}_{\infty,\chi}$. Thus, Lemma 3.3.16 implies that $(1-\gamma'_m)^2 2^{2k} e = 0$. Therefore, $(1-\gamma'_m)^2 2^{2k}$ annihilates the kernel and the cokernel of $\pi'_{n,\chi}$.

We are no able to construct the homomorphism $\vartheta_{m'+n-m}$: Let $e \in \overline{E}_{m'+n-m,\chi}$. Then $(1-\gamma'_m)^2 2^{2k} e$ has a preimage z in $\overline{E}_{\infty,\chi}/(1-\gamma'_n)\overline{E}_{\infty,\chi}$ and therefore also in $\overline{E}_{\infty,\chi}$. By abuse of notation we denote both preimages by z. Define

$$\vartheta_{m'+n-m}(e) = (1-\gamma'_m)^2 2^{2k}\alpha(z) \mod (1-\gamma'_n)\Lambda_\chi.$$

As the definition of $\vartheta_{m'+n-m}$ depends a priori on the choice of z, we first have to check that $\vartheta_{m'+n-m}$ is well defined. Assume that z' is another preimage, then the image of $z-z'$ in $\overline{E}_{\infty,\chi}/(1-\gamma'_n)\overline{E}_{\infty,\chi}$ lies in the kernel of $\pi'_{n,\chi}$. In particular,

$$(1-\gamma'_m)^2 2^{2k}(z-z') \in (1-\gamma'_n)\overline{E}_{\infty,\chi}$$

and $\vartheta_{m'+n-m}$ is indeed well defined.

From the exact sequence $0 \to \overline{C}_\infty \to \overline{E}_\infty \to \overline{E}_\infty/\overline{C}_\infty \to 0$ we obtain an embedding

$$\overline{E}_{\infty,\chi}/im(\overline{C}_{\infty,\chi}) \hookrightarrow (\overline{E}_\infty/\overline{C}_\infty)_\chi.$$

As $h_\chi(\overline{E}_\infty/\overline{C}_\infty)_\chi$ is finite the same holds for the quotients $h_\chi(\overline{E}_{\infty,\chi}/im(\overline{C}_{\infty,\chi}))$ and $h_\chi(\alpha(\overline{E}_{\infty,\chi})/\alpha(im(\overline{C}_{\infty,\chi})))$. Due to the definition of α we can find an integer s such that $2^s \in \alpha(\overline{E}_{\infty,\chi})$ and such that $2^s h_\chi \alpha(\overline{E}_{\infty,\chi}) \subset \alpha(im(\overline{C}_{\infty,\chi}))$. Hence $2^{2s}h_\chi$ lies in $\alpha(im(\overline{C}_{\infty,\chi}))$. Choose $z \in im(\overline{C}_{\infty,\chi})$ such that $\alpha(z) = 2^{2s}h_\chi$. Then we obtain

$$2^{2s+4k}(1-\gamma'_m)^4 h_\chi = 2^{4k}(1-\gamma'_m)^4\alpha(z).$$

Let $z_{m'+n-m} = \pi'_{n,\chi}(z) \in im(\overline{C}_{m'+n-m,\chi})$. Clearly, a preimage of $2^{2k}(1-\gamma'_m)^2 z_{m'+n-m}$ is $2^{2k}(1-\gamma'_m)^2 z$. Then we obtain

$$\vartheta_{m'+n-m}(z_{m'+n-m}) = 2^{4k}(1-\gamma'_m)^4\alpha(z) = 2^{4k}(1-\gamma'_m)2^{2s}h_\chi.$$

Note that $(1-\gamma'_n) \mid (1-\gamma'_{n'})$ for all $n' \geq n$. In particular, there is an $n \geq m$ and an c_1 such that $h_\chi(1-\gamma'_m)^4 \mid h'_\chi(1-\gamma'_{n_0})^{c_1}$. From this the claim is immediate. □

Lemma 3.3.19. *Let $\mathbb{M} = \mathbb{L}_n$ for some n and let Δ be a subgroup of $G = Gal(\mathbb{M}/\mathbb{K})$. Let χ be a character of Δ, $M = 2^l$ and $\mathfrak{A} = \prod_{i=1}^s \mathfrak{q}_i \in S_{n,l}$. Let $\mathfrak{Q}$ be a divisor of $\mathfrak{q}_s$ in $\mathbb{M}$ and let $C = [\mathfrak{Q}]$ the ideal class of $\mathfrak{Q}$. Let $B \subset A(\mathbb{M})$ be the subgroup generated by ideals dividing $\mathfrak{q}_1, \ldots, \mathfrak{q}_{s-1}$. Let $x \in \mathbb{M}^\times/(\mathbb{M}^\times)^M$ be such that $[x]_\mathfrak{r} = 0$ for all $(\mathfrak{r}, \mathfrak{A}) = 1$. Let $W \subset \mathbb{M}^\times/(\mathbb{M}^\times)^M$ be the $\mathbb{Z}_p[G]$-submodule generated by x. Assume that there are elements $E, \eta, g \in \mathbb{Z}_p[G]$ such that*

i) $E \cdot \mathrm{ann}_{\mathbb{Z}_p[G]}(\overline{C}_\chi) \subset g\mathbb{Z}_p[G]_\chi$, *where* $\overline{C}_\chi$ *is the image of* C *in* $(A/B)_\chi$.

ii) $\mathbb{Z}_p[G]_\chi / g(\mathbb{Z}_p[G])_\chi$ *is finite.*

iii) $M \geq |A_\chi(\mathbb{M})||\eta((I_{\mathfrak{q}_s}/MI_{\mathfrak{q}_s})/[W]_{\mathfrak{q}_s})_\chi|$.

Then there exists a G*-homomorphism*

$$\psi \colon W_\chi \to (\mathbb{Z}/M\mathbb{Z})[G]_\chi$$

such that $g\psi(x)\mathfrak{Q}_\chi = (E\eta[x]_{\mathfrak{q}_s})_\chi$ *in* $(I_{\mathfrak{q}_s}/MI_{\mathfrak{q}_s})_\chi$.

Proof. This is [Bl, Lemma 3.8]. The proof is the same as [Gr, Lemma 3.12]. □

To prove the central theorem of this section we need the following lemma.

Lemma 3.3.20. *[Gr, Lemma 3.13] Let* Δ *be any finite group and* N *a* $\mathbb{Z}_p[\Delta]$*-module. Let* χ *be a character of* Δ *and* $n : N \to N_\chi$ *the natural projection. Then there exists a* $\mathbb{Z}_p[\Delta]$*-homomorphism*

$$\varepsilon_\chi : N_\chi \to N$$

such that $n \circ \varepsilon_\chi = |\Delta|$.

Let $\mathfrak{q}$ be an element in $S_{n,l}$ and $\mathfrak{A}$ in $I_\mathfrak{q}$. Then there is an element $v_\mathfrak{Q}(\mathfrak{A})$ in $\mathbb{Z}/2^l\mathbb{Z}[\mathrm{Gal}(\mathbb{L}_n/\mathbb{K})]$ such that $\mathfrak{A} = v_\mathfrak{Q}(\mathfrak{A})\mathfrak{Q}$. We will use this notation in the following theorem, which allows us to relate the characteristic ideal of A_χ to the one of $(\overline{E}_\infty/\overline{C}_\infty)_\chi$. The proof follows the ideas of [Bl].

Theorem 3.3.21. *Let* $\mathbb{M} = \mathbb{L}_n$ *and* $G = Gal(\mathbb{M}/\mathbb{K})$ *for* n *large enough. Let* χ *be a character of* $H \subset Gal(\mathbb{M}/\mathbb{K})$. *For* $1 \leq i \leq k$ *let* $C_i \in A_\chi(\mathbb{M}) = A_\chi$ *be such that* $t(C_i) = (0, 0, \cdots, 2^{c_3}, 0 \cdots, 0)$ *in* $\bigoplus_{i=1}^k \Lambda_{\chi,m+n-m'}/(\overline{g}_i)$ *where* t *is the map defined in Lemma 3.3.13 and* 2^{c_3} *annihilates the cokernel. Let* C_{k+1} *in* A_χ *be arbitrary. Let* $d = 3c + 4$, *where* c *is defined in Theorem 3.3.8. Then there are prime ideals* $\mathfrak{Q}_i$ *in* $\mathbb{M}$ *such that*

i) $[\mathfrak{Q}_i]_\chi = 2^d C_i$.

ii) $\mathfrak{q}_i = \mathfrak{Q}_i \cap \mathbb{K}$ *is in* $S_{n,n}$.

iii) one has

$$(v_{\mathfrak{Q}_1}(\kappa(\mathfrak{q}_1))_\chi = u_1|H|(\gamma'_{n_0} - 1)^{c_1} 2^{d+c_2} h'_\chi \mod 2^n \tag{3.3}$$

$$(g_{i-1} v_{\mathfrak{Q}_i}(\kappa(\mathfrak{q}_1\mathfrak{q}_2 \ldots \mathfrak{q}_i))_\chi \tag{3.4}$$

$$= u_i|H|(\gamma'_{n_0} - 1)^{c_1^{i-1}} 2^{2d+c_3} (v_{\mathfrak{Q}_{i-1}}(\kappa(\mathfrak{q}_1 \ldots \mathfrak{q}_{i-1}))_\chi \mod 2^n \text{ for } 2 \leq i \leq k+1.$$

Proof. By Lemma 3.3.18 there exists an element ξ' in $im(\overline{C}_{n,\chi})$ with the property $\vartheta_n(\xi') = (1 - \gamma'_{n_0})^{c_1} 2^{c_2} h'_\chi$. By approximating ξ' with a global elliptic unit we can find $\xi \in C_n$ such that $\vartheta_n(\xi) = (1 - \gamma'_{n_0})^{c_1} 2^{c_2} h'_\chi \mod M\Lambda_{\chi,m+n-m'}$. We can apply Lemma 3.3.5 to find an Euler system $\alpha^\sigma(n, \mathfrak{r})$ such that $\alpha^\sigma(n, (1)) = \xi$. Let $i = 1$

and C be a preimage of C_i under the map $A_n \to A_{\chi,n}$. Choose $M = 2^n$ and $W = \mathcal{O}(\mathbb{M})^\times/(\mathcal{O}(\mathbb{M})^\times)^M$. Consider

$$\psi : W \to \mathbb{Z}/M\mathbb{Z}[G] \quad x \mapsto (\varepsilon_\chi \circ \vartheta_n)(x^v),$$

where v is such that $x^v \in E_n$ for all x and ε_χ is defined as in Lemma 3.3.20. Then Theorem 3.3.8 implies that we can find an ideal $\mathfrak{Q}_1$ satisfying i) and ii). We know further from Theorem 3.3.8 that $\varphi_{\mathfrak{q}_1}(w) = 2^d u\psi(w)\mathfrak{Q}_1$. As $\alpha^\sigma(n,(1))$ is a unit we can apply Proposition 3.3.7[2] and obtain

$$\begin{aligned} v_{\mathfrak{Q}_1}(\kappa(\mathfrak{q}_1))\mathfrak{Q}_1 &= [\kappa(\mathfrak{q}_1)]_{\mathfrak{q}_1} = \varphi_{\mathfrak{q}_1}(\kappa(1)) \\ &= \varphi_{\mathfrak{q}_1}(\xi) = 2^d u\psi(\xi)\mathfrak{Q}_1 = 2^d uv\varepsilon_\chi((\gamma'_{n_0}-1)^{c_1}2^{c_2}h'_\chi)\mathfrak{Q}_1 \mod 2^n. \end{aligned}$$

Projecting to the χ component and using the definition of ε_χ we get (3.3).

We will now define the ideals $\mathfrak{Q}_i$ inductively. Assume that we have already found the ideals $\mathfrak{Q}_1, \dots \mathfrak{Q}_{i-1}$ and let $\mathfrak{a}_{i-1} = \prod_{j=1}^{i-1} \mathfrak{q}_j$. Using point iii) recursively we see

$$\prod_{j\le i-2} g_j(v_{\mathfrak{Q}_{i-1}}(\kappa(\mathfrak{a}_{i-1}))_\chi = |H|^{i-1}u2^{(i-2)(2d+c_3)+d+c_2}(\gamma'_{n_0}-1)^{c_1+\sum_{j=1}^{i-2}c_1^j}h'_\chi.$$

Let $D_i = |H|^{i-1}u2^{(i-2)(2d+c_3)+d+c_2}$. By enlarging c_1 we can assume that $c_1 + \sum_{j=1}^{i-2} c_1^j$ is bounded by c_1^{i-1} and set $t_i = c_1^{i-1}$. It follows that $v_{\mathfrak{Q}_{i-1}}(\kappa(\mathfrak{a}_{i-1}))_\chi \mid D_i h'_\chi(\gamma'_{n_0}-1)^{t_i}$. Define $N = (\gamma'_{n_0}-1)^{t_i}(I_{\mathfrak{q}_{i-1}}/(MI_{\mathfrak{q}_{i-1}} + \mathbb{Z}_p[G][\kappa(\mathfrak{a}_{i-1})]_{\mathfrak{q}_{i-1}})_\chi)$. As h'_χ is coprime to every $\gamma'_n - 1$ we see that $\Lambda_{\chi,m+n-m'}/h'_\chi$ is finite and further

$$|N| \le |\Lambda_{\chi,m+n-m'}/D_i||\Lambda_{\chi,m+n-m'}/h'_\chi|.$$

Choose now $2^l = M > \max(|A_\chi(\mathbb{M})||\Lambda_{\chi,m+n-m'}/D_i||\Lambda_{\chi,m+n-m'}/h'_\chi|, 2^n)$. We want to apply Lemma 3.3.19 with $E = 2^{c_3+d}$, $\eta = (\gamma'_{n_0}-1)^{t_i}$, $g = g_{i-1}$, $\mathfrak{A} = \mathfrak{a}_{i-1}$, and $x = \kappa(\mathfrak{a}_{i-1})$. To do so we have to check the assumptions. It follows directly from Proposition 3.3.7 i) that $[x]_\mathfrak{r} = 0$ for all $\mathfrak{r}$ coprime to $\mathfrak{a}_{i-1}$. We now have to check the conditions i)-iii) from Lemma 3.3.19.

i) By definition $C_\chi = [\mathfrak{Q}_{i-1}]_\chi = 2^d C_{i-1}$. The annihilator of $t(C)$ is given by $g_{i-1}/(2^{c_3+d}, g_{i-1})$. As property i) holds for all $\mathfrak{Q}_j$ with $j \le i-2$ we obtain that $E \cdot \mathrm{ann}_{\mathbb{Z}_p[G]}(\overline{C}_\chi) \subset g_{i-1}\mathbb{Z}_p[G]_\chi$.

ii) It is immediate from Lemma 3.3.13 that $\mathbb{Z}_p[G]_\chi/g\mathbb{Z}_p[G]_\chi$ is finite.

iii) $M > |A_\chi||N| = |A_\chi||\eta(\frac{I_{\mathfrak{q}_{i-1}}/(MI_{\mathfrak{q}_{i-1}})}{\mathbb{Z}_p[G][\kappa(\mathfrak{a}_{i-1})]_{\mathfrak{q}_{i-1}}})_\chi|$.

Thus, we obtain a homomorphism

$$\psi_i \colon W_\chi \to \mathbb{Z}/M\mathbb{Z}[G]_\chi$$

[2] We have to ensure that $\mathfrak{q}_1$ lies in the domain of κ, i.e. $\mathfrak{q}_1$ has to satisfy a certain coprimality condition. As Theorem 3.3.8 gives us infinitely many primes we can just assume that $\mathfrak{q}_1$ lies in the domain of κ.

with $g_{i-1}\psi_i(\kappa(\mathfrak{a}_{i-1})) = (2^{c_3+d}(\gamma'_{n_0}-1)^{t_i}v_{\mathfrak{Q}_{i-1}}(\kappa(\mathfrak{a}_{i-1})))_\chi$. Let Π_χ be the projection $W \to W_\chi$ and define $\psi = \varepsilon_\chi \circ \psi_i \circ \Pi_\chi$. Let M be as in the previous paragraph and C a preimage of C_i. Then Theorem 3.3.8 gives us a prime ideal $\mathfrak{Q}_i$ satisfying i) and ii) (recall that $2^n \mid M$). Further, $\varphi_{\mathfrak{q}_i}(\kappa(\mathfrak{a}_{i-1})) = 2^d u\psi(\kappa(\mathfrak{a}_{i-1}))\mathfrak{Q}_i$. Then we obtain

$$\begin{aligned} v_{\mathfrak{Q}_i}(\kappa(\mathfrak{q}_1\dots\mathfrak{q}_i))\mathfrak{Q}_i = [\kappa(\mathfrak{q}_1\dots\mathfrak{q}_i)]_{\mathfrak{q}_i} &= \varphi_{\mathfrak{q}_i}(\kappa(\mathfrak{q}_1\dots\mathfrak{q}_{i-1})) \\ &= 2^d u\psi(\kappa(\mathfrak{a}_{i-1}))\mathfrak{Q}_i. \end{aligned}$$

Projecting to the χ-component and using the definition of ψ_i we obtain

$$(g_{i-1}v_{\mathfrak{Q}_i}(\kappa(\mathfrak{q}_1\mathfrak{q}_2\dots\mathfrak{q}_i))_\chi = u_i|H|(\gamma'_{n_0}-1)^{c_1^{i-1}}2^{2d+c_3}(v_{\mathfrak{Q}_{i-1}}(\kappa(\mathfrak{q}_1\dots\mathfrak{q}_{i-1}))_\chi,$$

which finishes the proof. □

To derive a relation between h_χ and $\prod_{i=1}^s g_i$ we need the following result:

Corollary 3.3.22. *Let $\mathbb{M}$ be a finite abelian extension of $\mathbb{K}$ and consider $\mathbb{H}/\mathbb{K}_\infty\mathbb{M}$ (the maximal p-abelian unramified extension of $\mathbb{K}_\infty\mathbb{M}$). Then $A_\infty = Gal(\mathbb{H}/\mathbb{K}_\infty\mathbb{M})$ is finitely generated as a $\mathbb{Z}_p$-module*

Proof. $\mathrm{Gal}(\mathbb{H}/\mathbb{K}_\infty\mathbb{M})$ is a quotient of $Gal(\mathbb{M}_\infty/\mathbb{K}_\infty\mathbb{M})$. The latter is finitely generated due to Theorem 2.1.1. □

Theorem 3.3.23. $\mathrm{Char}(A_{\infty,\chi}) \mid \mathrm{Char}((\overline{E}_\infty/\overline{C}_\infty)_\chi)$.

Proof. The main argument of this proof is analogous to [Wash, page 371]. From (3.3) and (3.4) we obtain that $\prod_{i=1}^k g_i v_{\mathfrak{Q}_{k+1}}(\kappa(\mathfrak{q}_1\dots\mathfrak{q}_{k+1}))_\chi = \eta h'_\chi \mod 2^n$, where $\eta = \tilde{u}|H|^{k+1}2^{k(2d+c_3)+d+c_2}(\gamma'_{n_0}-1)^{c_1+\sum_{j=1}^k c_1^j}$ for some unit $\tilde{u}$. It follows that $\prod_{i=1}^k g_i$ divides $\eta h'_\chi$ in $\Lambda_{\chi,m+n-m'}/2^n\Lambda_{\chi,m+n-m'}$. For every n we can find an element z_n such that $\prod_{i=1}^k g_i z_n = \eta h'_\chi$ in $\Lambda_{\chi,m+n-m'}/2^n\Lambda_{\chi,m+n-m'}$. The z_n's have a convergent subsequence and we obtain that $\prod_{i=1}^k g_i \mid \eta h'_\chi$ in Λ_χ. By Lemma 3.3.12 and Corollary 3.3.22 $\mathrm{Char}(A_{\infty,\chi})$ is coprime to η and the claim follows. □

Remark 3.3.24. *Viguié proves in [Vi-2] as well that there is a power of 2 such that* $\mathrm{Char}(A_{\infty,\chi}) \mid 2^v\mathrm{Char}((\overline{E}_\infty/\overline{C}_\infty)_\chi)$. *Using Corollary 3.3.22 this implies Theorem 3.3.23. He follows the proofs of Bley very closely as well but he uses a slightly different version of Theorem 3.3.8 and does not use the relation between Γ and Γ' in the same manner as we did here in Section 3.3.2 to construct the homorphism ϑ_n.*

Corollary 3.3.25. $\mathrm{Char}(A_\infty) \mid \mathrm{Char}(\overline{E}_\infty/\overline{C}_\infty)$

Proof. As Theorem 3.3.23 holds for all characters and $\mathrm{Char}(A_\infty)$ is coprime to 2 this is immediate. □

3.4 Characteristic ideals and the Main conjecture

Consider the exact sequence

$$0 \to \overline{E}_\infty/\overline{C}_\infty \to U_\infty/\overline{C}_\infty \to X \to A_\infty \to 0,$$

where $X = \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{L}_\infty)$. Then

$$\mathrm{Char}(A_\infty)\mathrm{Char}(U_\infty/\overline{C}_\infty) = \mathrm{Char}(X)\mathrm{Char}(\overline{E}_\infty/\overline{C}_\infty). \tag{3.5}$$

From Corollary 3.3.25 we deduce

$$\mathrm{Char}(X) \mid \mathrm{Char}(U_\infty/\overline{C}_\infty). \tag{3.6}$$

In the following we will establish a relation between p-adic L-functions and elliptic units to show that $\mathrm{Char}(X)$ is in fact equal to $\mathrm{Char}(U_\infty/\overline{C}_\infty)$.

Let $u \in U_\infty$ and let $g_u(w)$ be the Coleman power series of u (see [dS, I Theorem 2.2]). Let $\tilde{g}_u(W) = \log g_u(W) - \frac{1}{p}\sum_{w \in \widehat{E}_\mathfrak{p}} \log g_u(W \oplus w)$. There exists a measure ν_u on $\mathbb{Z}_p^\times$ having $\tilde{g}_u \circ \beta^v$ as characteristic series [dS, I 3.4]. Recall that $\mathcal{D}_\mathfrak{p} = \mathcal{I}_\mathfrak{p}(\zeta_m)$ and let $\Lambda(\mathcal{D}_\mathfrak{p}, \Gamma' \times H)$ be the algebra of $\mathcal{D}_\mathfrak{p}$-valued measures on $\Gamma' \times H$. Define

$$\iota(\mathfrak{f})\colon U_\infty \to \Lambda(\mathcal{I}_\mathfrak{p}, \Gamma' \times H) \subset \Lambda(\mathcal{D}_\mathfrak{p}, \Gamma' \times H), \quad u \mapsto \sum_{\sigma \in \mathrm{Gal}(\mathbb{F}/\mathbb{K})} \nu_{\sigma u} \circ \sigma.$$

Note that this construction of measures coincides with the one from Chapter 2 for elliptic units.

Lemma 3.4.1. *$\iota(\mathfrak{f})$ induces a homomorphism $\iota(\mathfrak{f})\colon U_\infty \hat{\otimes}_{\mathbb{Z}_p} \mathcal{I}_\mathfrak{p} \to \Lambda(\mathcal{I}_\mathfrak{p}, \Gamma' \times H)$ that is a pseudo isomorphism.*

Proof. By [dS, I Theorem 3.7] it suffices to prove that the completion of $\mathbb{L}_\infty$ at all primes above $\mathfrak{p}$ contains only finitely many 2-power roots of unity. But this follows from [Ke 1, proof of Proposition 4.3.10] (see also [dS, Chapter III, Proposition 1.3]). □

For every $\mathfrak{g} \mid \mathfrak{f}$ there is a map $\iota(\mathfrak{g})\colon U_\infty(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)) \to \Lambda(\mathcal{I}_\mathfrak{p}, \mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty/\mathbb{K})))$. Note that there are natural restriction and corestriction maps $\pi_{\mathfrak{f},\mathfrak{g}}$ and $\eta_{\mathfrak{f},\mathfrak{g}}$ such that $\pi_{\mathfrak{f},\mathfrak{g}} \circ \iota(\mathfrak{f}) = \iota(\mathfrak{g}) \circ N_{\mathfrak{f},\mathfrak{g}}$ and $\iota(f) \circ \text{inclusion} = \eta_{\mathfrak{f},\mathfrak{g}} \circ \iota(\mathfrak{g})$, where inclusion is the natural map $U_\infty(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)) \to U_\infty$ (see [dS, page 100] for details). If we want to apply the characters of H to the images of $\iota(\mathfrak{f})$ we have to extend the ring of definition for our measure to $\mathcal{D}_\mathfrak{p}$.

Proposition 3.4.2. *Let χ be a character of H of conductor dividing $\mathfrak{g}\mathfrak{p}^2$ such that the prime to $\mathfrak{p}$-part of the conductor is $\mathfrak{g}$. Then $\mathrm{Char}(U_\infty/\overline{C}_\infty)_\chi = \chi(\nu(\mathfrak{g}))$ if χ is non-trivial and $\mathrm{Char}(U_\infty/\overline{C}_\infty)_\chi = (\gamma' - 1)\chi(\nu(1))$ if χ is trivial.*

Proof. Analogous to [dS, III Lemma 1.10]. In view of Lemma 3.4.1 and due to the fact that characteristic ideals are well behaved under extensions of scalars, it suffices to determine the image of $\chi\circ\iota(\overline{C}_\infty)$. As the conductor of χ divides $\mathfrak{g}\mathfrak{p}^2$ and is divisible by $\mathfrak{g}$ it follows that $\chi\circ\iota(\mathfrak{f})(\overline{C_\infty(\mathfrak{f})}) = \chi\circ\pi_{\mathfrak{f},\mathfrak{g}}\circ\iota(\mathfrak{f})(\overline{C_\infty(\mathfrak{f})}) = \chi\circ\iota(\mathfrak{g})N_{\mathfrak{f},\mathfrak{g}}\overline{C_\infty(\mathfrak{f})}$. Assume first that $\mathfrak{g}\neq(1)$. It is immediate that $\sum_{\sigma\in\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty))/\mathbb{K}(\mathfrak{h}\mathfrak{p}^\infty))}\chi(\sigma)=0$ for any ideal $\mathfrak{h}\mid\mathfrak{g}$ different from $\mathfrak{g}$. Hence,

$$\chi\circ\iota(\mathfrak{g})(\overline{C_{\mathfrak{g},\infty}}) = \chi\circ\iota(\mathfrak{g})(\overline{C_\infty(\mathfrak{g})}). \tag{3.7}$$

If $\omega_\mathfrak{g}=1$, we can construct the measure $\nu(\mathfrak{g})$ as in Chapter 2 and obtain that $\iota(\mathfrak{g})(\overline{C_\mathfrak{g}})$ is the ideal generated by $\mathcal{J}\nu(\mathfrak{g})$, where $\mathcal{J}$ is the ideal generated by all the $\mu_\alpha := N\alpha-\sigma_\alpha$. If $\omega_\mathfrak{g}\neq 1$ there exists an integer k such that $\omega_{\mathfrak{g}^k}=1$ and then we can define the measure $\nu(\mathfrak{g}^k)$. But by (2.21) we have that $\nu(\mathfrak{g})$ is just the restriction of $\nu(\mathfrak{g}^k)$ and $N_{\mathfrak{g}^k,\mathfrak{g}}$ is surjective on the elliptic units. So in both cases the image under $\iota(\mathfrak{g})$ is precisely $\mathcal{J}\nu(\mathfrak{g})$.

If the norm $N_{\mathfrak{f},\mathfrak{g}}:\overline{C_\infty(\mathfrak{f})}\to\overline{C_\infty(\mathfrak{g})}$ is not surjective, it follows that the cokernel of the module $\chi\circ\iota(g)\circ N_{\mathfrak{f},\mathfrak{g}}(\overline{C_\infty(\mathfrak{f})})$ in $\chi\circ\iota(\mathfrak{g})(\overline{C_\infty(\mathfrak{g})})$ is annihilated by $[\mathbb{K}(\mathfrak{f}\mathfrak{p}^\infty):\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)]$ and the product $\prod_{l\mid\mathfrak{f},l\nmid\mathfrak{g}}(1-\chi(\sigma_l)\sigma_l^{-1}\mid_{\Gamma'})$. These elements are certainly coprime and we see that $\chi\circ\iota(\mathfrak{f})(\overline{C_\infty(\mathfrak{f})})\sim\chi\circ\iota(\mathfrak{g})(\overline{C_{\mathfrak{g},\infty}})$ due to (3.7), where $A\sim B$ means that A and B are pseudo isomorphic. But the $\chi(\mu_\alpha)$ are coprime due to the proof of Theorem 2.2.9 and the claim follows for $\mathfrak{g}\neq(1)$.

Assume now that $\mathfrak{g}=(1)$. Let $\tau\in\mathrm{Gal}(\mathbb{K}(\mathfrak{p}^n)/\mathbb{K})$ then the elements $\xi_{\alpha,\sigma}(P_n^\sigma)^{\tau-1}$ are norms of elliptic units from $\mathbb{K}(\mathfrak{h}\mathfrak{p}^n)$, where $\mathfrak{h}$ is a prime having Artin symbol τ^{-1} in $\mathrm{Gal}(\mathbb{K}(\mathfrak{p}^n)/\mathbb{K})$. It follows that a projective sequence of elements $\xi_{\alpha,\sigma}(P_n^\sigma)^{\tau-1}$ (all with the same τ) corresponds to the measure $\mu_\alpha(\tau-1)\nu(1)\circ\sigma^{-1}$ under $\iota(1)$. Consider now a generator of the form $\prod_{i=1}^s\xi_{\alpha_i,\sigma}(P_n^\sigma)^{m_i}$ with $\sum m_i(N\alpha_i-1)=0$. Let ν_π be the measure corresponding to a sequence of such products. Then we obtain $((\tau-1)\nu_\pi)\circ\sigma=\sum m_i\mu_{\alpha_i}(\tau-1)\nu(1)$. As $(\tau-1)\nu(1)$ is not contained in the augmentation of $\Lambda(\mathcal{D}_\mathfrak{p},\mathrm{Gal}(\mathbb{K}(\mathfrak{p}^\infty)/\mathbb{K}))$ we obtain that the ideal generated by the $\sum m_i\mu_{\alpha_i}$ is contained in the augmentation ideal and that the ideal generated by $\iota((1))(\overline{C_{(1),\infty}})$ is pseudo isomorphic to $\mathcal{A}\nu((1))$, where $\mathcal{A}$ denotes the augmentation of $\Lambda(\mathcal{D}_\mathfrak{p},\mathrm{Gal}(\mathbb{K}(\mathfrak{p}^\infty)/\mathbb{K}))$. Analogously to the case $\mathfrak{g}\neq(1)$ we can conclude that $\chi\circ\iota((1))\circ N_{\mathfrak{f},(1)}(\overline{C_\infty(\mathfrak{f})})$ is pseudo isomorphic to $\chi\circ\iota((1))(\overline{C_{(1),\infty}})$. Hence, it suffices to consider the image $\chi\circ\iota((1))(\overline{C_{(1),\infty}})$. If χ is a non-trivial character, then $\chi(\mathcal{A})$ contains $\chi(\tau)-1$ as well as $\gamma'-1$. Thus $\chi\circ\iota((1))(\overline{C_{(1),\infty}})\sim\chi(\nu(1))$. If χ is the trivial character, then $\chi\circ\iota((1))(\overline{C_{(1),\infty}})$ is generated by $(\gamma'-1)\chi(\nu(1))$. □

Corollary 3.4.3. *Let $F(w,\chi)$ be the Iwasawa function associated to $L_\mathfrak{p}(s,\chi)$ defined in Definition 2.2.12. Then* $\mathrm{Char}((U_\infty/\overline{C}_\infty)_\chi)=F(w,\chi^{-1})$.

Proof. Let $\mathfrak{g}$ be such that the conductor of χ is divisible by $\mathfrak{g}$ and divides $\mathfrak{g}\mathfrak{p}^2$. By Proposition 3.4.2 we see that the characteristic ideal of $(U_\infty/\overline{C}_\infty)_\chi$ is given by $\chi(\nu(\mathfrak{g}))$ if χ is non-trivial and $(1-\gamma')\chi(\nu(1))$ if χ is trivial. But these are precisely the measures used to define $L_\mathfrak{p}(s,\chi^{-1})$. Let $G_\mathfrak{g}$ be $\mathrm{Gal}(\mathbb{K}(\mathfrak{g}\mathfrak{p}^\infty)/\mathbb{K})$. Then we have the identity $\int_{\mathcal{G}_\mathfrak{g}}\kappa^s\chi d(1-\gamma)^e\nu(\mathfrak{g})=\int_{\Gamma'}\kappa^s d(1-\gamma)^e\chi(\nu(\mathfrak{g}))$, where $e=1$ if χ is trivial and $e=0$ in all other cases, the claim follows. □

3.4.1 Proof of the Main conjecture

In this section we use all the results proved before to prove the main conjecture.

Lemma 3.4.4. $\mathrm{Char}(X) = \mathrm{Char}(U_\infty/\overline{C}_\infty)$ *and* $\mathrm{Char}(A_{\infty,\chi}) = (\overline{E}_\infty/\overline{C}_\infty)_\chi$.

Proof. The first claim follows directly from (3.6), Corollary 3.4.3 and Theorem 2.4.5. From (3.5) we also obtain that $\mathrm{Char}(A_\infty) = \mathrm{Char}(\overline{E}_\infty/\overline{C}_\infty)$. Further Theorem 3.3.23 establishes that $\mathrm{Char}(A_{\infty,\chi})$ divides $\mathrm{Char}(\overline{E}_\infty/\overline{C}_\infty)_\chi$. Both together imply the second claim. □

This has also the following consequence:

Theorem 3.4.5. $\mathrm{Char}(X_\chi) = \mathrm{Char}((U_\infty/\overline{C}_\infty)_\chi)$ *for any* χ.

Proof. For any Λ-module we denote by M^χ the largest submodule in $M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p(\chi)$ on which H acts via χ. By [Ts, page 5] there exists a homomorphism between M_χ and M^χ such that the kernel and the cokernel are annihilated by $|H|$. As none of the characteristic ideals involved is divisible by 2 we can consider the characteristic ideals of M^χ instead of M_χ for any M in $\{A_\infty, U_\infty/\overline{C}_\infty, X, \overline{E}_\infty/\overline{C}_\infty\}$. The sequence

$$0 \to (\overline{E}_\infty/\overline{C}_\infty)^\chi \to (U_\infty/\overline{C}_\infty)^\chi \to X^\chi$$

is exact. Let e_χ in $\mathbb{Q}_p(\chi)[H]$ be the idempotent induced by the character χ. Then $e_\chi|H|$ is an element in $\mathbb{Z}_p(\chi)[H]$. In particular, $e_\chi|H|M \subset M^\chi$. It follows that the cokernel of the natural homomorphism $\phi_\chi : X^\chi \to A_\infty^\chi$ is annihilated by $|H|$. As A_∞ has bounded rank it follows that Coker (ϕ_χ) is finite. The module $\ker(\phi_\chi)$ equals $X^\chi \cap im(U_\infty/\overline{C}_\infty)$. Again the exponent of $X^\chi \cap im((U_\infty/\overline{C}_\infty))/im((U_\infty/\overline{C}_\infty)^\chi)$ is bounded by $|H|$. Hence, $\mathrm{Char}(A_\infty^\chi)\mathrm{Char}(im((U_\infty/\overline{C}_\infty)^\chi) = \mathrm{Char}(X^\chi)$. Using the exactness of the sequence above we obtain

$$\mathrm{Char}(A_\infty^\chi)\mathrm{Char}((U_\infty/\overline{C}_\infty)^\chi) = \mathrm{Char}((\overline{E}_\infty/\overline{C}_\infty)^\chi)\mathrm{Char}(X^\chi).$$

The claim follows now from Lemma 3.4.4. □

The second claim of Lemma 3.4.4 and Theorem 3.4.5 prove Theorem 3.1.1 for $\mathbb{L}_\infty$.

Chapter 4

Iwasawa Theory of abelian varieties

Acknowledgments

This chapter is joint work with Sören Kleine, Universität der Bundeswehr München.

4.1 Iwasawa theory of elliptic curves

Let $\mathbb{K}$ be a number field, p a rational prime and A an abelian variety defined over $\mathbb{K}$. Let Σ be a set of primes in $\mathbb{K}$ containing all places above p and all primes at which A has bad reduction. If $p = 2$, we assume that Σ contains the infinite primes as well. We write $\mathbb{Q}_\Sigma$ for the maximal Galois extension of $\mathbb{Q}$ unramified outside Σ. Recall that $\mathbb{Q}_\infty$ denotes the unique $\mathbb{Z}_p$-extension of $\mathbb{Q}$. To simplify notation we write $H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, \cdot)$ for $H^1(Gal(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty), \cdot)$ and $H^1(\mathbb{K}, \cdot)$ for $H^1(G_\mathbb{K}, \cdot)$, where $G_\mathbb{K}$ denotes the absolute Galois group of $\mathbb{K}$. For any number field $\mathbb{K}$ and any finite prime $v \in \mathbb{K}$ we write $\mathbb{K}_v$ for the completion of $\mathbb{K}$ at v.

Assume now that E is an elliptic curve defined over $\mathbb{Q}$. Let $T = \lim_{\infty \leftarrow n} E[p^n]$ be the Tate-module of E and $V = T \otimes \mathbb{Q}_p$. Note that V is a two dimensional $\mathbb{Q}_p$-vector space. Then we have that $V/A \cong E[p^\infty]$ as $G_\mathbb{Q}$-modules. Let $\tilde{E}$ be the reduction of E modulo p. We define

$$C = \ker(E[p^\infty] \to \tilde{E}[p^\infty])$$

and $D = A/C$. We define further the local condition $\mathcal{H}_v(\mathbb{Q}_{\infty,v}, E[p^\infty])$ as follows:

$$\mathcal{H}_v(\mathbb{Q}_{\infty,v}, E[p^\infty]) = \begin{cases} \prod_{\eta|v} H^1(\mathbb{Q}_{\infty,\eta}, E[p^\infty]) & v \neq p \\ H^1(\mathbb{Q}_{\infty,\eta_p}, E[p^\infty])/L_{\eta_p} & v = p \end{cases},$$

with $L_{\eta_p} = \ker(H^1(\mathbb{Q}_{\infty,v}, E[p^\infty] \to H^1(I_{\eta_p}, D))$, where I_{η_p} denotes the inertia subgroup of η_p the place above p in $\mathbb{Q}_\infty$. Then the p-primary Selmer group is defined as

$$\mathrm{Sel}(\mathbb{Q}_\infty) = \ker(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}_\infty, E[p^\infty]) \to \prod_{v \in \Sigma} \mathcal{H}_v(\mathbb{Q}_{\infty,v}, E[p^\infty]).$$

These Selmer groups are Λ-modules and each element is annihilated by some ω_n.

For any discrete $\mathbb{Z}_p$-module M, we define the Pontryagin dual of M as

$$M^\vee = \mathrm{Hom}_{\mathrm{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p)$$

(i.e. the set of continuous homomorphisms). In particular, we can plug in our Selmer groups defined above for M and obtain that their Pontryagin duals are compact noetherian torsion Λ-modules [Kat]. Recall from chapter 1 that M is pseduo isomorphic to a Λ-module of the form

$$\bigoplus_{i=1}^{k} \Lambda/p^{e_i} \bigoplus \bigoplus_{j=1}^{s} \Lambda/f_j(T)^{d_j},$$

for irreducible distinguished polynomials $f_j(T)$. To simplify notation we write $\mu(E)$ and $\lambda(E)$ for the μ- and λ-invariants of the Pontryagin dual of the Selmer group. As one of their main results Greenberg and Vatsal obtain [Gre-Vat, Theorem 1.4]:

Theorem 4.1.1. *Let E_1 and E_2 be modular elliptic curves defined over $\mathbb{Q}$. Assume that $E_1[p] \cong E_2[p]$ as $G_\mathbb{Q}$-modules. Then $\mu(E_1) = 0$ if and only if $\mu(E_2) = 0$. If both μ-invariants vanish then $\lambda(E_1) = \lambda(E_2)$.*

Remark 4.1.2. *The above theorem is stated as in [Gre-Vat]. Due to the modularity theorem we know that all elliptic curves defined over $\mathbb{Q}$ are modular. Therefore, the above theorem is true for all elliptic curves defined over $\mathbb{Q}$.*

Theorems of this form have been generalized to various settings, i.e. for the supersingular reduction case and plus/minus Selmer groups by Kim [Kim], for general modular forms in the supersingular setting by Hattley and Lei [Ha-Le] and by Ramdorai and Ray for elliptic curves of semistable reduction over a number field $\mathbb{F}$ [Ra-Ra]. There are further generalizations due to Hattley, Lei and Vigni ([Ha-Le-Vi]) using the anticyclotomic instead of the cyclotomic $\mathbb{Z}_p$-extension, but we will not go into details here. Interested readers my consult [Ha-Le-Vi].

4.2 μ and λ-invariants of isogenous varieties

In contrast to the works mentioned above we will focus on fine Selmer groups. These are much "smaller" then the Selmer groups considered by Greenberg and Vatsal or Ramdorai and Ray. On the one hand this allows us to work with arbitrary $\mathbb{Z}_p$-extensions instead of the cyclotomic one. On the other hand it also forces us to impose stronger assumptions on our abelian varieties, i.e. we require that $A(\mathbb{K}_v)[p]$ is trivial for all $v \in \Sigma$.

Let $\mathbb{K}$ be a global field, A an abelian variety defined over $\mathbb{K}$ and a p a prime number.

Definition 4.2.1. *Let Σ be a set of places of $\mathbb{K}$ containing all the places above p and all places where A has bad reduction (if $p = 2$ then Σ should also contain the infinite*

places). We define the (p-primary part of the) fine Selmer group *of A over $\mathbb{K}$ as*

$$\mathrm{Sel}_{0,A}(\mathbb{K}) = \ker\left(H^1(\mathbb{K}_\Sigma/\mathbb{K}, A[p^\infty]) \longrightarrow \prod_{v\in\Sigma} H^1(\mathbb{K}_v, A[p^\infty])\right),$$

where $\mathbb{K}_\Sigma$ denotes the maximal algebraic pro-p-extension of $\mathbb{K}$ which is unramified outside of Σ . Further, we define the p^i-fine Selmer groups, $i \in \mathbb{N}$, as

$$\mathrm{Sel}_{0,A[p^i]}(\mathbb{K}) = \ker\left(H^1(\mathbb{K}_\Sigma/\mathbb{K}, A[p^i]) \longrightarrow \prod_{v\in\Sigma} H^1(\mathbb{K}_v, A[p^i])\right).$$

Note that both definition depends a priori on the choice of the set Σ. If $\mathbb{K}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field or if Σ contains all infinite primes then the fine Selmer group is independent of the choice of Σ and can be rewritten as

$$\mathrm{Sel}_{0,A}(\mathbb{K}) = \ker\left(H^1(\mathbb{K}, A[p^\infty]) \longrightarrow \prod_{v} H^1(\mathbb{K}_v, A[p^\infty])\right),$$

where the product on the right hand side runs over all places of $\mathbb{K}$ [Ra-Wi][Li-Mu]. From now an we assume that $\mathbb{K}$ is a number field and consider a $\mathbb{Z}_p$-extension $\mathbb{K}_\infty/\mathbb{K}$ with intermediate fields $\mathbb{K}_n$. The extension $\mathbb{K}_\infty/\mathbb{K}$ is unramified outside p. In particular, $\mathbb{K}_\infty \subset \mathbb{K}_\Sigma$. By maximality $(\mathbb{K}_n)_\Sigma$ is Galois over $\mathbb{K}$ and $(\mathbb{K}_n)_\Sigma = \mathbb{K}_\Sigma$. Therefore, $\mathrm{Sel}_A(\mathbb{K}_n)$ is a subgroup of $H^1(\mathbb{K}_\Sigma/\mathbb{K}, A[p^\infty])$. We denote the corresponding Pontryagin duals by

$$Y_n^{(\mathbb{K}_n)} = \mathrm{Sel}_{0,A}(\mathbb{K}_n)^\vee,$$

and define the projective limits

$$Y_A^{(\mathbb{K}_\infty)} = \lim_{\infty\leftarrow n} Y_n^{(\mathbb{K}_n)}$$

with respect to the corestriction maps.

Our aim in this Chapter is to prove the following Theorem

Theorem 4.2.2. *Let $p \geq 3$. Consider two abelian varieties, A_1 and A_2, defined over the number field $\mathbb{K}$. Let Σ be a set of primes containing all primes above p and all primes at which either A_1 or A_2 has bad reduction. Assume that $A_i(\mathbb{K})[p] = \{0\}$ and that moreover $A_i(\mathbb{K}_v)[p] = \{0\}$ for every $v \in \Sigma$ and $i \in \{1, 2\}$. Let $\mathbb{K}_\infty/\mathbb{K}$ be a $\mathbb{Z}_p$-extension. We assume that the modules $Y_{A_i}^{(\mathbb{K}_\infty)}$ are noetherian Λ-torsion for $1 \leq i \leq 2$. Let l be an integer such that $p^l Y_{A_1}^{(\mathbb{K}_\infty)}$ has finite p-rank.*

Then the following statements hold.

a) If $A_1[p^l] \cong A_2[p^l]$ as $G_\mathbb{K}$-modules, then $\mu(Y_{A_1}^{(\mathbb{K}_\infty)}) \leq \mu(Y_{A_2}^{(\mathbb{K}_\infty)})$.

b) If $A_1[p^l] \cong A_2[p^l]$ for some l such that both $p^l Y_{A_1}^{(\mathbb{K}_\infty)}$ and $p^l Y_{A_1}^{(\mathbb{K}_\infty)}$ have finite p-rank, then $\mu(Y_{A_1}^{(\mathbb{K}_\infty)}) = \mu(Y_{A_2}^{(\mathbb{K}_\infty)})$.

c) If $A_1[p^{l+1}] \cong A_2[p^{l+1}]$ then $\mu(Y_{A_1}^{(\mathbb{K}_\infty)}) = \mu(Y_{A_2}^{(\mathbb{K}_\infty)})$. In particular, if $A_1[p] \cong A_2[p]$, then $\mu(Y_{A_1}^{(\mathbb{K}_\infty)}) = 0 \Longleftrightarrow \mu(Y_{A_2}^{(\mathbb{K}_\infty)}) = 0$.

d) Let l' be minimal such that $p^{l'}Y_{A_1}^{(\mathbb{K}_\infty)}$ is $\mathbb{Z}_p$-free. Assume that $A_1[p^{l'+1}] \cong A_2[p^{l'+1}]$. Then $\lambda(Y_{A_1}^{(\mathbb{K}_\infty)}) \geq \lambda(Y_{A_2}^{(\mathbb{K}_\infty)})$.

e) Let l' be as in the previous point. Assume that $A_1[p^{l'+1}] \cong A_2[p^{l'+1}]$. If $p^{l'}Y_{A_1}^{(\mathbb{K}_\infty)}$ is $\mathbb{Z}_p$-free as well, we obtain $\lambda(Y_{A_1}^{(\mathbb{K}_\infty)}) = \lambda(Y_{A_2}^{(\mathbb{K}_\infty)})$.

The second part of statment c) is proved in [Ra-Ra] for elliptic curves of good ordinary reduction at p and the p-primary Selmer group. Barman and Saikia proved the analogous result for Theorem 4.2.2 points a) and c) for $\mathbb{Q}_\infty$ and elliptic curves with good ordinary reduction [Ba-Sa].

The assumption that $Y_A^{(\mathbb{K}_\infty)}$ is Λ-torsion is a non-trivial condition. If A is an elliptic curve then it is equivalent to $H^2(\mathbb{K}_\Sigma/\mathbb{K}_\infty, A[p^\infty]) = 0$ [Ma]. The condition that $H^2(\mathbb{K}_\Sigma/\mathbb{K}_\infty, A[p^\infty])$ is trivial is often referred to as weak Leopoldt conjecture.

To prove our theorem we need the following auxiliary lemmas:

Lemma 4.2.3. *Let X be a finitely generated torsion Λ-module. Then*

$$\mu(X) = \sum_{i=0}^{\infty} \mathbb{F}_p[[T]]\text{-rank}(p^i X/p^{i+1}X).$$

Proof. This statement is well-known (e.g. [Ve, Section 3.4]), but we reprove it here for the convenience of the reader. Let E be the unique elementary Λ-module that is pseudo isomorphic to X. Thus, we can write $E = \bigoplus_{i=1}^{s} \Lambda/(p^{e_i}) \oplus E_\lambda$ for a Λ-module E_λ which is a finitely generated free $\mathbb{Z}_p$-module. Then

$$\mu(X) = \mu(E) = \sum_{i=0}^{\infty} |\{k \mid e_k > i\}| = \sum_{i=0}^{\infty} \mathbb{F}_p[[T]]\text{-rank}(p^i X/p^{i+1}X)$$

because

$$\mathbb{F}_p[[T]]\text{-rank}(p^i X/p^{i+1}X) = \mathbb{F}_p[[T]]\text{-rank}(p^i E/p^{i+1}E) = |\{k \mid e_k \geq i+1\}|$$

for every $i \in \mathbb{N}$. □

Lemma 4.2.4. *Let A be an abelian variety defined over $\mathbb{K}$ and let Σ be as in Theorem 4.2.2. Assume that $A(\mathbb{K})[p] = \{0\}$ and that moreover $A(\mathbb{K}_v)[p] = \{0\}$ for every $v \in \Sigma$. Then we have for every n and every $i \in \mathbb{N}$, $i \geq 1$*

$$\text{Sel}_{0,A}(\mathbb{K}_n)[p^i] \cong \text{Sel}_{0,A[p^i]}(\mathbb{K}_n).$$

Furthermore, we obtain

$$Y_A^{(\mathbb{K}_\infty)}/p^i Y_A^{(\mathbb{K}_\infty)} \cong \varprojlim_{\infty \leftarrow n} \text{Sel}_{0,A[p^i]}(\mathbb{K}_n)^\vee.$$

Proof. We know by assumption that $A(\mathbb{K})[p] = \{0\}$. Note that $\mathbb{K}_\infty/\mathbb{K}$ is a pro-p-extensions and we obtain that $H^0(\mathbb{K}_n, A[p^\infty]) = \{0\}$ [Ne-Sc-Wi, Corollary (1.6.13)] for all n. Since the extension $\mathbb{K}_\infty(A[p^\infty])/\mathbb{K}_n$ is unramified outside Σ (see for example

[Gre 5, page 258]), we can easily see that $H^0(\mathbb{K}_\Sigma/\mathbb{K}_n, A[p^\infty]) = 0$. Now consider the exact sequence

$$0 \longrightarrow A[p^i] \longrightarrow A[p^\infty] \xrightarrow{p^i} A[p^\infty] \longrightarrow 0.$$

Taking the $\mathbb{K}_\Sigma/\mathbb{K}_n$-cohomology we obtain a second exact sequence

$$0 \longrightarrow H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, A[p^i]) \longrightarrow H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, A[p^\infty]) \longrightarrow H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, A[p^\infty]),$$

where the last homomorphism is multiplication by p^i. Hence, we obtain the isomorphism

$$H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, A[p^i]) \cong H^1(\mathbb{K}_\Sigma/\mathbb{K}_\infty, A[p^\infty])[p^i].$$

Let w be a place in $\mathbb{K}_n$ above a prime v in Σ. Using the same reasoning as above we can show that

$$H^1(\mathbb{K}_{n,w}, A[p^i]) \cong H^1(\mathbb{K}_{n,w}, A[p^\infty])[p^i].$$

Hence, we obtain the following commutative diagram

$$\begin{array}{ccc} H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, A[p^i]) & \xrightarrow{\cong} & H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, A[p^\infty])[p^i] \\ \downarrow & & \downarrow \\ \prod_{v\in\Sigma}\prod_{w|v} H^1(\mathbb{K}_{n,w}, A[p^i]) & \xrightarrow{\cong} & \prod_{v\in\Sigma}\prod_{w|v} H^1(\mathbb{K}_{n,w}, A[p^\infty])[p^i]. \end{array}$$

Now the first claim is immediate for every finite level n. For the second claim note that $Y_A^{\mathbb{K}_n}/p^i Y_A^{\mathbb{K}_n} \cong (\mathrm{Sel}_{0,A}(\mathbb{K}_n)[p^i])^\vee$. Using the isomorphism proved in the first half of the lemma and taking the projective limit finishes the proof. □

Lemma 4.2.5. *Let A_1 and A_2 be two abelian varieties defined over $\mathbb{K}$. Let Z_1 and Z_2 be equal to $A_1[p^i]$ and $A_2[p^i]$ for some $i \in \mathbb{N}$. We assume that Z_1 and Z_2 are isomorphic as $G_\mathbb{K}$-modules. Then $\mathrm{Sel}_{0,Z_1}(\mathbb{K}_n) \cong \mathrm{Sel}_{0,Z_2}(\mathbb{K}_n)$ for all n.*

Proof. Let $\phi : Z_1 \longrightarrow Z_2$ be a $G_\mathbb{K}$-module homomorphism. As $\mathbb{K}(A_i[p^\infty])/\mathbb{K}$ is unramfied outside Σ, we can interpret ϕ as a $\mathrm{Gal}(\mathbb{K}_\Sigma/\mathbb{K})$-isomorphism. Then ϕ induces an isomorphism

$$\phi : H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, Z_1) \longrightarrow H^1(\mathbb{K}_\Sigma/\mathbb{K}_n, Z_2)$$

of $G_\mathbb{K}$-modules.

For any prime w of $\mathbb{K}_n$, the inclusion $G_{\mathbb{K}_w} \hookrightarrow G_\mathbb{K}$ of the local absolute Galois group at the completion $\mathbb{K}_{n,w}$ of $\mathbb{K}_\infty$ at w, induces an isomorphism

$$H^1(K_{n,w}, Z_1) \longrightarrow H^1(K_{n,w}, Z_2).$$

The claim follows now via a commutative diagram as in the proof of Lemma 4.2.4. □

Proof of Theorem 4.2.2. Let $Z_j = \mathrm{Sel}_{0,A}(\mathbb{K}_\infty)(A_j)$. Let l be such that $p^l Y_{A_1}^{\mathbb{K}_\infty}$ is of finite p-rank. By Lemma 4.2.3 we obtain that

$$\begin{aligned}\mu(Y_{A_1}^{(\mathbb{K}_\infty)}) &= \sum_{i=0}^{\infty} \mathbb{F}_p[[T]]\text{-rank}(p^i Y_{A_1}^{(\mathbb{K}_\infty)}/p^{i+1}Y_{A_1}^{(\mathbb{K}_\infty)}) \\ &= \sum_{i=0}^{l-1} \mathbb{F}_p[[T]]\text{-rank}(p^i Y_{A_1}^{(\mathbb{K}_\infty)}/p^{i+1}Y_{A_1}^{(\mathbb{K}_\infty)}). \end{aligned} \tag{4.1}$$

By Lemma 4.2.4 we have

$$p^i Y_{A_j}^{(\mathbb{K}_\infty)}/p^{i+1}Y_{A_j}^{(\mathbb{K}_\infty)} \cong \varprojlim_{\infty\leftarrow n} \mathrm{Sel}_{0,A_j[p^{i+1}]}(\mathbb{K}_n)^\vee / \varprojlim_{\infty\leftarrow n} \mathrm{Sel}_{0,A_j[p^i]}(\mathbb{K}_n)^\vee.$$

Using that $A_1[p^l] \cong A_2[p^l]$, Lemma 4.2.5 implies that

$$\mathrm{Sel}_{0,A_1[p^i]}(\mathbb{K}_n) \cong \mathrm{Sel}_{0,A_2[p^i]}(\mathbb{K}_n)$$

for $1 \leq i \leq l$ and all n. Using (4.1), we may conclude that

$$\begin{aligned}\mu(Y_{A_1}^{(\mathbb{K}_\infty)}) &= \sum_{i=0}^{l-1} \mathbb{F}_p[[T]]\text{-rank}(p^i Y_{A_1}^{(\mathbb{K}_\infty)}/p^{i+1}Y_{A_1}^{(\mathbb{K}_\infty)}) \\ &= \sum_{i=0}^{l-1} \mathbb{F}_p[[T]]\text{-rank}(p^i Y_{A_2}^{(\mathbb{K}_\infty)}/p^{i+1}Y_{A_2}^{(\mathbb{K}_\infty)}) \\ &\leq \sum_{i=0}^{\infty} \mathbb{F}_p[[T]]\text{-rank}(p^i Y_{A_2}^{(\mathbb{K}_\infty)}/p^{i+1}Y_{A_2}^{(\mathbb{K}_\infty)}) = \mu(Y_{A_2}^{(\mathbb{K}_\infty)}). \end{aligned} \tag{4.2}$$

If $p^l Y_{A_2}^{(\mathbb{K}_\infty)}$ is also of finite p-rank, then we can exchange the roles of A_1 and A_2 and obtain equality of μ-invariants, which concludes the proof of points a) and b)

Now we prove assertion c). If $A_1[p^{l+1}] \cong A_2[p^{l+1}]$ then

$$\begin{aligned} p^l Y_{A_1}^{(\mathbb{K}_\infty)}/p^{l+1}Y_{A_1}^{\mathbb{K}_\infty} &\cong \varprojlim_{\infty\leftarrow n} \mathrm{Sel}_{0,A_1[p^{l+1}]}(\mathbb{K}_n)^\vee / \varprojlim_{\infty\leftarrow n} \mathrm{Sel}_{0,A_1[p^l]}(\mathbb{K}_n)^\vee \\ &\cong \varprojlim_{\infty\leftarrow n} \mathrm{Sel}_{0,A_2[p^{l+1}]}(\mathbb{K}_n)^\vee / \varprojlim_{\infty\leftarrow n} \mathrm{Sel}_{0,A_2[p^l]}(\mathbb{K}_\infty)^\vee \\ &\cong p^l Y_{A_2}^{(\mathbb{K}_\infty)}/p^{l+1}Y_{A_2}^{(\mathbb{K}_\infty)}. \end{aligned}$$

As the left hand side is a finitely generated $\mathbb{F}_p$-module (i.e. it is finite), the same holds for the right hand side. So the inequality in (4.2) becomes an equality.

For assertions d) and e) note that under the assumption of these two points $p\text{-rank}(p^{l'} Y_{A_1}^{(\mathbb{K}_\infty)}) = \lambda(Y_{A_1}^{(\mathbb{K}_\infty)})$. From this it is immediate that $|p^{l'} Y_{A_1}^{(\mathbb{K}_\infty)}/p^{l'+1}Y_{A_1}^{\mathbb{K}_\infty}| = p^{\lambda(Y_{A_1}^{(\mathbb{K}_\infty)})}$. Let $m \geq 0$ be minimal such that $p^{l'+m} Y_{A_2}^{(\mathbb{K}_\infty)}$ is $\mathbb{Z}_p$-free. Then we obtain

$$\begin{aligned} p^{\lambda(Y_{A_2}^{(\mathbb{K}_\infty)})} &= |p^{l'+m} Y_{A_2}^{(\mathbb{K}_\infty)}/p^{l'+m+1}Y_{A_1}^{(\mathbb{K}_\infty)}| \\ &\leq |p^{l'} Y_{A_2}^{(\mathbb{K}_\infty)}/p^{l'+1}Y_{A_1}^{(\mathbb{K}_\infty)}| = p^{\lambda(Y_{A_1}^{(\mathbb{K}_\infty)})} \end{aligned}$$

If $m = 0$ this inequality becomes an equality which finishes the proof of the Theorem. □

Part II

Classical Conjectures in Iwasawa theory

Chapter 5

The Gross and the Gross-Kuz'min conjecture

Let $\mathbb{K}$ be a number field and $p > 2$ a rational prime. Let $\mathbb{K}_\infty/\mathbb{K}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ and $\mathbb{K}_n$ the intermediate fields (i.e. $[\mathbb{K}_n : \mathbb{K}] = p^n$). Recall that we denote the p-class group of $\mathbb{K}_n$ by A_n. Let B_n be the subgroup generated by ideal classes containing a prime above p. We define $A'_n = A_n/B_n$. The norms $N_{n,n-1}\colon \mathbb{K}_n \to \mathbb{K}_{n-1}$ induce homomorphisms

$$N_{n,n-1}\colon A_n \to A_{n-1}$$

and

$$N_{n,n-1}\colon A'_n \to A'_{n-1}.$$

This allows us to define the projective limits $A_\infty = \lim_{\infty\leftarrow n} A_n$ and $A'_\infty = \lim_{\infty\leftarrow n} A'_n$ with respect to the norms $N_{n,n-1}$. As $p > 2$, we obtain in the CM case a decomposition $A'_\infty = A'^{+}_\infty \oplus A'^{-}_\infty$. For any Λ-module we denote the T-torsion by $M[T]$ and the maximal submodule annihilated by some power of T by $M(T)$. The aim of this Chapter is to study the Gross conjecture for $p > 2$. Gross formulated the conjecture originally in terms of a certain p-adic map [Gro 1]. Later, in a joint paper with Federer he proved that his conjecture is equivalent to the following statement.

Conjecture 5.0.1. *If $\mathbb{K}$ is a CM field then*

$$A'^{-}_\infty[T] \quad \text{is finite.}$$

In the present chapter we will develop a Galois theoretic interpretation of this conjecture for CM fields $\mathbb{K}$, that contain ζ_p and for which all primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. To state this alternative formulation we first have to introduce some more notation.

Let s_n be the number of primes above p in $\mathbb{K}_n$ and $\mathfrak{P}_{n,i}$ for $1 \le i \le s_n$ be the primes above p in $\mathbb{K}_n$. Recall that we can decompose the complete field $\mathbb{K}^\times_{n,\mathfrak{P}_{n,i}}$ as $\pi^{\mathbb{Z}}_{n,i} U_{n,i} V_{n,i}$, where $\pi_{n,i}$ is a uniformizer for the maximal ideal of $\mathcal{O}(\mathbb{K}_{n,\mathfrak{P}_{n,i}})$, the group $V_{n,i}$ denotes the roots of unity of order coprime to p and $U_{n,i}$ describes the local units

that are congruent to 1 modulo $\pi_{n,i}$. As in the introduction we define $U_n = \prod_{i=1}^{s_n} U_{n,i}$. If $\mathbb{K}$ contains the p-th roots of unity, then $\mathbb{K}_n$ contains ζ_{p^n} and $U_{n,i}$ has a p^n-torsion subgroup. Let $W_{n,i}$ be the $\mathbb{Z}_p$-torsion of $U_{n,i}$. We define $W_n = \prod_{i=1}^{s_n} W_{n,i}$ and $W = \lim_{\infty \leftarrow n} W_n$ as well as $W_i = \lim_{\infty \leftarrow n} W_{n,i}$. We will denote the intersection $W \cap \overline{E}_\infty$ by $\widehat{W}$ and the$p$-power roots of unity in the field $\mathbb{K}_n$ by $R(\mathbb{K}_n)$.

Recall that $\mathbb{M}_\infty$ denotes the maximal p-abelian p-ramified extension of $\mathbb{K}_\infty$ and that $\mathbb{H}_\infty$ denotes the maximal p-abelian unramified extension of $\mathbb{K}_\infty$. Different from previous sections we will denote the whole group of units by E_n here. From the definition of the Artin homomorphism we obtain that

$$W/\widehat{W} \cong \phi(W) \subset \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{H}_\infty).$$

This subgroup will play a crucial role in our proof. We are in particular interested in its action on certain subextensions of $\mathbb{M}_\infty$ denoted by Ω_E and $\Omega_{E'}$. We define Ω_E as the extension of $\mathbb{K}_\infty$ generated by adjoining arbitrarily high p-power roots of the elements E_n for all n. Let E'_n be the p-units of $\mathbb{K}_n$. Then we define $\Omega_{E'}$ as the extension obtained by adjoining arbitrarily high roots of E'_n.

The last bit of notation we introduce here is the Iwasawa involution: Let σ be an arbitrary element in $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$. Then there is a unique p-adic integer $\chi(\sigma)$ forming a p-adic character (*the cyclotomic character*) on $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$ with values in $\mathbb{Z}_p^\times$ (if $\zeta_p \in \mathbb{K}$ even in $1 + p\mathbb{Z}_p$) such that

$$\sigma(\zeta_{p^n}) = \zeta_{p^n}^{\chi(\sigma)} \quad \text{for all } n \geq 1.$$

The Iwasawa involution is defined via $\sigma^* = \chi(\sigma)\sigma^{-1}$. Let M be a Λ-module. We will denote the Λ-module on which τ acts via τ^* by $M^\bullet$ (see also [Iw 2, page 278]). We will say that two Λ-modules M_1 and M_2 are dual to each other under the Iwasawa involution if $M_1^\bullet$ and M_2 are pseudo isomorphic. Using all this notation we can state our Galois theoretic formulation of the Gross conjecture

Theorem 5.0.2. *Let $\mathbb{K}$ be a CM field containing the p-th roots of unity. Assume that $\mathbb{K}_\infty/\mathbb{K}$ is totally ramified at all primes above p. The Gross conjecture is true if and only if $(U_\infty/\overline{E}_\infty W)^+[T^*]$ is finite. Further, if the Gross conjecture holds, then $Gal(\Omega_{E'}/\Omega_E)^+$ is naturally pseudo isomorphic to W^+.*

Kuz'min formulated in 1972 a hypothesis for arbitrary number fields whose validity implies the Gross conjecture for CM fields [Ku 1]. We will refer to this generalized conjecture as the Gross-Kuz'min conjecture.

Conjecture 5.0.3. *Let $\mathbb{K}$ be an arbitrary number field. Then*

$$A'_\infty[T] \quad \text{is finite.}$$

For the Gross-Kuz'min conjecture we will prove a result similar to Theorem 5.0.2:

Theorem 5.0.4. *Assume that $\mathbb{K}$ contains ζ_p and that all primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. If the Gross-Kuz'min conjecture holds for $\mathbb{K}$ then the quotient $(\phi(U_\infty)/\phi(W))(T^*)$ is finite. If conversely $(\phi(U_\infty)/\phi(W))(T^*)$ is finite and Leopoldt's conjecture holds for $\mathbb{K}$ then the Gross-Kuz'min conjecture holds for $\mathbb{K}$.*

One main ingredient in the proofs of Theorem 5.0.2 and Theorem 5.0.4 is the fact that the Λ-modules $A_\infty^+[T^*]$ and $A_\infty[T^*]$ are finite. While one can prove the first assertion without additional assumptions, the second one is an equivalent formulation of Leopoldt's conjecture. As far as the author knows the Gross-Kuz'min conjecture is known in the following cases:[1]

- Greenberg proved that the Gross-Kuz'min conjecture holds for all abelian extensions $\mathbb{K}/\mathbb{Q}$ [Gre 2].
- If $\mathbb{K}$ contains exactly one prime above p, then the Gross-Kuz'min conjecture follows from Chevalley's Theorem (c.f. [La, Chapter 13 Lemma 4.1]).
- Let $\mathbb{K}/\mathbb{Q}$ be a Galois extension such that the decomposition group D_p of some prime above p is normal in $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = G$. Assume that only terms of the form $M_n(R)$ with $n \leq 2$ and division fields R occur in the Artin-Wedderburn decomposition of the group ring $\mathbb{Q}_p[G/D_p]$. Then Jaulent showed that the Gross-Kuz'min conjecture holds for $\mathbb{K}$ [Jau 1].
- Let $\mathbb{K}$ be a number field containing an imaginary quadratic field such that $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is isomorphic to S_4. Assume that the decomposition group of some prime above p is a 3-Sylow subgroup. Kuz'min showed that then the Gross-Kuz'min conjecture holds.[Ku 2].
- Kleine proved that if $\mathbb{K}$ contains exactly two primes above p then the Gross-Kuz'min conjecture holds [Kl 2].

We will first give some preliminaries that are needed for both conjectures before we can give the proofs of Theorems 5.0.2 and 5.0.4.

5.1 Preliminaries for both conjectures

Assume in the following that p is an odd rational prime and $\mathbb{K}$ is a number field containing ζ_p and that all primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. In particular, the number of primes s_n above p in $\mathbb{K}_n$ is equal to a constant s independent of n. Recall that we denote by $\mathfrak{P}_{i,n}$ the prime ideals in $\mathbb{K}_n$. Without loss of generality we can assume that $N_{n,n-1}(\mathfrak{P}_{n,i}) = \mathfrak{P}_{n-1,i}$.

5.1.1 Ideal classes as radicals

One main building block in our analysis of the Gross and the Gross-Kuz'min conjecture is to use ideal classes as radicals over Ω_E. As a first step we need a more precise description of $\Omega_E/\mathbb{K}_\infty$.

Lemma 5.1.1. *Let $\Omega_{E,l}$ be the maximal subextension of $\Omega_E/\mathbb{K}_\infty$ of exponent p^l. Then the Kummer-radical of $\Omega_{E,l}$ is $\mathbb{K}_\infty^{\times\, p^l}(\bigcup_{n\in\mathbb{N}} E_n)/\mathbb{K}_\infty^{\times\, p^l}$. In particular, if $\alpha \in \mathbb{K}_\infty^\times$ and $\alpha^{1/p^l} \in \Omega_E$, then there is a unit $e \in \mathbb{K}_\infty$ and an element $\gamma \in \mathbb{K}_\infty$ such that $\alpha = \gamma^{p^l} e$.*

[1] We do not claim that this list is complete.

Proof. Let $\mathfrak{K} = \mathbb{K}_\infty^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$ and let $x = \alpha \otimes p^{-a}$ be an element in $\mathfrak{K}$. Let $\mathbb{K}_{ab}$ be the maximal p-abelian extension of $\mathbb{K}_\infty$ and $G = \mathrm{Gal}(\mathbb{K}_{ab}/\mathbb{K}_\infty)$. Iwasawa shows that there is a natural Kummer pairing

$$\langle \cdot, \cdot \rangle \colon \mathfrak{K} \times G \to R(\mathbb{K}_\infty)$$

such that $\langle \alpha \otimes p^{-a}, \sigma \rangle = \sigma(\sqrt[p^a]{\alpha})/\sqrt[p^a]{\alpha}$. Let $\mathrm{Gal}(\mathbb{K}_{ab}/\Omega_E)^\perp$ denote the annihilator of $\mathrm{Gal}(\mathbb{K}_{ab}/\Omega_E)$ with respect to this pairing. Iwasawa shows that $\mathrm{Gal}(\mathbb{K}_{ab}/\Omega_E)^\perp$ consist of the elements $e \otimes p^{-a}$ with $a \geq 0$ and $e \in \cup_{n\in\mathbb{N}} E_n$ [Iw 2, pages 271-274]. It is easy to see that $\mathrm{Gal}(\mathbb{K}_{ab}/\Omega_E)^\perp[p^l]$ consists of the elements $e \otimes p^{-a}$ with $0 \leq a \leq l$ and $e \in \bigcup_{n\in\mathbb{N}} E_n$. As the homomorphism

$$\{e \otimes p^{-a} \mid a \leq l\} \to \mathbb{K}_\infty^{\times\, p^l}(\bigcup_{n\in\mathbb{N}} E_n)/\mathbb{K}_\infty^{\times\, p^l}, \quad e \otimes p^{-a} \mapsto e^{p^{l-a}}$$

is an isomorphism the first claim is immediate.

Assume that α satisfys the assumptions of the second claim, then $\alpha^{1/p^l} \in \Omega_{E,l}$ and $\alpha \in \mathbb{K}_\infty \cap \Omega_{E,l}^{p^l}$. By Kummer-theory [Ne 1, Chapter IV Theorem 3.3] we obtain that α has a trivial image in $\mathbb{K}_\infty^{\times\, p^l}(\bigcup_{n\in\mathbb{N}} E_n)/\mathbb{K}_\infty^{\times\, p^l}$. In particular, $\alpha \in \mathbb{K}_\infty^{\times\, p^l}(\bigcup_{n\in\mathbb{N}} E_n)$. □

Theorem 5.1.2. *Let $\mathcal{M}$ be the $\mathbb{Z}_p$-torsion submodule of $Gal(\mathbb{M}_\infty/\Omega_E)$. Let c be such that $A_\infty^{p^c}$ does not contain $\mathbb{Z}_p$-torsion. Then there is a map*

$$f \colon A_\infty^{p^c} \to \{\mathbb{Z}_p\text{-subextensions of } \mathbb{M}_\infty^{\mathcal{M}}/\Omega_E\}$$

that is compatible with the action of τ (a topological generator of $Gal(\mathbb{K}_\infty/\mathbb{K})$). The map f has the following properties:

a) The field $f(a \cdot b)$ is contained in the compositum of $f(a)$ and $f(b)$.

b) For each $\mathbb{Z}_p$-extension $\mathbb{L}$ contained in the compositum of $f(a)$ and $f(b)$ there is an element c in $a^{\mathbb{Z}_p} \cdot b^{\mathbb{Z}_p}$ such that $f(c) = \mathbb{L}$.

c) The map f is rank preserving: If $C \subset A_\infty^{p^c}$ is a group of $\mathbb{Z}_p$-rank k, then the compositum $\mathbb{M}$ of the fields $f(x)$ for $x \in C$ is a $\mathbb{Z}_p^k$-extension over Ω_E.

d) Let $a = (a_n)_{n\in\mathbb{N}}$ be a sequence in $B_\infty \cap A_\infty^{p^c}$. Then $f(a)$ is a $\mathbb{Z}_p$-extension in $\Omega_{E'}/\Omega_E$.

To prove the above theorem we will need the following results on finite p-groups. Results of this form have been used by Preda Mihăilescu in various forms. We will reprove them here for the convenience of the reader.

Lemma 5.1.3. *Let A and B be finite abelian p-groups written additively, such that*

$$p\text{−rank}(A) = p\text{−rank}(B) = p\text{−rank}(pA) = r. \tag{5.1}$$

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 map corresponding to multiplication by p while N is surjective. Then we have $\iota(A) = pB$ and $B[p] = \iota(A)[p]$.

Proof. Since A and B have the same p-rank, the modules A/pA and B/pB have the same dimension as $\mathbb{F}_p$-vector spaces. Furthermore, the induced homomorphism $\tilde{N} : B/pB \to A/pA$ is surjective. Hence, it has to be an isomorphism. Define $\tilde{\iota} : A/pA \to B/pB$ to be the map induced by ι. Thus, there is a well defined map $\tilde{N} \circ \tilde{\iota} : A/pA \to A/pA$ induced by multiplication by p. The multiplication by p on A/pA is the zero map. Since $\tilde{N}$ is an isomorphism we obtain that $\tilde{\iota}$ is the zero map. Therefore $\iota(A) \subset pB$. To obtain equality, we need the following inequalities of p-ranks.

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

Hence, we see that $p{-}\mathrm{rank}(pB) = p{-}\mathrm{rank}(B) = p{-}\mathrm{rank}(A) = p{-}\mathrm{rank}(pA)$. Again we have that pA/p^2A and pB/p^2B have the same dimension as $\mathbb{F}_p$-vector spaces. N induces a map $\hat{N} : pB/p^2B \to pA/p^2A$ which is surjective and therefore an isomorphism. Let $\hat{\iota} : A/pA \to pB/p^2B$ be the map induced by ι. Then

$$\hat{N} \circ \hat{\iota} : A/pA \to pA/p^2A$$

is the homorphism induced by multiplication by p. Since both groups have the same p-rank, it is in fact an isomorphism. But $\hat{N}$ is an isomorphism and hence $\hat{\iota}$ is an isomorphism. That means, in particular, that $\iota(A)$ contains a set of generators of pB. Thus, $\iota(A) = pB$. We proved above that $p{-}\mathrm{rank}(pB) = p{-}\mathrm{rank}(B)$. This implies

$$r = p{-}\mathrm{rank}(B[p]) = p{-}\mathrm{rank}(B) = p{-}\mathrm{rank}(pB) = p{-}\mathrm{rank}(\iota(A)) = p{-}\mathrm{rank}((\iota(A))[p]).$$

Due to the equality $(\iota(A))[p] = (pB)[p] \subseteq B[p]$, and since both are $\mathbb{F}_p$-vector spaces of equal dimension, it follows that $B[p] = (pB)[p] = (\iota(A))[p]$. □

In the case when there is a group G acting on B, we have the following stronger form of the above lemma.

Corollary 5.1.4. *Let A, B, N and ι be like in the previous lemma. Assume that there is a cyclic group $G = \langle\tau\rangle$ 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 $\nu = \cdot p$ is the multiplication by p map and $\iota(N(x)) = px$ for all $x \in B$.*

Proof. Let $T = \tau - 1$. Then we obtain $\nu = p + \binom{p}{2}T + O(T^2)$. From Lemma 5.1.3, we know that $\iota(A) = pB$. Since τ fixes $\iota(A)$, it follows that $Tpy = 0$ for all $y \in B$. In particular, we have $Ty \in B[p] \subset pB$. We conclude that $pTy = T^2y = 0$. We can now compute νx for arbitrary $x \in B$ explicitly, according to the previous expansion of ν.

$$\nu x = px + Tp\frac{p-1}{2}x + xO(T^2) = px.$$

This completes the proof. □

We cannot apply these results directly to the modules A_n as we cannot guarantee that the condition (5.1) is satisfied for A_n and A_{n+1}. In order to modify A_∞ such that we can apply Lemma 5.1.3 we need the following result.

Lemma 5.1.5. *Let c be a constant such that $A_\infty^{p^c}$ does not contain $\mathbb{Z}_p$-torsion. Then $A_\infty^{p^c}$ projects onto $A_n^{p^c}$ and there is an n_0' such that the natural lifts $\iota_{n,n+1}$ are injective on $A_n^{p^c}$ for all $n \geq n_0'$.*

Proof. This proof follows the ideas of [Gre 6, proposition 2.5.2], which shows that the capitulation kernel is isomorphic to the maximal finite submodule of A_∞. For the convenience of the reader we reprove this fact here. Let $x_n \in A_n^{p^c}$ be a class that capitulates in A_m for some $m \geq n$. As $A_k = A_\infty/\nu_{k,0}Y$ for some submodule Y of A_∞, we can write the element $x_n \in A_n^{p^c}$ as the coclass $y + \nu_{n,0}Y$ for some element $y \in A_\infty[\nu_{m,n}]$. But $\mathbb{K}_\infty/\mathbb{K}$ is totally ramified at all primes above p. Hence, the characteristic polynomial of A_∞ is coprime to $\nu_{m,n}$ for all n and m. Therefore, y lies in the maximal finite Λ-submodule of A_∞. By the choice of c we know that $A_\infty^{p^c}$ does not contain $\mathbb{Z}_p$-torsion. Let Z be the maximal finite submodule of A_∞. Then, from a certain n on the images of Z and of $A_\infty^{p^c}$ in A_n are disjoint and the claim follows. □

Let n_0' and c be as in Lemma 5.1.5, choose $n_0 \geq n_0'$ large enough such that for all $n \geq n_0$ the ranks of $A_n^{p^c}$ and $A_n^{p^{c+1}}$ are both equal to the same constant independent of n. The quotient $\mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_{n-1}) = \Gamma^{p^{n-1}}/\Gamma^{p^n}$ acts naturally on A_n. Thus, we obtain the following

Corollary 5.1.6. *Let $(a_n)_{n\in\mathbb{N}}$ be a norm coherent sequence in $A_\infty^{p^c}$. Then*

$$\iota_{n,n+l}(a_n) = a_{n+l}^{p^l}$$

for all $n \geq n_0$ and all $l \in \mathbb{N}_0$.

Proof. This is just a repetitive application of Corollary 5.1.4 in this concrete context. □

Now we have all ingredients to prove Theorem 5.1.2.

Proof of Theorem 5.1.2. Let c be defined as before. Let $n \geq n_0$, $a_n \in A_n^{p^c}$ and $\mathfrak{A}_n \in a_n$. Let $(\alpha_n) = \mathfrak{A}_n^{\mathrm{ord}(a_n)}$. Then $\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)})/\Omega_E$ is unramified outside p and non-trivial (see [Wash, Exercise 9.1 and pages 294-295]). As the lift $\iota_{n,m}\colon A_n^{p^c} \to A_m^{p^c}$ is injective for all $m \geq n$, Lemma 5.1.1 implies that $[\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}) : \Omega_E] = \mathrm{ord}(a_n)$. Note that $\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)})/\Omega_E$ does not depend on the choice of α_n or $\mathfrak{A}_n$ but on a_n. Let $a_{n+1} \in A_{n+1}^{p^c}$ such that $N_{n+1,n}(a_{n+1}) = a_n$. Using Corollary 5.1.6 we see that $\iota_{n,n+1}(a_n) = a_{n+1}^p$. Hence, there is a principal ideal (γ) such that $\mathfrak{A}_n = (\gamma)\mathfrak{A}_{n+1}^p$. It follows that $\mathfrak{A}_n^{\mathrm{ord}(a_n)} = \mathfrak{A}_{n+1}^{\mathrm{ord}(a_{n+1})}(\gamma)^{\mathrm{ord}(a_n)}$. Therefore, the two elements $\alpha_n^{1/\mathrm{ord}(a_n)}$ and $\alpha_{n+1}^{1/\mathrm{ord}(a_n)}$ generate the same extension over Ω_E and the sequence $(a_n)_{n\in\mathbb{N}}$ defines a $\mathbb{Z}_p$-extension over Ω_E. If we act with τ on a_n, we obtain $\tau(\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)})) = \Omega_E(\tau(\alpha_n)^{1/\mathrm{ord}(a_n)})$. This defines the map f from Theorem 5.1.2.

Note that a and a^c define the same $\mathbb{Z}_p$-extension for any $c \in \mathbb{Z}_p \setminus \{0\}$ even if they generate different extensions at finite levels. Let $\mathbb{M}_{a,b}$ be the compositum of the extensions $f(a)$ and $f(b)$. There are constants c_a, c_b and $c_{a,b}$ such that

$$\mathrm{ord}(a_n)c_a = c_b\mathrm{ord}(b_n) = c_{a,b}\mathrm{ord}(a_n \cdot b_n)$$

for all n large enough. Let $(\alpha_n) = \mathfrak{A}_n^{\mathrm{ord}(a_n)}$, $(\beta_n) = \mathfrak{B}_n^{\mathrm{ord}(b_n)}$ and $(\gamma_n) = (\mathfrak{A}_n\mathfrak{B}_n)^{\mathrm{ord}(a_n\cdot b_n)}$. It follows that $(\gamma_n^{c_{a,b}}) = (\alpha_n)^{c_a}(\beta_n)^{c_b}$. Hence, $f(a\cdot b)$ is contained in $\mathbb{M}_{a,b}$ which proves property a).

To prove property b) let $\mathbb{L} \subset \mathbb{M}_{a,b}$ be a $\mathbb{Z}_p$-extension over Ω_E. If $f(a) = f(b)$, there is nothing to prove. Therefore we can assume that $f(a) \cap f(b) = \mathbb{M}_{a,b,f}$ is a finite extension of Ω_E. Let $n \geq n_0$ be minimal such that

$$\mathrm{ord}(a_n), \mathrm{ord}(b_n) \geq [\mathbb{M}_{a,b,f} : \Omega_E] = p^l.$$

Comparing radicals we obtain that $(\alpha_n) = (\beta_n^c)(\gamma)^{p^l}$ for some c coprime to p and $\mathfrak{A}_n^{\mathrm{ord}(a_n)/p^l}/\mathfrak{B}_n^{c\cdot\mathrm{ord}(b_n)/p^l}$ is a principal ideal in $\mathbb{K}_\infty$. As $\iota_{n,m}\colon A_n^{p^c} \to A_m^{p^c}$ is injective for $m \geq n \geq n_0$, we see that it is already a principal ideal in $\mathbb{K}_n$. Assume that $\mathrm{ord}(a_n) \geq \mathrm{ord}(b_n)$ and define $b' = a^{\mathrm{ord}(a_n)/\mathrm{ord}(b_n)}/b^c$. Then b'_n is a class of order at most $\mathrm{ord}(b_n)/p^l$. Let $p^v = \mathrm{ord}(b'_n)$. Then $\mathfrak{A}_n^{\mathrm{ord}(a_n)/\mathrm{ord}(b_n)\cdot p^v}/\mathfrak{B}_n^{cp^v} = (\gamma')$. This implies $(\alpha_n)/(\beta_n)^c = (\gamma')^{\mathrm{ord}(b_n)/p^v}$ and

$$p^l = [\mathbb{M}_{a,b,f} : \Omega_E] \geq \mathrm{ord}(b_n)/p^v.$$

It is immediate that $p^v \geq \mathrm{ord}(b_n)/p^l$ and we obtain indeed $\mathrm{ord}(b'_n) = \mathrm{ord}(b_n)/p^l$.

As $M_{a,b,f} = \Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}) \cap \Omega_E(\beta_n^{1/\mathrm{ord}(b_n)})$ it follows that

$$\begin{aligned}
&[\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}, \beta_n^{1/\mathrm{ord}(b_n)}) : \Omega_E] \\
&= [\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}, \beta_n^{1/\mathrm{ord}(b_n)}) : \mathbb{M}_{a,b,f}][\mathbb{M}_{a.b,f} : \Omega_E] \\
&= p^l \cdot \mathrm{ord}(a_n)/p^l \cdot \mathrm{ord}(b_n)/p^l \\
&= \mathrm{ord}(a_n) \cdot \mathrm{ord}(b_n)/p^l.
\end{aligned}$$

Let $\mathfrak{B}'_n$ be an ideal in b'_n and $(\beta'_n) = \mathfrak{B}'^{\mathrm{ord}(b'_n)}_n$. We obtain

$$\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}, {\beta'_n}^{1/\mathrm{ord}(b'_n)}) = \Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}, \beta_n^{1/\mathrm{ord}(b_n)}).$$

As $\mathrm{ord}(b'_n) = \mathrm{ord}(b_n)/p^l$, we see that

$$[\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}, {\beta'_n}^{1/\mathrm{ord}(b'_n)}) : \Omega_E] = \mathrm{ord}(b'_n) \cdot \mathrm{ord}(a_n)$$

and

$$\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)}) \cap \Omega_E({\beta'_n}^{1/\mathrm{ord}(b'_n)}) = \Omega_E.$$

The fields $\Omega_E(\alpha_n^{1/\mathrm{ord}(a_n)})$ and $\Omega_E({\beta'}_n^{1/\mathrm{ord}(b'_n)})$ contain the unique subextensions of degree p of $f(a)/\Omega_E$ and $f(b')/\Omega_E$, respectively. This implies that $f(a) \cap f(b') = \Omega_E$. As $a^{\mathbb{Z}_p}b^{\mathbb{Z}_p} = a^{\mathbb{Z}_p}b'^{\mathbb{Z}_p}$ we can assume that $f(a)$ and $f(b)$ intersect only in Ω_E and that $\mathrm{ord}(a_n) \geq \mathrm{ord}(b_n)$.

Let $\mathbb{M}_{a,b,n} = \Omega_E(\alpha_n^{1/\mathrm{ord}(b_n)}, \beta_n^{1/\mathrm{ord}(b_n)})$ be the maximal subextension of exponent $\mathrm{ord}(b_n)$ in $\mathbb{M}_{a,b}/\Omega_E$. Let $\gamma_n \in \alpha_n^{\mathbb{Z}}\beta_n^{\mathbb{Z}}$ be the radical for the unique subextension $\mathbb{L} \cap \mathbb{M}_{a,b,n}$ of degree $\mathrm{ord}(b_n)$ over Ω_E. As ideals we obtain the following equality

$$(\gamma_n) = (\beta_n)^{c_{1,n}}(\alpha_n)^{c_{2,n}}. \tag{5.2}$$

The integers $c_{1,n}$ and $c_{2,n}$ are unique modulo $\mathrm{ord}(b_n)$ and at least one of them is not divisible by p. It follows that $(\gamma_n) = \mathfrak{C}_n^{\mathrm{ord}(b_n)}$ with $\mathfrak{C}_n = \mathfrak{A}_n^{c_{2,n}\mathrm{ord}(a_n)/\mathrm{ord}(b_n)}\mathfrak{B}_n^{c_{1,n}}$. As the equation (5.2) can be formulated for every level n we see that $c_{i,n} \equiv c_{i,n+1} \mod \mathrm{ord}(b_n)$. Hence, in the limit we obtain p-adic integers c_1 and c_2 such that $[\mathfrak{C}_n] = b_n^{c_1} \cdot a_n^{c_2}$. As $f(a) \neq f(b)$, the class $[\mathfrak{C}_n] \in A_n^{p^c}$ is non-trivial. Let $c = (c_n)_{n\in\mathbb{N}}$. Then $f(c)$ is the field $\mathbb{L}$. This proves property b).

It remains to show properties c) and d). We will therefore first determine which elements have the same image under f and then conclude the proof by a rank computation. Assume that $f(a) = f(b)$ and that $\mathrm{ord}(a_n) \geq \mathrm{ord}(b_n)$ for all n large enough. By comparing radicals at finite level we obtain $(\alpha_n) = (\beta_n)^{c_n}(\gamma)^{\mathrm{ord}(b_n)}$. Note that c_n is a p-adic unit uniquely defined modulo $\mathrm{ord}(b_n)$. As before we can conclude $c_n \equiv c_{n+1} \mod \mathrm{ord}(b_n)$. Hence, we can assume that c_n is 1. It follows that $\mathfrak{B}_n = \mathfrak{A}_n^{\mathrm{ord}(a_n)/\mathrm{ord}(b_n)}(\gamma)$ and that $b_n = a_n^{\mathrm{ord}(a_n)/\mathrm{ord}(b_n)}$. As $\mathrm{ord}(a_n)/\mathrm{ord}(b_n)$ is a constant k independent of n we see that $a^k = b$, i.e. the group generated by a and b has $\mathbb{Z}_p$-rank 1.

Let X be a subgroup of $A_\infty^{p^c}$ of $\mathbb{Z}_p$-rank t and $\mathbb{M}_X$ the compositum of all $\mathbb{Z}_p$-extensions $f(a)$ for $a \in X$. Then the claim we just proved implies together with properties a) and b) that $\mathbb{M}_X/\Omega_E$ is a $\mathbb{Z}_p^t$-extension, i.e f preserves $\mathbb{Z}_p$-ranks of subgroups. This proves property c). If we take $f((a_n)_{n\in\mathbb{N}})$ for a sequence $(a_n)_{n\in\mathbb{N}}$ in $A_\infty^{p^c} \cap B_\infty$, we clearly obtain subextensions of $\Omega_{E'}$ proving property d).

□

5.1.2 The structure of $\mathbf{Gal}(\Omega_{E'}/\Omega_E)$

In this section we will describe the structure of the extension $\Omega_{E'}/\Omega_E$ focusing on the radicals of this extension. We start by recalling Iwasawa's results: Iwasawa investigated the structure of the group $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$ and proved (cf. [Iw 2, Theorems 15, 17])

$$\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty) \sim \Lambda^{[\mathbb{K}:\mathbb{Q}]/2} \oplus \Lambda\text{-torsion} \tag{5.3}$$

as well as

$$\mathrm{Gal}(\mathbb{M}_\infty/\mathbb{K}_\infty) \sim \Lambda^{[\mathbb{K}:\mathbb{Q}]/2} \oplus \Lambda\text{-torsion}. \tag{5.4}$$

We denote the Λ-torsion submodule of $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$ by Z. Iwasawa proved that Z is a $\mathbb{Z}_p$-free group of rank $s-1$. In the proof of [Iw 2, Theorem 15] Iwasawa considered $X = \mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)^\bullet$. He showed that

$$X/\omega_n X \cong \mathbb{Z}_p^{[\mathbb{K}:\mathbb{Q}]/2+s-1} \oplus (\text{uniformly bounded group})$$

for all $n \geq n_0$. Here n_0 is the minimal index such that $\mathbb{K}_\infty/\mathbb{K}_{n_0}$ is totally ramified at all primes above p (see [Iw 2, Section 3.4]). In our case we have $n_0 = 0$. It follows that X is pseudo isomorphic to $\Lambda^{[\mathbb{K}:\mathbb{Q}]/2} \oplus (\Lambda/T)^{s-1}$. By the definition of X we see that $Z \sim (\Lambda/T^*)^{s-1}$. Noting that W is annihilated by T^* and that $W/\widehat{W}$ has $\mathbb{Z}_p$-rank $s-1$ (see Lemma 5.1.16) it is a natural question whether $W/\widehat{W}$ is pseudo isomorphic to Z under Artin's isomorphism. In fact our central theorem on the Gross-Kuz'min

conjecture shows that the answer to this question is positive if the Gross-Kuz'min conjecture holds.

As a next step we want to describe $\Omega_{E'}/\Omega_E$ in terms of radicals.

Remark 5.1.7. *Let $b = (b_n)_{n\in\mathbb{N}} \in B_\infty$. If b generates an infinite $\mathbb{Z}_p$-module, then there are constants k and n_0 such that* $\mathrm{ord}(b_n) = p^{k+n}$ *for all $n \geq n_0$.*

In the following lemma we construct a $\mathbb{Z}_p$-extension in $\Omega_{E'}/\Omega_E$ directly from a sequence in B_∞. The difference to the construction in Theorem 5.1.2 is that this time the $\mathbb{Z}_p$-extension is constructed for every element of infinite order in B_∞ and not only for elements in $B_\infty \cap A_\infty^{p^c}$, where c is the constant defined in Theorem 5.1.2. Having this Lemma at hand will ease our work later on when we want to prove Theorem 5.0.2 and Theorem 5.0.4.

Lemma 5.1.8. *Let $(b_n)_{n\in\mathbb{N}} \in B_\infty$ be a norm coherent sequence generating an infinite $\mathbb{Z}_p$-module. Let $\mathfrak{B}_n$ be an ideal in b_n only divisible by primes above p and $(\beta_n) = \mathfrak{B}_n^{ord(b_n)}$. Let n_0 be minimal such that* $\mathrm{ord}(b_n) = p\mathrm{ord}(b_{n-1})$ *for all $n \geq n_0 + 1$, then $\cup_{n\geq n_0}\Omega_E(\beta_n^{1/\mathrm{ord}(b_n)})/\Omega_E$ is a $\mathbb{Z}_p$-extension.*

Proof. Let c be as in Theorem 5.1.2. Then $0 \neq b^{p^c} \in A_\infty^{p^c}$. As $f(b)$ is a $\mathbb{Z}_p$-extension of Ω_E we see that there is an index $n_0' \geq n_0$ such that $\Omega_E(\beta_n^{1/p^{\mathrm{ord}(b_n)}})$ is a non-trivial extension of Ω_E for all $n \geq n_0'$. By definition we have $(\beta_{n+1}) = \mathfrak{B}_{n+1}^{\mathrm{ord}(b_{n+1})}$. By definition $\mathfrak{B}_n(\gamma) = N_{n+1,n}(\mathfrak{B}_{n+1}) = \mathfrak{B}_{n+1}^p$. Then $\beta_{n+1} = \beta_n(\gamma)^{\mathrm{ord}(b_n)}e$ for some unit e and some γ in $\mathbb{K}_{n+1}$. It follows that $\Omega_E(\beta_n^{1/\mathrm{ord}(b_n)}) = \Omega_E(\beta_{n+1}^{1/\mathrm{ord}(b_{n+1})})$. Thus, $\bigcup_{n\geq n_0}\Omega_E(\beta_n^{1/\mathrm{ord}(b_n)})$ defines a $\mathbb{Z}_p$-extension over Ω_E. □

We have already seen that $f(b^{p^c}) \subset \Omega_{E'}$ for every element $b \in B_\infty$. The goal of the rest of this section is to prove that the compositum of all such extensions $f(b)$ is not only a subfield of $\Omega_{E'}$ but is already equal to $\Omega_{E'}$.

Remark 5.1.9. *Consider $\eta \in N_{n+l,n}(E'_{n+l})$. Let η' be such that $N_{n+l,n}(\eta') = \eta$. As η'^T is a unit, we see that $\eta = \eta'^{p^l}e$ for a global unit e and a p-unit $\eta' \in \mathbb{K}_{n+l}$. Hence, $\eta^{1/p^l} \in \Omega_E$.*

Using Remark 5.1.9 and Theorem 5.1.2 we obtain the following result.

Lemma 5.1.10. *Let $B_\infty = \lim_{\infty\leftarrow n} B_n$ and let r be the unique integer such that $B_\infty \cong \mathbb{Z}_p^r \times$ (finite group). Then $Gal(\Omega_{E'}/\Omega_E)$ has $\mathbb{Z}_p$-rank r.*

Proof. Clearly, $\mathbb{Z}_p\text{-rank}(B_\infty \cap A_\infty^{p^c}) = r$. From points c) and d) of Theorem 5.1.2 we obtain that the $\mathbb{Z}_p$-rank of $\Omega_{E'}/\Omega_E$ is at least r.

Let F_n be the free abelian group generated by the primes above p in $\mathbb{K}_n$. Then the norms induce isomorphisms:

$$N_{n+1,n}\colon F_{n+1} \to \iota(F_n),$$

where ι denotes the ideal lift from level n to level $n+1$. Let p^k be the exponent of the $\mathbb{Z}_p$-torsion part of B_∞. Then

$$N_{n+1,n}\colon F_{n+1}^{p^k} \to \iota(F_n^{p^k})$$

is bijective as well. Further, there is a natural homomorphism $R_n\colon F_n^{p^k} \to B_n$, whose image has p-rank r for n large enough. Choose r generators f_i for $1 \leq i \leq r$ of $F_n^{p^k}$ such that their images under R_n generate $R_n(F_n^{p^k})$ as abelian group. There are generators $e_1, \ldots, e_r$ of $F_n^{p^k}$ and integers α_i such that $f_i = e_i^{\alpha_i}$ for $1 \leq i \leq r$. Then we have $R_n(f_i) = R_n(e_i)^{\alpha_i}$. Thus, the α_i are coprime to p and $R_n(e_i)$ and $R_n(f_i)$ generate the same group in $R_n(F_n^{p^k})$. So without loss of generality we can assume $f_i = e_i$. We can complete this set to a set of $\mathbb{Z}$-generators of $F_n^{p^k}$ by choosing $s-r$ elements in the kernel of R_n. It follows that $F_n^{p^k}$ decomposes as abelian group into $F_n^{(1)} \oplus F_n^{(2)}$, where $F_n^{(1)}$ is generated by r non-principal ideals generating the image of $F_n^{p^k}$ in B_n and $F_n^{(2)}$ is contained in the kernel of R_n. $F_n^{(2)}$ has p-rank $s-r$ and consists only of principal ideals. Let l be arbitrary. As we can find such a decomposition for all levels $n+l$ we can choose $F_n^{(2)}$ such that $N_{n+l,n}(F_{n+l}^{(2)}) = F_n^{(2)}$. By Remark 5.1.9 it follows that $\eta^{1/p^l} \in \Omega_E$ for all η such that $(\eta) \in F_n^{(2)}$.

Let now $(\eta) \in F_n$ be arbitrary. Note that $(\eta)^{p^k} \in F_n^{(1)} \oplus F_n^{(2)}$. Assume that there is a p-power p^v such that $(\eta)^{p^v} \in F_n^{(2)}$. As $F_n^{(1)}$ does not contain p-torsion, we see that $v \leq k$. There is a natural map $\varphi\colon {E'}_n^{p^k} \to F_n^{p^k}$. Clearly, $\varphi({E'}_n^{p^k})/(\varphi({E'}_n^{p^k}) \bigcap F_n^{(2)})$ has p-rank at most r. It follows that the group $\mathrm{Gal}(\Omega_E({E'}_n^{p^{k-l}})/\Omega_E)$ has p-rank at most r. As this holds for all l and n we see that $\mathrm{Gal}(\Omega_{E'}/\Omega_E)$ has $\mathbb{Z}_p$-rank at most r.

□

Using Lemma 5.1.10 we can prove the following property of the map f defined in Theorem 5.1.2.

Lemma 5.1.11. *The map f is surjective.*

Proof. Note that by Lemma 5.1.10 the $\mathbb{Z}_p$-rank of $\Omega_{E'}/\Omega_E$ is exactly $r = \lambda(B_\infty)$. Hence, by property c) and d) the compositum $\mathbb{T}$ of all extensions $f(b)$ for b in $A_\infty^{p^c} \cap B_\infty$ generates a subextension of $\Omega_{E'}$ of finite index. By [Iw 2, Theorem 15] $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$ does not contain $\mathbb{Z}_p$-torsion and we have $\mathbb{T} = \Omega_{E'}$. Therefore, f induces a map

$$f'\colon (A'_\infty)^{p^c} \to \{\mathbb{Z}_p\text{-subextensions of } \mathbb{M}_\infty^{\mathcal{M}}/\Omega_{E'}\}.$$

By [Iw 2, Theorem 16] A'_∞ is pseudo isomorphic to $\mathrm{Gal}(\mathbb{M}_\infty/\Omega_{E'})^\bullet$. Then

$$\lambda(A'_\infty) = \lambda(A'^{p^c}_\infty) = \lambda(\mathrm{Gal}(\mathbb{M}_\infty/\Omega_{E'})^\bullet) = \lambda(\mathrm{Gal}(\mathbb{M}_\infty/\Omega_{E'})).$$

Since f preserves the $\mathbb{Z}_p$-rank of subgroups the same holds for f', and the claim follows from the fact that $\mathrm{Gal}(\mathbb{M}_\infty^{\mathcal{M}}/\mathbb{K}_\infty)$ does not contain $\mathbb{Z}_p$-torsion. □

Remark 5.1.12. *Consider a Λ-submodule C in $A_\infty^{p^c}$ and the compositum of the corresponding $\mathbb{Z}_p$-extensions $\mathbb{M} \subset \mathbb{M}_\infty$. Then $\mathbb{M}$ is Galois over $\mathbb{K}$. Note that if C is annihilated by $f(T)$ then $Gal(\mathbb{M}/\Omega_E)$ is annihilated by $f(T^*)$ and vice versa. To simplify notation we will also write $f(C)$ for $\mathbb{M}$.*

5.1.3 Homomorphisms between $A'_\infty[T]$ and p-units

A main building block in our results on the Gross and the Gross-Kuz'min conjecture is that we can identify elements in $A'_n[T]$ with certain coclasses in the p-units E'_0 of $\mathbb{K}$. Note that our construction of these homomorphisms is very similiar to Greenberg's construction for the abelian case [Gre 2].

Lemma 5.1.13. *There is a well defined homomorphism of abelian groups*

$$\psi_n : A'_n[T] \to E'_0/N_{n,0}(E'_n),$$

whose kernel is the subgroup $\iota_{0,n}(A_0)B_n/B_n$. Furthermore, we have

$$Im(\psi_n) = E'_0 \cap N_{n,0}(K_n^\times)/N_{n,0}(E'_n).$$

Proof. Let $a \in A'_n[T]$, $c \in A_n$ be such that $a = cB_n$ and let $\mathfrak{A}_n \in c$ be an ideal. Then we obtain $\mathfrak{A}_n^T = \prod_{i=1}^s \mathfrak{P}_{n,i}^{a_i}(\alpha_n)$ for some integers a_i and some α_n in $\mathbb{K}_n$. The norm $N_{n,0}(\alpha_n)$ lies in the group of p-units of $\mathbb{K}$. Let $\psi_n(a) = N_{n,0}(\alpha_n)N_{n,0}(E'_n)$. Note that the image of $N_{n,0}(\alpha_n)$ in $E'_0/N_{n,0}(E'_n)$ does neither depend on the representative $\mathfrak{A}_n$ in c nor on the choice of the generator α. Thus, ψ_n is a well defined homomorphism.

Assume that a_n lies in the kernel of ψ_n then we can write $N_{n,0}(\alpha_n) = N_{n,0}(\eta)$ for some element $\eta \in E'_n$. We obtain by Hilbert's Theorem 90 that there is an element γ in $\mathbb{K}_n$ such that $\alpha_n = \eta\gamma^T$. It follows that $\mathfrak{A}_n^T = (\gamma^T)(\eta)\prod_{i=1}^s \mathfrak{P}_{n,i}^{a_i}$. Hence, there are integers b_i such that $(\mathfrak{A}_n/\gamma)^T = \prod_{i=1}^s \mathfrak{P}_{n,i}^{b_i}$. Taking the norm to $\mathbb{K}$ shows that all the b_i are equal to zero. Therefore, $\mathfrak{A}_n/(\gamma)$ is a fractional ideal annihilated by T. Hence, it is the product of primes above p and a lift of an ideal from $\mathbb{K}$. The class $[\mathfrak{A}_n]B_n$ lies in $\iota_{0,n}(A_0)B_n/B_n$. On the other hand $\iota_{0,n}(A_0)B_n/B_n$ lies in the kernel of ψ_n.

Let now $y \in N_{n,0}(\mathbb{K}_n^\times) \cap E'_0$ and let $y = N_{n,0}(\alpha')$ for some $\alpha' \in \mathbb{K}_n$. Then Hilbert's Theorem 90 for ideals implies $(\alpha') = \mathfrak{A}^T \prod_{i=1}^s \mathfrak{P}_{n,i}^{a_i}$ for some integers a_i and an ideal $\mathfrak{A}$ in $\mathbb{K}_n$. It follows that the class $[\mathfrak{A}]B_n$ lies in $A'_n[T]$. Therefore, we see that $Im(\psi_n) = E'_0 \cap N_{n,0}(\mathbb{K}_n^\times)/N_{n,0}(E'_n)$. □

Lemma 5.1.14. *The maps ψ_n induce an injective homomorphism*

$$\psi\colon A'_\infty[T] \to \varprojlim_{\infty \leftarrow n} E'_0 \cap N_{n,0}(\mathbb{K}_n^\times)/N_{n,0}(E'_n).$$

Proof. Let $(a_n)_{n\in\mathbb{N}}$ be a sequence in $A'_\infty[T]$. Let $a_n = c_nB_n$ and $a_{n+1} = c_{n+1}B_{n+1}$. Choose $\mathfrak{A}_n \in c_n$ and $\mathfrak{A}_{n+1} \in c_{n+1}$. Then there is an ideal $\mathfrak{B}$ in $\mathbb{K}_n$ only divisible by ideals above p such that $N_{n+1,n}(\mathfrak{A}_{n+1}) = \mathfrak{A}_n(\gamma)(\mathfrak{B})$. Let $(\alpha_n)\prod_{i=1}^s \mathfrak{P}_{n,i}^{a_{i,n}} = \mathfrak{A}_n^T$ and $(\alpha_{n+1})\prod_{i=1}^s \mathfrak{P}_{n+1,i}^{a_{i,n+1}} = \mathfrak{A}_{n+1}^T$ be defined as above. Then there is a p-unit η in E'_n such that $N_{n+1,n}(\alpha_{n+1}) = \alpha_n\eta\gamma^T$. It follows that $N_{n+1,0}(\alpha_{n+1}) = N_{n,0}(\alpha_n)N_{n,0}(\eta)$. Hence, $N_{n+1,0}(\alpha_{n+1})$ and $N_{n,0}(\alpha_n)$ define the same class in $E'_0 \cap N_{n,0}(\mathbb{K}_n^\times)/N_{n,0}(E'_n)$.

Note that $E_0' \cap N_{n,0}(\mathbb{K}_n^\times) \subset E_0' \cap N_{n-1,0}(\mathbb{K}_{n-1}^\times)$ and that there is a natural restriction homomorphism of quotients

$$E_0' \cap N_{n,0}(\mathbb{K}_n^\times)/N_{n,0}(E_n') \to E_0' \cap N_{n-1,0}(\mathbb{K}_n^\times)/N_{n-1,0}(E_n').$$

As we showed above the elements $(N_{n,0}(\alpha_n))_{n\in\mathbb{N}}$ define a coherent sequence with respect to these restrictions. Hence, they give an element in

$$\lim_{\infty\leftarrow n} E_0' \cap N_{n,0}(\mathbb{K}_n^\times)/N_{n,0}(E_n').$$

As there are no non-trivial norm coherent sequences in $\lim_{\infty\leftarrow n} \iota_{0,n}(A_0)B_n/B_n$, Lemma 5.1.13 implies that the map ψ induced by the ψ_n is injective. □

In the course of this chapter we will also need a second homomorphism constructed below.

Lemma 5.1.15. *There are well defined homomorphisms*

$$\widehat{T}_n : A_n'[T] \to B_n \quad \text{for all } n \geq 0$$

and

$$\widehat{T} : A_\infty'[T] \to B_\infty.$$

Proof. Let $a \in A_n'[T]$, then there is a class $c \in A_n$ such that $a = cB_n$. Define $\widehat{T}_n(a) = Tc$. As $TB_n = \{0\}$ the map $\widehat{T}_n$ is well defined. The same definition works at level infinity. □

5.1.4 Consequences of the weak Leopoldt conjecture

It is well known that the weak Leopoldt conjecture holds for the cyclotomic $\mathbb{Z}_p$-extension of number fields $\mathbb{K}$. This fact has the following useful consequence for us.

Lemma 5.1.16. *Recall that $W = \lim_{\infty\leftarrow n} W_n$ is the projective limit of the p-power roots of unity in U_n and that $\widehat{W} = W \cap \overline{E}_\infty$. Then we have*

$$\mathbb{Z}_p\text{-rank}(W/\widehat{W}) = s - 1.$$

In particular, we obtain $\widehat{W} = \lim_{\infty\leftarrow n} R(\mathbb{K}_n)$, where $R(\mathbb{K}_n)$ denotes the p-power roots of unity of $\mathbb{K}_n$.

Proof. As $\mathbb{Z}_p$-rank$(\lim_{\infty\leftarrow n} R(\mathbb{K}_n)) = 1$ we see that $s-1$ is an upper bound for the $\mathbb{Z}_p$-rank of $W/\widehat{W}$. If Leopoldt's conjecture holds for $\mathbb{K}_n$ for all n there is nothing to prove. Let $\{e_i\}_{1\leq i\leq p^n r_2 - 1}$ be a set of fundamental units of $\mathbb{K}_n$ and assume that $\prod_{i=1}^{r_2 p^n - 1} e_i^{a_i} = 1$ for some elements $a_i \in \mathbb{Z}_p$ not all equal to zero, i.e. $\mathbb{K}_n$ has positive Leopoldt defect. The units e_i are a subset of a set of fundamental units for $\mathbb{K}_{n+l}$ for all $l \geq 0$. By choosing n large enough we can assume that $\mathbb{K}_n$ and $\mathbb{K}_{n+l}$ have the same Leopoldt defect. It follows that the only non-trivial elements in $\widehat{W}_{n+l}/W(\mathbb{K}_{n+l})$ are represented by linear combinations of $e_1 \dots e_{r_2 p^n - 1}$. Consider a linear combination $z = \prod_{i=1}^{p^n r_2 - 1} e_i^{b_i} \in W_{n+l}$. Then we see that $\omega_n z = 1$ and $z \in W_{n+l}[\omega_n] = W_n$. Hence, $\widehat{W}_{n+l} \cong W(\mathbb{K}_{n+l}) \times$(group of uniformly bounded order). Thus, in the projective limit we obtain that the $\mathbb{Z}_p$-rank of $\widehat{W}$ is 1 and $\widehat{W} = \lim_{\infty\leftarrow n} W(\mathbb{K}_n)$. □

5.1.5 Local extensions

To use the full power of the idelic class field theory later we first have to understand local Kummer conditions in more detail.

Lemma 5.1.17. *Let $\hat{N}_{n,i} \subset U_{n,i}$ be a maximal $\mathbb{Z}_p$-free subgroup of the universal norms which are defined as $\bigcap_{m \geq n} N_{m,n}(\mathbb{K}_{m,i}^{\times})$. Let $\pi_{n,i}$ be a uniformizer of the maximal ideal of $\mathbb{K}_{n,i}$ that is a universal norm for the tower $\mathbb{K}_{\infty,i}/\mathbb{K}_{n,i}$. Then the group $W_{n,i}$ acts trivially on the extension $\mathbb{K}_{n,i}((\hat{N}_{n,i})\pi_{n,i}^{\mathbb{Z}} W_{n,i})^{1/p^n})$. If $\alpha \in \mathbb{K}_{n,i}$ has a non-trivial image in the quotient $\mathbb{K}_{n,i}/(\mathbb{K}_{n,i}^{p^n} \hat{N}_{n,i} W_{n,i} \pi_{n,i}^{\mathbb{Z}})$ then $W_{n,i}$ acts non-trivially on the extension $\mathbb{K}_{n,i}(\alpha^{1/p^n})$.*

Proof. As the elements in $\widehat{N}_{n,i}\pi_{n,i}^{\mathbb{Z}} W_{n,i}$ are universal norms their Artin symbols act trivially on the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}_{n,i}$. By [Ne 1, Chapter 5 Proposition 3.2 (iv)] the group $W_{n,i}$ acts trivially on $\mathbb{K}_{n,i}((\widehat{N}_{n,i}\pi_{n,i}^{\mathbb{Z}} W_{n,i})^{1/p^n})$. If α is as in the assumptions, then α has a non-trivial Artin symbol in the extension $\mathbb{K}_{2n,i}/\mathbb{K}_{n,i}$. Again by [Ne 1, Chapter 5 Proposition 3.2 (iv)] the group $W_{n,i}$ acts non-trivially on the extension $\mathbb{K}_{n,i}(\alpha^{1/p^n})$. □

Remark 5.1.18. *By definition $\pi_{0,i}$ is a universal norm. Thus, $\pi_{0,i}$ lies in the subgroup $\pi_{n,i}^{\mathbb{Z}} \widehat{N}_{n,i} V_{n,i} W_{n,i}$.*

5.2 The Gross conjecture

In this section we will prove Theorem 5.0.2. Recall that we denoted the Λ-torsion submodule of $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_{\infty})$ by Z. With this notation one can reformulate Theorem 5.0.2 as follows.

Theorem 5.2.1. *The Gross conjecture holds for a CM field $\mathbb{K}$ if and only if $\phi(W^+) \sim Z^+$ under Artin's isomorphism.*

This equivalent formulation (Theorem 5.0.2) allows us to prove the Gross conjecture in the following cases (cf. Section 5.2.3):

Theorem 5.2.2. *Assume that $\mathbb{K}$ is CM, contains ζ_p and that $\mathbb{K}_{\infty}/\mathbb{K}$ is totally ramified at all primes above p. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ be the primes above p in $\mathbb{K}^+$. Let $s' \leq t$ be the number of primes above p that split in $\mathbb{K}/\mathbb{K}^+$.*

1.) *Assume that $\mathfrak{p}_1$ splits in $\mathbb{K}/\mathbb{K}^+$ and that $\mathfrak{p}_i$ is unsplit in $\mathbb{K}/\mathbb{K}^+$ for $2 \leq i \leq t$. Then the Gross conjecture holds for $\mathbb{K}$.*

2.) a.) *Assume that $s' = 2$. Let the primes above p that are not fixed by the complex conjugation be $\mathfrak{P}_1, \ldots, \mathfrak{P}_4$ and assume that $\mathfrak{P}_{2k} = \overline{\mathfrak{P}_{2k-1}}$ for $k \in \{1, 2\}$. Assume that there is an automorphism $\sigma\colon \mathbb{K} \to \mathbb{K}$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_3$. Assume that either $\sigma^2(\mathfrak{P}_1) = \mathfrak{P}_1$ or that $p \equiv 3 \mod 4$. Then the Gross conjecture holds for $\mathbb{K}$. In particular, the Gross conjecture holds for $\mathbb{K}$ if there is a subfield $\mathbb{M} \subset \mathbb{K}$ such that $s'(\mathbb{M}) = 1$ and $[\mathbb{K} : \mathbb{M}] = 2$.*

b.) Let q be an odd prime different from p and assume $s' = q$. Let the primes above p that are not fixed by the complex conjugation be $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2s'}$ and assume that $\mathfrak{P}_{2k} = \overline{\mathfrak{P}_{2k-1}}$ for $k \in \{1, 2 \ldots s'\}$. Assume that there is an automorphism $\sigma\colon \mathbb{K} \to \mathbb{K}$ acting transitively on the set of pairs of complex conjugate primes above p. Assume that the cyclotomic polynomials $\phi_{s'}(x)$ and $\phi_{2s'}(x)$ are irreducible in $\mathbb{Q}_p[x]$. Then the Gross conjecture holds for $\mathbb{K}$.

The above theorem adds additional cases to the following known ones:

- Let $\mathbb{K}$ be a CM number field satisfying Leopoldt's conjecture such that the prime p is totally split in $\mathbb{K}/\mathbb{Q}$. Then the Gross conjecture holds for $\mathbb{K}$. (cf. [Ho-Kl]).
- Let $\mathbb{K}$ be a CM field such that there is a totally real subfield R with $|\mathrm{Gal}(\mathbb{K}/R)| = 2^k m$ with $k \geq 1$. Assume that $\mathbb{K}/R$ is abelian and that there is a prime $\mathfrak{P}$ above p such that $R_{\mathfrak{P}} = \mathbb{Q}_p$ and such that $\mathfrak{P}$ is totally split in $\mathbb{K}/R$. Assume further that all other primes above p in $\mathbb{K}^+$ are unsplit in $\mathbb{K}/\mathbb{K}^+$. Then the Gross conjecture holds for $\mathbb{K}$ (cf.[Ho-Kl]).

Remark 5.2.3. *In fact one can deduce point 1.) of Theorem 5.2.2 directly from the work of Hofer and Kleine: In the setting of the theorem one can show that the Gross order of vanishing conjecture holds for the unique non-trivial character χ of $Gal(\mathbb{K}/\mathbb{K}^+)$ [Ho-Kl, Remark 2.11 (3)]. As the Gross order of vanishing conjecture for χ is equivalent to the Gross conjecture [Ho-Kl, Theorem A], one can deduce the Gross conjecture[2] for $\mathbb{K}$. Our proof will not use this equivalence and is purely algebraic. That Gross' conjecture holds under the premises of Theorem 5.2.2 point 1.) can also be seen relatively easily from Gross' original formulation of the conjecture. The second point of the theorem cannot be deduced directly from these results and uses the equivalent formulation of Theorem 5.0.2.*

As a further direct consequence of Theorem 5.0.2 we obtain

Corollary 5.2.4. *Assume that $\mathbb{K}$ satisfies the assumptions of Theorem 5.0.2. Let $\mathbb{L}/\mathbb{K}$ be a finite extension such that $\mathbb{L}_n$ and $\mathbb{K}_n$ have the same number of pairs of complex conjugate primes above p for all n. Assume that $\mathbb{L}$ is a CM field as well. If the Gross conjecture holds for $\mathbb{K}$, then it holds for $\mathbb{L}$.*

In Corollary 5.2.4 we allow that the primes above p that are fixed by the complex conjugation split in $\mathbb{L}_n/\mathbb{K}_n$. Therefore, Theorem 5.2.4 is a a generalization of the following theorem which was proved implicitly by Greenberg [Gre 2] and reproved by Jaulent [Jau 2]. Jaulent actually proves the statement for the Gross-Kuz'min conjecture but one can easily specialize to the $1-j$-component in the CM-case. One could also obtain Theorem 5.2.4 relatively easily by using Gross's original formulation in terms of p-adic regulators of p-units.

Theorem 5.2.5. *If $\mathbb{K}$ is a CM field such that the Gross conjecture holds for $\mathbb{K}$ then it also holds for any CM extension of $\mathbb{K}$ in which all primes above p are undecomposed.*

[2] I thank Sören Kleine for pointing this out to me

5.2.1 The failure of the Gross conjecture in terms of potentially ramified extensions

In this section we will consider CM number fields $\mathbb{K}$ containing ζ_p with the property that all primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. We will describe the non-validity of the Gross conjecture in terms of Ω_E and $\Omega_{E'}$.

Theorem 5.2.6. *If the restriction of $\phi(W^+)$ to $Gal(\Omega^+_{E'}/\mathbb{K}_\infty)$ generates a subgroup of finite index in $Gal(\Omega^+_{E'}/\mathbb{K}_\infty)$, then the Gross conjecture holds for $\mathbb{K}$.*

Let $e \in E_n$ for some n. Then e^{1-j} is a root of unity. It follows that the image of e^{1-j} in $\mathbb{K}_\infty/\mathbb{K}_\infty^{p^m}$ is trivial for all m. As this holds for all units we see that $\mathrm{Gal}(\Omega_E/\mathbb{K}_\infty)^{1+j}$ is the trivial group. In particular, $\phi(W^+)$ acts trivially on Ω_E. Hence, $\phi(W^+)$ generates a priori a subgroup of $\mathrm{Gal}(\mathbb{M}_\infty/\Omega_E)^+$ and by restriction in $\mathrm{Gal}(\Omega_{E'}/\Omega_E)^+ \cong \mathrm{Gal}(\Omega^+_{E'}/\mathbb{K}_\infty) \sim (\Lambda/T^*)^k$ for some integer k.

Recall that we defined the maps ψ_n (Lemma 5.1.13), ψ (Lemma 5.1.14) and $\widehat{T}$ (Lemma 5.1.15) in Section 5.1.3.

Lemma 5.2.7. *The map $\widehat{T}\colon A'_\infty[T] \to B_\infty$ is injective on $A'^-_\infty[T]$. In particular, $A^-_\infty[T] = B^-_\infty$*

Proof. Let $a = (a_n)_{n\in\mathbb{N}} \in A'^-_\infty[T]$ be a non-trivial element. Note that for all $n \geq m \geq 0$ the cohomology group $\widehat{H}^1(E'_n, \mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m))^{1-j}$ is trivial. Indeed, $\ker(N_{n,m}) \cap E'_n \subset E_n$ and ${E'_n}^{1-j} \cap E_n$ consists only of roots of unity in $\mathbb{K}_n$. But $\widehat{H}^1(R(\mathbb{K}_n), \mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m))$ is trivial [Wash, Lemma 13.27] which implies the claim. Then [Iw 2, Theorem 12][3] implies that the lift $\iota_{m,n}\colon {A'_m}^- \to {A'_n}^-$ is injective. As $Ta_n = 0$ for all n the homomorphism $\iota_{m,n} \circ N_{n,m}$ acts as multiplication by p^{n-m} on a_n. Together with the injectivity of $\iota_{m,n}$ we obtain that $\mathrm{ord}(a_n) = p^{n-m}\mathrm{ord}(a_m)$. In particular, $\mathrm{ord}(a_n)$ diverges to infinity. Let $b_n = \widehat{T}_n a_n$. We have to show that $b_n \neq 1$ for all n. Assume by contradiction that $b_n = 1$ and let as before $a_n = c_n B_n$ and $\mathfrak{A}_n$ in c_n. Then we have $\mathfrak{A}_n^T = (\alpha_n)$. Without loss of generality we can assume that α_n lies in $\mathbb{K}_n^{1-j}$. There is a natural embedding

$$E_0/N_{n,0}(E_n) \to E'_0/N_{n,0}(E'_n).$$

It follows that the class of $N_{n,0}(\alpha_n)$ in $E'_0/N_{n,0}(E'_n)$ lies in $E_0/N_{n,0}(E'_n) \cap E_0$. As all p-power roots of unity are norms of roots of unity of level n, we see that the group $(E_0/N_{n,0}(E'_n) \cap E_0)^{1-j}$ is trivial. Hence, a_n lies in the kernel of ψ_n for all n and by Lemma 5.1.13 we see that a_n lies in $\iota_{0,n}(A_0)B_n/B_n$. Therefore, a_n has uniformly bounded order in contradiction with the choice of a. This proves the injectivity of $\widehat{T}$.

Clearly, $B^-_\infty \subset A^-_\infty[T]$. Consider the composite map

$$A^-_\infty[T] \to A'^-_\infty[T] \to B^-_\infty$$

induced by $\widehat{T}$. By construction $A^-_\infty[T]$ gets mapped to zero, i.e. the image of $A^-_\infty[T]$ in $A'^-_\infty[T]$ lies in the kernel of $\widehat{T}$. Hence, we obtain $A^-_\infty[T] = B^-_\infty$. □

[3] Iwasawa constructed an isomorphism $\widehat{H}^1(E'_n, \mathrm{Gal}(\mathbb{K}_n/\mathbb{K}_m)) \cong \ker(\iota_{m,n}\colon A'_m \to A'_n)$. One can easily restrict this isomorphism to minus parts.

As B_∞^- does not contain a finite submodule, Lemma 5.2.7 has the following simple consequence.

Corollary 5.2.8. *If B_∞^- is trivial then the Gross conjecture holds for $\mathbb{K}$.*

Ultimately we want to use $\psi_n(A'^-_n[T])$ as radicals over Ω_E and we will do so in Lemma 5.2.12. As a first step we make the following observation.

Remark 5.2.9. *Let $a \in A'^-_\infty[T]$ and $b = \widehat{T}a$. Let, as in the proof of Lemma 5.1.13, $a_n = c_n B_n$ and $\mathfrak{A}_n \in c_n$. Then $\mathfrak{A}_n^T = (\alpha_n)\mathfrak{B}_n$ for an ideal $\mathfrak{B}_n$ in b_n only divisible by primes above p. Let $(\beta_n) = \mathfrak{B}_n^{\mathrm{ord}(b_n)}$. Then there are constants c and c' such that $(\beta_n)^c = (N_{n,0}(\alpha_n))^{c'}$.*

Note that there is a canonical decomposition $B_\infty = B_\infty^+ \oplus B_\infty^-$. We denote the $\mathbb{Z}_p$-rank of B_∞^- by r^- and the one of B_∞^+ by r^+. Then $r = r^- + r^+$. Let s' be the number of primes above p in $\mathbb{K}^+$ that are split in $\mathbb{K}/\mathbb{K}^+$. Let $Y = \mathrm{Gal}(\mathbb{M}_\infty/\Omega_E)$. As $\widehat{T}$ is injective on $A'^-_\infty[T]$, the number s' is a natural upper bound on the rank of A'^-_∞.

Lemma 5.2.10. *We have $(Y^+ \cap \phi(U_\infty/\overline{E}_\infty))[T^*] \sim \phi(W^+)$. Further, $r^- = s'$ and $\mathbb{Z}_p$-rank$((Y^+ \cap \phi(U_\infty/\overline{E}_\infty))[T^*]) = s'$.*

Proof. Let l be maximal such that $\zeta_{p^{n+l}} \in \mathbb{K}_n$ for all $n \geq 0$. We fix n for a moment. For each natural number k we can find elements $x_{k,i} \in \mathbb{K}_n$ such that $x_{k,i} \equiv \zeta_{p^{n+l}} \mod \mathfrak{P}_{n,i}^k$ and $x_{k,i} \equiv 1 \mod \mathfrak{P}_{n,v}^k$ for all $v \neq i$. If $j(\mathfrak{P}_{n,i}) = \mathfrak{P}_{n,i}$, we see that $j(x_{i,k}) \equiv \zeta_{p^{n+l}}^{-1} \mod \mathfrak{P}_{n,i}^k$ and $j(x_{i,k}) \equiv 1 \mod \mathfrak{P}_{n,v}^k$ for all $v \neq i$. We obtain that $x_{i,k}^{1+j} \equiv 1 \mod \mathfrak{P}_{n,v}^k$ for all v and $W_i^{1+j} = \{1\}$. If $j(\mathfrak{P}_{n,i}) \neq \mathfrak{P}_{n,i}$, it follows that $j(x_{k,i}) \equiv 1 \mod \mathfrak{P}_{n,i}^k$. Let $\mathfrak{P}_{n,i+s'} = j(\mathfrak{P}_{n,i})$. In this case $x_{k,i}^{1+j} \equiv \zeta_{p^{n+l}} \mod \mathfrak{P}_{n,i}^k$ and $x_{k,i}^{1+j} \equiv \zeta_{p^{n+l}}^{-1} \mod \mathfrak{P}_{n,i+s'}^k$, while $x_{k,i}^{1+j} \equiv 1 \mod \mathfrak{P}_{n,v}^k$ for $v \notin \{i, i+s'\}$. Note that the group $W_i \times W_{i+s'}$ has $\mathbb{Z}_p$-rank 2. By the above computation we obtain that $(W_i \times W_{i+s'})^{1+j}$ has $\mathbb{Z}_p$-rank 1. Then the $\mathbb{Z}_p$-rank of W^+ is s'.

Clearly, we have $\mathbb{Z}_p$-rank$(B_\infty^-) = r^- \leq s'$. By Lemma 5.2.7 we know that $A_\infty^-[T] = B_\infty^-$. Let $\mathbb{F} = \mathbb{M}_\infty^{T^*Y+Y^-}$. By Proposition 5.1.2, Lemma 5.1.11 and Remark 5.1.12 the extension $\mathbb{M}/f(A_\infty^-[T]^{p^c})$ is finite. As the $\mathbb{Z}_p$-rank of $B_\infty^-[T]$ is r^-, we see that the $\mathbb{Z}_p$-rank of $Y^+(T^*)/T^*Y^+(T^*)$ is also r^-. It follows that $\mathbb{Z}_p$-rank$(Y^+[T^*]) = r^-$. In particular, the rank of $(\phi(U_\infty/\overline{E}_\infty) \bigcap Y^+)[T^*]$ is bounded by r^-.

As $\mathrm{Gal}(\Omega_E/\mathbb{K}_\infty)$ is annihilated by $1+j$, we see that $\phi(W^+) = \phi(W)^{1+j}$ fixes Ω_E. Therefore, $\phi(W^+)$ is a subgroup of Y^+. As $\widehat{W}^{1+j} = \{1\}$ (compare with (5.1.16)) we see $W^+ \bigcap \widehat{W} = \{1\}$. We obtain an isomorphism $\phi(W^+) \cong W^+$ and both have $\mathbb{Z}_p$-rank s'. We obtain the following inequality of $\mathbb{Z}_p$-ranks

$$r^- \leq s' = \mathbb{Z}_p\text{-rank}(W^+) \leq \mathbb{Z}_p\text{-rank}(\phi(U_\infty/\overline{E}_\infty) \bigcap Y^+[T^*]) \leq r^-.$$

It follows that $s' = r^-$. We conclude that

$$(\phi(U_\infty/\overline{E}_\infty) \bigcap Y^+)[T^*] \sim \phi(W^+).$$

□

As an immediate consequence we obtain

Corollary 5.2.11. *We have*

$$\Omega_{E'}^{+} = \bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(E_0'^{(1-j)/p^n}).$$

Furthermore, we have $\mathbb{K}_\infty((N_{n,0}(E_n') \cap E_0'^{1-j})^{1/p^n}) = \mathbb{K}_\infty$.

Proof. The extension $\bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(E_0'^{(1-j)/p^n})/\mathbb{K}_\infty$ is a $\mathbb{Z}_p^{s'}$ extension that is contained in $\Omega_{E'}^{+}$. As $\mathbb{Z}_p$-rank$(\mathrm{Gal}(\Omega_{E'}/\Omega_E)^{+}) = s' = r^{-}$ and as $\mathrm{Gal}(\Omega_E/\mathbb{K}_\infty)$ is annihilated by $1+j$, we obtain that $\Omega_{E'}^{+}/\bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(E_0'^{(1-j)/p^n})$ is a finite extension. Since $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$ does not contain $\mathbb{Z}_p$-torsion [Iw 2, Theorem 15], this implies that $\Omega_{E'}^{+} = \bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(E_0'^{(1-j)/p^n})$.

Let now $e \in N_{n,0}(E_n') \cap E_0'^{1-j}$, i.e. $N_{n,0}(\eta) = e$. By Remark 5.1.9 we have that $e^{1/p^n} \in \Omega_E$. As $e^{1+j} = 1$ we see that $e^{1/p^n} \in \Omega_{E'}^{+} \cap \Omega_E = \mathbb{K}_\infty$, which implies the claim. □

Lemma 5.2.12. *Each non-trivial sequence* $\psi(a) = (N_{n,0}(\alpha_n))_{n\in\mathbb{N}}$ *in* $\lim_{\infty\leftarrow n} \psi_n(A_n'^{-}[T])$ *defines a* $\mathbb{Z}_p$*-extension in* $\Omega_{E'}^{+}/\mathbb{K}_\infty$.

Proof. Let $a = (a')^{1-j}$. Then we see that $\psi_n(a) = \psi_n(a_n'^{1-j}) = (\psi_n(a_n'))^{1-j}$. Hence, $\psi_n(a)$ defines a well defined class in $E_0'^{1-j}/(N_{n,0}(E_n') \cap E_0'^{1-j})$. By Corollary 5.2.11 we see that $\mathbb{K}_\infty((N_{n,0}(E_n') \cap E_0'^{1-j})^{1/p^n}) = \mathbb{K}_\infty$ and $\bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(N_{n,0}(\alpha_n)^{1/p^n})$ defines indeed a $\mathbb{Z}_p$-cyclic extension over $\mathbb{K}_\infty$. Let $b = \widehat{T}a$, $\mathfrak{B}_n \in b_n$ and $\mathfrak{B}_n^{ord(b_n)} = (\beta_n)$. Let α_n be as in Remark 5.2.9. and $(N_{n,0}(\alpha_n))^{c'} = (\beta_n)^c$ (see Remark 5.2.9). Without loss of generality we can assume that $\beta_n^{1+j} = 1$. Let $l(n) = min(p^n, \mathrm{ord}(b_n))$. We obtain that $\Omega_E(N_{n,0}(\alpha_n)^{c'/l(n)}) = \Omega_E(\beta_n^{c/l(n)})$. Note that there is an n_0 such that for all $n \geq n_0$ we have $p \cdot l(n) = l(n+1)$ and $\mathrm{ord}(b_n)/l(n) = \mathrm{ord}(b_{n_0})/l(n_0)$. By Lemma 5.1.8 we get that

$$\bigcup_{n\geq n_0} \Omega_E(N_{n,0}(\alpha_n)^{c'/l(n)}) = \bigcup_{n\geq n_0} \Omega_E(\beta_n^{c/l(n)})$$

defines a $\mathbb{Z}_p$-extension in $\Omega_{E'}/\Omega_E$. As

$$\bigcup_{n\in\mathbb{N}} \Omega_E(N_{n,0}(\alpha_n)^{c'/l(n)}) = \Omega_E \bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(N_{n,0}(\alpha_n)^{c'/l(n)})$$

and $\bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(N_{n,0}(\alpha_n)^{c'/l(n)}) \subset \mathbb{M}_\infty^{+}$, the claim follows. □

The $\mathbb{Z}_p$-extension we constructed in the above lemma is the extension $f(b)$, where $b = \widehat{T}(a)$. The reason that we used b directly to construct a $\mathbb{Z}_p$-extension and not the map f is that we want to spare us technical index shifts at finite level in the above proof.

Using Lemma 5.1.17 we can now show that the extensions constructed in Lemma 5.2.12 are in fact fixed by $\phi(W^{+})$.

Proof of Theorem 5.2.6. Assume that the Gross conjecture is false for $\mathbb{K}$. Then we can choose a non-trivial element $(N_{n,0}(\alpha_n))_{n\in\mathbb{N}} \in \psi(A'^{-}_{\infty}[T])$. Define the field

$$\mathbb{F} = \bigcup_{n\geq n_0} \mathbb{K}_\infty(N_{n,0}(\alpha_n)^{1/l(n)})$$

as in Lemma 5.2.12. Note that for large n and every prime $\mathfrak{P}_{0,i}$ above p in $\mathbb{K}$ and $\mathfrak{P}_{n,i}$ in $\mathbb{K}_n$ we have

$$N_{n,0}(\mathbb{K}^\times_{n,i}) \subset \pi_{0,i}^{\mathbb{Z}} \times \widehat{N}_{0,i} \times W_{0,i} \times U_{0,i}^{p^n} \times V_{0,i} \subset \pi_{m,i}^{\mathbb{Z}} \times \widehat{N}_{m,i} \times W_{m,i} \times V_{m,i} \times U_{m,i}^{p^n}$$

for some uniformizer $\pi_{0,i}$ (see also Lemma 5.1.17 for the definition of $\pi_{0,i}$ and Remark 5.1.18) and all $m \geq 0$. Let $\delta_n \in N_{n,0}(\mathbb{K}_n)$ be a representative for $\psi_n(a_n)$ in $(E'_0)^{1-j}/(N_{n,0}(E'_n) \cap E_0'^{1-j})$. By Corollary 5.2.11 we have $\mathbb{K}_\infty(N_{n,0}(\alpha_n)^{1/l(n)}) = \mathbb{K}_\infty(\delta_n^{1/l(n)})$, by Lemma 5.1.17 we obtain that for $m \geq n$ and all $1 \leq i \leq s$, the group $\phi(W_{m,i})$ acts trivially on the field $\mathbb{K}_n(\delta_n^{1/l(n)})$. Note that $\cup_{n\geq n_0}\mathbb{K}_\infty(\delta_n^{1/p^{l(n)}}) = \mathbb{F}$. Hence, the group $\phi(W^+)$ acts by restriction trivially on $\mathbb{F}$ and it follows that the restriction of $\phi(W^+)$ to $\mathrm{Gal}(\Omega^+_{E'}/\mathbb{K}_\infty)$ does not generate a subgroup of finite index in $\mathrm{Gal}(\Omega^+_{E'}/\mathbb{K}_\infty)^+$. □

5.2.2 Proof of Theorem 5.0.2

In this section we will prove Theorem 5.0.2. As before we consider CM extensions $\mathbb{K}/\mathbb{Q}$ containing ζ_p and with the property that all primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. For these extensions we can use Theorem 5.2.6.

Lemma 5.2.13. *We have*

$$A^+_\infty(T^*) \quad \text{is finite.}$$

Proof. Assume that $A^+_\infty(T^*)$ is infinite. Using Theorem 5.1.2, Lemma 5.1.11 and Remark 5.1.12 we obtain that $\mathrm{Gal}(\mathbb{M}_\infty/\Omega_E)^-(T)$ is infinite. Let $\mathbb{L} = \mathbb{M}_\infty^{TY+Y^+}$. Hence, $\mathrm{Gal}(\mathbb{L}/\Omega_E)$ is as abelian group pseudo isomorphic to $\mathbb{Z}_p^{\lambda(\mathbb{L}/\Omega_E)}$. Note that by (5.3), (5.4) and the fact that $T^*Z = \{0\}$, we have $\mathrm{Gal}(\Omega_E/\mathbb{K}_\infty) \sim \Lambda^{r_2} \oplus (\Lambda/T^*)^v$ for some $v \geq 0$. As $\mathrm{Gal}(\mathbb{L}/\Omega_E)$ is annihilated by T, we obtain

$$\mathrm{Gal}(\mathbb{L}/\mathbb{K}_\infty) \sim \Lambda^{r_2} \oplus (\Lambda/T)^v \oplus (\Lambda/T^*)^k$$

for some $v \geq 1$. Further, $(1+j)$ annihilates $\mathrm{Gal}(\mathbb{L}/\mathbb{K}_\infty)$. Consider $\mathbb{M}_0 \cap \mathbb{L}$ (recall that $\mathbb{M}_0$ is the maximal p-abelian, p-ramified extension of $\mathbb{K}$). Then we have the following short exact sequence

$$1 \to \mathrm{Gal}(\mathbb{L} \cap \mathbb{M}_0/\mathbb{K}_\infty) \to \mathrm{Gal}(\mathbb{L} \cap \mathbb{M}_0/\mathbb{K}) \to \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}) \to 1.$$

Note that $\mathrm{Gal}(\mathbb{L} \cap \mathbb{M}_0/\mathbb{K}_\infty) = \mathrm{Gal}(\mathbb{L}/\mathbb{K}_\infty)/T\mathrm{Gal}(\mathbb{L}/\mathbb{K}_\infty)$ has $\mathbb{Z}_p$-rank $r_2 + v$ and is annihilated by $(1+j)$. As we have $U(\mathbb{K})/\overline{E}_0 \cong \mathrm{Gal}(\mathbb{M}_0/\mathbb{H}(\mathbb{K}))$, it follows that $U(\mathbb{K})^-$ has $\mathbb{Z}_p$-rank at least $r_2 + v$. It is easy to see [4] that $U(\mathbb{K})^-$ has $\mathbb{Z}_p$-rank $r_2 = [\mathbb{K} : \mathbb{Q}]/2$ in contradiction with $v \geq 1$. □

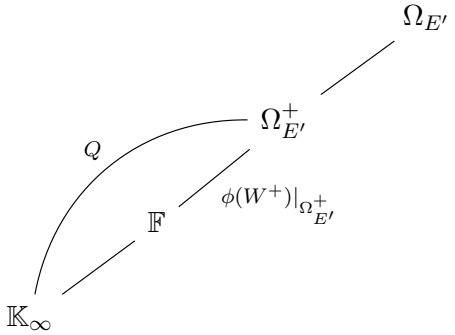
[4] As $U(\mathbb{K})$ is pseudo isomorphic to $\mathbb{Z}_p^{[\mathbb{K}:\mathbb{Q}]}$ while $U(\mathbb{K})^+ \cong U(\mathbb{K}^+)$ is pseudo isomorphic to $\mathbb{Z}_p^{[\mathbb{K}:\mathbb{Q}]/2}$ we obtain that $U(\mathbb{K})^-$ is pseudo-isomorphic to $\mathbb{Z}_p^{r_2}$.

Now we have all ingredients to prove the central theorem of this section.

Proof of Theorem 5.0.2. Assume first that $(U_\infty/\overline{E}_\infty W)^+[T^*]$ is finite. Then Lemma 5.2.10 implies that $(Y^+ \cap \phi(U_\infty/\overline{E}_\infty))(T^*) \sim \phi(W^+)$. Assume in addition that the Gross conjecture is false. Then Theorem 5.2.6 implies that the restriction of $\phi(W^+)$ to $\mathrm{Gal}(\Omega^+_{E'}/\mathbb{K}_\infty)$ does not generate a subgroup of finite index in $\mathrm{Gal}(\Omega^+_{E'}/\mathbb{K}_\infty)$. Denote $\mathrm{Gal}(\Omega^+_{E'}/\mathbb{K}_\infty)$ by Q. Define

$$\mathbb{F} \subset \Omega^{+\,\phi(W^+)}_{E'}$$

as the maximal subfield such that $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$ is $\mathbb{Z}_p$-free. By Theorem 5.2.6 the extension $\mathbb{F}/\mathbb{K}_\infty$ has positive $\mathbb{Z}_p$-rank.



Let $X = \mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$. Then we have $X = X^+$. Recall that $Y = \mathrm{Gal}(\mathbb{M}_\infty/\Omega_E)$. Note that $Y^+ \cong \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{K}_\infty)^+$. As $\phi(W^+)$ fixes $\mathbb{F}$ and $(Y^+ \cap \phi(U_\infty/\overline{E}_\infty))(T^*) \sim \phi(W^+)$ we obtain that $\mathbb{F}/\mathbb{F}\cap\mathbb{H}_\infty$ is finite. Since $\mathbb{F}/\mathbb{K}_\infty$ is $\mathbb{Z}_p$-free, we obtain $\mathbb{F} \subset \mathbb{H}_\infty$. Then there is a subgroup $C \subset A^+(T^*)$ surjecting to a subgroup of finite index in $\mathrm{Gal}(\mathbb{F}/\mathbb{K}_\infty)$. Therefore, $A^+(T^*)$ is infinite, yielding a contradiction to Lemma 5.2.13. So if $(U_\infty/\overline{E}_\infty W)^+[T^*]$ is finite then the Gross conjecture holds for $\mathbb{K}$.

It remains to show the second implication. Assume that the Gross conjecture is true. The injectivity of $\widehat{T}$ (Lemma 5.2.7) and the fact that A^-_∞ does not contain a finite submodule [Wash, Proposition 13.28] imply that $A^-_\infty(T) = B^-_\infty$. It is easy to see that the fixed field of $T^*Y + Y^-$ in $(\Omega_E\mathbb{H}_\infty \cap \Omega_{E'})$ is a finite extension of Ω_E. Indeed, if it was infinite, the group $A^+_\infty(T^*)$ would also be infinite yielding a contradiction. Hence, $Gal(\Omega_{E'}/\Omega_E)^+$ is pseudo isomorphic to a quotient of $\phi(U_\infty/\overline{E}_\infty)$. By Theorem 5.1.2, Lemma 5.1.11 and Remark 5.1.12 it follows that $\phi(U_\infty/\overline{E}_\infty)^+(T^*) \subset Y^+$ is pseudo isomorphic to $\mathrm{Gal}(\Omega_{E'}/\Omega_E)^+$ under Artin's isomorphism. As $T^*\mathrm{Gal}(\Omega_{E'}/\Omega_E)$ is trivial, we conclude that $(U_\infty/\overline{E}_\infty)^+(T^*) \sim (U_\infty/\overline{E}_\infty)^+[T^*] \sim W^+ \sim \mathrm{Gal}(\Omega_{E'}/\Omega_E)^+$. □

Having proved Theorem 5.0.2 we can proceed with the proof of Corollary 5.2.4.

proof of Corollary 5.2.4. Let N be the norm from $\mathbb{L}_n$ to $\mathbb{K}_n$ for all n. Assume that the Gross conjecture is false for $\mathbb{L}$. By Theorem 5.0.2 the group $(U_\infty/\overline{E}_\infty W)^+[T^*]$ is infinite. By Lemma 5.2.10 we have $(U_\infty/\overline{E}_\infty)^+[T^*] \sim W^+$. Hence, there is an element $u = (u_n^{1+j})_{n\in\mathbb{N}}$ such that $u^{(T^*)^2} \in \overline{E}_\infty$ but $u^{T^*} \notin \overline{E}_\infty$. It follows that $N(u)$ is a local unit in $U_\infty(\mathbb{K})$ such that $N(u)^{(T^*)^2} \in \overline{E}_\infty$. Let $w \in W^+$ be such that $u^{T^*} \equiv w \mod \overline{E}_\infty$. Then $N(u^{T^*}) \equiv N(w) \mod N(\overline{E}_\infty)$. Let $\pi_i : U_\infty \to$

$U_{\infty,i}$. If $j(\mathfrak{P}_{n,i}) = \mathfrak{P}_{n,i}$ for all n then $\pi_i(W^+) = \{1\}$. Let $\mathfrak{P}_{n,i} \neq j(\mathfrak{P}_{n,i})$. Then $\mathfrak{P}_{n,i}$ is totally undecomposed in $\mathbb{L}_n/\mathbb{K}_n$ by assumption. Hence, N acts as raising to the power $[\mathbb{L} : \mathbb{K}]$ on $\pi_i(W^+)$. Thus, there is a canonical isomorphism $N(W^+) \cong W^+$. Further, we see that $W^+ \cap \overline{E}_\infty(\mathbb{K}) = \{1\}$ and that $N(w)$ does not lie in $\overline{E}_\infty(\mathbb{K})$. Therefore, $N(u)^{T^*}$ is not an element in $\overline{E}_\infty(\mathbb{K})$. By [Iw 2, Theorem 18] the group $\mathrm{Gal}(\mathbb{M}_\infty(\mathbb{K}_\infty)/\mathbb{K}_\infty)$ does not contain a finite submodule. It follows that $(\Lambda N(u)\overline{E}_\infty(\mathbb{K}))/\overline{E}_\infty(\mathbb{K})$ is pseudo isomorphic to $\Lambda/(T^*)^2$. As $(U_\infty(\mathbb{K})/\overline{E}_\infty(\mathbb{K}))^- \sim \Lambda^{r_2} \oplus T^*$-torsion this yields a contradiction to the fact that the Gross conjecture holds for $\mathbb{K}$. □

5.2.3 Applications

Assume that $\mathbb{K}$ contains ζ_p and is such that $\mathbb{K}_\infty/\mathbb{K}$ is totally ramified at all primes above p. Recall that we denote by $\pi_{0,i}$ a generator of the maximal ideal in $\mathbb{K}_{0,i}$ that is a universal norm for $\mathbb{K}_{\infty,i}/\mathbb{K}_{0,i}$. Let $\iota_i \colon \mathbb{K} \to \mathbb{K}_{0,i}$ be the natural embedding. Let $v_i \colon \mathbb{K}_{0,i} \to \mathbb{Z}$ be the $\pi_{0,i}$-adic valuation map. For every $e \in E_0'$ we define $w_i(e) \in V_{0,i}$ to be the element such that $\iota_i(e)/(\pi_{0,i}^{v_i(e)} w_i(e)) \in U_{0,i}$. Define $\kappa_i(e) = \iota_i(e)/\pi_{0,i}^{v_i(e)} w_i(e)$ and let $\kappa \colon E_0' \to U_0$ be be defined via $\kappa(e) = (\kappa_i(e))_{1 \leq i \leq s} \in U_0$. Let $\tilde{E} = \bigcap_{n \in \mathbb{N}} N_{n,0}(\mathbb{K}_n^\times)$ be the universal norms in $\mathbb{K}_0$. Then we know $\tilde{E} \subset E_0'$ by [Jau 2, page 546].

Lemma 5.2.14. *The group*

$$E_0'^{1-j} \cap \tilde{E} \quad \text{is finite}$$

Proof. p is a universal norm and the $\mathbb{Z}$-rank of $\tilde{E}/\tilde{E} \cap E_0$ is at most 1 [Kl 2, Lemma 3.5]. Hence, $\tilde{E}/(E_0 \cap \tilde{E})p^{\mathbb{Z}}$ is finite and $\tilde{E} \cap E_0'^{1-j}$ is finite as well. □

Let $\tilde{U}_n$ be the universal norms in U_n and define $\theta_i \colon U_{0,i} \to \mathbb{K}_{0,i}$ via $\theta_i(u_i) = \log_p(N_{\mathbb{K}_{0,i}/\mathbb{Q}_p}(u_i))$. Let $\theta \colon U_0 \to \prod_{i=1}^s \mathbb{K}_{0,i}$ be the $\mathbb{Z}_p$-linear map obtained from the θ_i, i.e. if $u = (u_1, \ldots, u_s)$ then $\theta(u) = (\theta_1(u_1), \ldots, \theta_s(u_s))$. The kernel of θ is $\tilde{U}_0$ [Jau 2, page 548]. Note that the Hasse-Norm-principle implies that a p-unit e is a universal norm if and only if it is a universal norm at every prime above p, i.e. $e \in \tilde{E} \Leftrightarrow \kappa(e) \in \tilde{U}_0$. By Lemma 5.2.14 we see that the set $\{e \in E_0'^{1-j} \mid \kappa(e) \in \tilde{U}_0\}$ is finite. Hence, $(\theta \circ \kappa)\,|_{E_0'^{1-j}}$ has finite kernel and the $\mathbb{Z}$-rank of $\theta \circ \kappa(E_0'^{1-j})$ is s'.

Remark 5.2.15. *Note that $\theta \circ \kappa$ coincides with the homomorphism λ_p that Gross defined to state his original conjecture [Gro 1, Conjecture 1.15]. In his definition Gross did not divide by $w_i(e)$ in each component. But as $\log_p(\zeta) = 0$ for every root of unity, we obtain $\lambda_p(u) = \theta \circ \kappa(u)$.*

Lemma 5.2.16. *Let $z \in E_0'^{1-j} \setminus R(\mathbb{K}_0)$. Then $\phi(W^+)$ generates a subgroup of finite index in Gal$(\bigcup_{n \in \mathbb{N}} \mathbb{K}_\infty(z^{1/p^n})/\mathbb{K}_\infty)$.*

Proof. Let Z be the $\mathbb{Z}$-module generated by z. By Lemma 5.2.14 and the definition of θ we see that the $\mathbb{Z}_p$-rank of the p-adic closure $\overline{\theta \circ \kappa(Z)}$ is equal to 1.

By local class field theory $N_{n,0}(U_{n,i})$ are the elements with trivial Artin-symbol in $\mathbb{K}_{n,i}/\mathbb{K}_{0,i}$. These are exactly the elements in $W_{0,i}\tilde{U}_{0,i}U_{0,i}^{p^n}$. From this we obtain that $N_{n,0}(U_n) = U_0^{p^n}\tilde{U}_0W_0$. An element in the kernel $N_{n,0}\mid_{U_n}$ has a trivial Artin-symbol in $\mathbb{K}_\infty/\mathbb{K}_n$ and is therefore a universal norm. We obtain that $U_n = U_0\tilde{U}_nW_n$.

For every k there exists an n such that $\kappa(z)$ has order p^k in $U_n/U_n^{p^n}\tilde{U}_nW_n$. By Lemma 5.1.17 we obtain that for n large enough there exists an i such that $\phi(W_{n,i})$ acts non-trivially on $\mathbb{K}_{n,i}(\kappa(z)^{1/p^n})$.

Recall from Lemma 5.1.17 that the group $\phi(W_{n,i})$ acts trivially on the field extension $\mathbb{K}_{n,i}((\pi_{n,i}\tilde{U}_{n,i}W_{n,i}V_{n,i})^{1/p^n})$. As $\kappa_i(z) = \iota_i(z)/\pi_{0,i}^{v_i(z)}w_i(z)$ we obtain that $\phi(W_{n,i})$ acts non-trivially on $\mathbb{K}_{n,i}(z^{1/p^n})/\mathbb{K}_{n,i}$.

Hence, $\mathbb{K}_{\infty,z} = \bigcup_{n\in\mathbb{N}}\mathbb{K}_\infty(z^{1/p^n})$ defines a $\mathbb{Z}_p$-extension over $\mathbb{K}_\infty$ that is annihilated by $1-j$ and not fixed by $\phi(W)$. As every non-trivial subgroup has finite index in $\mathbb{Z}_p$, it follows that the restriction of $\phi(W)$ to $\mathrm{Gal}(\mathbb{K}_{\infty,z}/\mathbb{K}_\infty)$ generates a subgroup of finite index. □

Theorem 5.2.17. *If $s' = 1$ the Gross conjecture holds for $\mathbb{K}$.*

Proof. Let $\pi_1 \in \mathbb{K}$ be a generator of $\mathfrak{P}_{1,0}^{\mathrm{ord}(b_{1,0})}$. It follows from Corollary that 5.2.11 $\bigcup_{n\in\mathbb{N}}\Omega_E(\pi_1^{(1-j)/p^n}) = \Omega_{E'}^+$.

Together with Lemma 5.2.16 we obtain that $\phi(W^+)$ generates by restriction the group $\mathrm{Gal}(\Omega_{E'}^+/\mathbb{K}_\infty)$ up to finite index, i.e. $W^+ \cong \phi(W^+) \sim \mathrm{Gal}(\Omega_{E'}^+/\mathbb{K}_\infty) \sim \mathrm{Gal}(\Omega_{E'}/\Omega_E)^+$. Hence,

$$\chi\colon W^+ \to (U_\infty/\overline{E}_\infty U_\infty^{T^*})^+$$

has a finite kernel. By Lemma 5.2.10 and the fact that $\phi(U_\infty/\overline{E}_\infty)^+$ fixes Ω_E we see that $\phi(W^+) \sim \phi(U_\infty/\overline{E}_\infty)^+(T^*)$. Using that ϕ is an isomorphism and that the kernel of χ is finite, we obtain that $(U_\infty/\overline{E}_\infty W)^+[T^*]$ is finite and the claim follows from Theorem 5.0.2.

□

Outside of the $s' = 1$ case we have to make sure that $\mathbb{Z}$-independent elements in ${E'_0}^{1-j}$ stay independent when we apply $\theta\circ\kappa$ and take the p-adic closure in the image. In the following we will use group ring theoretic results to ensure this condition holds for certain extensions.

Theorem 5.2.18. *1.) Assume that $s' = 2$. Let the primes above p that are not fixed by the complex conjugation be $\mathfrak{P}_1,\dots,\mathfrak{P}_4$ and assume that $\mathfrak{P}_{2k} = \overline{\mathfrak{P}_{2k-1}}$ for $k \in \{1,2\}$. Assume that there is an automorphism $\sigma\colon \mathbb{K}\to\mathbb{K}$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_3$ and such that either $\sigma^2(\mathfrak{P}_1) = \mathfrak{P}_1$ or that $p \equiv 3 \mod 4$. Then the Gross conjecture holds for $\mathbb{K}$. In particular, the Gross conjecture holds for $\mathbb{K}$ if there is a subfield $\mathbb{M}\subset\mathbb{K}$ such that $s'(\mathbb{M}) = 1$ and $[\mathbb{K}:\mathbb{M}] = 2$.*

2.) Let q be an odd prime different from p and assume $s' = q$. Let the primes above p that are not fixed by the complex conjugation be $\mathfrak{P}_1,\dots,\mathfrak{P}_{2s'}$ and assume that $\mathfrak{P}_{2k} = \overline{\mathfrak{P}_{2k-1}}$ for $k \in \{1,2\dots s'\}$. Assume that there is an automorphism $\sigma\colon\mathbb{K}\to\mathbb{K}$ acting transitively on the set of pairs of complex conjugate primes

above p in $\mathbb{K}$. Assume that the cyclotomic polynomials $\phi_{s'}(x)$ and $\phi_{2s'}(x)$ are irreducible in $\mathbb{Q}_p$. Then the Gross conjecture holds for $\mathbb{K}$.

Remark 5.2.19. *By the definition of σ we see that $\sigma^{s'}(\mathfrak{P}_1) \in \{\mathfrak{P}_1, \mathfrak{P}_2\}$. So the minimal k such that σ^k fixes $\mathfrak{P}_1$ is either s' or $2s'$.*

To prove the above theorem we need the following two auxiliary lemmata on group rings.

Lemma 5.2.20. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial that is irreducible in $\mathbb{Q}_p[x]$. Let $R = \mathbb{Z}_p[x]/(f(x))$. Then each non-zero R-submodule of R has finite index in R.*

Proof. Let $0 \neq \alpha \in R$ and consider $R\alpha$. Then $R\alpha \cong \mathbb{Z}_p[x]/I$, where I is an ideal in $\mathbb{Z}_p[x]$. Clearly $f(x) \in I$. If I is generated by $f(x)$ then $R\alpha$ and R have the same rank as $\mathbb{Z}_p$-modules and $R\alpha$ has finite index in R. If $I \neq (f(x))$ we can find an element $g(x) \in I$ that is coprime to $f(x)$. Then there are polynomials $u(x), v(x)$ such that $u(x)f(x) + v(x)g(x) = a \in \mathbb{Z}_p$. Hence, a annihilates α and $R\alpha$ contains $\mathbb{Z}_p$-torsion. But the ring R is $\mathbb{Z}_p$-torsion free yielding a contradiction. Hence, I is always generated by $f(x)$ and the claim follows. □

Lemma 5.2.21. *Let s' be an odd prime coprime to p and assume that the cyclotomic polynomials $\phi_{s'}(x)$ and $\phi_{2s'}(x)$ are irreducible in $\mathbb{Q}_p[x]$. Let $R = \mathbb{Z}_p[x]/(x^{s'} - 1)$ and $R' = \mathbb{Z}_p[x]/(x^{s'} + 1)$. Then we have the following decompositions:*

1.) *$R = R_1 \oplus R_2$, where $R_1 = \phi_{s'}(x)R \cong \mathbb{Z}_p[x]/(x-1)$ and $R_2 = (s' - \phi_{s'}(x))R \cong \mathbb{Z}_p[x]/(\phi_{s'}(x))$ and*

2.) *$R' = R'_1 \oplus R'_2$, where $R'_1 = \phi_{2s'}(x)R' \cong \mathbb{Z}_p[x]/(x+1)$ and $R'_2 = (s' - \phi_{2s'}(x))R' \cong \mathbb{Z}_p[x]/(\phi_{2s'}(x))$.*

In both cases every non-zero submodule of R (resp. of R') is of finite index in R, R_1 or R_2 (resp. in R'_1, R'_2 or R').

Proof. The elements $\frac{1}{s'}\phi_{s'}(x)$ and $\frac{1}{s'}\phi_{2s'}(x)$ are idempotents in R and R', respectively. As s' is a unit in $\mathbb{Z}_p$, this gives the desired decompositions. Clearly, we have

$$\phi_{s'}(x)(\mathbb{Z}_p[x]/(x^{s'}-1)) \cong \mathbb{Z}_p[x]/(x-1) \quad \text{and} \quad \phi_{2s'}(x)(\mathbb{Z}_p[x]/(x^{s'}+1)) \cong \mathbb{Z}_p[x]/(x+1).$$

The modules $(s' - \phi_{s'}(x))R$ and $(s' - \phi_{2s'}(x))R'$ are annihilated by $\phi_{s'}(x)$ and $\phi_{2s'}(x)$, respectively. Then by the cyclicity of the modules R_2 and R'_2, and by the irreducibility of $\phi_{s'}(x)$ and $\phi_{2s'}(x)$ we obtain the isomorphism $R_2 \cong \mathbb{Z}_p[x]/\phi_{s'}(x)$ and $R'_2 \cong \mathbb{Z}_p[x]/\phi_{2s'}(x)$ finishing the proof of points 1.) and 2.).

Let now A be a non-zero submodule of R. Then we can use the idempotents $\frac{1}{s'}\phi_{s'}(x)$ and $\frac{1}{s'}(s' - \phi_{s'}(x))$ to decompose $A = A_1 \oplus A_2$ as R-modules with $A_1 \subset R_1$ and $A_2 \subset R_2$. Then by Lemma 5.2.20 A_1 has finite index in R_1 or A_2 has finite index in R_2. If $A_1 = 0$ or $A_2 = 0$, then $A = A_2$ or $A = A_1$, respectively. If $A_1 \neq 0 \neq A_2$, then A has finite index in R. We can prove the result for submodules A' of R' analogously. □

Proof of Theorem 5.2.18. Let σ' be a lift of σ to $\mathbb{K}_\infty$. By Corollary 5.2.11 there are s' elements $\pi_1, \pi_3 \ldots, \pi_{2s'-1} \in E_0'$ such that $\bigcup_{n\in\mathbb{N}} \mathbb{K}_\infty(\pi_1^{(1-j)/p^n}, \pi_3^{(1-j)/p^n}, \ldots, \pi_{2s'-1}^{(1-j)/p^n})$ equals $\Omega_{E'}^+$. Without loss of generality we can assume that $\sigma^k(\pi_1) = \pi_{2(k+1)-1}$ for $1 \leq k \leq s'-1$. Let Q_W be the restriction of $\phi(W^+)$ to $\mathrm{Gal}(\Omega_{E'}^+/\mathbb{K}_\infty)$ and consider $(\Omega_{E'}^+)^{Q_W}$. The group Q_W is invariant under the action of σ'.

Define the Kummer-radical

$$R_n = (\pi_1^{(1-j)\mathbb{Z}}\pi_3^{(1-j)\mathbb{Z}} \ldots \pi_{2s'-1}^{(1-j)\mathbb{Z}})/(\pi_1^{(1-j)\mathbb{Z}}\pi_3^{(1-j)\mathbb{Z}} \ldots \pi_{2s'-1}^{(1-j)\mathbb{Z}} \cap \mathbb{K}_\infty^{p^n})$$

and define the projective limit $R_\infty = \lim_{\infty\leftarrow n} R_n$. The automorphism σ' acts naturally on R_n and R_∞. Let $R_n' \subset R_n$ be the radical of

$$\mathbb{K}_\infty(\pi_1^{(1-j)/p^n}, \pi_3^{(1-j)/p^n}, \ldots, \pi_{2s'-1}^{(1-j)/p^n}) \cap (\Omega_{E'}^+)^{Q_W}.$$

Then $R_\infty' = \lim_{\infty\leftarrow n} R_n'$ defines a σ'-invariant submodule of R_∞ (meaning that σ' maps R_∞' to itself but might have a non-trivial action element wise).

Assume first that $s' = 2$. If $\sigma^2(\mathfrak{P}_1) = \mathfrak{P}_1$ then $\sigma^2(\pi_1^{1-j}) = \pi_1^{1-j}w$ for some root of unity w. Hence, $(\sigma')^2$ acts trivially on R_∞ and every $\mathbb{Z}_p[\sigma']$ submodule of R_∞ of $\mathbb{Z}_p$-rank one has finite index in $R_\infty^{(1-\sigma)/2}$ or in $R_\infty^{(1+\sigma)/2}$. As 2 is a unit in $\mathbb{Z}_p$ the elements $\pi_1^{(1-j)(1\pm\sigma)}$ generate these $\mathbb{Z}_p[\sigma']$-submodules. Hence, if $(\Omega_{E'}^+)^{Q_W}$ is a $\mathbb{Z}_p$-extension of $\mathbb{K}_\infty$, then

$$(\Omega_{E'}^+)^{Q_W} = \mathbb{K}_\infty(\pi_1^{(1-j)(1\pm\sigma)/p^\infty})$$

which is impossible by Lemma 5.2.16. It remains the case that R_∞' has finite index in R_∞. But by Lemma 5.2.16 $\phi(W)$ does not act trivially on $\Omega_{E'}^+$ (take for example $z = \pi_1^{1-j}$). It follows that Q_W generates $\mathrm{Gal}(\Omega_{E'}^+/\mathbb{K}_\infty)$ up to finite index.

If $\sigma^2(\mathfrak{P}_1) \neq \mathfrak{P}_1$, we obtain that $\sigma^2\mathfrak{P}_1 = \mathfrak{P}_2$ and $\sigma^2(\pi_1^{1-j}) = \pi_1^{j-1}w$ for some root of unity w. It follows that $(\sigma')^2$ acts on R_∞ as -1. Hence we obtain an isomorphism $R_\infty \cong \mathbb{Z}_p[x]/(x^2+1)$. We assumed that $p \equiv 3 \mod 4$ in this case and obtain that every $\mathbb{Z}_p[\sigma']$ submodule of R_∞ has finite index in R_∞. As Q_W does not act trivially on $\Omega_{E'}^+$ by Lemma 5.2.16 we obtain again that Q_W generates $\mathrm{Gal}(\Omega_{E'}^+/\mathbb{K}_\infty)$ up to finite index in both cases and we can proceed as in the proof of Theorem 5.2.17.

Assume now that $s' \neq 2$ and that $\sigma^{s'}(\mathfrak{P}_1) = \mathfrak{P}_1$. Then we have an isomorphism $R_\infty \cong \mathbb{Z}_p[x]/(x^{s'}-1)$. By Lemma 5.2.21 $R_\infty' \cap R_1 = \phi_{s'}(x)R_\infty'$ has finite index in R_1 or $R_\infty' \cap R_2 = (s' - \phi_{s'}(x))R_\infty'$ has finite index in R_2. The modules R_1 and R_2 are generated by $\pi_1^{(1-j)\phi_{s'}(x)}$ and $\pi_1^{(1-j)(s'-\phi_{s'})}$, respectively. Let π be one of these generators. Then by Lemma 5.2.16, Q_W acts non-trivially on $\mathbb{K}_\infty(\pi^{1/p^\infty})$ and we obtain that Q_W generates $\mathrm{Gal}(\Omega_{E'}^+/\mathbb{K}_\infty)$ up to finite index.

If $\sigma^{s'}(\mathfrak{P}_1) \neq \mathfrak{P}_1$, we see that $R_\infty \cong \mathbb{Z}_p[x]/(x^{s'}+1)$. Then $R_\infty' \cap R_1'$ has finite index in R_1' or $R_\infty' \cap R_2'$ has finite index in R_2'. The generators of R_1' and R_2' are $\pi_1^{(1-j)\phi_{2s'}(x)}$ and $\pi_1^{(1-j)(s'-\phi_{2s'})}$, respectively. As in the case that $\sigma^{s'}(\mathfrak{P}_1) = \mathfrak{P}_1$ we obtain that Q_W generates $\mathrm{Gal}(\Omega_{E'}^+/\mathbb{K}_\infty)$ up to finite index and we can proceed as in the proof of Theorem 5.2.17. □

Together Theorem 5.2.17 and Theorem 5.2.18 imply Theorem 5.2.2.

5.3 Gross-Kuz'min conjecture

The aim of this section is to prove an equivalent formulation of the Gross-Kuz'min conjecture for number fields as we did in the last section for the Gross conjecture. So in this section we will no longer restrict ourselves to the CM case. It turns out that if we assume Leopoldt's conjecture, we get a condition very similar to the one we proved for the Gross conjecture, i.e Theorem 5.0.4.

Theorem. *Assume that $\mathbb{K}$ contains ζ_p and that all primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$. If the Gross-Kuz'min conjecture holds for $\mathbb{K}$ (i.e. $A'_\infty[T]$ is finite), then $(\phi(U_\infty)/\phi(W))(T^*)$ is finite. If conversely $(\phi(U_\infty)/\phi(W))(T^*)$ is finite and Leopoldt's conjecture holds for $\mathbb{K}$, then the Gross-Kuz'min conjecture holds for $\mathbb{K}$.*

Proof of the first implication of the theorem. Assume that the Gross-Kuz'min conjecture holds for $\mathbb{K}$. Then by Theorem 5.1.2, Lemma 5.1.11 and Remark 5.1.12 we see that $\mathrm{Gal}(\mathbb{M}_\infty/\Omega_{E'})(T^*)$ is finite. In particular, $\phi(U_\infty)(T^*) \cap \mathrm{Gal}(\mathbb{M}_\infty/\Omega_{E'})$ is finite. Hence, the natural restriction homomorphism

$$\phi(U_\infty)(T^*) \to \mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$$

has a finite kernel. As the Λ-torsion submodule Z of $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$ is annihilated by T^* and of $\mathbb{Z}_p$-rank $s-1$, we see that $T^*(\phi(U_\infty)(T^*))$ is finite and $\mathbb{Z}_p$-rank$(\phi(U_\infty)(T^*)) = s-1$. It follows that $\phi(U_\infty)(T^*) \sim \phi(W)$. □

Remark 5.3.1. *If $\mathbb{K}$ is a CM field then $(U_\infty/\overline{E}_\infty W)^- = U_\infty^-/W^-$ does not contain T^*-torsion. Hence, in this case $(\phi(U_\infty)/\phi(W))(T^*)$ being finite is equivalent to $(U_\infty/W\overline{E}_\infty)^+(T^*)$ being finite. $(U_\infty/W\overline{E}_\infty)^+(T^*)$ being finite implies Gross' conjecture by Theorem 5.0.2. Assuming Leopoldt's conjecture in addition implies the Gross-Kuz'min conjecture trivially.*

Let us now prove some preliminary results to enable us to show the second implication of Theorem 5.0.4. Recall that Z denotes the torsion submodule of $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$.

Lemma 5.3.2. *Assume that $(\phi(U_\infty)/\phi(W))(T^*)$ is finite and that Leopoldt's conjecture holds for $\mathbb{K}$. Then $\phi(W)$ generates by restriction a subgroup of finite index in $Gal(\Omega_{E'}/\tilde{\Omega})$, where $\tilde{\Omega} = \mathbb{M}_\infty^Z$.*

Proof. We will first show that $A_\infty(T^*)$ is finite. Assume that it is infinite, then by Theorem 5.1.2, Lemma 5.1.11 and Remark 5.1.12 $\mathrm{Gal}(\mathbb{M}_\infty/\Omega_{E'})(T)$ is infinite. It follows that the quotient $\mathrm{Gal}(\mathbb{M}_\infty/\mathbb{K}_\infty)/T\mathrm{Gal}(\mathbb{M}_\infty/\mathbb{K}_\infty)$ has $\mathbb{Z}_p$-rank $r_2 + v$, where $v = \mathbb{Z}_p$-rank$(A_\infty^{p^c}[T^*])$ (c is the constant of Theorem 5.1.2). Using the exact sequence

$$0 \to \mathrm{Gal}(\mathbb{M}_\infty/\mathbb{K}_\infty)/T\mathrm{Gal}(\mathbb{M}_\infty/\mathbb{K}_\infty) \to \mathrm{Gal}(\mathbb{M}_0/\mathbb{K}) \to \mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K}) \to 0$$

we obtain that $\mathrm{Gal}(\mathbb{M}_0/\mathbb{K})$ has $\mathbb{Z}_p$-rank $r_2 + 1 + v$ yielding a contradiction to the validity of Leopoldt's conjecture. So $A(T^*)$ is finite.

Let $\mathcal{T}$ be the Λ-torsion submodule of $\phi(U_\infty)$. It follows that $\mathrm{Gal}(\Omega_{E'}/\tilde{\Omega})$ is canonically pseudo isomorphic to a quotient of $\mathcal{T}/\mathcal{T}^{T^*}$ of $\mathbb{Z}_p$-rank $s-1$. Recall that $\phi(W)$

has $\mathbb{Z}_p$-rank $s-1$. As $(\phi(U_\infty)/\phi(W))(T^*)$ is finite, $\phi(W)$ generates a subgroup of the same rank in the quotient $\mathcal{T}/\mathcal{T}^{T^*}$. From this the claim follows.

□

Remark 5.3.3. *If $\mathbb{K}$ is in addition to the assumptions of Lemma 5.3.2 a CM field, then $\phi(W^+) \sim Gal(\Omega_{E'}/\Omega_E)$ and $\phi(W^-) \sim Gal(\Omega_E/\tilde{\Omega})$. To see this recall that $\Omega_{E'}/\Omega_E$ is a $\mathbb{Z}_p^r$-extension (see Lemma 5.1.10). As B_∞^+ is finite, it follows that $r = r^-$. Thus,we have $Gal(\Omega_{E'}/\Omega_E) = Gal(\Omega_{E'}/\Omega_E)^+$. As $Gal(\Omega_E/\mathbb{K}_\infty) = Gal(\Omega_E/\mathbb{K}_\infty)^-$, the claim follows.*

For the rest of this section we will make the following assumption:

Assumption 5.3.4. *$\mathbb{K}$ satisfies Leopoldt's conjecture and $(\phi(U_\infty)/\phi(W))(T^*)$ is finite.*

Lemma 5.3.5. *Let $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ be a tower of local abelian extensions such that $\mathbb{M}/\mathbb{K}$ is finite. Let $\phi_\mathbb{K}$ and $\phi_\mathbb{L}$ denote the corresponding local Artin isomorphisms. Then the following diagram commutes.*

$$\begin{array}{ccc} \mathbb{L}^\times & \xrightarrow{\phi_\mathbb{L}} & Gal(\mathbb{M}/\mathbb{L}) \\ \downarrow N & & \downarrow res \\ \mathbb{K}^\times & \xrightarrow{\phi_\mathbb{K}} & Gal(\mathbb{M}/\mathbb{K})^{ab} \end{array},$$

where G^{ab} denotes the abelianization of the group G, res is the natural restriction and N is the norm from $\mathbb{L}$ to $\mathbb{K}$.

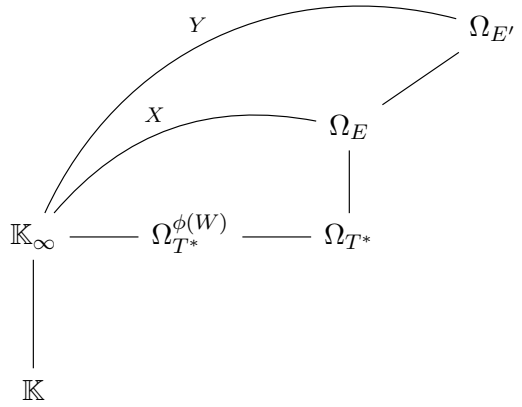
Proof. This is a well known result. As the author did not find this particular formulation in any textbook we will reprove it here. By [Iw 3, Theorem 6.9] the diagram commutes when we replace $\mathbb{M}$ by $\mathbb{L}^{ab}$, the maximal abelian extension of $\mathbb{L}$. As

$$\begin{array}{ccc} \mathrm{Gal}(\mathbb{L}^{ab}/\mathbb{L}) & \xrightarrow{res} & \mathrm{Gal}(\mathbb{M}/\mathbb{L}) \\ \downarrow res & & \downarrow res \\ \mathrm{Gal}(\mathbb{K}^{ab}/\mathbb{K}) & \xrightarrow{res} & \mathrm{Gal}(\mathbb{M}/\mathbb{K})^{ab} \end{array},$$

commutes, the claim is immediate. □

For the remainder of this section we will denote the group $\mathrm{Gal}(\Omega_E/\mathbb{K}_\infty)$ by X and $\mathrm{Gal}(\Omega_{E'}/\mathbb{K}_\infty)$ by Y. By Lemma 5.1.10 we have that $\mathbb{Z}_p$-rank$(Y/T^*Y) = r_2 + s - 1$ and that Y/X has $\mathbb{Z}_p$-rank r. We obtain that $\mathbb{Z}_p$-rank$(X/T^*X) = r_2 + s - 1 - r$. By Lemma 5.3.2 the subgroup of X/T^*X generated by the restriction of $\phi(W)$ is precisely of $\mathbb{Z}_p$-rank $s-1-r$. Let Ω_{T^*} be defined as the maximal $\mathbb{Z}_p$-free subextension of $\Omega_E^{T^*X}/\mathbb{K}_\infty$. Then $\mathrm{Gal}(\Omega_{T^*}/\Omega_{T^*}^{\phi(W)})$ is annihilated by T^* and of $\mathbb{Z}_p$-rank $s-1-r$.

Let $\mathcal{X} = \mathrm{Gal}(\Omega_{T^*}/\mathbb{K}_\infty)$. Then $\mathcal{X}$ is annihilated by T^* and $\mathbb{Z}_p$-free.



For any field $\mathbb{L}$ we denote by $P(\mathbb{L})$ the group of principal ideals generated by p-units. There is a natural map $\vartheta_n \colon E_0' \to P(\mathbb{K})/N_{n,0}(P(\mathbb{K}_n))$. Let $\tilde{E}_n = \ker(\vartheta_n)$. Let $\vartheta \colon E_0' \to P(\mathbb{K})/\bigcap_{n\in\mathbb{N}} N_{n,0}(P(\mathbb{K}_n))$ and $\tilde{E} = \ker(\vartheta)$. Note that there are constant k and c (c coprime to p) such that $(\vartheta(E_0'))^{p^k c} \cong \mathbb{Z}^r$. We have already seen in the proof of Lemma 5.1.10 that $(\vartheta(E_0'))^{cp^k}$ defines the radical for $\Omega_{E'}/\Omega_E$. Hence, $\Omega_{T^*}/\mathbb{K}_\infty(\tilde{E}^{1/p^\infty})$ is a finite extension. As $\mathrm{Gal}(\Omega_{T^*}/\mathbb{K}_\infty)$ is $\mathbb{Z}_p$-torsion free we obtain that $\Omega_{T^*} = \mathbb{K}_\infty(\tilde{E}^{1/p^\infty})$. In particular,

$$\text{the exponent of } \mathrm{Gal}(\Omega_{T^*} \cap \mathbb{M}_n/\mathbb{K}_\infty(\tilde{E}^{1/p^n})) \text{ is uniformly bounded.} \tag{5.5}$$

We obtain the following diagram

$$\begin{array}{ccc} \mathbb{K}_\infty(\tilde{E}^{1/p^n}) & \xrightarrow{\textit{bounded exponent}} & \Omega_{T^*} \cap \mathbb{M}_n \\ \big| & & \big| \\ \mathbb{K}_\infty(\tilde{E}^{1/p^n})^{\phi(W_n)} & \xrightarrow{\textit{bounded exponent}} & (\Omega_{T^*} \cap \mathbb{M}_n)^{\phi(W_n)} \end{array} .$$

Remark 5.3.6. *Note that*

$$\mathit{Gal}(\mathbb{K}_\infty(\tilde{E}^{1/p^n})/\mathbb{K}_\infty(\tilde{E}^{1/p^n})^{\phi(W_n)}) \cong \mathit{Gal}(\mathbb{K}_n(\tilde{E}^{1/p^n})/\mathbb{K}_n(\tilde{E}^{1/p^n})^{\phi(W_n)}).$$

Indeed, the natural restriction homomorphism is surjective as

$$\mathbb{K}_\infty(\tilde{E}^{1/p^n})^{\phi(W_n)} \cap \mathbb{K}_n(\tilde{E}^{1/p^n}) = \mathbb{K}_n(\tilde{E}^{1/p^n})^{\phi(W_n)}$$

and it is injective as

$$\mathbb{K}_\infty(\tilde{E}^{1/p^n}) = \mathbb{K}_\infty\mathbb{K}_n(\tilde{E}^{1/p^n}) \subset \mathbb{K}_n(\tilde{E}^{1/p^n})\mathbb{K}_\infty(\tilde{E}^{1/p^n})^{\phi(W_n)}.$$

Lemma 5.3.7. *Under Assumption 5.3.4 there are constants c_i and an index n_0 such that the quotient $\tilde{E}/\tilde{E} \cap N_{n,0}(\mathbb{K}_n^\times)$ contains a subgroup of the form $\prod_{i=1}^{s-r-1} \mathbb{Z}/p^{n-c_i}\mathbb{Z}$ for all $n \geq n_0$.*

Proof. Let $e \in \tilde{E} \setminus N_{n,0}(\mathbb{K}_n^\times)$ and let $\iota_i(e) \in \mathbb{K}_{0,i}$ be the corresponding embedding for $1 \leq i \leq s$. Then there exists an i such that $\iota_i(e) \notin N_{n,0}(\mathbb{K}_{n,i}^\times)$. Hence, the Artin-symbol of $\iota_i(e) \in \mathrm{Gal}(\mathbb{K}_{n,i}/\mathbb{K}_{0,i})$ is non-trivial. If we see $\iota_i(e)$ as element in $\mathbb{K}_{n,i}$ we obtain by Lemma 5.3.5 that the Artin-symbol of $\iota_i(e)$ in $\mathrm{Gal}(\mathbb{K}_{2n,i}/\mathbb{K}_{n,i})$ is non-trivial and by [Ne 1, Chapter 5 Proposition 3.2 (iv)] $\phi(W_{n,i})$ acts non-trivially on $\mathbb{K}_{n,i}(e^{1/p^n})$. Thus, $\mathbb{K}_n(e^{1/p^n})$ is not fixed by $\phi(W_n)$. If conversely $e \in N_{n,0}(\mathbb{K}_n^\times)$, then the Artin-symbol of $\iota_i(e)$ seen as element in $\mathbb{K}_{n,i}$ fixes $\mathbb{K}_{2n,i}$ (again by Lemma 5.3.5). Hence, $\phi(W_{n,i})$ acts trivially on $\mathbb{K}_{n,i}(e^{1/p^n})$ for all i and therefore $\phi(W_n)$ acts trivially on $\mathbb{K}_n(e^{1/p^n})$. It follows that $\tilde{E}/(\tilde{E} \cap N_{n,0}(\mathbb{K}_n^\times))$ is canonically isomorphic to the Kummer-radical for the extension $\mathbb{K}_n(\tilde{E}^{1/p^n})/\mathbb{K}_n(\tilde{E}^{1/p^n})^{\phi(W_n)}$. As the extension $\mathbb{K}_n(\tilde{E}^{1/p^n})/\mathbb{K}_n(\tilde{E}^{1/p^n})^{\phi(W_n)}$ is finite, we will show that the corresponding Galois group contains a subgroup of the desired form, then $\tilde{E}/(\tilde{E} \cap N_{n,0}(\mathbb{K}_n^\times))$ will contain such a subgroup automatically.

To simplify notation we write $\mathcal{G}_n = \mathrm{Gal}((\Omega_{T^*} \cap \mathbb{M}_n)/(\Omega_{T^*} \cap \mathbb{M}_n)^{\phi(W_n)})$ and $\mathcal{H}_n = \mathrm{Gal}(\mathbb{K}_n(\tilde{E}^{1/p^n})/\mathbb{K}_n(\tilde{E}^{1/p^n})^{\phi(W_n)})$. Consider the natural restriction homomorphism

$$\Delta_n \colon \mathcal{G}_n \to \mathcal{H}_n.$$

Note that $\mathrm{Gal}((\Omega_{T^*} \cap \mathbb{M}_n)/(\Omega_{T^*} \cap \mathbb{M}_n)^{\phi(W_n)})$ is an abelian group of uniformly bounded rank. From equation (5.5) and Remark 5.3.6 we obtain that the kernel of Δ_n is uniformly bounded. From the fact that

$$\mathbb{K}_n(\tilde{E}^{1/p^n}) \cap (\Omega_{T^*} \cap \mathbb{M}_n)^{\phi(W_n)} = \mathbb{K}_n(\tilde{E}^{1/p^n})^{\phi(W_n)}$$

we see that Δ_n is surjective.

Let p^w be an upper bound for the size of the groups $\ker(\Delta_n)$. Then we obtain an isomorphism

$$\Delta_n' \colon \mathcal{G}_n/\mathcal{G}_n[p^w] \to \mathcal{H}_n/\Delta_n(\mathcal{G}_n[p^w]).$$

Using that $\mathrm{Gal}(\mathbb{M}_n \cap \Omega_{T^*}/\mathbb{K}_\infty) \cong \mathrm{Gal}(\Omega_{T^*}/\mathbb{K}_\infty)/\omega_n \mathrm{Gal}(\Omega_{T^*}/\mathbb{K}_\infty)$, the structure theorem for noetherian Λ-torsion modules implies that for all n large enough we have $|\mathrm{Gal}(\mathbb{M}_n \cap \Omega_{T^*}/\mathbb{K}_\infty)| = p^{n(r_2+s-1-r)+c}$ as well as $|\mathrm{Gal}(\mathbb{M}_n \cap \Omega_{T^*}^{\phi(W)}/\mathbb{K}_\infty)| = p^{nr_2+d}$ for some constants c and d. As $\Omega_{T^*}^{\phi(W)} \cap \mathbb{M}_n = (\Omega_{T^*} \cap \mathbb{M}_n)^{\phi(W_n)}$, we see that $|\mathcal{G}_n| = p^{n(s-1-r)+c'}$ for some constant c'. As the p-rank of $\mathcal{G}_n$ is $s-1-r$ and $\mathrm{ord}(g_{n+1}) \leq p\mathrm{ord}(g_n)$ for all $g \in \mathrm{Gal}(\Omega_{T^*} \cap \mathbb{M}_n/\mathbb{K}_n)$ and all n large enough, there are constants c_i independent of n such that $\mathcal{G}_n/\mathcal{G}_n[p^w]$ contains a subgroup of the form $\prod_{i=1}^{s-r-1} \mathbb{Z}/p^{n-c_i}\mathbb{Z}$. Hence, the finite abelian group $\mathcal{H}_n$ contains a subgroup of the form $\prod_{i=1}^{s-r-1} \mathbb{Z}/p^{n-c_i}\mathbb{Z}$. □

Let $\Gamma_n = \Gamma/\Gamma^{p^n}$ and τ be a topological generator of Γ. Recall that we define for every Γ_n-module M the Tate-cohomology groups

$$\widehat{H}^1(M, \Gamma_n) = \frac{Ker(N_{\mathbb{K}_n/\mathbb{K}} \mid_M)}{(\tau - 1)M} \text{ and } \widehat{H}^0(M, \Gamma_n) = \frac{\ker(\tau - 1 \mid_M)}{N_{\mathbb{K}_n/\mathbb{K}}(M)}.$$

In the next lemma we describe the cohomology group $\widehat{H}^0(E_n, \Gamma_n)$ in more detail.

Lemma 5.3.8. *There is a constant k independent of n such that for all n large enough $|\widehat{H}^0(E_n, \Gamma_n)| = p^{n(s-1-r)+k}$.*

Proof. Consider the exact sequence

$$0 \to E_n \to E'_n \to E'_n/E_n \to 0.$$

As all primes above p are totally ramified in $\mathbb{K}_\infty/\mathbb{K}$, we see that $\widehat{H}^1(E'_n/E_n, \Gamma_n) = 0$. We obtain an exact sequence

$$\widehat{H}^1(E_n, \Gamma_n) \to \widehat{H}^1(E'_n, \Gamma_n) \to 0.$$

Using that $\widehat{H}^1(E'_n, \Gamma_n)$ is uniformly bounded independent of n ([Iw 2, page 267]) it suffices to compute the size of the kernel of the first homomorphism. This kernel is precisely ${E'_n}^T/{E'}_n^T$. We obtain an isomorphism $P(\mathbb{K}_n)/P(\mathbb{K}) \cong {E'_n}^T/E_n^T$ given by $(\pi) \mapsto \pi^T$. Indeed, if $\pi^T = e^T$ then $\pi/e \in \mathbb{K}$ and $(\pi) = (\pi/e) \in P(\mathbb{K})$. Let $\pi^T \in {E'_n}^T$, then (π) is in fact a preimage. So the map constructed above is indeed an isomorphism. Next we want to show that $P(\mathbb{K}_n)/P(\mathbb{K})$ has size $p^{k+n(s-r)}$ for some constant k independent of n. Let $Z(\mathbb{K}_n)$ be the free abelian group generated by the ideals above p and let B_n be the subgroup of A_n generated by the ideals only divisible by primes above p. Consider the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P(\mathbb{K}) & \longrightarrow & Z(\mathbb{K}) & \longrightarrow & B_0 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & P(\mathbb{K}_n) & \longrightarrow & Z(\mathbb{K}_n) & \longrightarrow & B_n & \longrightarrow & 0 \end{array} .$$

The lifts $P(\mathbb{K}) \to P(\mathbb{K}_n)$ and $Z(\mathbb{K}) \to Z(\mathbb{K}_n)$ are injective. From the snake lemma we obtain

$$|P(\mathbb{K}_n)/P(\mathbb{K})| = |\ker(B_0 \to B_n)| \frac{|Z(\mathbb{K}_n)/Z(\mathbb{K})|}{|B_n/\iota(B_0)|} = \frac{|B_0|}{|B_n|} |Z(\mathbb{K}_n)/Z(\mathbb{K})|.$$

As $|Z(\mathbb{K}_n)/Z(\mathbb{K})| = p^{ns}$ and $|B_n| = p^{nr+c}$ for n large enough and some constant c, we obtain $|P(\mathbb{K}_n)/P(\mathbb{K})| = p^{k+n(s-r)}$. As the Herbrand quotient $q(E_n)$ equals p^n, the lemma follows. □

There is a natural map $\delta_n \colon \widehat{H}^0(E_n, \Gamma_n) \to \tilde{E}/\tilde{E} \cap N_{n,0}(\mathbb{K}_n^\times)$: Let ε be in $\tilde{E} \setminus E_0$. Then there is a an element $\pi \in \mathbb{K}_n^\times$ such that $(\varepsilon) = (N_{n,0}(\pi))$. It follows that there is a unit $e \in E_0$ such that $e\varepsilon \in N_{n,0}(\mathbb{K}_n^\times)$. Hence, the homomorphism δ_n is surjective. This implies the following.

Lemma 5.3.9. *Under Assumption 5.3.4 there is an index n_0 such that for all $n \geq n_0$ the group $\widehat{H}^0(E_n, \Gamma_n)$ contains a subgroup of the form $\prod_{i=1}^{s-r-1} \mathbb{Z}/p^{n-c_i}\mathbb{Z}$ and the index of this subgroup in $\widehat{H}^0(E_n, \Gamma_n)$ is uniformly bounded. Further, $|\ker(\delta_n)|$ is uniformly bounded.*

Proof. By Lemma 5.3.7 the group $\tilde{E}/\tilde{E} \cap N_{n,0}(\mathbb{K}_n^\times)$ contains a subgroup of the form $\prod_{i=1}^{s-r-1} \mathbb{Z}/p^{n-c_i}\mathbb{Z}$. As δ_n is surjective, the same follows for $\widehat{H}^0(E_n, \Gamma_n)$. By Lemma 5.3.8 it follows that the index of this subgroup in $\widehat{H}^0(E_n, \Gamma_n)$ is uniformly bounded and also that the kernel of δ_n is uniformly bounded. □

Lemma 5.3.10. *Under assumption 5.3.4 the homomorphism $\widehat{T}\colon A'_\infty[T^*] \to B_\infty$ defined as in Lemma 5.1.15 has the following property.*

$$\ker(\widehat{T}) \text{ is finite.}$$

Proof. Let $a_n = c_n B_n$ and assume that $\widehat{T}a_n = b_n = 1$. Let $\mathfrak{A} \in c_n$. Then $\mathfrak{A}^T = (\alpha)$. It follows that $N_{n,0}(\alpha) \in E_0$ and hence $N_{n,0}(\alpha)N_{n,0}(E_n) \in ker(\delta_n)$. By Lemma 5.3.9 we obtain that there is a constant c independent of n such that $N_{n,0}(\alpha)^{p^c} \in N_{n,0}(E_n)$ and therefore $a_n^{p^c} \in \ker(\psi_n)$ for all n (here ψ_n is defined as in Lemma 5.1.13). Hence, $a^{p^c} = 0$ by Lemma 5.1.14. As $A'[T]$ has finite rank as $\mathbb{Z}_p$-module, this gives the claim. □

As an immediate corollary we obtain

Corollary 5.3.11. *If B_∞ is finite and Assumption 5.3.4 holds for $\mathbb{K}$, then the Gross-Kuz'min conjecture holds.*

Remark 5.3.12. *Let $a \in A'_\infty[T]$ generate an infinite $\mathbb{Z}_p$-module and let $b = \widehat{T}a$. Let $a_n = c_n B_n$ and $\mathfrak{A}_n \in c_n$ as in the proof of Lemma 5.1.13. Then we can write $\mathfrak{A}_n^T = (\alpha_n)\mathfrak{B}_n$ for an ideal $\mathfrak{B}_n$ in b_n only divisible by primes above p. Let $(\beta_n) = \mathfrak{B}_n^{\mathrm{ord}(b_n)}$. Then there are constants c and c' such that $(\beta_n)^c = (N_{n,0}(\alpha_n))^{c'}$.*

Note that this is Remark 5.2.9. But this time we do not restrict to the minus part but to a cyclic subgroup on which $\widehat{T}$ is injective.

Now we have all ingredients to finish the proof of Theorem 5.0.4.

Proof of Theorem 5.0.4 – second implication. Let $a \in A'_\infty[T]$ be a class of infinite order. Then by Lemma 5.3.10 $\widehat{T}$ acts injectively on $\mathbb{Z}_p a$. By Remark 5.1.9 we see that $\Omega_E(N_{n,0}(E'_n)^{1/p^n}) = \Omega_E$. Let $b = \widehat{T}a$, $\mathfrak{B}_n \in b_n$ and $\mathfrak{B}_n^{ord(b_n)} = (\beta_n)$. Let α_n be as in Remark 5.3.12. Then we have $(N_{n,0}(\alpha_n))^{c'} = (\beta_n)^c$ (see Remark 5.3.12). Let $l(n) = min(p^n, \mathrm{ord}(b_n))$. We obtain that $\Omega_E(N_{n,0}(\alpha_n)^{c'/l(n)}) = \Omega_E(\beta_n^{c/l(n)})$. Note that there is an n_0 such that for all $n \geq n_0$ we have $p \cdot l(n) = l(n+1)$ and $\mathrm{ord}(b_n)/l(n) = \mathrm{ord}(b_{n_0})/l(n_0)$. By Lemma 5.1.8 we get that

$$\mathbb{F} = \bigcup_{n \geq n_0} \Omega_E(N_{n,0}(\alpha_n)^{c'/l(n)}) = \bigcup_{n \geq n_0} \Omega_E(\beta_n^{c/l(n)})$$

defines a $\mathbb{Z}_p$-extension in $\Omega_{E'}/\Omega_E$. As in the proof of Theorem 5.2.6 we have

$$N_{n,0}(\mathbb{K}_{n,i}^\times) \subset \pi_{0,i}^{\mathbb{Z}} \times \widehat{N}_{0,i} \times W_{0,i} \times U_{0,i}^{p^n} \times V_{0,i} \subset \pi_{m,i}^{\mathbb{Z}} \times \widehat{N}_{m,i} \times W_{m,i} \times V_{m,i} \times U_{m,i}^{p^n}$$

for all $m \geq 0$. Let $\delta_n \in N_{n,0}(\mathbb{K}_n)$ be a representative for $\psi_n(a_n) \in E'_0/N_{n,0}(E'_n)$. Recall from Remark 5.1.9 that $\Omega_E(N_{n,0}(\alpha_n)^{1/l(n)}) = \Omega_E(\delta_n^{1/l(n)})$. By Lemma 5.1.17

we obtain that $\phi(W_{m,i})$ acts trivially on the field $\mathbb{K}_n(\delta_n^{1/l(n)})$ for all $m \geq n$ and $1 \leq i \leq s$. Let $W_E \subset W$ be the maximal subgroup such that $\phi(W_E)$ fixes Ω_E. Let $W_{E,m}$ be the maximal subgroup of W_m such that $\phi(W_{E,m})$ fixes $\Omega_E \cap \mathbb{M}_m$. It follows that $\phi(W_{E,m})$ fixes $(\Omega_E \cap \mathbb{M}_n)(\delta_n^{1/l(n)})$ for all $m \geq n$. Using that $\bigcup_{n \geq n_0}(\Omega_E \cap \mathbb{M}_n)(\delta_n^{1/l(n)}) = \mathbb{F}$ we see that $\phi(W_E)$ fixes $\mathbb{M}$. But by Lemma 5.3.2 $\phi(W)$ generates by restriction a subgroup of finite index in $\mathrm{Gal}(\Omega_{E'}/\tilde{\Omega})$. In particular, $\phi(W_E)$ generates $\mathrm{Gal}(\Omega_{E'}/\Omega_E)$ up to finite index, yielding a contradiction to the existence of $\mathbb{F}$. □

5.4 Outlook

If we want to apply our equivalent formulation of the Gross-Kuz'min conjecture to construct fields in which the Gross-Kuz'min conjecture holds, we have two major obstacles:

- We do not have a canonical extension $\Omega_{E'}^+/\mathbb{K}_\infty$ such that $\Omega_{E'} = \Omega_E\Omega_{E'}^+$. We can still find a $\mathbb{Z}_p^r$ extension with this property but it depends on the choice of the p-units we take as generators for the radical.

- If we want to verify that $(U_\infty/\overline{E}_\infty W)(T^*)$ is finite it is no longer sufficient to consider $\Omega_{E'}/\Omega_E$. In fact we have seen above that, if the Gross conjecture is true, there is a non-trivial action of $\phi(W)$ on Ω_E and it is not clear how one can describe the radical of Ω_E/Ω_E^Z and how W acts on it.

Chapter 6

A conditional proof of Leopoldt's conjecture

The results in this chapter stem from joint work with Preda Mihăilescu torwards a proof of Leopoldt's conjecture. Preda Mihăilescu recently gave a much simpler proof of Theorem 6.2.1 not using group cohomology but a simple counting argument instead. We still provide a full proof here as the author is convinced that the analysis of the cohomology groups gives additional insight.

Throughout this section we will assume that $p > 2$ and $\mathbb{K}$ is a CM number field. Let $\mathbb{K}_\infty/\mathbb{K}$ be a CM $\mathbb{Z}_p$-extension. Let A_n be the p-class group of the field $\mathbb{K}_n$ and define $A_\infty = \lim_{\infty\leftarrow n} A_n$. It is well known that A_∞^- is a finitely generated Λ-torsion module and pseudo isomorphic to a module of the form

$$\bigoplus_{i=1}^{k} \Lambda/p^{e_i} \bigoplus \bigoplus_{j=1}^{s} \Lambda/f_j(T)^{d_j}$$

for irreducible distinguished polynomials $f_j(T)$. As in Chapter 1 we define $\mu(A_\infty^-) = \sum_{i=1}^k e_i$ and $\lambda(A_\infty^-) = \sum_{j=1}^s \deg(f_j(T))d_j$. We will refer to the following conjecture as $\mu = 0$ conjecture:

Conjecture 6.0.1. *For any CM $\mathbb{Z}_p$-extension of a number field $\mathbb{K}$ we have*

$$\mu(A_\infty^-) = 0.$$

If $\mathbb{K}_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension and if $\zeta_p \in \mathbb{K}$ it is well known [Wash, Proposition 13.24] that $\mu(A_\infty) = 0$ if and only if $\mu(A_\infty^-) = 0$. Note that the cyclotomic $\mathbb{Z}_p$-extension is the only CM $\mathbb{Z}_p$-extension of $\mathbb{K}$, if $\mathbb{K}$ satisfies Leopoldt's conjecture (we give the precise statement below). To abbreviate notation we will also write μ and μ^- for $\mu(A_\infty)$ and $\mu(A_\infty^-)$, respectively.

The second conjecture we want to consider in this chapter is the Leopoldt conjecture:

Conjecture 6.0.2 (Leopoldt's conjecture)**.** *Let E be the units of $\mathbb{K}$ and $\overline{E}$ their p-adic closure in U. Then $\mathbb{Z}_p$-rank$(\overline{E}) = \mathbb{Z}$-rank$(E)$.*

This conjecture can be reformulated as follows.

Conjecture 6.0.3 (Leopoldt's conjecture – second statement)**.** $\mathbb{K}$ *admits exactly* $r_2 + 1$ *independent* $\mathbb{Z}_p$*-extensions, where* r_2 *denotes the number of pairs of complex conjugate embeddings of* $\mathbb{K}$*.*

It is easy to show that each number fields has at least $r_2 + 1$ independent $\mathbb{Z}_p$-extensions. Thus, to prove Leopoldt's conjecture it suffices to prove that $r_2 + 1$ is an upper bound.

Both conjectures, the Leopoldt conjecture and the $\mu = 0$ conjecture have the property that they remain false under finite extensions of the base field. These results are folklore and were already known by Iwasawa [Iw 2].

Lemma 6.0.4. *Let* $\mathbb{L}/\mathbb{K}$ *be a finite Galois extension of CM number fields. Assume that the Leopoldt conjecture or the* $\mu = 0$ *conjecture does not hold for* $\mathbb{K}$*. Then they do not hold for* $\mathbb{L}$*.*

To analyze the Leopoldt conjecture more carefully we need the following reformulation of the Leopoldt conjecture.

Lemma 6.0.5. *Let* $\mathbb{K}$ *be a CM number field. Then the Leopoldt conjecture fails for* $\mathbb{K}$ *if and only if* $\mathbb{K}$ *admits at least two CM* $\mathbb{Z}_p$*-extensions.*

Proof. Let U be the local units of $\mathbb{K}$ as defined in the introduction and $\overline{E}$ the closure of the image of the group of units of $\mathbb{K}$ in U. Let $\mathbb{M}$ be the maximal p-ramified, p-abelian extension of $\mathbb{K}$ and $\mathbb{H}$ the p-Hilbert class field of $\mathbb{K}$. Then by [Wash, Corollary 13.6] and the definition of U

$$\mathrm{Gal}(\mathbb{M}/\mathbb{H}) \cong U/\overline{E}.$$

U has $\mathbb{Z}_p$-rank $2r_2 = [\mathbb{K} : \mathbb{Q}]$ and $\overline{E}$ has the rank $r_2 - 1 - \delta$, where δ denotes the Leopoldt defect. δ is a non-negative integer and vanishes if and only if the Leopoldt conjecture is true for $\mathbb{K}$. As usual, let j denote the complex conjugation then E^{1-j} is a finite group and we see that $\mathbb{Z}_p\text{-rank}(U^{1-j}/(U^{1-j} \cap \overline{E})) = \mathbb{Z}_p\text{-rank}(U^{1-j}) = r_2$. As $p \neq 2$ there is a decomposition $U = U^{1-j} \oplus U^{1+j}$ and we see that there are exactly $1 + \delta$ independent $\mathbb{Z}_p$-extensions that are fixed by U^{1-j}. Let $\mathbb{M}$ be the compositum of these $\mathbb{Z}_p$-extensions then $\mathrm{Gal}(\mathbb{M}/\mathbb{H})$ is annihilated by $(1 - j)$. Let $\mathbb{M}^+ \subset \mathbb{M}$ be the maximal subextension of $\mathbb{M}$ that is abelian over $\mathbb{K}^+$, the maximal real subfield of $\mathbb{K}$. Then $\mathrm{Gal}(\mathbb{M}^+/\mathbb{K}^+)$ has $\mathbb{Z}_p$-rank $1 + \delta$ and all $\mathbb{Z}_p$-extensions in $\mathbb{M}^+\mathbb{K}$ are indeed CM extensions. □

Now we have all ingredients to prove Lemma 6.0.4.

Proof of Lemma 6.0.4. Assume first that the Leopoldt conjecture is false for $\mathbb{K}$. Then $\mathbb{K}$ admits at least two CM $\mathbb{Z}_p$-extension (one of these extensions is the cyclotomic $\mathbb{Z}_p$-extension). As $\mathbb{L}/\mathbb{K}$ is finite the same holds for $\mathbb{L}$.

Assume now that the $\mu = 0$ conjecture is false for $\mathbb{K}$ and recall that $\mathbb{H}_\infty^- = \mathbb{H}_\infty^{A_\infty^+}$. We have a short exact sequence

$$0 \to \mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})\mathbb{L}_\infty/\mathbb{L}_\infty) \to \mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})\mathbb{L}_\infty/\mathbb{K}_\infty) \to \mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}_\infty) \to 0$$

As $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})/\mathbb{K}_\infty)$ is a quotient of $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})\mathbb{L}_\infty/\mathbb{K}_\infty)$ and $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})/\mathbb{K}_\infty)$ has infinite p-rank, the same holds for $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})\mathbb{L}_\infty/\mathbb{K}_\infty)$. The term $\mathrm{Gal}(\mathbb{L}_\infty/\mathbb{K}_\infty)$ is finite by assumption. Therefore, $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})\mathbb{L}_\infty/\mathbb{L}_\infty)$ has a positive μ-invariant. As $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{K})\mathbb{L}_\infty/\mathbb{L}_\infty)$ is a quotient of $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{L})/\mathbb{L}_\infty)$ the same follows for the group $\mathrm{Gal}(\mathbb{H}_\infty^-(\mathbb{L})/\mathbb{L}_\infty)$. □

In view of Lemma 6.0.4 we impose the following conditions on our base field $\mathbb{K}$:

- $\mathbb{K}$ is a *CM* field and Galois over $\mathbb{Q}$.
- $\zeta_p \in \mathbb{K}$.
- The cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ is totally ramified at all ideals above p.

6.1 Radicals and their cohomologies

Vlad Crişan developed in his thesis the theory of projective radicals for $\mathbb{Z}_p$-free Galois extensions $\mathbb{F}/\mathbb{K}_\infty$ of finite rank [Cr]. In the following we will show that it is also possible to construct projective radicals for extensions of μ-type, i.e. for extensions of finite exponent but infinite rank.

Assume that $\zeta_{p^k} \in \mathbb{K}$. Let $\mathbb{L}/\mathbb{K}$ be a finite Kummer extension of exponent p^k. Let $\mathbb{K}' \subset \mathbb{K}$ be a subfield such that $\mathbb{L}/\mathbb{K}'$ and $\mathbb{K}/\mathbb{K}'$ are Galois. There is a natural action of $\Gamma = \mathrm{Gal}(\mathbb{K}/\mathbb{K}')$ on $X = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Let B be the Kummer-radical of $\mathbb{L}/\mathbb{K}$. Then Γ acts naturally on B as well. We write $X \leftrightarrow B$ to indicate that B is the Kummer-radical for an extension with Galois group X and vice versa. There is a canonical non-degenerate Kummer pairing

$$\langle \cdot, \cdot \rangle \colon B \times X \to \mu_{p^k}$$

such that $\langle \rho, x \rangle = \frac{x(\rho^{1/p^k})}{\rho^{1/p^k}}$. Consider the canonical restriction of the cyclotomic character

$$\chi \colon \Gamma \to (\mathbb{Z}/p^k\mathbb{Z})^\times, \qquad \gamma(\zeta_{p^k}) = \zeta_{p^k}^{\chi(\gamma)}.$$

Note that $\langle \gamma\rho, x \rangle = \langle \rho, \chi(\gamma)\gamma^{-1}x \rangle$ (this is a simple reformulation of the equivariance of the Kummer pairing [Gu, Theorem 1.26]). To simplify notation we write $\gamma^* = \chi(\gamma)\gamma^{-1}$. Thus, $*$ induces an involution on the group ring $(\mathbb{Z}/p^k)[\Gamma]$. With these definitions, we have the following relations:

Lemma 6.1.1. *Let $f \in (\mathbb{Z}/p^k)[\Gamma]$. Then $f \colon X \to X$ induces a group homomorphism and we obtain*

$$|X| = |fX| \cdot |X[f]| = |B| = |B[f^*]| \cdot |f^*B|, \tag{6.1}$$

$$B[f^*] \leftrightarrow X/fX \tag{6.2}$$

$$B/f^*B \leftrightarrow X[f]. \tag{6.3}$$

Proof. Since $X \cong B$ as $\mathbb{Z}_p$-modules, we obviously have $|X| = |B|$. The other two equalities in (6.1) follow directly from the isomorphism theorem for finite modules. Next we prove (6.2). Let $\mathbb{L}' = \mathbb{L}^{fX}$ be the field fixed by fX. Let $B_f \subset B$ be the Kummer radical of $\mathbb{L}'$. For every $fx \in fX$ and every $\rho \in B_f$ we obtain

$$1 = \langle \rho, fx \rangle = \langle f^*\rho, x \rangle$$

As this holds for all $x \in X$ we see that X acts trivially on $\mathbb{K}((f^*B_f)^{1/p^k})$. The pairing is non-degenerate and we obtain that $f^*B_f = \{0\}$ as well as $B_f \subset B[f^*]$. Let now $\rho \in B[f^*]$ then

$$\langle \rho, fx \rangle = \langle f^*\rho, x \rangle = 1.$$

So fX acts trivially on $\mathbb{K}(B[f^*]^{1/p^k})$ which implies $B[f^*] \subset B_f$. Hence, $B_f = B[f^*]$ and (6.2) follows.

For (6.3) define $\mathbb{L}' = \mathbb{L}^{X[f]}$ and let $B'_f \subset B$ be the radical of $\mathbb{L}'/\mathbb{K}$. There is a natural homomorphism

$$B \to \mathbb{L}'/{\mathbb{L}'}^{p^k},$$

whose kernel is B'_f. Therefore, $X[f] \leftrightarrow B/B'_f$. It remains to show that $B'_f = f^*B$. Let $f^*\rho \in f^*B$ and $x \in X[f]$ then

$$\langle f^*\rho, x \rangle = \langle \rho, fx \rangle = 1.$$

As this holds for all $\rho \in B$ we see that $X[f]$ acts trivially on $\mathbb{K}((f^*B)^{1/p^k})$. Hence, $f^*B \subset B'_f$. Let $\tilde{\mathbb{L}} = \mathbb{K}((f^*B)^{1/p^k}) \subset \mathbb{L}'$ and let $Y \subset X$ be the fixing group of $\tilde{\mathbb{L}}$. Let $f^*\rho \in f^*B$ and $x \in Y$. Then

$$1 = \langle f^*\rho, x \rangle = \langle \rho, fx \rangle$$

As this holds for all ρ, the non-degeneracy of the pairing implies that $fx = 0$. Hence, $Y \subset X[f]$ and $\mathbb{L}' = \mathbb{L}^{X[f]} \subset \tilde{\mathbb{L}} = \mathbb{L}^Y$. We showed already that $\tilde{\mathbb{L}} \subset \mathbb{L}'$. Thus, we obtain equality and indeed (6.3). □

Assume for the remainder of this section that $\mathbb{K}/\mathbb{K}'$ is cyclic. Let γ be a generator. Then we can write the algebraic norm as $N = \sum_{i=1}^{[\mathbb{K}:\mathbb{K}']} \gamma^i$ and $\Delta = \gamma - 1$. The Tate cohomologies of $\widehat{H}^i(\Gamma, X), i = 0, 1$ are defined as usual:

$$\widehat{H}^0(\Gamma, X) = \frac{X[\Delta]}{NX}, \quad \widehat{H}^1(\Gamma, X) = \frac{X[N]}{\Delta X}.$$

To use the correspondence we proved in Lemma 6.1.1 we define the cohomologies for B with respect to the twisted action:

$$\widehat{H}^0(\Gamma, B) = \frac{B[\Delta^*]}{N^*B}, \quad \widehat{H}^1(\Gamma, B) = \frac{B[N^*]}{\Delta^*B}.$$

With these definition, we deduce from Lemma 6.1.1

Corollary 6.1.2. *We have the following relations:*

$$\widehat{H}^0(\Gamma, B) \leftrightarrow \widehat{H}^1(\Gamma, X) \quad \textit{and} \quad \widehat{H}^1(\Gamma, B) \leftrightarrow \widehat{H}^0(\Gamma, X). \tag{6.4}$$

Proof. Consider the fields $\mathbb{L}' = \mathbb{L}^{X[\Delta]} \subseteq \mathbb{L}'' = \mathbb{L}^{NX}$. We obtain

$$\mathrm{Gal}(\mathbb{L}''/\mathbb{L}') \cong X[\Delta]/NX \cong \widehat{H}^0(\Gamma, X). \tag{6.5}$$

In view of (6.2) we have,

$$\mathrm{Gal}(\mathbb{L}''/\mathbb{K}) \leftrightarrow B[N^*].$$

There is a natural homomorphism

$$B \to \mathbb{L}'/\mathbb{L}'^{p^k}. \tag{6.6}$$

By (6.3) we know that $X[\Delta] \leftrightarrow B/\Delta^* B$. Therefore, the kernel of the natural projection (6.6) is $\Delta^* B$ and we obtain

$$\mathrm{Gal}(\mathbb{L}'/\mathbb{K}) \leftrightarrow \Delta^* B.$$

Hence,

$$\mathrm{Gal}(\mathbb{L}''/\mathbb{L}') \leftrightarrow B[N^*]/\Delta^* B \cong \widehat{H}^1(\Gamma, B).$$

Together with (6.5) we obtain $\widehat{H}^1(\Gamma, B) \leftrightarrow \widehat{H}^0(\Gamma, X)$.

For the second implication consider $\mathbb{L}' = \mathbb{L}^{X[N]} \subseteq \mathbb{L}'' = \mathbb{L}^{\Delta X}$. Then

$$Gal(\mathbb{L}''/\mathbb{L}') \cong X[N]/\Delta X = \widehat{H}^1(\Gamma, X)$$

We know from (6.2) that $\mathrm{Gal}(\mathbb{L}''/\mathbb{K}) \cong X/\Delta X \leftrightarrow B[\Delta^*]$. From (6.3) we have

$$X[N] \leftrightarrow B/N^* B.$$

Hence, $N^* B$ is the kernel of the natural map $B \to \mathbb{L}'/\mathbb{L}'^{p^k}$. Therefore,

$$\mathrm{Gal}(\mathbb{L}'/\mathbb{K}) \leftrightarrow N^* B.$$

We obtain

$$\mathrm{Gal}(\mathbb{L}''/\mathbb{L}') \leftrightarrow B[\Delta^*]/N^* B \cong \widehat{H}^0(\Gamma, B).$$

□

We want to apply these general results to indicate that we can define norm coherent radicals for μ-type subfields of $\mathbb{H}_\infty/\mathbb{K}_\infty$. Let $\mathbb{H}_\mu$ be the maximal subextension of $\mathbb{H}_\infty^-$ such that $X = \mathrm{Gal}(\mathbb{H}_\mu/\mathbb{K}_\infty)$ is of finite exponent and does not contain a finite Λ-submodule. Let $\mathbb{M}_k$ be the maximal p-abelian p-ramified extension of $\mathbb{K}_k$ and $\mathbb{M}_k^-$ the fixed field under the pluspart. We define $\overline{\mathbb{H}}_k = \mathbb{H}_\mu \cap \mathbb{M}_k^-$ for all k and $X_k = \mathrm{Gal}(\overline{\mathbb{H}}_k/\mathbb{K}_k)$. Note that $X_k = X/\omega_k X$. The multiplication with $\nu_{k,k+v}$ induces a homomorphism

$$\psi_{k,k+v} \colon X_k \to X_{k+v}.$$

As X does not contain $\nu_{k,k+v}$-torsion this homomorphism is injective. Let

$$\phi_{k,k+v}\colon X_{k+v} \to X_k$$

be the natural restriction homomorphism. Let

$$\cdot\nu_{k,k+v}\colon X_{k+v} \to X_{k+v}$$

be the homomorphism on X_{k+v} sending x to $\nu_{k,k+v}x$. Clearly $\cdot\nu_{k,k+v} = \psi_{k,k+v}\circ\phi_{k,k+v}$. As $\psi_{k,k+v}$ is injective and $\ker(\phi_{k,k+v}) = \omega_k X_{k+v}$ we see that $\ker(\cdot\nu_{k,k+v}) = \omega_k X_{k+v}$.

The exponent of X_k is uniformly bounded by p^l. Assume that there is an index n_0 such that $\mathbb{K}_n$ contains μ_{p^l} for all $n \geq n_0$. Note that $\omega_n \equiv -\tau^{p^n}\omega_n^* \mod p^n$, where τ is a topological generator of $\mathrm{Gal}(\mathbb{K}_\infty/\mathbb{K})$. So we can choose n_0 large enough such that $\omega_n \equiv -\tau^{p^n}\omega_n^* \mod p^l$ for all $n \geq n_0$. Let B_n be the radical of $\overline{\mathbb{H}}_n/\mathbb{K}_n$. As $\mathbb{K}_\infty/\mathbb{K}_n$ is disjoint to $\overline{\mathbb{H}}_n/\mathbb{K}_n$ we see that the natural homomorhism $B_n \to B_{n'}$ is injective for all $n' \geq n \geq n_0$.

Lemma 6.1.3. *For $n' \geq n > n_0$ we have $B_{n'}[\omega_n] = B_n$ and $B_n = N_{n',n}(B_{n'})$.*

Proof. Let $\rho \in \mathbb{K}_{n'}$ be a representative of a class z in $B_{n'}$. As by Kummer duality $B_{n'}^{1-j} = 1$ and $p \neq 2$ we can assume that $\rho^{1-j} = 1$. Then $N_{n',n}(\rho) \in \mathbb{K}_n$ and $\mathbb{W}_n = \mathbb{K}_n(N_{n',n}(\rho)^{1/p^l})/\mathbb{K}_n$ is abelian over $\mathbb{K}_n$. As $\overline{\mathbb{H}}_{n'}/\mathbb{K}_n$ is Galois we see that $\mathbb{W}_n \subset \overline{\mathbb{H}}_{n'}$. Hence, $\mathbb{W}_n/\mathbb{K}_n$ is unramified outside p and $\mathbb{W}_n\mathbb{K}_\infty \subset \mathbb{H}_\mu$. Therefore, $\mathbb{W}_n \subset \overline{\mathbb{H}}_n$. This shows that $N_{n',n}(B'_n) \subset B_n$ for all possible choices of n and n'.

We have already seen that $\ker(\nu_{n,n'} \mid X_{n'}) = \omega_n X_{n'}$. As $\nu_{n,n'} = \sum_{g\in\mathrm{Gal}(\mathbb{K}_{n'}/\mathbb{K}_n)} g$ it follows that $\widehat{H}^1(\mathrm{Gal}(\mathbb{K}_{n'}/\mathbb{K}_n), X_{n'}) = 0$. By Lemma 6.1.2 this implies that the group $\widehat{H}^0(\mathrm{Gal}(\mathbb{K}_{n'}/\mathbb{K}_n), B_{n'})$ is trivial. Thus, $B_{n'}[\omega_n^*] = N_{n',n}^*(B_{n'})$. As $\omega_n \equiv -\tau^{p^n}\omega_n^* \mod p^l$ and $\nu_{n,n'} = \sum_{g\in\mathrm{Gal}(\mathbb{K}_{n'}/\mathbb{K}_n)} g \equiv \sum_{g\in\mathrm{Gal}(\mathbb{K}_{n'}/\mathbb{K}_n)} \chi(g^{-1})g = \nu_{n,n'}^*$ we see that

$$B_{n'}[\omega_n] = B_{n'}[\omega_n^*] = N_{n',n}(B_{n'}).$$

Therefore,

$$B_n \subset B_{n'}[\omega_n] = N_{n',n}(B_{n'}) \subset B_n$$

from which the claim is immediate. □

Remark 6.1.4. *The condition that $\mathbb{K}_n$ contains μ_{p^l} for n large enough is trivially satisfied for the cyclotomic $\mathbb{Z}_p$-extension of a number field containing the p-th roots of unity. If $\mathbb{K}_\infty$ is not the cyclotomic $\mathbb{Z}_p$-extension, i.e. a Leopoldt defect extension then the extension $\mathbb{K}_\infty(\zeta_{p^l})/\mathbb{K}_\infty$ is finite. So we can just replace $\mathbb{K}$ by $\mathbb{K}(\zeta_{p^l})$ and $\mathbb{K}_\infty$ by $\mathbb{K}_\infty(\zeta_{p^l})$.*

6.2 Thaine lifts

We know already that if the μ-conjecture or the Leopoldt conjecture are false for a certain number field then they remain false upon shifting the base field $\mathbb{K}$ by a finite Galois extension. Nevertheless these shifts enable us to use group cohomological tools on our obstruction fields. Using these shifts we will prove the following

Theorem 6.2.1. *If $\mu(A_\infty^-) = 0$ for all CM $\mathbb{Z}_p$-extensions, then Leopoldt's conjecture holds for $\mathbb{K}$.*

6.2.1 The split Thaine lift

Assume that Leopoldt's conjecture does not hold for $\mathbb{K}$. Let $\mathbb{K}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{K}$ with intermediate fields $\mathbb{K}_n$. In the following we will show that we can construct a finite shift of $\mathbb{K}$ and a CM $\mathbb{Z}_p$-extension $\mathbb{L}_\infty$ such that $\mu(A_\infty^-) > 0$. Let $N > 1$ and choose a principal prime Q in $\mathbb{K}_N$ that is totally split in $\mathbb{K}_N/\mathbb{Q}$ and inert in $\mathbb{K}_\infty/\mathbb{K}_N$. Let Ω_N^+ be the compositum of all CM $\mathbb{Z}_p$-extensions of $\mathbb{K}$ containing $\mathbb{K}_N$. Clearly, $\mathbb{K}_\infty \subset \Omega_N^+$.

Lemma 6.2.2. *We have*

$$\mathbb{Z}_p\text{-rank}(\mathit{Gal}(\Omega_N^+/\mathbb{K})) > 1.$$

Proof. Let $\mathbb{K}'_\infty \neq \mathbb{K}_\infty$ be a CM $\mathbb{Z}_p$-extension of $\mathbb{K}$ that is independent from the cyclotomic one. Such an extension exists as the Leopoldt conjecture is false for $\mathbb{K}$ (see lemma 6.0.5). Then $G = \mathrm{Gal}(\mathbb{K}_\infty\mathbb{K}'_\infty/\mathbb{K}) \cong \mathbb{Z}_p^2$. Clearly, $\mathbb{K}_N \subset (\mathbb{K}_\infty\mathbb{K}'_\infty)^{p^mG}$ for all $m \geq N$. Define $\mathbb{L}'_N = \mathbb{K}_N$. We will inductively construct cyclic extensions $\mathbb{L}'_m$ of $\mathbb{K}$ such that

$$\mathbb{L}_N \subset \mathbb{L}'_{N+1} \subset \cdots \subset \mathbb{L}'_m \subset \ldots$$

and such that $\mathbb{L}'_m \cap \mathbb{K}_\infty = \mathbb{K}_N$. Assume that we have already defined the field $\mathbb{L}'_m$. Let $H \subset G/p^mG$ be the subgroup fixing $\mathbb{L}'_m$. According to [Kl 1, page 42-43] there are exactly $p+1$ cyclic subgroups H' in $G/p^{m+1}G$ that restrict to H under the natural projection

$$G/p^{m+1}G \to G/p^mG.$$

If $m = N$ choose H' such that the fixed field of H in $(\mathbb{K}_\infty\mathbb{K}'_\infty)^{p^{N+1}G}$ is not equal to $\mathbb{K}_{N+1}$. If $m > N$ choose one arbitrary group among the possible candidates for H'. Define $\mathbb{L}'_{m+1}$ as the fixed field of H' in $(\mathbb{K}_\infty\mathbb{K}'_\infty)^{p^{m+1}G}$. Then the extension $\mathbb{L}'_\infty = \bigcup_{m\geq N} \mathbb{L}'_m$ defines a $\mathbb{Z}_p$-extension of $\mathbb{K}$ such that $\mathbb{L}'_\infty \cap \mathbb{K}_\infty = \mathbb{K}_N$. This proves that there are at least two independent $\mathbb{Z}_p$-extensions that contain $\mathbb{K}_N$. □

Clearly, $\Omega_N^+/\mathbb{K}$ is unramified outside p. Let $D(Q)$ be the decomposition group of Q in $\mathrm{Gal}(\Omega_N^+/\mathbb{K}_N)$. Let q be the rational prime below Q. As any finite extension of $\mathbb{Q}_p$ admits only one unramified $\mathbb{Z}_p$-extension we see that $D(Q) \cong \mathbb{Z}_p$. In particular, there is a $\mathbb{Z}_p$-extension $\mathbb{K}'_\infty \subset \Omega_N^+$ such that Q is totally split in $\mathbb{K}'_\infty/\mathbb{K}_N$. Let τ be a topological generator of $\mathrm{Gal}(\mathbb{K}'_\infty/\mathbb{K}_N)$ and define the Iwasawa algebra Λ with respect to τ.

Let q be a rational prime below Q. Then we see that $q \equiv 1 \mod p^N$. So we can extract a subfield $\mathbb{F}$ of degree p in $\mathbb{Q}(\zeta_q)/\mathbb{Q}$. Define $\mathbb{L}_n = \mathbb{K}'_n\mathbb{F}$ and $\mathbb{L}_\infty = \mathbb{K}'_\infty\mathbb{F}$. Let $\Phi = \mathrm{Gal}(\mathbb{L}_n/\mathbb{K}'_n)$ and let σ be a generator. Define, as usual, $s = \sigma - 1$ and $\mathcal{N} = \sum_{i=0}^{p-1} \sigma^i$. In the following we want to analyze the cohomology groups $\widehat{H}^0(\Phi, A_n^-(\mathbb{L}))$. To simplify notation we will write A_n^- for $A^-(\mathbb{L}_n)$. For each n we fix an ideal Q_n above Q in $\mathbb{K}'_n$ and an ideal $\tilde{Q}_n$ above Q_n in $\mathbb{L}_n$. Without loss of generality we can

assume that the Q_n and the $\tilde{Q}_n$ form a norm coherent sequence. We obtain the following lower bound on the size of the cohomology groups.

Lemma 6.2.3. *We have*

$$|\widehat{H}^0(\Phi, A_n^-)| = |\widehat{H}^1(\Phi, A_n^-)| \geq p^{p^{n-N}} \quad \text{for all } n \geq N.$$

Further, $\widehat{H}^0(\Phi, A_n^-)$ contains a Λ-cyclic submodule generated by the class of $\tilde{Q}_n^{1-j}$ that is isomorphic to $\Lambda/(p, \omega_{n-N})$.

Proof. As a first step we will show that $\widehat{H}^0(\Phi, A_n^-)$ is generated by B_n^-, the submodule of A_n^- generated by the primes above q. Let $a \in A_n^-(\mathbb{L}_n)$ such that $a_n^s = 1$. Let $\mathfrak{A}$ be an ideal in a and $\mathfrak{A}^s = (\xi)$. By definition $\mathcal{N}(\xi^{1-j}) = \mu'$ for some root of unity μ' in $\mathbb{K}_n$. Let l be maximal such that $\mathbb{K}_N$ contains the p^l-th roots of unity. Then $\mathbb{K}'_{n,Q_n} \cong \mathbb{K}_{N,Q}$. As Q is inert in $\mathbb{K}_\infty/\mathbb{K}_N$ it follows that $\zeta_{p^{l+1}} \notin \mathbb{K}_{N,Q} \cong \mathbb{K}'_{n,Q_n}$. As $\mathbb{L}_n/\mathbb{K}_n$ is tamely ramified the Hasse norm principle implies that $W(\mathbb{K}_n) \cap \mathcal{N}(\mathbb{L}_n) = W(\mathbb{K}_n)^p$. Then there is a root of unity μ such that $\mathcal{N}(\xi^{1-j}/\mu) = 1$. Hence, $\xi^{1-j}/\mu = w^s$ for some $w \in \mathbb{L}_n$. As ideals we obtain $(\xi^{1-j}) = w^s$. Therefore $(\mathfrak{A}^{1-j}/w)^s = 1$ and $\mathfrak{A}^{1-j}/w$ is a product of ramified primes and ideals of $\mathcal{O}(\mathbb{K}_n)$. Hence, $a^{1-j} = a^2$ lies in $B_n \iota_{\mathbb{K}_n,\mathbb{L}_n}(A^{1-j}(\mathbb{K}_n))$ which proves that $\widehat{H}^0(\Phi, A_n^-)$ is indeed generated by the image of B_n^-.

Let $t \in (\Lambda/\omega_{n-N}) \setminus p(\Lambda/\omega_{n-N})$ and assume that the ideal class $[\tilde{Q}_n^{(1-j)t}]$ has trivial image in $\widehat{H}^0(\Phi, A_n^-)$. Then there is an ideal $\mathfrak{A}$ in $\mathbb{K}'_n$ and an element $w' \in \mathbb{L}_n$ such that

$$\tilde{Q}_n^{(1-j)t} = \mathfrak{A}(w').$$

As Q_n is ramified in $\mathbb{L}_n/\mathbb{K}'_n$ we see that $w'^{s(1-j)} = \zeta$ is a root of unity. Let $w = w'^{1-j}$ then we obtain $w^{\sigma^p} = \zeta^p w = w$ and we see that ζ is a p-th root of unity. If $\zeta = 1$ then $w \in \mathbb{K}'_n$, which is impossible as $\tilde{Q}_n^{2(1-j)t}$ is not an ideal from $\mathbb{K}'_n$. It remains the case that ζ is a primitive p-th root of unity. Then $w^p \in \mathbb{K}'_n$ is the Kummer-radical of the extension $\mathbb{L}_n/\mathbb{K}'_n$. Hence, as ideal, $(w)^p = \mathfrak{Q}\mathfrak{A}'^p$, where $\mathfrak{Q}$ is divisible by all primes above q in $\mathbb{K}'_n$ but is not divisible by any p-th power, while $\mathfrak{A}'$ is an arbitrary ideal in $\mathbb{K}'_n$. Taking p-th roots we obtain

$$\tilde{Q}_n^{2(1-j)t} = \mathfrak{A}^{1-j}\mathfrak{A}'\mathfrak{Q}^{1/p}.$$

Note that $\mathfrak{Q}^{1/p}$ is well defined as ideal of $\mathbb{L}_n$. The right hand side is divisible by all ideals above q, while the left hand side is only divisible by the $\mathrm{Gal}(\mathbb{K}'_n/\mathbb{K}'_N)$-conjugates of $\tilde{Q}_n$ yielding a contradiction. Hence, $\widehat{H}^0(\Phi, A_n^-)$ contains a submodule isomorphic to $\Lambda/(p, \omega_{n-N})\Lambda$ generated by the class of $\tilde{Q}_n^{1-j}$. As A_n^- is finite the vanishing of the Herbrand quotient completes the proof. □

Lemma 6.2.4. *We have*

$$\mu(A_\infty^-(\mathbb{L})) > 0.$$

Proof. The ideals $\tilde{Q}_n$ form a norm coherent sequence. Let $b \in A_\infty^-$ be the element such that $b_n = [\tilde{Q}_n^{1-j}]$. By definition $sb = 0$ and $pb \in \iota(A_\infty^-(\mathbb{K}'_\infty))$. Consider the natural homomorphism

$$\psi\colon \Lambda/p\Lambda b \to \widehat{H}^0(\Phi, A_\infty^-).$$

If we are able to show that this map is injective we are done. Assume by contrary that $T^k b + \Lambda p b \in \ker(\psi)$ then $T^k b_n \in \iota(A^-(\mathbb{K}'_n))$ for all n. If $p^{n-N} > k$ this yields a contradiction to Lemma 6.2.3. □

Now we are able to prove Theorem 6.2.1

Proof of Theorem 6.2.1. Recall that $\mathbb{L}_\infty/\mathbb{K}$ is a CM $\mathbb{Z}_p$-extension. By Lemma 6.2.4 we know that it has positive μ-invariant. But this contradicts our assumption that μ vanishes for every CM $\mathbb{Z}_p$-extension and any number field $\mathbb{L}$.

□

Part III

2-class groups of CM fields

Chapter 7

Capitulation for the cyclotomic extensions and $p = 2$

7.1 Introduction to the capitulation problem

Let $\mathbb{K}$ and $\mathbb{L}$ be number fields such that $\mathbb{K} \subset \mathbb{L}$. Let $\mathcal{O}(\mathbb{K})$ and $\mathcal{O}(\mathbb{L})$ denote the rings of algebraic integers. Define $I(\mathbb{K})$ and $I(\mathbb{L})$ as the groups of fractional ideals, respectively. There is a natural homomorphism

$$\phi\colon I(\mathbb{K}) \to I(\mathbb{L})$$

given by $\mathfrak{A} \to \mathfrak{A}\mathcal{O}(\mathbb{L})$. Let $\mathrm{Cl}(\mathbb{K})$ and $\mathrm{Cl}(\mathbb{L})$ denote the class groups of $\mathbb{K}$ and $\mathbb{L}$, respectively. The homomorphism defined above induces an homomorphism on the class groups $\phi'\colon \mathrm{Cl}(\mathbb{K}) \to \mathrm{Cl}(\mathbb{L})$. It is an interesting question whether this homomorphism is injective.

We say that an ideal $\mathfrak{A} \subset \mathbb{K}$ capitulates in $\mathbb{L}/\mathbb{K}$ if $\mathfrak{A}$ is non-principal in $\mathbb{K}$ and becomes principal in $\mathbb{L}$. Note that for a class a in the class group of $\mathbb{K}$ an ideal $\mathfrak{A} \in a$ capitulates if and only if every ideal $\mathfrak{B} \in a$ capitulates. Let $\mathbb{K}$ be a CM field and, as before, $\mathbb{Q}_\infty$ be the only $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $\mathbb{K}_\infty = \mathbb{K}\mathbb{Q}_\infty$ with intermediate fields $\mathbb{K}_n$. Let A_n be the p-class group of $\mathbb{K}_n$. Let j denote the complex conjugation of $\mathbb{K}$. For $p \neq 2$ one defines the idempotents $\frac{1}{2}(1-j)$ and $\frac{1}{2}(1+j)$ in $\mathbb{Z}_p[G]$ where G denotes the automorphisms acting on the CM field $\mathbb{K}$. The minus part is given by $\frac{1}{2}(1-j)A_n$ and the plus part is given by $\frac{1}{2}(1+j)A_n$. In particular, we obtain an isomorphism $A_n^- \cong A_n/A_n^+$. For $p = 2$ we cannot work with this definition as $\frac{1}{2} \notin \mathbb{Z}_2$. In most textbooks the minus part for $p = 2$ is defined as $\widehat{A}_n^- = \{a \in A_n \mid ja = a^{-1}\}$ and the plus part as $\widehat{A}_n^+ = \{a \in A_n \mid ja = a\}$.

It is a well known fact that for any prime $p \neq 2$ there is no capitulation on $\widehat{A}_n^-$. The proof (as given for example in Washington [Wash, Proposition 13.26]) uses the fact that a capitulated class should have order 2 which confirms the claim in the case $p \neq 2$. In order to prove results for $p = 2$ which are known for $p \neq 2$ we introduce a slightly different definition.

Definition 7.1.1. *Let p be a prime, $\mathbb{K}$ be a CM number field and A be its p-class*

group. We call fractional ideal $\mathfrak{a}$ *real if* $j(\mathfrak{a}) = \mathfrak{a}$. *We define the group*

$$A^+ = \{a \in A \mid a \text{ contains a real ideal}\}.$$

We define further $A^- = A/A^+$. *For the cyclotomic* $\mathbb{Z}_p$*-extension we denote by* A_n^+ *the plus part of the p-class group of* $\mathbb{K}_n$ *and by* A_n^- *the minus part. We denote the projective limit by* $A_\infty = \lim_{\infty \leftarrow n} A_n$ *and* $A_\infty^- = \lim_{\infty \leftarrow n} A_n^-$.

For $p \neq 2$ one has $A^+ = (1+j)A = \{a \in A \mid ja = a\}$, since there is a decomposition $A = (1-j)A \oplus (1+j)A$. Hence, for $p \neq 2$ the definition by idempotents and the one given above are equivalent.

The purpose of this chapter is to investigate the minus part for all primes including $p = 2$. Most results in this chapter stem from the author's Master's thesis and are published in [Mu]. Only Corollary 7.3.2, Lemma 7.4.5 and its corollary as well as subsection 7.5 are results which have not been published before. We also present a new and less complicated proof of Proposition 7.4.2 and reformulate the proofs in Section 7.2 for all primes and not only for $p = 2$ as the author did in [Mu]. Only in Sections 7.3 and 7.4 we restrict ourselves to the case $p = 2$. In section 7.3 we motivate our alternative definition of the minus part and in Section 7.4 we prove a result that is well known for $p \geq 3$ for the prime $p = 2$.

7.2 The capitulation question

The main purpose of this section is to prove that there is no finite submodule in A_∞^- if $\mathbb{K}$ contains a primitive p-th roots of unity ζ_p ($i = \sqrt{-1}$ if $p = 2$). This is a well known result for $p \neq 2$, but it is not a priori clear for $p = 2$.

We fix a rational prime p. Hence, all class groups occurring in this section denoted by A are p-groups. Let $\mathbb{L}$ be a CM field containing ζ_p (i if $p = 2$) and let furthermore $\mathbb{L}_2 = \mathbb{L}[\zeta']$ where ζ' is a p^k-th root of unity such that $\zeta'^p \in \mathbb{L}$ but ζ' is not. Denote a generator of $Gal(\mathbb{L}_2/\mathbb{L})$ by τ and let $\mathcal{N}$ denote the algebraic norm from $\mathbb{L}_2$ to $\mathbb{L}$.

For the proofs in this section we shall use the following auxiliary lemma whose proof is inspired by [Wash, Lemma 13.27]. But Washington proves the statement only for odd primes.

Lemma 7.2.1. *Denote the roots of unity of* $\mathbb{L}$ *by* W *and the one of* $\mathbb{L}_2$ *by* W_2. *If* ν *is in* $W_2 \cap ker(\mathcal{N})$, *then there is an* $\nu_2 \in W_2$ *such that* $\nu = \nu_2^{\tau-1}$.

Proof. Consider the sequence

$$1 \to W_2 \cap ker(\mathcal{N}) \to W_2 \to W \to 1,$$

where the map from $W_2 \to W$ is the norm $\mathcal{N}$. The roots of unity of $\mathbb{L}$ have the structure $\langle \zeta'^p \rangle \times \langle \zeta_t \rangle$ with t coprime to p. Then $\mathcal{N}(\zeta') = (-1)^{p-1}\zeta'^p$ and $\mathcal{N}(\zeta_t) = \zeta_t^p$ is a primitive t-th root of unity. As $\langle \zeta' \rangle \times \langle \zeta_t \rangle \subset W_2$ we obtain that the norm is surjective and the sequence is exact. Consider furthermore

$$1 \to W \to W_2 \to W_2^{\tau-1} \to 1,$$

where τ is a generator of $Gal(\mathbb{L}_2/\mathbb{L})$. Then we get

$$|W_2^{\tau-1}| = |W_2|/|W| = |W_2 \cap ker(\mathcal{N})|$$

and since $W_1^{\tau-1}$ is contained in $W_2 \cap \ker(\mathcal{N})$, we get equality. □

Lemma 7.2.2. *The map $\iota : A(\mathbb{L})^- \to A(\mathbb{L}_2)^-$ is injective, where ι is the map induced by the ideal lift from $\mathbb{L}$ to $\mathbb{L}_2$. If $p \geq 3$ and $\mathbb{M}/\mathbb{L}$ is an arbitrary Kummer-extension of degree p, then the capitulation kernel $\iota : A(\mathbb{L})^- \to A(\mathbb{M})^-$ is cyclic of order dividing p.*

Proof. Assume that there is a class $x \in A(\mathbb{L})^-$ such that $\iota(x) = 1$ in $A(\mathbb{L}_2)^-$. Let a be an ideal class such that $x = aA(\mathbb{L})^+$. We obtain that $\iota(a) \in A(\mathbb{L}_2)^+$. Let now $\mathfrak{A}$ be an ideal in a. Then we can find a real ideal $\mathfrak{C} \subset \mathbb{L}_2$ such that $\iota(\mathfrak{A})\mathfrak{C} = (\alpha)$ is principal. Then we have $\iota(\mathfrak{A})/\overline{\iota(\mathfrak{A})} = (\alpha/\overline{\alpha})$ and

$$\nu = (\alpha/\overline{\alpha})^{\tau-1} = \alpha^{\tau-1}/\overline{\alpha^{\tau-1}}$$

is a unit of absolute value 1 and norm 1, hence it is a root of unity of norm 1. According to Lemma 7.2.1 there is a root of unity ν_2 such that $\nu = \nu_2^{\tau-1}$. Then

$$(\alpha/\overline{\alpha} \cdot \nu_2^{-1})^{\tau-1} = 1.$$

Therefore, $\gamma = \alpha/\overline{\alpha} \cdot \nu_2^{-1}$ is in $\mathbb{L}$ and $\mathfrak{A}/\overline{\mathfrak{A}} = (\gamma)$. Since $|\gamma| = 1$, we have $1+\gamma = (1+\overline{\gamma})\gamma$. Choose $r \in \mathbb{L}^+$ such that $v = r(1+\gamma)$ is integral. Then $\mathfrak{A}/\overline{\mathfrak{A}} = (v/\overline{v})$ and $(v) = \mathfrak{A}\mathfrak{C}$ for a real ideal $\mathfrak{C}$. Therefore, a contains a real ideal. Hence, a is in $A(\mathbb{L})^+$ and $x = 1$ in $A(\mathbb{L})^-$.

Assume now that $p \geq 3$ and let $x \in A(\mathbb{L})^-$ be such that $\iota(x) = 1 \in A^-(\mathbb{M})$. As $p \geq 3$ we can write $A^-(\mathbb{L}) = (1-j)A(\mathbb{L})$ and $(1-j)$ acts as multiplication by 2 on A_n^-. Let $\mathfrak{A} \in x$. Then we obtain that $\iota(\mathfrak{A}/\overline{\mathfrak{A}}) = (\alpha/\overline{\alpha})$. Let $\beta \in \mathbb{L}$ be such that $(\beta) = \mathfrak{A}^p$. Then there is a root of unity μ such that $\alpha^{(1-j)p} = \beta^{1-j}\mu$. Without loss of generality we can assume that μ has p-power order. We can further assume that $\mathbb{L}$ and $\mathbb{M}$ have the same p-power roots of unity. Otherwise, we have $\mathbb{M} = \mathbb{L}_2$ and we see immediately that there is no capitulation. We obtain that $\alpha^{(1-j)p} \in \mathbb{L}$ which implies that $\alpha^{(1-j)p}$ is the Kummer radical for $\mathbb{M}/\mathbb{L}$. As the Kummer radical is unique up to $(\mathbb{L}^\times)^p$ we see that the the capitulation kernel is cyclic and that its size is bounded by p. □

Note that the new definition of the minus class groups provides – compared to standard textbooks – a shorter and less computational proof of the fact that ι is injective.

Corollary 7.2.3. *Let $\mathbb{K}$ be a CM field containing ζ_p (i if $p = 2$) and let $\mathbb{K}_n$ be the intermediate fields of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$. Let A_n^- be the minus part of the 2-class group of $\mathbb{K}_n$. Then the lift $\iota_{n,n+1} : A_n^- \to A_{n+1}^-$ is injective.*

Proof. By renumbering our fields we can assume that $\mathbb{K}_n = \mathbb{Q}_n\mathbb{K}$, where $\mathbb{Q}_n$ is the n-th intermediate field in the unique cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. If $\mathbb{K}$ contains ζ_p (i if $p = 2$) then $\mathbb{K}_n$ contains $\zeta_{p^{n+e+1}}$, where $e = 1$ if $p = 2$ and $e = 0$ otherwise. Since $\mathbb{K}$ is a CM field, the fields $\mathbb{K}_n$ and $\mathbb{K}_{n+1}$ satisfy the assumptions on $\mathbb{L}$ and $\mathbb{L}_2$ as above. Hence, we can apply Lemma 7.2.2 with $\mathbb{L} = \mathbb{K}_n$ and $\mathbb{L}_2 = \mathbb{K}_{n+1}$. □

If $p = 2$ then there could be capitulation on $\widehat{A}_n^-$. To show that our new definition of the minus part is necessary to obtain a capitulation free minus part we give the following example [Mu, Example 2.4]

Example 7.2.4. *Let $\mathbb{K} = \mathbb{Q}(i, \sqrt{10})$. Then $\mathbb{K}_1 = \mathbb{Q}(i, \sqrt{10}, \sqrt{2})$ is the first step in the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{K}$. Consider the ideal $\mathfrak{A} = (\sqrt{10}, 5)$ in $\mathbb{K}$. Let $a = [\mathfrak{A}]$. Then $\mathfrak{A}^2 = (5)$ and $ja = a$. This implies $a^2 = 1$ and $ja = a^{-1}$. Then $(\sqrt{10}, 5) = (\sqrt{5})$ is principal in $\mathbb{K}_1$. It follows by genus theory that $(\sqrt{10}, 5)$ is not principal in $\mathbb{K}$. Thus, a is a capitulated class.*

Note that in this example the first step in the cyclotomic $\mathbb{Z}_2$-extension is unramified. But ramification is not a condition needed in the proof of Theorem 7.2.2.

Theorem 7.2.5. *There is no finite submodule in A_∞^- if $\mathbb{K}$ is a CM field containing ζ_p (i if $p = 2$).*

Proof. Analogously to [Wash, Proposition 13.28]. Let τ be a generator of $Gal(\mathbb{K}_\infty/\mathbb{K})$ and assume that there is a finite submodule D. Then, there is an $n \in \mathbb{N}$ such that τ^n acts as the identity on D. But then for all $m \geq n$ we have $\iota_{m,m+1} \circ \mathcal{N}_{m+1,m}(x_{m+1}) = x_{m+1}^p$ for all $x \in D$. In particular for every $x \in D$ we can choose m large enough such that $x_m \neq 0$ and $\mathrm{ord}(x_m) = \mathrm{ord}(x_{m+1})$. But then $\iota_{m,m+1}(x_m)$ has the same order as x_m, since $\iota_{m,m+1}$ is injective on the minus part. This implies that x_{m+1} and x_{m+1}^p have the same order yielding a contradiction. Hence there is no finite module D. □

7.3 Capitulation in $\{a \in A \mid ja = a^{-1}\}$

Let $\mathbb{L}$, $\mathbb{L}_2$ and A be defined as in the previous section. In this section we investigate classes in $\{a \in A_n \mid ja = a^{-1}\}$ which lie in the kernel of the ideal lift. It turns out that these classes lie in A^+ as we will prove in Theorem 7.3.1. In the case $p \neq 2$ one has the equality $A^- = \{a \in A \mid ja = a^{-1}\}$. Hence there are no such classes. But the question remains for $p = 2$.

Theorem 7.3.1. *[Mu, Theorem 3.7] Let $p = 2$. If a class a in $\widehat{A}^- = \{a \in A \mid ja = a^{-1}\}$ is in the kernel of the lift $\iota_{\mathbb{L},\mathbb{L}_2}$, then it belongs to A^+. In particular, in the 2-cyclotomic tower of a CM field containing i every such class belongs to A_n^+.*

Clearly, if a class a satisfies the assumptions of the above theorem then it is of order dividing 2. But that means that $a = a^{-1} = ja$. Therefore, we get $a \in \widehat{A}^+ = \{a \in A_n \mid ja = a\}$ as well. Hence, the kernel of the lift lies in the intersection $\widehat{A}^+ \cap \widehat{A}^-$. In particular, the theorem shows that it lies in $A^+ \cap \widehat{A}^+ \cap \widehat{A}^- = A^+[2]$ since A^+ is contained in $\widehat{A}^+$. Further, this theorem can serve a as a motivation for our definition

of A_n^- and A_n^+. In the definition of A_n^- we take the quotient by a subgroup containing all the possible capitulation.

Corollary 7.3.2. *Let $p = 2$ and $\mathbb{K}_\infty/\mathbb{K}$ be the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{K}$ with intermediate fields $\mathbb{K}_n$. Let A_n be the 2-class group of $\mathbb{K}_n$. There exists an index n_0 such that we have the following property for all $n \geq n_0$: If a class a in $\widehat{A}_n^- = \{a \in A_n \mid ja = a^{-1}\}$ lies in the kernel of the lift $\iota_{\mathbb{K}_n,\mathbb{K}_{n+1}}$, then it belongs to $A_n^+ \cap \widehat{A}_n^- \setminus 2\widehat{A}_n^-$ for $n \geq n_0$. In particular, the maximal finite submodule of $\widehat{A}_n^-$ has exponent 2.*

Proof. By [Fe, Theorem 8.8] there is a constant n_0 such that the lift $\iota_{\mathbb{K}_n,\mathbb{K}_{n+1}}$ is injective on A_n^{1-j} for $n \geq n_0$. As $2\widehat{A}_n^- \subset A_n^{1-j}$ the claim follows from Theorem 7.3.1. □

7.4 Boundedness of the rank of A_∞^- and A_∞

The purpose of this section is to show that the rank of A_∞ is uniformly bounded if and only if the rank of A_∞^- is uniformly bounded. This result is well known if we replace A_∞^- by $\widehat{A}_\infty^-$ and assume that $\zeta_p \in \mathbb{K}$ [Wash, Proposition 13.24]. As $A_\infty^- \cong \widehat{A}_\infty^-$ for $p \geq 3$, we only consider $p = 2$ in this section. We fix a CM number field $\mathbb{K}$ and let $\mathbb{K}_n$ be the intermediate fields of the cyclotomic $\mathbb{Z}_2$-extension thereof. Denote as before the 2-class group of $\mathbb{K}_n$ by A_n. Note that in [Mu] we assumed that $\mathbb{K}$ contains i. In the following we will show that this assumption is not necessary.

Remark 7.4.1. *Let $\mathfrak{Q}$ be the product of all primes in $\mathbb{K}^+$ that ramify in $\mathbb{K}/\mathbb{K}^+$. Then every ramified ideal in $\mathbb{K}_n/\mathbb{K}_n^+$ divides $\mathfrak{Q}$. As the number of primes in $\mathbb{K}_n^+$ dividing $\mathfrak{Q}$ is uniformly bounded, we see that the 2-rank of $A_n^+/\iota_{\mathbb{K}_n^+,\mathbb{K}_n}(A(\mathbb{K}_n^+))$ is uniformly bounded.*

The goal of this section is to prove the following Proposition:

Proposition 7.4.2. *The rank of A_n is uniformly bounded if and only if the rank of A_n^- is uniformly bounded.*

Recall from Chapter 1 that the noetherian torsion Λ-module A_∞^- (here we have $\Lambda = \mathbb{Z}_2[[T]]$) is pseudo isomorphic to a module of the form

$$\bigoplus_{i=1}^{s} \Lambda/2^{e_i} \bigoplus \bigoplus_{j=1}^{k} \Lambda/(f_j(T))^{d_j}.$$

The Λ-modules A_n^- have uniformly bounded rank if and only if $\mu = \sum_{i=1}^{s} e_i = 0$

The proof of Proposition 7.4.2 consists of the following two lemmas:

Lemma 7.4.3. *A_n has uniformly bounded rank if and only if A_n^- and $A_n^+[2]$ have uniformly bounded rank.*

Proof. Let $\widehat{A}_n^- = \{a \in A_n \mid ja = a^{-1}\}$ be the classical plus part. Clearly, if the rank of A_n is uniformly bounded, then the ranks of $A_n^+[2]$ and of A_n^- are uniformly bounded. For the other direction one can use a result of Washington [Wash, Proposition 10.12]:

$$2\text{-rank}(A(\mathbb{K}_n^+)) \leq 1 + 2\text{-rank}(\widehat{A}_n^-). \tag{7.1}$$

There is a natural map $\phi : \widehat{A}_n^- \to A_n^-$ and

$$x \in Ker(\phi) \Leftrightarrow x \in A_n^+ \cap \{x \mid jx = x^{-1}\} = A_n^+[2].$$

This implies $2\text{-rank}(\widehat{A}_n^-) \leq 2\text{-rank}(A_n^-) + 2\text{-rank}(A_n^+[2])$.

Since we assumed that $2\text{-rank}(A_n^-)$ and $2\text{-rank}(A_n^+[2])$ are uniformly bounded, we can conclude that $2\text{-rank}(A_n^+)$ is uniformly bounded, due to (7.1) and Remark 7.4.1. Then the rank of A_n is uniformly bounded, due to $2\text{-rank}(A_n) \leq 2\text{-rank}(A_n^-) + 2\text{-rank}(A_n^+)$. □

$\mathbb{K}_\infty/\mathbb{K}_\infty^+$ is an extension of degree 2 ramified at all infinite primes. Hence, the natural norm $A_\infty \to A_\infty(\mathbb{K}_\infty^+)$ is surjective. Note that $A_\infty^{(1+j)} = \iota_{\mathbb{K}_\infty^+,\mathbb{K}_\infty} \circ N_{\mathbb{K}_\infty/\mathbb{K}_\infty^+}(A_\infty(\mathbb{K}^+))$. Hence, by Remark 7.4.1 we see that $A_\infty^+/A_\infty^{(1+j)}$ is of finite rank.

Lemma 7.4.4. *If* $2\text{-rank}(A_n^+)$ *is unbounded then* $2\text{-rank}(A_n^-)$ *is unbounded.*

Proof. Let $a \in A_\infty^+$ be a class such that Λa has unbounded rank. We know that the maximal submodule of finite exponent in A_∞^+ is pseudo isomorphic to $E = \bigoplus_{i=1}^k \Lambda/p^{e_i}$ [Wash, Theorem 13.12]. Without loss of generality we can assume that $e_1 \geq e_i$ for all i and that the image of a in E has order p^{e_1}. By multiplying with a distinguished polynomial $f(T)$ we can assume that $\text{ord}(a) = p^{e_1}$ and that $a \in A_\infty^{1+j}$. Let c be such that $c^{1+j} = a$. Clearly, Λc generates a submodule of A_∞ of infinite rank.

Let $\phi : A_\infty \to A_\infty^-$ be the natural map. Assume that there is a distinguished polynomial $h(T)$ such that $\phi(h(T)c) = 0$. Then $h(T)c = b$ for some b in A_∞^+. But then $h(T)a = b^2$. Clearly b generates a Λ-submodule of infinite rank and for every distinguished polynomial $g(T)$ we have $\text{ord}(g(T)b) = 2\text{ord}(g(T)h(T)a) = 2\text{ord}(a)$, yielding a contradiction to the choice of a and $e_1 \geq e_i$. Therefore, there is no such polynomial $h(T)$ and the rank of Λc is infinite in A_∞^-. □

Now we can prove Proposition 7.4.2.

Proof. One implication is clear. For the other one we know from Lemma 7.4.4 that $2\text{-rank}(A_n^-)$ being bounded implies that $\mathbb{Z}_p\text{-rank}(A_n^+)$ is bounded. In particular $2\text{-rank}(A_n^+[2])$ is uniformly bounded. We can now use Lemma 7.4.3 and get that $2\text{-rank}(A_n)$ is uniformly bounded. □

In the following result we prove a relation between the μ-invariant of A_∞^- and $\widehat{A}_\infty^+$.

Lemma 7.4.5. *For every* n *we have*

$$A_n^-[2] \cong \widehat{A}_n^+/A_n^+.$$

Proof. Consider the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n^+ & \longrightarrow & A_n & \longrightarrow & A_n^- & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \widehat{A}_n^+ & \longrightarrow & A_n & \longrightarrow & A_n^{1-j} & \longrightarrow & 0 \end{array}$$

The middle vertical map is an isomorphism, the left vertical map is injective and the right vertical map is the multiplication by $1-j$ and is surjective. Its kernel is the group $A_n^-[2]$. Then the snake Lemma gives us the isomorphism $A_n^-[2] \cong \widehat{A}_n^+/A_n^+$. □

Corollary 7.4.6. *We obtain*

$$\mu(A_\infty^-) > 0 \Leftrightarrow \mu(\widehat{A}_\infty^+) > 0.$$

Proof. If $\mu(\widehat{A}_\infty^+) > 0$ then $\mu(A_\infty) > 0$ and by Proposition 7.4.2 we see that $\mu(A_\infty^-) > 0$. If conversely $\mu(A_\infty^-) > 0$, then we see by Lemma 7.4.5 that $\widehat{A}_n^+/A_n^+$ has unbounded rank. Hence, the 2-rank of $\widehat{A}_n^+$ is unbounded and $\mu(\widehat{A}_\infty^+) > 0$. □

7.5 Further applications and properties

Assume that $\mathbb{K}$ is a *CM* number field containing ζ_p (i if $p = 2$). Let as before $\mathbb{K}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{K}$ and $\mathbb{K}_n$ the intermediate fields. The results in this section require our new definition of plus and minus parts to obtain class fields that have A_n^- as Galois group.

Theorem 7.5.1. *Assume that Greenberg's conjecture holds for $\mathbb{K}$, i.e. that the class number of $\mathbb{K}_n^+$ is uniformly bounded independent of n, then $\mathbb{H}_\infty^- := \mathbb{H}_\infty^{A_\infty^+}$ is contained in Ω_E.*

This is proved for $p \geq 3$ under the additional assumption that $A_n(\mathbb{K}_n^+)$ is trivial for all n in [La, Chapter 6 Theorem 4.2]. As we are only assuming that A_n^+ is finite for all n we give a full proof here. In Theorem 8.3.5 we will provide a family of triquadratic fields such that Greenberg's conjecture holds for $p = 2$. Further families of quadratic and quartic extensions in which Greenberg's conjecture holds for $p = 2$ are given in [Miz] and [Kum].

Proof. Let $\alpha^{1/p^t} \in \mathbb{H}_\infty^-$ and $\alpha \in \mathbb{K}_\infty$. As $\mathrm{Gal}(\mathbb{H}_\infty^-/\mathbb{K}_\infty)$ is annihilated by $1+j$ we see that for every $\sigma \in \mathrm{Gal}(\mathbb{H}_\infty^-/\mathbb{K}_\infty)$ we have $j\sigma j = \sigma^{-1}$. Hence[1], $\sigma(\overline{\alpha^{1/p^t}}) = \zeta\overline{\alpha^{1/p^t}}$ Thus, σ fixes $\alpha' = \alpha^{1/p^t}/\overline{\alpha^{1/p^t}}$ and $\alpha' \in \mathbb{K}_\infty$. As $N_{\mathbb{K}_\infty/\mathbb{K}_\infty^+}(\alpha') = 1$ we see that there is an element $\beta \in \mathbb{K}_\infty$ such that $\alpha^{(1-j)} = \beta^{p^t(1-j)}$. If we substitute α by α/β^{p^t}, we can assume that α is real.

Assume that $\alpha^{1/p^t} \notin \Omega_E$ and choose $n \geq t$ minimal such that $\alpha \in \mathbb{K}_n$ and such that $\mathbb{K}_n(\alpha^{1/p^t})/\mathbb{K}_n$ is unramified. Then $(\alpha) = \mathfrak{A}^{p^t}$ for some non-trivial ideal $\mathfrak{A}$ that is fixed

[1]The overline stands for one fixed complex conjugation in $\mathrm{Gal}(\mathbb{H}_\infty/\mathbb{K}_\infty^+)$. Note that this lift is not unique.

by j. Hence, α^{1/p^t} induces a well defined class in A_n^+. Note that $A_n^+/\iota_{\mathbb{K}_n^+,\mathbb{K}_n}(A(\mathbb{K}_n^+))$ is generated by the classes of ramified primes. Since $\mathbb{K}$ contains ζ_p (i if $p = 2$) we see that $\mathbb{K}_n/\mathbb{K}_n^+$ is unramified outside p. Hence, $A_n^+/\iota_{\mathbb{K}_n^+,\mathbb{K}_n}(A(\mathbb{K}_n^+))$ has uniformly bounded rank. Let $b \in A_n^+ \setminus \iota_{\mathbb{K}_n^+,\mathbb{K}_n}(A(\mathbb{K}_n^+))$. We see that $b^2 \in \iota_{\mathbb{K}_n^+,\mathbb{K}_n}(A(\mathbb{K}_n^+))$. Hence, our assumption that Greenberg's conjecture holds for $\mathbb{K}_n$ implies that the size of A_n^+ is uniformly bounded. In particular, there is a k such that $p^k A_n^+$ is trivial.

We want to show that $\mathbb{H}_\infty^-/\mathbb{H}_\infty^- \cap \Omega_E$ is an extension of finite exponent: If $t \leq k$ for all possible α, there is nothing to prove. Assume now that there is an element α^{1/p^t} such that $t > k$. Then we have $\alpha = \beta^{p^{t-k}} e$ for some unit e. We see that $\mathbb{K}_\infty(\alpha^{1/p^{t-k}}) = \mathbb{K}_\infty(e^{p^{t-k}}) \subset \Omega_E$. Hence, the extension $\mathbb{H}_\infty^-/\mathbb{H}_\infty^- \cap \Omega_E$ is indeed of finite exponent bounded by p^k.

Let $\mathbb{H}_{\infty,\mu}^-$ be the fixed field under the maximal Λ-submodule of A_∞^- of finite p-rank. Let $\mathbb{H}_{n,\mu}^-$ be the intersection of $\mathbb{H}_{\infty,\mu}^-$ and $\mathbb{H}_n$. As this is an extension of uniformly bounded exponent we can assume that it is a Kummer extension. Let $R \subset \mathbb{K}_n^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$ such that for every $\alpha \otimes p^{-t}$ in R the element α^{1/p^t} lies in $\mathbb{H}_{n,\mu}^-$. Then we can conclude as before that $\alpha = (\mathfrak{A})^{p^t}$ for a non-trivial ideal that is fixed by j. We obtain a well defined homomorphism $R \to A_n^+$. If $\alpha \otimes p^{-t}$ lies in the kernel of this homorphism, then α^{1/p^t} lies in Ω_E. As the size of A_n^+ is uniformly bounded we see that $\mathbb{H}_{n,\mu}^-/\mathbb{H}_{n,\mu}^- \cap \Omega_E$ is a uniformly bounded extension. It follows that $\mathbb{H}_{\infty,\mu}^-/\mathbb{H}_{\infty,\mu}^- \cap \Omega_E$ is a finite extension. We obtain the following equality (we allow the values in the following equation to be infinite. We will actually see in the next paragraph that all the terms are finite)

$$[\mathbb{H}_\infty^- : \mathbb{H}_\infty^- \cap \Omega_E] = [\mathbb{H}_\infty^- : (\mathbb{H}_\infty^- \cap \Omega_E)\mathbb{H}_{\infty,\mu}^-] \cdot [(\mathbb{H}_\infty^- \cap \Omega_E)\mathbb{H}_{\infty,\mu}^- : \mathbb{H}_\infty^- \cap \Omega_E]$$

Recall that $p^k \mathrm{Gal}(\mathbb{H}_\infty^-/\mathbb{H}_\infty^- \cap \Omega_E)$ is trivial and that by definition $\mathrm{Gal}(\mathbb{H}_\infty^-/\mathbb{H}_{\infty,\mu}^-)$ is of finite rank. So we obtain that $[\mathbb{H}_\infty^- : (\mathbb{H}_\infty^- \cap \Omega_E)\mathbb{H}_{\infty,\mu}^-]$ is finite. Note that

$$[(\mathbb{H}_\infty^- \cap \Omega_E)\mathbb{H}_{\infty,\mu}^- : \mathbb{H}_\infty^- \cap \Omega_E] \leq [\mathbb{H}_{\infty,\mu}^- : \mathbb{H}_{\infty,\mu}^- \cap \Omega_E] < \infty.$$

Hence, $\mathbb{H}_\infty^-/\mathbb{H}_\infty^- \cap \Omega_E$ is a finite extension and $\mathrm{Gal}(\mathbb{H}_\infty^-/\mathbb{H}_\infty^- \cap \Omega_E)$ is a finite Λ-submodule of A_∞^-. But this is impossible by Theorem 7.2.5. □

The next Theorem does not really require our alternative definition of the plus and minus parts, but it is one of the rare cases where the results for $p = 2$ are actually stronger then for $p \geq 3$.

Theorem 7.5.2. *Assume that $p = 2$. Let $\mathbb{M}_n$ be the maximal 2-abelian 2-ramified extension of $\mathbb{Q}(\zeta_{2^n})$ and X_n its Galois group over $\mathbb{Q}(\zeta_{2^n})$. Then X_n is cyclic as $\mathbb{Z}_p[Gal(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})]$-module.*

Proof. The proof follows closely the ideas of [Wash, Theorem 10.14] for odd p. By [Wash, Theorem 10.4 b)] we know that the class number of $\mathbb{Q}(\zeta_{2^n})$ is coprime to 2 for all n . Let $\mathbb{L}'$ be the maximal abelian 2-ramified extension of $\mathbb{Q}(\zeta_{2^n})$ of exponent 2 and let A be the class group of $\mathbb{Q}(\zeta_{2^n})$. Let B be the Kummer-radical of $\mathbb{L}'/\mathbb{Q}(\zeta_{2^n})$. Let $b \in \mathbb{Q}(\zeta_{2^n})$ be a representative of a class in B. Then $(b) = \mathfrak{B}^2(1 - \zeta_{2^n})^d$ for

some ideal $\mathfrak{B}$ coprime to 2. We obtain a well defined homomorphism $\phi\colon B \to A[2]$ assigning $b\mathbb{Q}(\zeta_{2^n})$ to the ideal class $[\mathfrak{B}]$. Since $A[2]$ is trivial we see that ϕ is the zero homomorphism. As $h(\mathbb{Q}(\zeta_{2^n})^+)$ is coprime to 2 we obtain from [Wash, Theorems 8.1 and 8.2] that $(1-\zeta_{2^n})$ is a $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q})]$ generator of $\ker(\phi) = B$.

Let $H' = \mathrm{Gal}(\mathbb{L}'/\mathbb{Q}(\zeta_{2^n}))$. By definition we have a non degenerate pairing

$$H' \times B \to W_2.$$

Let b_1 be a generator for B and let us complete it to a $\mathbb{F}_2$-basis $b_1, \dots b_r$ such that there are elements $g_i \in Gal(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q})$ such that $g_i b_1 = b_i$. Then we can choose elements h_i such that $\langle h_i, b_j\rangle = (-1)^{\delta_{i,j}}$. Let H_1' be the subgroup generated by h_1 under $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q})]$ and assume that $H_1' \neq H'$. Then there is an element $b = \prod b_i^{x_i}$ such that $\langle h, b\rangle = 1$ for all $h \in H_1'$. Then we have

$$1 = \langle h_1^{g_i}, b\rangle = \langle h_1, b^{g_i^{-1}}\rangle = (-1)^{x_i}.$$

Hence, $x_i = 0$ for all i and we see that H' is cyclic. As $H' = X_n/2X_n$ the claim follows. □

Remark 7.5.3. *If $p \geq 3$ and if Vandiver's conjecture holds for $\mathbb{Q}(\zeta_p)$ (i.e. the class number of $\mathbb{Q}(\zeta_p)^+$ is coprime to p) one can show that $X_n/(1+j)X_n$ is cyclic [Wash, Theorem 10.14].*

Chapter 8

The Structure of the 2-class group

Acknowledgments

This chapter is joint work with Mohamed Mahmoud Chems-Eddin form the University of Oujda in Morocco. This work was accepted for publication in the International Journal of Number Theory.

8.1 2-class groups along the cyclotomic $\mathbb{Z}_p$-extensions

Let $\mathbb{L}_0$ be a quadratic extension of $\mathbb{Q}$ and $\mathbb{L}_n$ the intermediate fields of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{L}_0(i)$. In this chapter we want to compute the 2-class group of $\mathbb{L}_n$ explicitly for certain classes of base fields $\mathbb{L}_0$ and corresponding fields $\mathbb{L}_n$. To simplify notation and to avoid unnecessary index shifts we will write $\mathbb{K}_n$ for the field $\mathbb{Q}(\zeta_{2^{n+2}})$ in this chapter (where ζ_m denotes a m-th primitive root of unity). Note that $\mathbb{L}_n$ is the compositum of $\mathbb{K}_n$ and $\mathbb{L}_0$. A crucial step in this context is to determine the Iwasawa invariants of A_∞ and the maximal finite submodule.

Let $\mathbb{F}$ be an arbitrary finite extension of $\mathbb{Q}$, and $\mathbb{F}_\infty$ the cyclotomic $\mathbb{Z}_2$-extension thereof. Let $\mathbb{H}_\infty$ be the maximal 2-abelian unramified extension of $\mathbb{F}_\infty$. Let $\mathbb{F}_n \subset \mathbb{F}_\infty$ be the unique subfield such that $[\mathbb{F}_n : \mathbb{F}] = 2^n$. By class field theory we have an isomorphism

$$X := Gal(\mathbb{H}_\infty/\mathbb{F}_\infty) \cong \lim_{\infty \leftarrow n} A_n,$$

where A_n denotes the 2-class group of $\mathbb{F}_n$. For a topological generator τ of $\mathrm{Gal}(\mathbb{F}_\infty/\mathbb{F})$ we define the Iwasawa algebra $\Lambda = \mathbb{Z}_2[[T]]$ with respect to $T = \tau - 1$. The natural action of τ on A_n turns X into a Λ-module. As explained in Chapter 1, X is a Λ-torsion module and pseudo isomorphic to a module of the form

$$\bigoplus_{i=1}^{s} \Lambda/2^{e_i} \bigoplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{d_j},$$

for distinguished irreducible polynomials $f_j(T)$. The Ferrero-Washington theorem shows that all the $e_i = 0$ if $\mathbb{F}/\mathbb{Q}$ is abelian [Fe-Wa].

In this chapter we will concentrate on CM fields of the following form: Let $n \geq 0$ be a natural number, d be an odd square-free integer and $\mathbb{L}_{n,d} := \mathbb{Q}(\zeta_{2^{n+2}}, \sqrt{d})$. We will use results by Azizi, Chems-Eddin and Zekhnini on the rank of the 2-class group of $\mathbb{L}_{n,d}$, the layers of the $\mathbb{Z}_2$-extension of some special Dirichlet fields of the form $\mathbb{L}_{0,d} = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$ (cf. [A-C-Z1, C-A-Z, C]). Combining them with the results form the previous chapter we obtain our central theorem. Li, Ouyang, Xu and Zhang computed the 2-class groups of $L_{n,d}$ for d being a prime congruent to 3 (mod 8), 5 (mod 8) and 7 (mod 16) (cf. [L-Y-X-Z]) but the family of extensions we consider here is disjoint to the one considered by Li, Ouyang, Xu and Zhang.

Throughout this chapter we denote by $h_2(d)$ the 2-class number of the quadratic field $\mathbb{Q}(\sqrt{d})$. Further, we fix the following notation:

- Let p be an odd prime and a an integer then we denote the quadratic Legendre Symbol by $(\frac{a}{p})$.
- If $p \equiv 1 \pmod 4$ is a prime and $(\frac{a}{p}) = 1$, then we define $(\frac{a}{p})_4 = \pm 1 \equiv a^{\frac{p-1}{4}} \pmod p$. This symbol is 1 if a is a 4-th power modulo p and -1 otherwise. Note that this symbol is only defined on the set of quadratic residues. In contrast to the quartic residue symbol taking values in the 4-th roots of unity the symbol $(\frac{a}{p})_4 = \pm 1 \equiv a^{\frac{p-1}{4}}$ is multiplicative.
- If $a \equiv 1 \pmod 8$ we define $(\frac{a}{2})_4 = (-1)^{\frac{a-1}{8}}$.
- Let $\mathbb{K}$ be a finite abelian extension of $\mathbb{Q}$ and $\mathfrak{p}$ a prime in $\mathcal{O}(\mathbb{K})$. Let $\alpha, \beta \in \mathbb{K}_\mathfrak{p}$. Then we write $(\frac{\alpha,\beta}{\mathfrak{p}})$ for the Hilbert symbol of α in the extension $\mathbb{K}_\mathfrak{p}(\beta^{1/2})/\mathbb{K}_\mathfrak{p}$, i.e.
$$\left(\frac{\alpha, \beta}{\mathfrak{p}}\right) = \sigma_\alpha(\beta^{1/2})/\beta^{1/2},$$
where σ_α denotes the local Artin-symbol of α. Note that $(\frac{\alpha,\beta}{\mathfrak{p}}) = 1$ if and only if α lies in the image of the norm $N\colon \mathbb{K}_\mathfrak{p}(\beta^{1/2}) \to \mathbb{K}_\mathfrak{p}$.
- E_k are the units in the CM field k,
- Q_k denotes the Hasse's unit index of k, i.e. the index $[E_k : E_{k^+}W]$, where W denotes the roots of unity in k.
- $q(L_{1,d}) := (E_{L_{1,d}} : \prod_i E_{k_i})$, where k_i are the quadratic subfields of $L_{1,d}$.
- $\mathbb{K}_n = \mathbb{Q}(\zeta_{2^{n+2}}) \subset \mathbb{L}_{n,d}$.

The main aim of this chapter is to prove the following

Theorem 8.1.1. *Let d be a positive square-free integer and $n \geq 1$ be an integer.*

a) Assume d has one of the following forms:

- $d = p$, *for a prime* $p \equiv 9 \pmod{16}$ *such that* $(\frac{2}{p})_4 = 1$,
- $d = pq$, *for two distinct primes* $p \equiv q \equiv 3 \pmod{8}$.

Then the 2-class group of $\mathbb{L}_{n,d}$ *is isomorphic to* $\mathbb{Z}/2^{n+r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *for a constant* r *such that* $2^r = h_2(-2d)$.

b) Let $d = pq$, *for two primes* p *and* q *such that* $p \equiv -q \equiv 5 \pmod{8}$. *Then the 2-class group of* $\mathbb{L}_{n,d}$ *is isomorphic to* $\mathbb{Z}/2^{n+r-2}\mathbb{Z}$ *for a constant* r *such that* $2^r = 2 \cdot h_2(-pq)$. *Further, Greenberg's conjecture holds for the field* $\mathbb{L}^+_{n,d}$, *i.e. the 2-class number of* $\mathbb{L}^+_{n,d}$ *is uniformly bounded.*

In the last section of this chapter we apply Theorem 8.1.1 to describe the 2-class groups of the layers of the cyclotomic $\mathbb{Z}_2$-extension $\mathbb{K}_\infty$ of some imaginary quadratic field $\mathbb{K}$. The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields were already investigated by Mizusawa [Miz]. In contrast to our results Mizusawa described the Galois group of the maximal unramified pro 2 extension of $\mathbb{K}_\infty$ while we describe the class group at every finite level n.

Theorem 8.1.2. *Let* d *be a positive square-free integer and* $n \geq 1$. *Let* $\mathbb{K}_{0,d} = \mathbb{Q}(\sqrt{-d})$ *and define the field* $\mathbb{K}_{n,d}$ *as the* n*-th layer of the cyclotomic* $\mathbb{Z}_2$*-extension of* $\mathbb{K}_{0,d}$.

a) Let d *have one of the following forms:*

- $d = p$ *for a prime* $p \equiv 9 \pmod{16}$ *such that* $(\frac{2}{p})_4 = 1$.
- $d = pq$ *for two different primes* $p \equiv q \equiv 3 \pmod{8}$,

Let $2^r = h_2(-2d)$. *Then the 2-class group of* $\mathbb{K}_{n,d}$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+r-1}\mathbb{Z}$.

b) Assume that $d = pq$ *is the product of two primes* $p \equiv -q \equiv 5 \pmod{8}$ *and let* $2^r = 2 \cdot h_2(-pq)$. *Then the 2-class group of* $\mathbb{K}_{n,d}$ *is isomorphic to* $\mathbb{Z}/2^{n+r-1}\mathbb{Z}$.

8.2 Some preliminary results on the minus part of the 2-class group

Denote, as before, by A_n the 2-Sylow subgroup of the class group of the intermediate fields $\mathbb{L}_n$. The complex conjugation of $\mathbb{L}_0$, denoted by j, acts on A_n as well as on the projective limit $A_\infty = \lim_{\infty \leftarrow n} A_n$. As in the previous chapter we define A_n^+ as the group of strongly ambiguous classes with respect to the extension $\mathbb{L}_n/\mathbb{L}_n^+$ and $A_n^- = A_n/A_n^+$. As in Chapter 7 we denote the subgroup $\{a \in A_n \mid ja = -a\}$ by $\widehat{A_n^-}$. Analogously to A_∞ we define $A_\infty^- = \lim_{\infty \leftarrow n} A_n^-$ and $\widehat{A}_\infty^- = \lim_{\infty \leftarrow n} \widehat{A_n^-}$. We will frequently need the following two lemmata on the Iwasawa invariants of A_∞^-.

Lemma 8.2.1. *We have* $\lambda(A_\infty^-) \geq 2\text{-rank}(A_n^-)$ *for all* $n \geq 0$.

Proof. By Theorem 7.2.5 there is no finite submodule in A_∞^-. As $\mu(A_\infty^-) = 0$ the 2-rank and λ-invariant of A_∞^- are equal. Since $\mathbb{L}_\infty/\mathbb{L}_0$ is totally ramified the claim is immediate. □

Lemma 8.2.2. *We have*

$$\lambda(A_\infty^-) = \lambda(\widehat{A_\infty^-}).$$

Proof. Note that $2A_\infty \subset (1+j)A_\infty + (1-j)A_\infty \subset A_\infty$. Clearly, all elements in $(1+j)A_\infty$ are strongly ambiguous. Thus, if we consider the projection

$$\pi : A_\infty \to A_\infty^-$$

we see that $(1+j)A_\infty$ lies in the kernel of π. On the other hand $j(1-j)a = -(1-j)a$. So if a class in $(1-j)A_\infty$ is strongly ambiguous with respect to the extension $\mathbb{K}_\infty/\mathbb{K}_\infty^+$ then it is of order dividing 2. As $\mu(A_\infty) = 0$ we obtain that $(1-j)A_\infty$ intersects the kernel of π only in a finite submodule. It follows that

$$\lambda(A_\infty^-) = \lambda((1-j)A_\infty).$$

Note that $2\widehat{A_\infty^-} \subset (1-j)A_\infty^- \subset \widehat{A_\infty^-}$. Hence, we see that

$$\lambda(A_\infty^-) = \lambda(\widehat{A_\infty^-}).$$

□

8.3 Preliminaries on the fields $\mathbb{L}_{n,d}$ and $\mathbb{L}_{n,d}^+$

To determine the structure of the 2-class groups along a cyclotomic tower the λ-invariants of A_n are of particular interest. In the sequel we will consider the modules A_∞ defined for different base fields $\mathbb{F}$. To simplify notation we will also write $\lambda(\mathbb{F})$ for $\lambda(A_\infty(\mathbb{F}))$ and $\lambda^-(\mathbb{F})$ for $\lambda(A_\infty^-(\mathbb{F}))$. We will use the same abbreviated notations $\mu^-(\mathbb{F})$ and $\mu(\mathbb{F})$ for $\mu(A_\infty^-(\mathbb{F}))$ and $\mu(A_\infty(\mathbb{F}))$, respectively. The following theorem is a useful tool to compute λ^- for the family of fields we are interested in.

Theorem 8.3.1 (Kida's formula)**.** *[Ki, Theorem 3] Let $\mathbb{F}'$ and $\mathbb{F}$ be CM fields and $\mathbb{F}'/\mathbb{F}$ a finite 2 extension. Assume that $\mu^-(\mathbb{F}) = 0$. Then*

$$\lambda^-(\mathbb{F}') - \delta(\mathbb{F}') = [\mathbb{F}'_\infty : \mathbb{F}_\infty]\left(\lambda^-(F) - \delta(\mathbb{F})\right) + \sum(e_\beta - 1) - \sum(e_{\beta^+} - 1),$$

where for any CM field K the variable $\delta(K)$ takes the values 1 or 0 according to whether K_∞ contains the 4-th roots of unity or not. The e_β is the ramification index of a prime β in $\mathbb{F}'_\infty/\mathbb{F}_\infty$ coprime to 2 and e_{β^+} is the ramification index for a prime coprime to 2 in ${\mathbb{F}'}_\infty^+/\mathbb{F}_\infty^+$.

Note that Kida proves Theorem 8.3.1 for $\lambda(\widehat{A_\infty^-})$. But due to Lemma 8.2.2 this λ-invariant equals the λ-invariant of A_∞^-.

Theorem 8.3.2. *Assume that d is the product of r primes congruent to 7 or 9 (mod 16) and s primes congruent to 3 or 5 (mod 8). Then*

$$\lambda^- = 2r + s - 1.$$

Proof. Let $\mathbb{F}' = \mathbb{L}_{0,d} = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$ and $\mathbb{K}_0 = \mathbb{F} = \mathbb{Q}(\sqrt{-1})$. Then $\delta(\mathbb{F}) = \delta(\mathbb{F}') = 1$ and $\lambda^-(\mathbb{F}) = 0$. The only primes that ramify in $\mathbb{F}'_\infty/\mathbb{F}_\infty$ and $\mathbb{F}'^+_\infty/\mathbb{F}^+_\infty$ are the primes dividing d.

Every prime congruent to 7 or 9 modulo 16 splits into 4 primes in $\mathbb{K}_n$ for n large enough, while it splits only into 2 primes in $\mathbb{K}^+_n$ (see [C, Proposition 1]). Primes congruent to 3 or 5 modulo 8 decompose into 2 primes in $\mathbb{K}_n$, while $\mathbb{K}^+_n$ contains only one prime above p (see [C-A-Z, Proposition 2]). As $[\mathbb{F}'_\infty : \mathbb{F}_\infty] = [\mathbb{F}'^+_\infty : \mathbb{F}^+_\infty] = 2$ either $e_\beta = e_{\beta^+} = 1$ or $e_\beta = e_{\beta^+} = 2$. Plugging all of this into Kida's formula we obtain

$$\lambda^- - 1 = 2(0 - 1) + 4r + 2s - 2r - s = 2r + s - 2$$

and the claim follows. □

The above result determines λ^- for a certain family of fields $\mathbb{L}_{0,d}$. As we are interested in the whole 2-class group and not only in its minus part we also need to understand the plus part in the cases we consider in Theorem 8.1.1.

Theorem 8.3.3. *Let d be an odd square-free integer and $n \geq 1$. Then, the class number of $\mathbb{L}^+_{n,d}$ is odd if and only if d takes one of the following forms*

a) $d = q_1 q_2$ where the $q_i \equiv 3 \pmod 4$ and q_1 or $q_2 \equiv 3 \pmod 8$.

b) d is a prime congruent to $3 \pmod 4$.

c) d is a prime congruent to $5 \pmod 8$.

d) d is a prime congruent to $1 \pmod 8$ and $(\frac{2}{p})_4(\frac{p}{2})_4 = -1$.

Proof. The extension $\mathbb{L}^+_{n+1,d}/\mathbb{L}^+_{n,d}$ is a quadratic extension that ramifies only at the prime ideals above 2 of $\mathbb{L}^+_{n,d}$ for all $n \geq 1$. Let $\mathbb{H}(\mathbb{L}^+_{n,d})$ be the 2-Hilbert class field of $\mathbb{L}^+_{n,d}$ and X_n its Galois group over $\mathbb{L}^+_{n,d}$. Let Y be the Λ-submodule of $X_\infty = \lim_{\infty \leftarrow n} X_n$ such that $X_0 \cong X_\infty/Y$. Then $X_n \cong X_\infty/\nu_{n,0}Y$ [Wash, Lemma 13.18]. In particular, if X_n is trivial then $X_\infty = \nu_{n,0}X_\infty$ and X_∞ is indeed trivial by Nakayama's lemma. Hence, the class number of $\mathbb{L}^+_{1,d}$ being odd implies that the class number of $\mathbb{L}^+_{n,d}$ is odd. The converse follows from Theorem 10.1 of [Wash] and the fact that the extension $\mathbb{L}^+_{n+1,d}/\mathbb{L}^+_{n,d}$ is totally ramified. Hence, the class number of $\mathbb{L}^+_{n,d}$ is odd if and only if the class number of $\mathbb{L}^+_{1,d} = \mathbb{Q}(\sqrt{2}, \sqrt{d})$ is odd. See [Co-Hu, pp. 155-157] and [Fr, p. 78] for the rest. □

Theorem 8.3.4. *Let $d > 2$ be an odd square-free integer and $n \geq 1$ a positive integer. Then the 2-class group of $\mathbb{L}_{n,d}$ is cyclic non-trivial if and only if d takes one of the following forms:*

a) d is a prime congruent to 7 (mod 16).

b) $d = pq$, where p and q are two primes such that $q \equiv 3 \pmod 8$ and $p \equiv 5 \pmod 8$.

Proof. If d is not a prime congruent to 7 (mod 8) then the 2-class group of $L_{n,d}$ is cyclic non-trivial if and only if $d = pq$, where p and q satisfy the assumptions of point b) [C-A-Z, Theorem 6]. For the rest of the proof we consider only the case $d = p \equiv 7 \pmod 8$ and distinguish two cases:

- Suppose that p is congruent to 15 (mod 16) and let σ denote its Frobenius homomorphism in $Gal(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$. Then $\sigma(\zeta_{16}) = \sigma^p(\zeta_{16})$ by the definition of the Frobenius homomorphism. Let H be the group generated by σ. Then p is totally split in $\mathbb{Q}(\zeta_{16})^H/\mathbb{Q}$. Since $p \equiv 15 \pmod{16}$, σ is the complex conjugation. Hence, p is totally split in $\mathbb{Q}(\zeta_{16})^+/\mathbb{Q}$ and inert in $\mathbb{Q}(\zeta_{16})/\mathbb{Q}(\zeta_{16})^+$.

  In particular, there are 4 primes of $\mathbb{K}_2$ lying over p. Then, by the ambiguous class number formula [Qi 2, Lemma 2.4], we obtain that 2-rank$(\mathrm{Cl}(\mathbb{L}_{2,d})) = 4 - 1 - e$, where e is defined by $2^e = [E_{\mathbb{K}_2} : E_{\mathbb{K}_2} \cap \mathcal{N}(\mathbb{L}_{2,d}^*)]$. The unit group of $\mathbb{K}_2$ is given by $E_{\mathbb{K}_2} = \langle \zeta_{16}, \xi_3, \xi_5, \xi_7 \rangle$, where $\xi_k = \zeta_{16}^{(1-k)/2} \frac{1-\zeta_{16}^k}{1-\zeta_{16}}$. Let $\mathcal{N}'$ be the norm from $\mathbb{K}_2$ to $\mathbb{K}_2^+$. Since p is inert in $\mathbb{K}_2/\mathbb{K}_2^+$ we obtain for $k = 3, 5$ or 7

$$\left(\frac{\xi_k, p}{\mathfrak{p}_{\mathbb{K}_2}}\right) = \left(\frac{\mathcal{N}'(\xi_k), p}{\mathfrak{p}_{\mathbb{K}_2^+}}\right) = \left(\frac{\xi_k^2, p}{\mathfrak{p}_{\mathbb{K}_2^+}}\right) = 1.$$

  Hence, the units ξ_k have a trivial Artin-symbol in $\mathbb{K}_2(\sqrt{p})_{\mathfrak{p}_{\mathbb{K}_2}}/\mathbb{K}_{2\mathfrak{p}_{\mathbb{K}_2}}$. In particular, these units are norms from $\mathbb{K}_2(\sqrt{p})_{\mathfrak{p}_{\mathbb{K}_2}} = \mathbb{K}_{2\mathfrak{p}_{\mathbb{K}_2}}(\sqrt{d})$. As $\mathbb{L}_{2,d}/\mathbb{K}_2$ is unramified outside p, the Hasse norm principle implies that $\xi_k \in E_{\mathbb{K}_2} \cap \mathcal{N}(\mathbb{L}_{2,d}^*)$ Then e is bounded by 1 and 2-rank$(\mathrm{Cl}(\mathbb{L}_{2,d})) \geq 4-1-1 = 2$. Hence, the 2-class group of $\mathbb{L}_{n,d}$ is not cyclic.

- Suppose now that p is congruent to 7 (mod 16), then by Theorem 8.3.3, the class number of $\mathbb{L}_{n,d}^+$ is odd. Since the primes above 2 are unramified in $\mathbb{L}_{n,p}/\mathbb{L}_{n,p}^+$ for n large enough, all strongly ambiguous ideals in $\mathbb{L}_{n,d}$ are actually ideals from $\mathbb{L}_{n,d}^+$ and the 2-rank of A_n is bounded by λ^-. By [A-C-Z1, Theorem 4.4], the 2-class group of $\mathbb{L}_{1,d}$ is cyclic non-trivial and by Theorem 8.3.2 we have $\lambda^- = 1$ which completes the proof.

□

Theorem 8.3.5. *Assume that d takes one of the forms of Theorem 8.3.4. Then $\lambda = 1$ and Greenberg's conjecture holds for $\mathbb{L}_{n,d}^+$.*

Note that Greenberg's conjecture follows immediately from Theorem 8.3.3 if d is a prime congruent to 7 (mod 16). If $d = pq$ where p and q are primes such that $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$ we obtain that Greenberg's conjecture holds but the 2 class group of $\mathbb{L}_{n,d}^+$ is non-trivial. The case $d = pq$ is also proved in [Oz-Ta].

Proof. By Theorem 8.3.4 the 2-class group of $\mathbb{L}_{n,d}$ is cyclic. By Theorem 8.3.2, we have $\lambda^- = 1$. Thus, $\lambda = \lambda^- = 1$ and the first claim follows

For the second claim recall from Lemma 8.2.2 that $\lambda(\widehat{A_\infty^-}) = \lambda(A_\infty^-)$. Note that the groups $\widehat{A_n^-} \cap A_n^+$ are of exponent 2. So if we know that the 2-class group of $\mathbb{L}_{n,d}$ is cyclic and that $\lambda(\widehat{A_\infty^-}) = 1$, then A_n^+ contains at most 2 elements. As the capitulation kernel $A_n(\mathbb{L}_{n,d}^+) \to A_n(\mathbb{L}_{n,d})$ contains at most 2 elements due to [Wash, Theorem 10.3], we see that the 2-class group of $\mathbb{L}_{n,d}^+$ is uniformly bounded. □

In order to prove our main result (Theorem 8.1.1) we will also need [C-A-Z, Theorem 5] and [C, Theorem 1] which are summarized in the following Theorem.

Theorem 8.3.6. *Let $n \geq 1$ and assume that d takes one of the following forms:*

a) $d = pq$, for two distinct primes p and q congruent to 3 (mod 8).

b) d, is a prime congruent to 9 (mod 16).

Then the rank of the 2-class group of $\mathbb{L}_{n,d}$ is 2.

8.4 Proof of the Structure Theorem

We will first compute the cardinality of $h_2(\mathbb{L}_{1,d})$ and then use this result to prove Theorem 8.1.1.

Lemma 8.4.1. *Let d be an odd positive square-free integer. We have:*

a) $h_2(\mathbb{L}_{1,d}) = 2 \cdot h_2(-d)$, if $d = pq$, for two distinct primes $p \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 8$.

b) $h_2(\mathbb{L}_{1,d}) = h_2(-2d)$, if $d = pq$, for two distinct primes $p \equiv q \equiv 3 \pmod 8$ or $d = p$ for a prime p such that $p \equiv 9 \pmod{16}$ and $(\frac{2}{p})_4 = 1$.

Proof. The proof is basically a computation in units and class number formulas.

a) Denote by ε_{2pq} the fundamental unit of the quadratic field $\mathbb{Q}(\sqrt{2pq})$. We have $\varepsilon_{2pq} = x + y\sqrt{2pq}$ for some integers x and y. Since ε_{2pq} has a positive norm we obtain $x^2 - 2pqy^2 = 1$. Thus $x^2 - 1 = 2pqy^2$. Set $y = y_1y_2$ for $y_i \in \mathbb{Z}$. Assume for a moment that

$$\begin{cases} x \pm 1 &= y_1^2 \\ x \mp 1 &= 2pqy_2^2. \end{cases}$$

Then it follows that $1 = \left(\frac{y_1^2}{p}\right) = \left(\frac{x\pm1}{p}\right) = \left(\frac{x\mp1\pm2}{p}\right) = \left(\frac{\pm2}{p}\right) = \left(\frac{2}{p}\right) = -1$, which is impossible. So $x \pm 1$ is not square in $\mathbb{N}$. From the third and the fourth item of [A-Z-T, Proposition 3.3], we deduce that $q(\mathbb{L}_{1,d}) = 4$. By Kuroda's class

number formula (cf. [Wa, p. 201]), we have

$$\begin{aligned} h_2(\mathbb{L}_{1,d}) &= \frac{1}{2^5} q(\mathbb{L}_{1,d}) h_2(pq) h_2(-pq) h_2(2pq) h_2(-2qp) h_2(2) h_2(-2) h_2(-1) \\ &= \frac{1}{2^5} q(\mathbb{L}_{1,d}) h_2(pq) h_2(-pq) h_2(2pq) h_2(-2qp) \\ &= \frac{1}{2^5} \cdot 4 \cdot 2 \cdot h_2(-pq) \cdot 2 \cdot 4 \\ &= 2 \cdot h_2(-pq), \end{aligned}$$

which proves the first claim.

b) Suppose now that d is the product of two primes p and q that congruent to 3 mod 8 then we obtain the desired result by [A-C-Z2, Corollary 2]. If $d = p$ is a prime congruent to 9 (mod 16) the result follows from the proof of Theorem 1 of [A-C-Z2, p. 7].

□

Now we have all ingredients to provide a partial proof of our first main Theorem:

Theorem 8.4.2. *Let d be of one of the following forms:*

- *$d = p$ be a prime congruent to 9 (mod 16) and assume that $(\frac{2}{p})_4 = 1$.*
- *$d = pq$ for two primes congruent to 3 (mod 8).*

Let $2^r = h_2(-2d)$. Then for $n \geq 1$ the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+r-2}\mathbb{Z}$. In the projective limit we obtain $\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Note that Theorem 8.4.2 is point a) of Theorem 8.1.1

Proof. By Theorem 8.3.6 we know that the 2-rank of the 2-class group of $\mathbb{L}_{n,d}$ equals 2 for $n \geq 1$. Furthermore, we have $\lambda^- = 1$ due to Theorem 8.3.2, and $h_2(\mathbb{L}_{1,d}) = 2^r$ by Lemma 8.4.1. By Theorem 8.3.3 the class number of $\mathbb{L}^+_{n,d}$ is odd for all n. As there is no capitulation in A^-_n according to Theorem 7.3.1 and $\lambda^- = 1$, we see that A^-_n has rank one for n large enough (see also Lemma 8.2.1). This implies that the second generator of the 2-class group of $\mathbb{L}_{n,d}$ is a class of a ramified prime in $\mathbb{L}_{n,d}/\mathbb{L}^+_{n,d}$. As the class number of $\mathbb{L}^+_{n,d}$ is odd, these ramified classes have order 2 and we obtain that the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{l_n}\mathbb{Z}$.

Let E be the elementary Λ-module associated to A_∞. Then according to [Wash, page 282-283] $\nu_{n,0}E = 2\nu_{n-1,0}E$ for all $n \geq 2$. Indeed, $\nu_{n,0} = \nu_{n,n-1}\nu_{n-1,0}$. As E has $\mathbb{Z}_2$-rank 1, we know that T acts as $2v$ on E for some $v \in \mathbb{Z}_2$. For $n \geq 2$ we have $\nu_{n,n-1} = (T+1)^{2^{n-1}} - 1 + 2$. For $n \geq 2$ the term $(T+1)^{2^{n-1}} - 1 = T^{2^{n-1}} + O(2T)$ acts as $4v'$ on E for some $v' \in \mathbb{Z}_2$. Hence, $\nu_{n,n-1}$ acts as $2(1+2v') = 2u$ on E for some unit $u \in \mathbb{Z}_2$ and all $n \geq 2$.

Consequently,

$$|E/\nu_{n,0}E| = |E/2^{n-1}E||E/\nu_{1,0}E| = 2^{n-1+c'}$$

for $n \geq 1$ and some constant $c' \geq 1$ independent of n. Note that we can rewrite this as $|E/\nu_{n,0}E| = 2^{n+c}$. Since E has only one $\mathbb{Z}_2$-generator we can assume that the pseudo-isomorphism $\phi : A_\infty \to E$ is surjective. The maximal finite submodule of A_∞ is generated by the classes $(c_n)_{n\in\mathbb{N}}$ of the ramified primes above 2. Let τ be a generator of $Gal(\mathbb{L}_{d,\infty}/\mathbb{L}_{0,d})$. Then $\tau(c_n) = c_n$ as the primes above 2 are totally ramified in $\mathbb{L}_{\infty,d}/\mathbb{L}_{0,d}$. It follows that $Tc_n = 0$. Using that $\nu_{n,0}$ is coprime to the characteristic ideal of A_∞ for all n, we obtain for every $n \geq 1$ that the kernel of $\overline{\phi} : A_\infty/\nu_{n,0}A_\infty \to E/\nu_{n,0}E$ is isomorphic to the maximal finite submodule in A_∞ and contains 2 elements. Let Y be such that $A_\infty/Y \cong A_0$. Then $A_n \cong A_\infty/\nu_{n,0}Y$ (see [Wash, page 281]). We obtain

$$|A_n| = |A_\infty/\nu_{n,0}Y| = |A_\infty/\nu_{n,0}A_\infty||\nu_{n,0}A_\infty/\nu_{n,0}Y| = 2^{n+c+1}|\nu_{n,0}A_\infty/\nu_{n,0}Y| \text{ for } n \geq 1.$$

As the maximal finite submodule in A_∞ is annihilated by $\nu_{n,0}$, we see that the size of $\nu_{n,0}A_\infty/\nu_{n,0}Y$ is constant independent of n. Hence, we obtain that the 2-class group of $\mathbb{L}_{n,d}$ is of size $2^{n+\nu}$ for all $n \geq 1$. Using that $h_2(\mathbb{L}_{1,d}) = 2^r$, we obtain $\nu = r - 1$. This yields $2 \cdot 2^{l_n} = 2^{n+r-1}$ and we obtain $l_n = n + r - 2$. Noting that $\mathbb{L}_{n,d}$ is the n-th step of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{L}_{0,d}$ finishes the proof of the first claim. As the direct term $\mathbb{Z}/2\mathbb{Z}$ is norm coherent the second claim is immediate. □

Corollary 8.4.3. *Let d be of one of the following two forms:*

a) $d = p$ a prime congruent to $9 \pmod{16}$ and assume that $(\frac{2}{p})_4 = 1$,

b) $d = pq$ for two distinct primes congruent to $3 \pmod 8$.

If d takes the first form, set $p = u^2 - 2v^2$ where u and v are two positive integers such that $u \equiv 1 \pmod 8$.
If d takes the second form set $(\frac{p}{q}) = 1$ and let the integers X, Y, k, l and m be such that $2q = k^2X^2 + 2lXY + 2mY^2$ and $p = l^2 - 2k^2m$ (see [Ka, p. 356] for their existence).
For all $n \geq 1$, we have:

a) If d is of the first form, then the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+1}\mathbb{Z}$, if and only if $(\frac{u}{p})_4 = -1$.
Outside of this particular case it is isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+r-2}\mathbb{Z}$, where $r \geq 4$ was defined in Theorem 8.4.2.

b) If d is of the second form then the 2-class group of $L_{n,d}$ is isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+1}\mathbb{Z}$ if and only if $(\frac{-2}{|X+lY|}) = -1$.

Outside of this case it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+r-2}\mathbb{Z}$, where $r \geq 4$ was defined in Theorem 8.4.2.

Proof. By Lemma 8.4.1 we know that $h_2(\mathbb{L}_{1,d}) = h_2(-2d)$. Since the 2-rank of $\mathrm{Cl}(\mathbb{L}_{1,d})$ equals 2 and $|\mathrm{Cl}_2(\mathbb{L}_{n,d})| \neq 4$ (see [A-C-Z1, Theorem 5.7]) it follows that $h_2(-2d)$ is divisible by 8. Thus if d is as in point a) [L-W 1, Theorem 2] shows that $h_2(-2d)$ is not divisible by 16 and we obtain $r = 3$.

If d is in the second case then [Ka, pp. 356-357]) implies that $h_2(-2d)$ is not divisible by 16 and again $r = 3$. □

Let us give the following example for Corollary 1.

Example 8.4.4.

- *Set $p = 89$, $u = 17$ and $v = 10$. We have $p = u^2 - 2v^2$ and $\left(\frac{2}{p}\right)_4 = -\left(\frac{u}{p}\right)_4 = 1$. So the 2-class group of $\mathbb{L}_{n,p}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+1}\mathbb{Z}$ for all $n \geq 1$.*
- *Let $p = 11$, $q = 19$, $k = 1$, $l = 3$, $m = -1$, $X = 4$ and $Y = 1$. We have: $p = l^2 - 2k^2m$ and $2q = k^2X^2 + 2lXY + 2mY^2$. Since $\left(\frac{-2}{|X+lY|}\right) = \left(\frac{-2}{7}\right) = -1$. By Corollary 8.4.3 2-class group of $\mathbb{L}_{n,p}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+1}\mathbb{Z}$ for all $n \geq 1$.*

Now we finish the proof of Theorem 8.1.1.

Theorem 8.4.5. *Assume that $d = pq$ is the product of two primes $p \equiv -q \equiv 5 \pmod 8$ and $2^r = 2 \cdot h_2(-pq)$. Then for $n \geq 1$ the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+r-1}\mathbb{Z}$.*

Note that this is point 2 of Theorem 8.1.1.

Proof. We know already from Theorem 8.3.4 that the 2-class group of $\mathbb{L}_{n,d}$ is cyclic, and by Theorem 8.3.2 we know that $\lambda(L_{0,d}) = 1$. In particular, the module A_∞ does not contain a finite submodule and is hence isomorphic to its elementary module E. Let Y be defined as in the proof of Theorem 8.4.2, then there is no $\nu_{n,0}$-torsion and we obtain that the size of $\nu_{n,0}A_\infty/\nu_{n,0}Y$ is constant independent of n. As before we obtain $|A_n| = |A_\infty/\nu_{n,0}A_\infty||\nu_{n,0}A_\infty/\nu_{n,0}Y| = 2^{n+d}$. In particular, Iwasawa's formula holds for all $n \geq 1$. Hence, $h_2(\mathbb{L}_{1,d}) = 2^r = 2^{1+\nu}$ and $\nu = r - 1$. From this the claim follows. □

Corollary 8.4.6. *Let $d = pq$ be the product of two primes p and q such that $p \equiv -q \equiv 5 \pmod 8$. Then for all $n \geq 1$, we have*

a) If $(\frac{p}{q}) = -1$, the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+1}\mathbb{Z}$.

b) If $(\frac{p}{q}) = 1$ and $(\frac{q}{p})_4 = 1$, the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+2}\mathbb{Z}$.

Outside of these two cases, the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+r-1}\mathbb{Z}$, where $r \geq 4$ was defined in Theorem 8.4.5.

Proof. Assume that d is of the first form. By [Co-Hu, 19.6 Corollary] we have $h_2(-pq) \equiv 2 \pmod 4$. Hence, $r = 2$. If d is of the second form we know that $Cl_2(\mathbb{Q}(\sqrt{-d}))$ is cyclic and divisible by 4 [Qi 1, page 1427]. As $p \equiv 5 \mod 8$ we see that $(\frac{2}{p}) = -1$ and therefore $(\frac{4}{p})_4 = -1$. Then $(\frac{4q}{p}) = -1$ and [Qi 1, Theorem 3.9] implies that $h_2(-pq)$ is not divisible by 8. Hence, $h_2(-pq) = 4$ and $r = 3$. □

For the above corollary we provide the following

Example 8.4.7.

- *Let $d = 13 \cdot 19$. We have $\left(\frac{13}{19}\right) = -1$. So the 2-class group of $\mathbb{L}_{n,p}$ is isomorphic to $\mathbb{Z}/2^{n+1}\mathbb{Z}$ for all $n \geq 1$.*

- *Let $d = 5 \cdot 11$. We have $\left(\frac{5}{11}\right) = 1$ and $\left(\frac{11}{5}\right)_4 = 1$. So the 2-class group of $\mathbb{L}_{n,p}$ is isomorphic to $\mathbb{Z}/2^{n+2}\mathbb{Z}$ for all $n \geq 1$.*

Let now X', Y' and Z be three positive integers satisfying the Legendre equation

$$pX'^2 + qY'^2 - Z^2 = 0 \tag{8.1}$$

such that

$$(X', Y') = (Y', Z) = (Z', X') = (p, Y'Z) = (q, X'Z) = 1, \tag{8.2}$$

and

$$X' \text{ odd}, Y' \text{ even and } Z \equiv 1 \pmod 4. \tag{8.3}$$

(see [L-W2] for more details)

Corollary 8.4.8. *Let $d = pq$ be the product of two primes p and q satisfying $p \equiv -q \equiv 5 \pmod 8$, $(\frac{p}{q}) = 1$ and $(\frac{-q}{p})_4 = 1$. Let X', Y' and Z be three positive integers satisfying equation* (8.1) *and the conditions* (8.2) *and* (8.3)*. If $(\frac{Z}{p})_4 \neq (\frac{2X'}{Z})$, the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+3}\mathbb{Z}$. Otherwise, it is isomorphic to $\mathbb{Z}/2^{n+r-1}\mathbb{Z}$, for $r \geq 5$ defined as in Theorem 8.4.5.*

Proof. It is immediate that the assumptions of Corollary 8.4.6 are not satisfied. Hence, we have $r \geq 4$. By [L-W2, Theorem 2] $h_2(-pq)$ is divisible by 16 if and only if $\left(\frac{Z}{p}\right)_4 = \left(\frac{2X'}{Z}\right)$. Hence if $(\frac{Z}{p})_4 \neq (\frac{2X'}{Z})$ we get $4 \leq r < 5$. Otherwise we obtain that $2 \cdot 16 \mid 2^r$ and $r \geq 5$. □

Now we close this section with some numerical examples illustrating the above corollary

Example 8.4.9.

- *Let $p = 5$, $q = 19$ and $d = -pq$. Then $X' = 1$, $Y' = 2$ and $Z = 9$ are solutions of equation* (8.1) *satisfying the condition* (8.2) *and* (8.3)*. Furthermore, $(\frac{9}{5})_4 = -(\frac{2}{9}) = -1$. Thus, the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+3}\mathbb{Z}$.*

- *Let $p = 37$, $q = 11$ and $d = -pq = -407$. Then $X' = 1$, $Y' = 56518$ and $Z = 187449$ are solutions of equation* (8.1) *satisfying the condition* (8.2) *and* (8.3)*. Furthermore, $(\frac{187449}{37})_4 = (\frac{2}{187449}) = 1$. Thus, the 2-class group of $\mathbb{L}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+r-1}\mathbb{Z}$ for some $r \geq 5$. Indeed with these settings $r = 5$ (see [L-W2, p. 230]).*

8.5 Applications

Note that Theorem 7.3.1 and Theorem 7.2.5 only hold for CM fields containing the 4-th root of unity i. Therefore, we cannot compute the 2-class groups of layers of the cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields using the same techniques as in the proof of Theorem 8.1.1. But we can still use Theorem 8.4.2 to deduce results on the class field tower of imaginary quadratic fields.

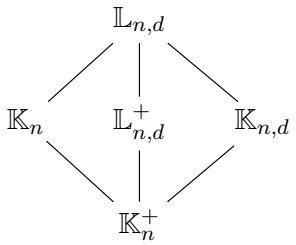


Figure 8.1: Subfields of $\mathbb{L}_{n,d}/\mathbb{K}^+_n$.

Theorem 8.5.1. *Let d be a positive square-free integer and r such that $2^r = h_2(-2d)$. Let $\mathbb{K}_{0,d} = \mathbb{Q}(\sqrt{-d})$ and denote by $\mathbb{K}_{n,d}$ the n-th step of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{K}_{0,d}$. Suppose that d takes one of the following forms:*

a) $d = pq$, for two distinct primes p and q congruent to $3 \pmod 8$.

b) $d = p$, for a prime $p \equiv 9 \pmod{16}$ such that that $(\frac{2}{p})_4 = 1$.

Then for all $n \geq 1$ the 2-class group of $\mathbb{K}_{n,d}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n+r-1}\mathbb{Z}$. In the projective limit we obtain $\mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$.

Note that this is point 1 of Theorem 8.1.2.

Proof. Let $\mathbb{K}_n = \mathbb{Q}(\zeta_{2^{n+2}})$ and $\mathbb{K}_{n,d} = \mathbb{Q}(\zeta_{2^{n+2}} + \zeta^{-1}_{2^{n+2}}, \sqrt{-d}) = \mathbb{K}^+_n(\sqrt{-d})$ (see Figure 8.1). By the class number formula (cf. [Le 1, Proposition 3 and equation (1)]) we have:

$$h_2(\mathbb{L}_{n,d}) \quad = \quad \frac{Q_{\mathbb{L}_{n,d}}}{Q_{\mathbb{K}_n} Q_{\mathbb{K}_{n,d}}} \cdot \frac{\mu_{\mathbb{L}_{n,d}}}{\mu_{\mathbb{K}_n} \mu_{\mathbb{K}_{n,d}}} \cdot \frac{h_2(\mathbb{K}_n) h_2(\mathbb{K}_{n,d}) h_2(\mathbb{L}^+_{n,d})}{h_2(\mathbb{K}^+_n)^2}.$$

It is known that $h_2(\mathbb{K}_n) = 1$ and by Theorems 8.3.3 and 8.4.2 we have $h_2(\mathbb{L}^+_{n,d}) = 1$ and $h_2(\mathbb{L}_{n,d}) = 2^{n+r-1}$, respectively. Therefore

$$2 \cdot 2^{n+r-1} = \frac{Q_{\mathbb{L}_{n,d}}}{Q_{\mathbb{K}_n} Q_{\mathbb{K}_{n,d}}} \cdot h_2(\mathbb{K}_{n,d}). \tag{8.4}$$

It is also known that $Q_{\mathbb{K}_n} = 1$. Let $k = \mathbb{Q}(i, \sqrt{d})$. As the natural norm

$$N_{\mathbb{L}_{1,d}/k} : W_{\mathbb{L}_{1,d}}/W^2_{\mathbb{L}_{1,d}} \to W_k/W^2_k$$

is surjective, we obtain that $Q_{\mathbb{L}_{1,d}}$ divides Q_k (cf. [Le 1, Proposition 1]). Since $Q_k = 1$ (cf. [Az, p. 19] and the proof of [A-C-Z2, Lemma 4]), we have $Q_{\mathbb{L}_1} = 1$. Since $N_{\mathbb{L}_{n,d}/\mathbb{L}_{n-1,d}} : W_{\mathbb{L}_{n,d}}/W^2_{\mathbb{L}_n} \to W_{\mathbb{L}_{n-1}}/W^2_{\mathbb{L}_{n-1}}$ is onto, it follows that $Q_{\mathbb{L}_{n,d}}$ divides $Q_{\mathbb{L}_{n-1,d}}$. Thus, by induction $Q_{\mathbb{L}_{n,d}} = 1$.

Note that the extensions $\mathbb{K}_{n,d}$ are essentially ramified (cf. [Le 1, p. 349]) for all $n \geq 1$. Since $\mu_{\mathbb{K}_{n,d}} = 2$ we obtain $Q_{\mathbb{K}_{n,d}} = 1$ by [Le 1, Theorem 1] . Hence, $h_2(\mathbb{K}_{n,d}) = 2^{n+r}$ for all $n \geq 1$. Since the rank of the 2-class group of $\mathbb{K}_{1,d}$ equals 2 (cf. [M-C-R, Proposition 4]) and the 2-class group of $\mathbb{K}_{n,d}$ is of type $(2, 2^\bullet)$ for n large enough (cf [Miz, p. 119]), we achieve the result. □

Now using Theorem 8.4.5 we can finish the proof of Theorem 8.1.2.

Theorem 8.5.2. *Assume that $d = pq$ is the product of two primes $p \equiv -q \equiv 5 \pmod 8$ and $2^r = 2 \cdot h_2(-pq)$. Let $\mathbb{K}_{0,d} = \mathbb{Q}(\sqrt{-d})$ and denote for $n \geq 3$ by $\mathbb{K}_{n,d}$ the n-th step of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{K}_{0,d}$. Then for $n \geq 1$ the 2-class group of $\mathbb{K}_{n,d}$ is isomorphic to $\mathbb{Z}/2^{n+r-1}\mathbb{Z}$.*

Note that this is point 2 of Theorem 8.1.2

Proof. We keep similar notations and proceed as in the proof of Theorem 8.5.1. Note that by [A-C-Z2, Proposition 3], we have $h_2(\mathbb{L}^+_{n,d}) = 2$. So as above we obtain

$$h_2(\mathbb{L}_{n,d}) \;=\; \frac{Q_{\mathbb{L}_{n,d}}}{Q_{\mathbb{K}_n} Q_{\mathbb{K}_{n,d}}} \cdot \frac{\mu_{\mathbb{L}_{n,d}}}{\mu_{\mathbb{K}_n} \mu_{\mathbb{K}_{n,d}}} \cdot \frac{h_2(\mathbb{K}_n) h_2(\mathbb{K}_{n,d}) h_2(\mathbb{L}^+_{n,d})}{h_2(\mathbb{K}^+_n)^2}.$$

Thus,

$$2^{n+r-1} \;=\; \frac{1}{1 \cdot 1} \cdot \frac{2^n}{2^n \cdot 2} \cdot \frac{1 \cdot h_2(\mathbb{K}_{n,d}) \cdot 2}{1}.$$

It follows that $h_2(\mathbb{K}_{n,d}) = 2^{n+r-1}$ for all n. Since $\mathbb{L}_{n,d}/\mathbb{K}_{n,d}$ is ramified, it is obvious that 2-rank$(\mathrm{Cl}(\mathbb{K}_{n,d})) \leq$ 2-rank$(\mathrm{Cl}(\mathbb{L}_{n,d})) = 1$ (Theorem 8.4.5). In particular, $\mathrm{Cl}(\mathbb{K}_{n,d})$ is cyclic. □

Bibliography

[Ax] Ax, J.,(1965) *On the units of an algebraic number field* Illinois Journal of Mathematics, **9**, pp. 584-589.

[Az] Azizi, A., (1999) *Unités de certains corps de nombres imaginaires et abéliens sur* $\mathbb{Q}$*,* Ann. Sci. Math. Québec, **23** , 15-21.

[A-C-Z1] Azizi, A., Chems-Eddin, M.M. and Zekhnini, A., *On the rank of the* 2*-class group of some imaginary triquadratic number fields.* arXiv:1905.01225v3. To appear in Rendiconti del Circolo Matematico di Palermo series 2.

[A-C-Z2] Azizi, A., Chems-Eddin, M. M. and Zekhnini, A., *On some imaginary triquadratic number fields* k *with* $cl_2(k) = (2, 4)$ *or* $(2, 2, 2)$ arXiv:2002.03094. To appear in Commentationes Mathematicae Universitatis Carolinae.

[A-Z-T] Azizi, A., Zekhnini, A. and Taous, M. (2016) *On the strongly ambiguous classes of some biquadratic number fields. Math. Bohem.,* **141** , 363–384.

[Ba-Sa] Barman, R. and Saikia A. (2010) *A note on Iwasawa* μ*-invariants of ellipitc curves* Bull Baz. Math Soc. New Series 41(3), pp. 399-407.

[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.

[Bl] Bley, W. (2006) *Equivariant tamagawa conjecture for abelian extensions of a auadratic imaginary field*: Dokumenta Mathematica 11, pp 73-118

[Br] Brumer, A. (1967) *On the units of algebraic number fields* Mathematika 14(2), pp. 121-124.

[C] Chems-Eddin, M. M., *The rank of the* 2*-class group of some number fields with large degree.* arXiv:2001.00865v2.

[C-A-Z] Chems-Eddin, M. M, Azizi, A. and Zekhnini, A., *On the* 2*-class group of some number fields with large degree.* arXiv:1911.11198. To appear in Algebra colloquium

[C-K-L] Choi, J., Kezuka, Y., Li, Y. (2019). *Analogues of Iwasawa's* $\mu = 0$ *conjecture and weak Leopoldt theorem for certain non-cyclotomic* $\mathbb{Z}_2$*-extensions*: Asian Journal of Mathematics, Vol. 23, No. 3, pp 383-400

[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-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.

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

[Co-Hu] Conner, P. E. and Hurrelbrink, J., (1988) *Class number parity* Ser. Pure Math., vol. **8**, World Scientific, Singapore .

[Cr] Crişan, V. (2019) *The split prime μ conjecture and further topics in Iwasawa theory* PhD Thesis University Göttingen.

[Cr-M] Crişan, V., Müller, K. (2020) *The Vanishing of the μ-Invariant for Split Prime $\mathbb{Z}_p$-extensions over Imaginary Quadratic Fields* The Asian Journal of Mathematics, 24(**2**), 267-302.

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

[Fe] Federer, L. (1982) *p-adic L-functions, regulators and Iwasawa modules* Phd Thesis, Princton.

[Fe-Gr] Federer, L., Gross, B.H: (1981) *Regulators and Iwasawa modules* (1981) Invent. Mathematicae 62, pp. 443-457.

[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.

[Fr] Fröhlich, A., (1983) Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields, Contemporary Mathematics vol. **24** American Mathematicla Society, Providence .

[Gil 1] 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 2] 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 d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe*: Journal für die Reine und Angewandte Mathematik 327, pp. 184-218 .

[Gre 1] Greenberg, R. (1971) *On some questions concerning the Iwasawa invariants* Princton University Thesis.

[Gre 2] Greenberg, R. (1973) *On a certain l-adic representation* Inventiones math. 21 pp. 117-124.

[Gre 3] Greenberg, R. (1976) *On the Iwasawa invariants of totally real number fields* American Journal of Mathematics, Vol.98, No1. pp. 263-284.

[Gre 4] Greenberg, R. (1978). *On the structure of certain Galois groups*: Invent. Math., 47, pp. 85-99.

[Gre 5] Greenberg, R. (2003) *Galois theory of the Selmer group of an abelian variety* Compositio Mathematicae (136) pp. 255-297.

[Gre 6] Greenberg, R. *Topics in Iwasawa theory* `https://sites.math.washington.edu/~greenber/book.pdf`

[Gre-Vat] Greenberg, R. and Vatsal, V. (2000) *On the Iwasawa inariants of elliptic curves* Invent. Math. 142 , pp 17-63.

[Gr] Greither, C. (1992). *Class groups of abelian fields, and the main conjecture* Annales de L'Institut Fourier 42, no 3, pp 449-499.

[Gro 1] Gross, B.H. (1981) *p-adic L-series at* $s = 0$ J. Math Sci. University Tokyo Sec. Math 28(3), pp. 979-994.

[Gro 02] Gross, B. (1980) *Arithmetic on elliptic curves with complex multiplication*: Lecture Notes in Mathematics 766, Springer-Verlag. Berlin Heidelberg.

[Gu] Guillott, P. (2018) *A Gentle Course in Local Class Field Theory* Cambridge University Press, Cambridge.

[Ho-Kl] Hofer, M. and Kleine, S.(2020) *On the Gross Order of Vanishing Conjecture for Large Vanishing Orders*, preprint arXiv:2102.01573.

[Ha-Le] Hatley, J. and Lei, A. (2019) *Arithmetic Properties of Signed Selmer Groups at Non-Ordinary Primes* Annales de l'Institut Fourier, Tome 69 no 3, pp. 1259-1294.

[Ha-Le-Vi] Hatley J. Lei, A. and Vigni S. (2020) *On* Λ*-Submodules of Finite Index of Anticyclotomic Plus an Minus Selmer Groups* preprint arXiv:2003.10301

[Iw 1] Iwasawa, K., (1959) *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc., **65** , 183–226.

[Iw 2] Iwasasawa, K. (1973) *On $\mathbb{Z}_l$-extensions of algebraic number fields* Annales of Mathematics, 2nd series, 98 (2) pp. 246-326.

[Iw 3] Iwasawa, K. (1986) *Local class field theory* Oxford mathematical Monographs, Oxford University Press, New York.

[Ja] Janusz, G. J. (1973), *Algebraic number fields* Pure and Applied Mathematics Volume 55, !st edition, Academic Press, New York.

[Jau 1] Jaulent, J.-F. (2002) *Classes logarithmiques des corps totalement réels* Acta Arith., 103(1), pp. 1-7.

[Jau 2] Jaulent, J.-F. (2017) *Normes cyclotomiques naïves et unités logarithmiques* Acta Math., 108(6) pp. 545-554.

[Ka] Kaplan, P., (1976) *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math., **283-284** , 313–363.

[Kat] Kato, K. (2004) *P-adic hodge theory and values of Zeta-functions of modular forms* Astérisque, tome 295, pp.117-290.

[Ke 1] Kezuka, Y. (2017) *On the Main Conjecture of Iwasawa theory for certain elliptic curves with complex multiplication*, PhD-Thesis, University of Cambridge, Cambridge.

[Ke 2] Kezuka, Y. (2019) *On the Main conjecture of Iwasawa theory for certain non-cyclotomic $\mathbb{Z}_p$-Extension* J. London Math. Soc., Vol. 100, pp. 107-136.

[Ki] Kida,Y. *Cyclotomic $\mathbb{Z}_2$-extensions of J-fields*,(1982) J. Number Theory, **14** , 340-352.

[Kim] Kim, B.D. (2009) *The Iwasawa invariants of Plus/Minus Selmer groups* Asian Journal of Mathematics, 13 **2** pp.181-190.

[Kl 1] Kleine, S. (2015) *A new approach to the investigation of Iwasawa invariants* PhD-Thesis University Göttingen.

[Kl 2] Kleine, S. (2019) *T-ranks of Iwasawa modules* Journal of Number Theory, Vol 196, pp. 61-86.

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

[Kum] Kumakawa M. (2016) *Greenberg's Conjecture for the cyclotomic $\mathbb{Z}_2$-extension of Certain Number Fields of Degree 4* Tokyo J. Math Vol 39 Nr 1.

[Ku 1] Kuz'min, L.v. (1972) *The Tate module for algebraic number fields* Izv. Akad. Nauk SSSR Ser. Mat. 36(2), pp. 267-327.

[Ku 2] Kuz'min, L.v. (2018) *Local and global universal norms in the cyclotomic $\mathbb{Z}_p$ extension of an algebraic number field* Izvestiya: Mathematics, Volume 82, Issue 3, pp. 532-548.

[La] Lang, S. (1990) *Cyclotomic Fields I and II. With an Appendix by Karl Rubin* 2nd edition, New York, Springer.

[Le 1] F. Lemmermeyer,(1995) *Ideal class groups of cyclotomic number fields I,* Acta Arith., 72 , 347–359..

[Le 2] Lemmermeyer, F. (2013) *The ambigous class number formula revisted* Journal of the Ramanujan Math. Soc. Vol. 28 (4), pp. 415-421.

[L-W 1] Leonard, P. A. and Williams,K. S. (1982) *On the divisibility of the class numbers of $\mathbb{Q}(\sqrt{-d})$ and $\mathbb{Q}(\sqrt{-2d})$ by* 16, Can. Math. Bull., **25** , 200-206.

[L-W2] Leonard, P. A. and Williams,K. S. (1983) *On the divisibility of the class number of $\mathbb{Q}(\sqrt{-pq})$ by 16*, Proc. Edinburgh Math. Soc., **26** , 221-231.

[Li-Mu] Lim, M.F. and Murty, V.K. (2016) *The growth of fine Selmer Groups* Journal of the Ramanujan Math Soc. Voulme 31, Issue 1, pp. 79-94.

[L-Y-X-Z] Li,J., Ouyang Y., Xu, Y.and Zhang,S. *l-class groups of fields in Kummer towers*, arXiv:1905.04966.

[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.

[Ma] Matar, A. (2020) *On the Lambda-Cotorsion subgroup of the Selmer group* Asian Journal of Mathematics, Volume 24, no 3, pp. 437-456.

[M-C-R] McCall, T. M, Parry,C. J., Ranalli,R. R. (1995) *Imaginary bicyclic biquadratic fields with cyclic* 2*-class group*, J. Number Theory, 53 , 88-99.

[Mil] Milne, J.S. (2006) *Arithmetic Duality Theorems* BookSurge, LLC, Charleston, SC.

[Miz] Mizusawa, Y. (2010) *On the maximal unramified pro-2-extension over the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic field*, J. de Theor. des Nr. de Bordeaux, **22** , 115-138.

[Mu] K. Müller. (2019) *Capitulation in the $\mathbb{Z}_2$ extension of CM number fields*, Math. Proc. Camb. Phil. Soc., **166** , 371-380.

[Ne 1] Neukirch, J. (1999) *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften (A series of comprehensive studies in mathematics) volume 322, Springer, Berlin-Heidelberg.

[Ne 2] Neukirch, J. (2013) *Class field Theory*, Springer Berlin-Heidelber

[Ne-Sc-Wi] Neukirch, J. , Schmidt, A. and Wingberg, A. (2008) *Cohomology of Number Fields*, Grundlehren der mathematischen Wissenschaften (A series of comprehensive studies in mathematics) volume 323 2nd edition, Springer, Beerlin Heidelberg.

[Ou] Oukhaba, H. (2012) *On Iwasawa Theory of elliptic units and 2-class groups* J. Ramanujan Math. Soc. 27, no 3, pp 255-373.

[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.

[Oz-Ta] Ozaki, M. and Taya, H. (1997) *On the Iwasawa λ_2-invariants of certain families of real quadratic fields* manuscripta math. 94, 437-444.

[Qi 1] Yue,Q.(2011) *8-ranks of class groups of quadratic number fields and their densities*, Acta Math. Sin. **17** , 1419–1434.

[Qi 2] Q. Yue, (2009)*The generalized Rédei-matrix*, *Mathematische Zeitschrift* **261**, 23–37.

[Ra-Wi] (2018) Ramdorai, S. and Witte, M. *Fine Selmer Groups and Isogeny invariance* In: Akbary A., Gun S. (eds) Geometry, Algebra, Number Theory, and Their Information Technology Applications. GANITA 2016. Springer Proceedings in Mathematics & Statistics, vol 251. Springer.

[Ra-Ra] (2020) Ray, A. and Ramdorai, S. *Euler Characteristics and their Congruences for Multisigned Selmer groups* preprint arXiv:2011.05387.

[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 1] Rubin, K. (1988)*On the main conjecture of Iwasawa theory for imaginary quadratic fields*: Invent. Math. 93, pp 701-7013

[Ru 2] Rubin, K. (1991). *The "main conjectures" of Iwasawa Theory for imaginary quadratic fields*: Invent. Math., 103, pp. 25-68.

[Ru 3] Rubin, K. (1990). *The Main Conjecture Appendix to the second edition of S. Lang: Cyclotomic Fields I and II* Graduate Texts in Mathematics 121, Springer.

[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.

[Ts] Tsuji, T. (1999) *Semi-Local Units modulo Cyclotomic Units* J. Nubmer Theory, Volume 78, Issue 1, pp 1-26.

[Ve] Venjakob, O. (2002) *On the Structure Theory of the Iwasawa Algebra of a p-adic Lie Group* J. Eur. Math. Soc. (4) pp. 271-311.

[Vi-1] Viguié, S (2012) *Global Units modulo elliptic units and* 2 *class groups* Internationl Journal of number Theory, volume 8, nr. 3, pp 569-588.

[Vi-2] Viguié, S. (2016) *On the classical main conjecture for imaginary quadratic fields* Pioneer Journal of Algebra, Number Theory and its applications, Volume 12, Issue 1-2, pp. 1-27. See also arXiv:1103.1125 (2011).

[Wa] Wada,H. (1966) *On the class number and the unit group of certain algebraic number fields*, J. Fac. Sci. Univ. Tokyo, **13** , 201–209.

[Wash] Washington, L.C. (1997) *Introduction to cyclotomic fields*, 2nd Edition, Graduate Texts in Mathematics 83: Springer, New York.

[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.