Iwasawa Theory

Bence Forrás

13th April 2020

Master's Thesis Mathematics

Advisor: Prof. Dr. Peter Scholze

Second Advisor: Dr. Dustin Clausen
Mathematisches Institut

Mathematisch-Naturwissenschaftliche Fakultät der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Acknowledgements

First and foremost, I wish to express my gratitude to my (unofficial) advisor, Dr Dustin Clausen, for introducing me to the fascinating world of Iwasawa theory. I am grateful for all his explanations and ideas as well as the constant support and encouragement he provided during this time. I also thank Professor Peter Scholze for taking on the role of official advisor and all the duties that came with that.

I am grateful to the Bonn International Graduate School (BIGS) for awarding me a Two-Year Qualifying Scholarship, which made it possible for me to truly focus on my studies. Furthermore, I recognise the invaluable contribution of those who share their wisdom online or are committed to the unhindered flow of human knowledge, from professors making their notes freely available to students asking and answering questions on Stackexchange. These people make the world a better place.

Last but not least, I express my appreciation for all the help and support I received during my Master's studies, most notably from my family and friends. You know who you are.

Contents

Introduction

The main goal of this thesis is to give an introduction into some basic concepts of Iwasawa theory, most importantly a proof of the so-called main conjecture. Our aim is to present this in a very detailed way, suitable for anyone with a background in algebraic number theory. While there already exist quite a few accounts of the topics this thesis covers, the level to which they are able to be readily understood may be deemed a bit too low, especially when it comes to the proof of the main conjecture. Our hope is that this thesis may provide some help on this front.

Outline

The thesis is structured as follows.

Chapter 1 introduces some basic notions of Iwasawa theory, including the structure theory of modules over the completed group ring $\mathbb{Z}_p[\![T]\!]$ and Iwasawa's theorem on the p-part of class numbers in a $\mathbb{Z}_p$-extension. The proof involves standard techniques of Iwasawa theory, which will be used in the sequel.

Chapter 2 gives a very brief overview of the theory of (analytic) p-adic L-functions. The aim here was not to present a thorough exposition but to give just enough context for the interpretation of the Iwasawa main conjecture in the next chapter.

Chapter 3 is the heart of the thesis. Here we explain the statement of the Iwasawa main conjecture. Roughly speaking, this asserts the equivalence of the p-adic L-functions of Chapter 2 with the characteristic power series—introduced in Chapter 1—of an Iwasawa module. We then present Rubin's proof of the main conjecture using so-called Euler systems. The proof is rather complex, so in order to ease understanding, we have included a discussion of the ideas at play before performing the actual proof.

Finally, in **Appendix A** we discuss how the analogy between function fields and number fields, and thus the theory of curves over finite fields, motivates the study of Iwasawa theory. The appendix can be read mostly independently of the rest of the text; it requires some familiarity with algebraic geometry.

About notations

As of yet, there appears to be no wide consensus on notation in Iwasawa theory: that used by Iwasawa in his seminal papers has been superseded by various different systems of notation. To make things more complicated, authors frequently use the same notation for similar but different objects. In the present text we aimed to conform with notation used in some recent works, in particular those used by Sharifi in e.g. [Sha]. A list of notations can be found on page 69.

Throughout the whole text, $\mathbb{N} = \{1, 2, \ldots\}$ shall denote the set of positive integers, and p shall be an odd rational prime. Most statements can be extended to the case $p = 2$ with slight modifications.

We fix, once and for all, a compatible system of primitive p-power roots of unity ζ_{p^n} for $n \in \mathbb{N}$, compatibility meaning that $\zeta_{p^{n+1}}^p = \zeta_{p^n}$. As usual, we let μ_r denote the group of r^{th} roots of unity for $r \in \mathbb{N}$, $\mu_{p^\infty} := \bigcup_{n \geqslant 0}$ be the group of p-power roots of unity, and

$$\mathbb{Q}(\mu_{p^\infty}) := \bigcup_{n \geqslant 0} \mathbb{Q}(\mu_{p^{n+1}})$$

About references

The present text is primarily based upon the books of Lang [Lan90] and Washington [Was97]. Both are comprehensive accounts of the theory of cyclotomic fields, including basic Iwasawa theory and a proof of the main conjecture, covering a much larger amount of material than the present text. Whenever we do not state otherwise, these should be understood to be the references.

Coates and Sujatha's book [CS06] was also used as a reference; it is focused on the p-adic zeta function and Rubin's proof of the main conjecture. Their exposition of the material is self-contained but less elementary than that of the present text; in particular, it relies heavily on using measures.

A good reference for some of the key ideas is [KKS12]. We also recommend the lecture notes [Sha]. The reader is encouraged to consult any and all of these references for slightly different perspectives.

Chapter 1

$\mathbb{Z}_p$-extensions

In this chapter we shall introduce some basic notions of Iwasawa theory. In the first section we will survey a few results about modules over the ring $\Lambda = \mathbb{Z}_p[\![T]\!]$. This ring is called the *Iwasawa algebra*, and we will refer to Λ-modules as *Iwasawa modules*. There is a structure theorem of finitely generated Λ-modules, which will be of paramount importance.

To illustrate this, let K_∞/K be a Galois extension with Galois group $\mathbb{Z}_p$; such a field extension is called a *$\mathbb{Z}_p$-extension.* Then the non-trivial closed subgroups of the Galois group are $p^n\mathbb{Z}_p$, and it follows from the fundamental theorem of infinite Galois theory that the Galois subextensions form a tower

$$K_\infty \subset \ldots \subset K_n \subset \ldots \subset K_1 \subset K_0 = K$$

where $\mathrm{Gal}(K_\infty/K_n) = p^n\mathbb{Z}_p$. It turns out that in this setting, certain groups can be endowed with a Λ-module structure, allowing us to use the aforementioned structure theorem to extract more information about the extension.

In Section 1.1 we give will discuss the structure theorem and some related notions which will be used extensively in the sequel.

Section 1.2 contains a standard proof of Iwasawa's theorem on the orders of p-parts of class groups in a $\mathbb{Z}_p$-extension of a number field. The proof we give is rather elementary and detailed, aimed at a reader with modest background. In particular, we will only use basic algebraic number theory, with the unavoidable exception of using the existence of Hilbert class fields as well as the isomorphism between their Galois groups and the ideal class groups. A reader unfamiliar with class field theory may take these statements for granted.

In Section 1.3, we will present some further results on various Iwasawa modules, using the machinery of the preceding section. Here we will already need to use a lot of class field theory. The results in this section will be used in the proof of the main conjecture in Chapter 3.

The default references for this chapter are [Was97, Chapter 13] and [Lan90, Chapter 5].

1.1 The structure of Λ-modules

We will often work with fields resp. field extensions whose class groups, Galois groups, groups of units etc. possess a $\mathbb{Z}_p[\![T]\!]$-module structure. We call $\Lambda := \mathbb{Z}_p[\![T]\!]$ the *Iwasawa algebra.* In this section we survey some of the basic results concerning Λ-modules. For a more detailed exposition, see [Was97, §13.2] or [Lan86, Chapter 5, §§1–3].

We recall two important theorems from p-adic analysis [Was97, §7.1].

Definition 1.1.1. A nonconstant polynomial in $\mathbb{Z}_p[T]$ *distinguished* if it is monic and all coefficients but the leading one are divisible by p.

The following theorem states that there is a division algorithm for distinguished polynomials. (Note that we cannot hope for a division algorithm for the whole ring Λ, because that would imply being a principal ideal domain, which Λ is not: the ideal (p, T) is not principal.)

Theorem 1.1.2 (p-adic Weierstrass division theorem). *Let $f \in \Lambda$ be a power series, $P \in \mathbb{Z}_p[T]$ a distinguished polynomial. Then there exist unique $q \in \Lambda$ and $r \in \mathbb{Z}_p[T]$ such that $f = qP + r$ and $\deg r < \deg P$.* □

Theorem 1.1.3 (p-adic Weierstrass preparation theorem). *Any nonzero $f(T) \in \Lambda = \mathbb{Z}_p[\![T]\!]$ can be written uniquely as $f(T) = p^\mu P(T)U(T)$ where $\mu \geqslant 0$ is an integer, $P(T) \in \mathbb{Z}_p[T]$ is a distinguished polynomial, and $U(T) \in \Lambda^\times$ is a unit.* □

Corollary 1.1.4. *Λ is a UFD.*

Proof. Apply Weierstrass preparation, then repeated Weierstrass division for the distinguished factor. It follows that Λ is a UFD with the irreducible elements being p and the irreducible distinguished polynomials. □

We return to the study of Λ-modules; specifically, to one of the many incarnations of Nakayama's lemma. Note that Λ is a topological module.

Lemma 1.1.5 (Nakayama). *Let X be a compact Λ-module. Then the following hold.*

(1) X is finitely generated over Λ iff $X/(p, T)X$ is finite;
(2) $X = 0$ iff $X/(p, T)X = 0$.

Proof. If X is finitely generated then $X/(p, T)X$ is finite because $\Lambda/(p, T)\Lambda$ is finite.

For the other direction of the first assertion, we first claim that for any compact Λ-module X we have

$$\bigcap_{n=0}^{\infty} (p, T)^n X = 0 \tag{1.1}$$

Let U be a neighbourhood of 0. For each $x \in X$ there is a neighbourhood U_x such that $(p, T)^n U_x \subseteq U$ because $(p, T)^n \to 0$ in Λ. Finitely many of these sets U_x cover X by compactness. Since we may choose U to be arbitrarily small, this proves the claim.

Now suppose that $X/(p, T)X$ is finite, in particular, let $X/(p, T)X = \{\overline{x_1}, \ldots, \overline{x_k}\}$ where $\overline{x_i}$ is the image of $x_i \in X$ under the quotient map. Let $Y := \Lambda x_1 + \ldots + \Lambda x_k$. This is a compact Λ-module because X is, and therefore so is X/Y. By definition, $Y + (p, T)X = X$, which implies $(p, T)X/Y = X/Y$. It follows by induction that $(p, T)^n X/Y = X/Y$ for all $n \geqslant 0$. Then (1.1) proves $X/Y = 0$. Hence X is generated by $x_1, \ldots, x_k$. This finishes the proof of the first assertion.

The second assertion follows from this proof by letting $k := 0$. □

Definition 1.1.6. A morphism of Λ-modules $\varphi : X \to Y$ with finite kernel and cokernel is called a *pseudo-isomorphism.* Two Λ-modules X and Y are *pseudo-isomorphic* if there exists a pseudo-isomorphism $X \to Y$. This is denoted by $X \sim Y$.

Remark 1.1.7. Some authors use the term *quasi-isomorphic.*

Theorem 1.1.8 (Structure theorem of finitely generated Λ-modules)**.** *Let X be a finitely generated module over Λ. Then there exist distinguished irreducible polynomials $f_j \in \mathbb{Z}_p[T]$ such that*

$$X \sim \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{n_i}\Lambda \oplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j}\Lambda$$

where $r, s, t, n_i, m_j \in \mathbb{N}$.

Proof. Here we only sketch the proof; for details see [Was97, Theorem 13.12]. The proof is similar to that of the structure theorem of finitely generated modules over PIDs. (For a more general statement and proof, cf. [NSW15, (5.1.10)].)

Let X have generators $u_1, \ldots, u_n$, let the relations between these generators be given by equations $\lambda_{1,j}u_1 + \ldots + \lambda_{n,j}u_n = 0$. Then the matrix $(\lambda_{i,j})$ describes the structure of X.

We will perform the following operations on $(\lambda_{i,j})$. The first three are the usual row and column operations providing isomorphisms of modules, while the other three are specific to Λ and only provide pseudo-isomorphisms from X to another module. It is clear that the composition of pseudo-isomorphisms is a pseudo-isomorphism, that is, the pseudo-isomorphism relation is transitive.

A. Permute rows or columns.
B. Add a multiple of a row resp. column to another row resp. column.
C. Multiply a row or column by a unit in Λ.

1. If all elements of a row except for one are divisible by p then we may divide these elements by p and multiply all other elements in the column of the exceptional element by p. We obtain a pseudo-isomorphism $X \hookrightarrow X' = X \oplus v\Lambda$ for a new generator v (and some relations). (In the formula below, this operation is applied k times.)

$$\begin{pmatrix} \lambda_{1,1} & p^k\lambda'_{1,2} & \cdots & p^k\lambda'_{1,m} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,m} \end{pmatrix} \rightsquigarrow \begin{pmatrix} \lambda_{1,1} & \lambda'_{1,2} & \cdots & \lambda'_{1,m} \\ p^k\lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ p^k\lambda_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,m} \end{pmatrix}$$

2. If all entries of a row as well as a column are divisible by p^k ($k \in \mathbb{N}$) and the entry in their intersection isn't divisible by p^{k+1} then we may divide all elements of the row by p^k. (In the formula below, $p \nmid \lambda'_{1,1}$.) We obtain a pseudo-isomorphism $X \hookrightarrow X \oplus v\Lambda = X' \oplus \Lambda/(p^k)$ where the newly constructed matrix describes the relations in X'. Since $\Lambda/(p^k)$ is already of the desired form, we need only focus on X'.

$$\begin{pmatrix} p^k\lambda'_{1,1} & p^k\lambda'_{1,2} & \cdots & p^k\lambda'_{1,m} \\ p^k\lambda'_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ p^k\lambda'_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,m} \end{pmatrix} \rightsquigarrow \begin{pmatrix} \lambda'_{1,1} & \lambda'_{1,2} & \cdots & \lambda'_{1,m} \\ p^k\lambda'_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ p^k\lambda'_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,m} \end{pmatrix}$$

3. If all entries of a row $(\lambda_{i,1}, \ldots, \lambda_{i,m})$ are divisible by p^k, and for some $p \nmid \lambda \in \Lambda$, we have that $(\lambda\lambda_{i,1}, \ldots, \lambda\lambda_{i,m})$ is also a relation in X (but not necessarily a row of our matrix) then we may divide all elements of the row by p^k. We obtain a pseudo-isomorphism $X \twoheadrightarrow X'$.

$$\begin{pmatrix} p^k\lambda'_{1,1} & p^k\lambda'_{1,2} & \cdots & p^k\lambda'_{1,m} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,m} \end{pmatrix} \rightsquigarrow \begin{pmatrix} \lambda'_{1,1} & \lambda'_{1,2} & \cdots & \lambda'_{1,m} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,m} \end{pmatrix}$$

Using operations A, B, C, 1, and 2 inductively, we can bring our matrix to a diagonal form, with the elements in the diagonal consisting of distinguished polynomials and zeros. Operation 3 is used only at the end of the process when we deal with zeros in the diagonal. Putting the summands $\Lambda/(p^k)$ back, we obtain a pseudo-isomorphism

$$X \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{n_i}\Lambda \oplus \bigoplus_{j=1}^{q} \Lambda/\lambda_{j,j}\lambda_\Lambda$$

Here the $\lambda_{j,j}$'s may not be irreducible, but this can be resolved by using that the natural morphism $\Lambda/(fg) \hookrightarrow \Lambda/(f) \oplus \Lambda/(g)$ has finite cokernel whenever $f, g \in \Lambda$ are coprime (cf. [Was97, Lemma 13.8.1]). This finishes the proof. □

Example 1.1.9 (Pseudo-isomorphism is not symmetric). To construct a counterexample, consider the inclusion of the ideal $(p, T) \hookrightarrow \Lambda$. This is a pseudo-isomorphism of Λ-modules: the kernel is trivial and the cokernel is $\mathbb{Z}_p[\![T]\!]/(p, T) \simeq \mathbb{Z}_p/(p) \simeq \mathbb{Z}/p\mathbb{Z}$, so we have $(p, T) \sim \Lambda$. However, we claim that $\Lambda \nsim (p, T)$. Indeed, suppose we have a pseudo-isomorphism $\varphi : \Lambda \to (p, T)$. Then $\operatorname{Im}\varphi = (f(T))$ where $f(T) = \varphi(1)$, and $\operatorname{Coker}\varphi = (p, T)/(f)$. Since $\Lambda/(p, T) \simeq \mathbb{Z}/p\mathbb{Z}$ is finite, the cokernel is finite iff $\Lambda/(f)$ is finite. This is not the case: write $f = p^k g$ where $p \nmid g$. Then $\Lambda/(p^k) \sim (\mathbb{Z}/p^k\mathbb{Z})[\![T]\!]$ is infinite, and $\Lambda/(g)$ is infinite as well by the p-adic Weierstrass division theorem (Theorem 1.1.2), hence $\Lambda/(f)$ is infinite.

This demonstrates that the obstruction to symmetry in the pseudo-isomorphism relation lies in the free part. The following lemma makes this more precise.

Lemma 1.1.10. *The pseudo-isomorphism relation is symmetric for finitely generated torsion Λ-modules.*

Proof. This will follow once we show that the pseudo-isomorphism in the structure theorem can be reversed in this case. To construct this morphism, run the algorithm in the proof of the structure theorem. The morphisms obtained by using operations A, B, and C are isomorphisms, hence they can be reversed. Morphisms coming from operations 1 and 2 are inclusions of X into a direct sum $X \oplus v\Lambda$; replace them with projections $X \oplus v\Lambda \twoheadrightarrow X$. These will have finite kernels for the same reason the inclusions had finite cokernels. By using these operations, we bring our matrix to diagonal form. We know that there are no zeros in the diagonal since those would correspond to free parts of which there is none due to the module being torsion. Thus we obtain a pseudo-isomorphism

$$\bigoplus_{i=1}^{s} \Lambda/p^{n_i}\Lambda \oplus \bigoplus_{j=1}^{q} \Lambda/\lambda_{j,j}\lambda_\Lambda \to X$$

We again factor the $\lambda'_{j,j}s$ using that there is an injection $\Lambda/(f) \oplus \Lambda/(g) \hookrightarrow \Lambda/(fg)$ with finite cokernel whenever $f, g \in \Lambda$ are coprime (cf. [Was97, Lemma 13.8.2]). □

A more general—but not more illuminating—proof of Lemma 1.1.10 can be found in [NSW15, p. 271, Remark 1.].

Corollary 1.1.11. *The pseudo-isomorphism relation is an equivalence relation for finitely generated torsion Λ-modules.*

Proof. Reflexivity is clear, and symmetry has just been proven in Lemma 1.1.10. It is easily seen that the composite of two morphisms with finite kernel and cokernel also has finite kernel and cokernel, proving transitivity. □

Definition 1.1.12. Consider a finitely generated torsion Λ-module X. Using Theorem 1.1.8, write

$$X \sim \bigoplus_{i=1}^{s} \Lambda/p^{n_i}\Lambda \oplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j}\Lambda$$

We define the characteristic ideal of X by

$$\mathrm{Char}(X) := \left(\prod_{i=1}^{s} p^{n_i}\right)\left(\prod_{j=1}^{t} f_j(T)^{m_j}\right)\Lambda$$

This is easily seen to be well-defined and invariant under pseudo-isomorphisms. A generator of the characteristic ideal is called a *characteristic polynomial* of X. If all $n_i = 0$ (which we will later call the $\mu = 0$ case, see Definition 1.1.14 below) then the characteristic ideal is generated by the characteristic polynomial of the multiplication-by-T linear map; cf. [KKS12, Proposition 10.23] for details.

Lemma 1.1.13. *Characteristic ideals are multiplicative in short exact sequences. That is, if*

$$0 \to Y' \to Y \to Y'' \to 0$$

is a short exact sequence of finitely generated torsion Λ-modules then

$$\mathrm{Char}(Y) = \mathrm{Char}(Y')\,\mathrm{Char}(Y'')$$

Proof. Let

$$0 \to Y \xrightarrow{\varphi} \bigoplus_{i} \Lambda/f_i(T)^{m_i}\Lambda \to \mathrm{Coker}\,\varphi \to 0$$

where $f_i(T) \in \Lambda$ is either irreducible or p, and $\mathrm{Coker}\,\varphi$ is finite (the kernel is zero because Y is torsion, see the proof of Theorem 1.1.8). Let $f \in \Lambda$ be either an irreducible polynomial or p, and tensor by $\Lambda_{(f)}$; this preserves exactness [Stacks, Tag 00CS].

$$0 \to Y \otimes_\Lambda \Lambda_{(f)} \xrightarrow{\varphi} \bigoplus_{i} \Lambda_{(f)}/f_i(T)^{m_i}\Lambda_{(f)} \to \mathrm{Coker}\,\varphi \otimes_\Lambda \Lambda_{(f)} \to 0$$

For any $g \in \Lambda\backslash((p,T) \cup (f))$ there is some $n \in \mathbb{N}$ such that $g^n\,\mathrm{Coker}\,\varphi = 0$ by finiteness, and g becomes a unit under localisation, thus $\mathrm{Coker}\,\varphi \otimes_\Lambda \Lambda_{(f)} = 0$. Moreover, for all i such that $(f) \neq (f_i)$, f_i also becomes a unit, thus these terms in the direct sum vanish. We have proved

$$Y \otimes_\Lambda \Lambda_{(f)} = \bigoplus_{(f_i)=(f)} \Lambda_{(f)}/f_i(T)^m_i\Lambda_{(f)}$$

Doing this for Y' and Y'', and all $f := f_i$'s finishes the proof. □

Definition 1.1.14. Let X be a finitely generated Λ-module and write

$$X \sim \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{n_i}\Lambda \oplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j}\Lambda$$

Let $\mu := \sum_{i=1}^{s} n_i$ and $\lambda := \sum_{j=1}^{t} \deg f_j(T)^{m_j}$. These λ resp. μ are called the λ- resp. *μ-invariant* of the module X.

1.2 Iwasawa's theorem on the growth of the class number

Let K be a number field and K_∞/K a $\mathbb{Z}_p$-extension, i.e. $\Gamma := \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, and let K_n be the subextension corresponding to the subgroup $p^n\mathbb{Z}_p$ for $n \geqslant 0$ (in particular, $K_0 = K$). Then the ideal class group $\mathrm{Cl}(K_n)$ is a finite abelian group, and therefore can be decomposed as

$$\mathrm{Cl}(K_n) = A_n \oplus A'_n \tag{1.2}$$

where A_n is the p-Sylow subgroup. In particular, A_n has order p^{e_n} for some exponent e_n.

Theorem 1.2.1 (Iwasawa). *There exist $n_0, c \in \mathbb{N}_0$ such that for all $n \geqslant n_0$ we have $e_n = \mu p^n + \lambda n + c$.*

Remark 1.2.2. Theorem 1.2.14 is a generalisation of this statement.

Remark 1.2.3. It is conjectured that $\mu = 0$ whenever K_∞/K is a *cyclotomic $\mathbb{Z}_p$-extension*, that is, one obtained by adjoining p-power roots of unity. This is the so-called *Iwasawa $\mu = 0$ conjecture*; for a survey, cf. [Suj11]. It has been proven for abelian number fields K by Ferrero and Washington [FW79] but remains open when K is an arbitrary number field. There exists a counterexample for non-cyclotomic $\mathbb{Z}_p$-extensions. There is another statement called the Ferrero–Washington theorem, concerning the p-adic L-function, stating that at least one of its coefficients is a p-unit, cf. [Lan90, Chapter 10, Theorem 2.3] or [KKS12, Therorem 10.9]. The Iwasawa main conjecture implies the equivalence of these two assertions. We further remark that even though Barsky proposed a proof of the $\mu = 0$ conjecture for all totally real fields [Bar04], and thus it was stated in [MP05, §5.4.5] that this case of the conjecture had been proven, Barsky later retracted the paper due to an error.

Remark 1.2.4. In the proof of Theorem 1.2.1 we will use the structure theorem (Theorem 1.1.8) for a finitely generated torsion Λ-module. As we shall see towards the end of the proof, the exponential part μp^n comes from the direct summands $\Lambda/p^{n_i}\Lambda$ whereas the linear part λn comes from the summands $\Lambda/f_j(T)^{m_j}\Lambda$. This is in line with the definition of these invariants in Definition 1.1.14. See Theorem 1.2.14 for a generalisation.

The rest of this section will be devoted to the proof of Theorem 1.2.1. During the proof, we will establish basic notions of Iwasawa theory. In particular, we will discuss through an example how some groups associated with fields within a $\mathbb{Z}_p$-extension such as various Galois groups can be endowed with a Λ-module structure. As it will be obvious, this construction can be applied to other groups too, and in later sections we will do so without further comment. There are also other important steps within the proof that are interesting in their own right. Some of these will be highlighted in Section 1.3.

Proof. First we will use class field theory to pass from the ideal class groups above to certain Galois groups. Let M_n the unique maximal unramified abelian extension of K_n, called the *Hilbert*

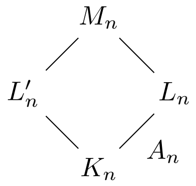

Figure 1.1: The p-Hilbert class field L_n of K_n

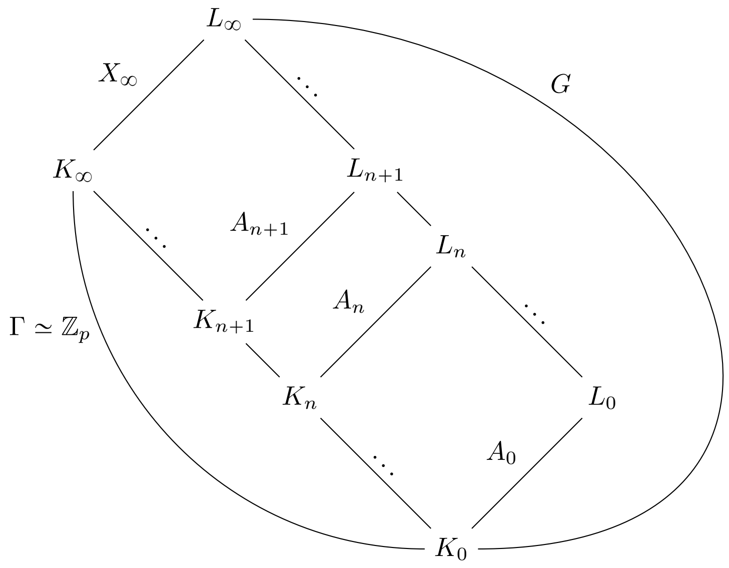

Figure 1.2: A $\mathbb{Z}_p$-extension with the tower of corresponding p-Hilbert class fields

class field, the existence of which is proven in class field theory. Let L_n be the unique maximal unramified abelian p-extension of K_n, L'_n the unique maximal unramified abelian extension of K_n of degree coprime to p; then L_n and L'_n are subfields of M_n, and we call L_n the *p-Hilbert class field* of K_n. We have

$$\mathrm{Gal}(M_n/K_n) = \mathrm{Gal}(L_n/K_n) \times \mathrm{Gal}(L'_n/K_n) \tag{1.3}$$

where $\mathrm{Gal}(L_n/K_n)$ is a p-group and $\mathrm{Gal}(L'_n/K_n)$ has order coprime to p. By class field theory we have an isomorphism (the Artin map)

$$\mathrm{Cl}(K_n) \xrightarrow{\sim} \mathrm{Gal}(M_n/K_n)$$

Comparing this with (1.2) and (1.3), we conclude that there is an isomorphism

$$A_n \xrightarrow{\sim} \mathrm{Gal}(L_n/K_n)$$

In particular, $\#A_n = \#\,\mathrm{Gal}(L_n/K_n)$, thus from now on we may focus on Galois groups instead of ideal class groups. We will, in fact, by abuse of notation, also denote this Galois group by A_n, with the remark that for the rest of this proof, one should think of it as a Galois group.

Let $L_\infty := \bigcup_{n\geqslant 0} L_n$, $G := \mathrm{Gal}(L_\infty/K)$. Then $X_\infty := \mathrm{Gal}(L_\infty/K_\infty) = \varprojlim A_n$ with respect to the norm maps. (This is the notation most widely used, but alas, it is rather counterintuitive here. The symbol A_∞ is commonly used for the injective limit.) As this projective limit contains all the information about the groups A_n, we will now concentrate on X_∞. We will endow X_∞ with a $\Lambda = \mathbb{Z}_p[\![T]\!]$-module structure and then show that X_∞ (or rather a submodule of it) is finitely generated over Λ, which will mean that the structure theorem of such modules will be applicable, meaning that we will obtain a relatively explicit description of X_∞.

We construct the aforementioned module structure on G in a slightly more abstract setting in Lemma 1.2.5 so that it remains clear that we only need abelianity of Γ and X_∞ for this, nothing more.

Lemma 1.2.5. *Let $\mathcal{G}$ be a group and $\mathcal{N} \lhd \mathcal{G}$ an abelian normal subgroup such that the quotient $\mathcal{H} = \mathcal{G}/\mathcal{N}$ is also abelian. Then $\mathcal{H}$ acts on $\mathcal{N}$ in the following way: for $g\mathcal{N} \in \mathcal{H}$ and $n \in \mathcal{N}$, let $n^g := n^{g\mathcal{N}} := gng^{-1}$.*

Proof. We first check that $n^{g\mathcal{N}}$ is well-defined, i.e. it does not depend on the choice of representative $g \in \mathcal{G}$ of the coset $g\mathcal{N}$. Another representative is gn' where $n' \in \mathcal{N}$, and since $\mathcal{N}$ is abelian we have

$$(gn')n(gn')^{-1} = gn'n(n')^{-1}g^{-1} = gn'(n')^{-1}ng^{-1} = gng^{-1}$$

This shows that $n^{g\mathcal{N}}$ is indeed well-defined.

We now show that $\mathcal{H} \curvearrowright \mathcal{N}$. It is clear that $n^{1\mathcal{N}} = n$, so it only remains to prove $(n^{g\mathcal{N}})^{h\mathcal{N}} = n^{(g\mathcal{N})(h\mathcal{N})}$ for $g, h \in \mathcal{G}$. By definition,

$$(n^{g\mathcal{N}})^{h\mathcal{N}} = hgng^{-1}h^{-1}$$

and using that $\mathcal{H}$ is abelian, we have

$$n^{(g\mathcal{N})(h\mathcal{N})} = n^{(h\mathcal{N})(g\mathcal{N})} = n^{(hg)\mathcal{N}} = hgng^{-1}h^{-1}$$

This finishes the proof. □

In the setting of the previous lemma, let $\mathcal{H}$ have the structure of a topological ring, and let $h_0 \in \mathcal{H}$ be a fixed topological generator of $\mathcal{H}$, meaning that the multiplicative subgroup $\langle h_0 \rangle \subseteq \mathcal{H}$ is dense. Notice that $(1+T) \in \mathcal{H}[\![T]\!]$ is a topological generator of $\mathcal{H}[\![T]\!]$. Therefore letting

$$(1+T)n := n^{h_0} \text{ for } n \in \mathcal{N},$$

combined with the action $\mathcal{H} \curvearrowright \mathcal{N}$ gives $\mathcal{N}$ the structure of a $\mathcal{H}[\![T]\!]$-module.

Lemma 1.2.6. *Assume that the exact sequence of groups*

$$1 \to \mathcal{N} \to \mathcal{G} \to \mathcal{H} \to 1$$

splits, that is, $\mathcal{G} \simeq \mathcal{N} \rtimes \mathcal{H}$. Then $\mathcal{G}' = T\mathcal{N} = \mathcal{N}^{h_0-1}$ where $\mathcal{G}'$ denotes the closure of the commutator subgroup of $\mathcal{G}$.

Proof. For any $n \in \mathcal{N}$ we have

$$n^{h_0-1} = n^{h_0}n^{-1} = h_0nh_0^{-1}n = [h_0, n],$$

which proves $\mathcal{N}^{h_0-1} \subseteq \mathcal{G}'$.

Conversely, consider a commutator $[a, b]$ for $a, b \in \mathcal{G}$. Since $\mathcal{G} \simeq \mathcal{N} \rtimes \mathcal{H}$ we may, by slight abuse of notation, write $a = n\alpha$, $b = m\beta$ where $n, m \in \mathcal{N}$, $\alpha, \beta \in \mathcal{H}$.

$$\begin{aligned}
[a,b] &= [n\alpha, m\beta] \\
&= n\alpha m\beta\alpha^{-1}n^{-1}\beta^{-1}m^{-1} \\
&= n\alpha m\alpha^{-1}\beta n^{-1}\beta^{-1}m^{-1} && \mathcal{H} \text{ is abelian} \\
&= nm^{\alpha}\left(n^{-1}\right)^{\beta}m^{-1} \\
&= n\left(n^{-1}\right)^{\beta}m^{\alpha}m^{-1} && \mathcal{N} \text{ is abelian} \\
&= n^{1-\beta}m^{\alpha-1}
\end{aligned}$$

Since h_0 is a topological generator of $\mathcal{H}$, we have $\beta = \lim_{i\to\infty} h_0^{c_i}$ for some $c_i \in \mathbb{Z}$. Therefore

$$1 - \beta = \lim_{i\to\infty}\left(1 - h_0^{c_i}\right) = \lim_{i\to\infty}\left(1 - (1+T)^{c_i}\right)$$

Since $(1 - (1+T)^{c_i}) \in T\mathcal{H}[\![T]\!]$ for all $i \in \mathbb{N}$, we have $1 - \beta \in T\mathcal{H}[\![T]\!]$. Hence $n^{1-\beta} \in T\mathcal{N}$, and similarly $m^{\alpha-1} \in T\mathcal{N}$, proving $\mathcal{G}' \subseteq T\mathcal{N}$. □

Apply Lemma 1.2.5 with $\mathcal{G} := G$, $\mathcal{N} := X_\infty$ and $\mathcal{H} := \Gamma$ to obtain an action $\Gamma \curvearrowright X_\infty$ and thus a $\Lambda = \mathbb{Z}_p[\![T]\!]$-module structure on X_∞. Fix a topological generator $h_0 := \gamma$ of Γ.

We will later use Lemma 1.2.6 to give an isomorphism between A_n and a certain quotient of X_∞. To be able to use the Lemma, we need to verify the splitting condition. This will be done using inertia groups, which behave nicely if the corresponding primes ramify totally, which will turn out to be the case for some subextension K_∞/K_e of K_∞/K.

Thus we need to contemplate what happens when we pass from K_∞/K_0 to a subextension K_∞/K_n (see Table 1.1). The latter is also a $\mathbb{Z}_p$-extension with Galois group $\Gamma_n := \Gamma^{p^n}$ (the group Γ is written multiplicatively); this has topological generator γ^{p^n}. Since γ corresponds to $(1+T)$ and γ gets replaced by γ^{p^n}, and T gets replaced by

$$(1+T)^{p^n} - 1 = T \cdot \frac{(1+T)^{p^n} - 1}{T}$$

Therefore Λ becomes

$$\Lambda_n = \mathbb{Z}_p[\![(1+T)^{p^n} - 1]\!]$$

Note that a module over Λ_n is finitely generated iff it is finitely generated over Λ. Finally notice that L_∞ for K_0 is the same as for K_n, with the Galois group becoming $\mathrm{Gal}(L_\infty/K_n) = G^{p^n}$.

	K_∞/K_0	K_∞/K_n
Galois group	Γ	$\Gamma_n = \Gamma^{p^n}$
topological generator	γ	γ^{p^n}
Iwasawa algebra	$\Lambda = \mathbb{Z}_p[\![T]\!]$	$\Lambda_n = \mathbb{Z}_p[\![(1+T)^{p^n} - 1]\!]$
generator	T	$(1+T)^{p^n} - 1$
maximal unramified abelian extension	L_∞	L_∞
Galois group	G	G^{p^n}

Table 1.1: Passing between extensions

Claim 1.2.7. *There are only finitely many prime ideals ramifying in K_∞/K, namely those above p.*

Proof. Let $\mathfrak{p}$ be a prime in K which ramifies in K_∞/K. As there are only finitely many prime ideals above p, it is sufficient to show that $\mathfrak{p}$ lies above p in the extension $K/\mathbb{Q}$.

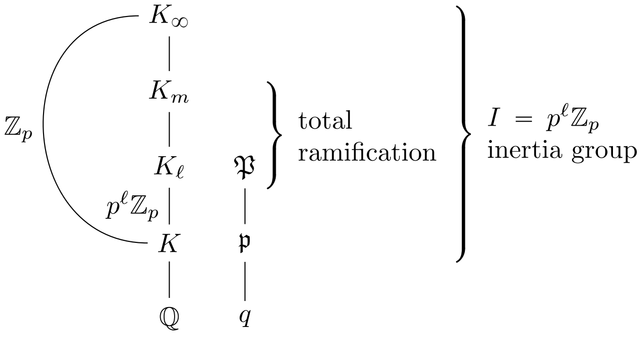

Figure 1.3: Objects in the proof of Claim 1.2.7: fields and Galois groups on the left, prime ideals on the right

We argue by contradiction: suppose $\mathfrak{p}$ lies above some rational prime $q \neq p$. (See Figure 1.3.) Let I be the inertia group of $\mathfrak{p}$ in K_∞/K. As $\mathfrak{p}$ ramifies, $I \neq \{0\}$, hence $I = p^\ell\mathbb{Z}_p$ for some $\ell \geqslant 0$. In particular, I is infinite, and as archimedean primes have inertia group of order either 1 or 2, it follows that $\mathfrak{p}$ is non-archimedean.

Now consider the fixed field of I: this is K_ℓ. Let $\mathfrak{P}$ be a prime in K_ℓ above $\mathfrak{p}$. For every $m \geqslant \ell$, $\mathfrak{P}$ ramifies totally in K_m/K_ℓ by construction, and the ramification degree is $[K_m : K_\ell] = p^{m-\ell}$. By the upcoming Lemma 1.2.8, $\mathfrak{N}(\mathfrak{P}) \equiv 1 \bmod p^{m-\ell}$ for all $m \geqslant \ell$ where $\mathfrak{N}$ denotes the absolute norm. Taking m large enough, this implies $\mathfrak{P} = (1)$ which is a contradiction. □

Lemma 1.2.8. *Let F'/F be a finite abelian extension of the algebraic number field F. Let $\mathfrak{p}$ be a prime of F not lying above $[F' : F]$. Then for any prime $\mathfrak{P}$ of F' above $\mathfrak{p}$, the inertia group I at $\mathfrak{P}$ relative to $\mathfrak{p}$ is cyclic and $\mathfrak{N}(\mathfrak{p}) \equiv 1 \bmod \#I$.*

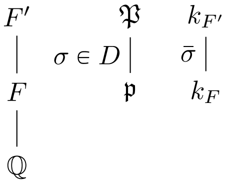

Figure 1.4: Objects in the proof of Lemma 1.2.8

Proof. Let $k_F = \mathcal{O}_F/\mathfrak{p}$ and $k_{F'} = \mathcal{O}_{F'}/\mathfrak{P}$ be the residue fields (see Figure 1.4). Let D denote the decomposition group at $\mathfrak{P}$ relative to $\mathfrak{p}$ in F'/F. Recall the short exact sequence

$$\begin{array}{c} 1 \to I \to D \to \mathrm{Gal}(k_{F'}/k_F) \to 1 \\ \sigma \mapsto \bar{\sigma} \end{array}$$

Let $\pi \in \mathfrak{P}\backslash\mathfrak{P}^2 \neq \varnothing$, and consider the map

$$\begin{aligned} f : D &\to k_{F'}^{\times} \\ \sigma &\mapsto \frac{\sigma(\pi)}{\pi} \end{aligned}$$

It is easily checked that $f(\sigma\tau) = f(\sigma)\bar{\sigma}f(\tau)$ for $\sigma, \tau \in D$. Since $I = \{\sigma \in D \mid \bar{\sigma} = 1\}$, $f|_I$ is a homomorphism. We will show that $f|_I$ is injective and has image in $k_F^{\times}$, which implies the statement of the lemma.

We first show injectivity. Let $\sigma \in \operatorname{Ker} f$ be an element of order m. It suffices to show $\sigma(\pi) = \pi$; we know that $\sigma(\pi) \equiv \pi \bmod \mathfrak{P}^2$. Let $k \geqslant 2$ be fixed. Then

$$\sigma(\pi) \equiv \pi + a\pi^k \bmod \mathfrak{P}^{k+1} \tag{1.4}$$

for some $a \in \mathcal{O}_{F'}$. Actually, we may assume $a \in \mathcal{O}_{(F')^I}$ where $(F')^I$ denotes the fixed field. Iterative application of σ to (1.4) yields

$$\begin{aligned} \pi = \sigma^m(\pi) &\equiv \pi + a\left(\pi^k + \sigma(\pi)^k + \ldots + \sigma^{m-1}(\pi)^k\right) \bmod \mathfrak{P}^{k+1} \\ &\equiv \pi + a\left(\pi^k + \pi^k + \ldots + \pi^k\right) \bmod \mathfrak{P}^{k+1} && \text{using (1.4)} \\ &= \pi + am\pi^k \bmod \mathfrak{P}^{k+1} \end{aligned}$$

Since $\mathfrak{p} \nmid [F' : F]$, $\mathfrak{P} \nmid m$, and thus $a \equiv 0$, $\sigma(\pi) \equiv \pi \bmod \mathfrak{P}^{k+1}$ for all $k \geqslant 2$. Hence $\sigma(\pi) = \pi$, showing injectivity of $f|_I$.

We now prove $\operatorname{Im} f|_I \subseteq k_F^{\times}$. Let $\sigma \in I$; we will show that $f(\sigma)$ is fixed by all automorphisms in $\operatorname{Gal}(k_{F'}/k_F)$. Let $\bar{\tau} \in \operatorname{Gal}(k_{F'}/k_F)$, $\tau \in D$. We have $\sigma\tau = \tau\sigma$ since F'/F is abelian, thus

$$f(\sigma\tau) = f(\tau\sigma) = f(\tau)\bar{\tau}f(\sigma),$$

hence $f(\sigma) = \bar{\tau}f(\sigma)$. This finishes the proof. □

Remark 1.2.9. For a slightly shorter but less elementary proof of Claim 1.2.7 using local class field theory, see [Was97, Proposition 13.2]. The proof of Lemma 1.2.8 is from [Lon77, page 94].

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the primes ramifying in K_∞/K. Let $I_1, \ldots, I_s \leqslant \Gamma$ be the respective inertia subgroups. As in the proof of Claim 1.2.7, $I_i = p^{\ell_i}\mathbb{Z}_p$ for some $\ell_i \geqslant 0$. Let

$$I = \bigcap_{i=1}^{s} I_i = p^e\mathbb{Z}_p,$$

where $e = \max(\ell_1, \ldots, \ell_s)$. Then I has fixed field K_e, and since $\operatorname{Gal}(K_\infty/K_e) \leqslant I \leqslant I_i$ for all i, we have that each $\bar{\mathfrak{p}}_i$ ramifies totally in the subextension K_∞/K_e where $\bar{\mathfrak{p}}_i$ is an extension of $\mathfrak{p}_i$ to K_e.

Thus for any $\mathbb{Z}_p$-extension it is possible to pass to a subextension where every prime is either unramified or totally ramified. From now on until the end of the proof of Claim 1.2.10 we assume K_∞/K itself to be such an extension; this will greatly simplify our formulæ. Using the considerations summarised in Table 1.1, we will then generalise the results to an arbitrary $\mathbb{Z}_p$-extension: this will be Claim 1.2.11.

The extension L_∞/K_∞ is unramified since each L_n/K_n is, hence $I_i \cap X_\infty = \{1\}$. Also since $\mathfrak{p}_i$ ramifies totally in K_∞/K, the inclusion $I_i \hookrightarrow G$ induces $I_i = \Gamma = G/X_\infty$. Therefore

$$G = I_iX_\infty = X_\infty I_i \quad i = 1, \ldots, s \tag{1.5}$$

In particular, Lemma 1.2.6 can be applied to obtain

$$G' = TX_\infty = X_\infty^{\gamma - 1} \tag{1.6}$$

Let $\sigma_i \in I_i$ be the element corresponding to γ under the above isomorphism $I_i \simeq \Gamma$. Since $I_i \subseteq G = X_\infty I_1$, there exist $a_i \in X_\infty$ for which $\sigma_i = a_i \sigma_1$ ($i = 2, \ldots, s$). By Table 1.1, if we switch from K_0 to some extension K_n, γ gets replaced by γ^{p^n}, thus σ_i becomes $\sigma_i^{p^n}$, and a_i becomes $a_i^{1+\sigma_1+\ldots+\sigma_1^{p^n-1}} = \nu_n a_i$ where

$$\nu_n := \frac{\gamma^{p^n} - 1}{\gamma - 1} = \frac{(1+T)^{p^n} - 1}{T}$$

This can be seen as follows:

$$\begin{aligned} \sigma_i^{p^n} &= (a_i \sigma_1)^{p^n} \\ &= a_i (\sigma_1 a_i \sigma_1^{-1})(\sigma_1^2 a_i \sigma_1^{-2}) \cdots (\sigma_1^{p^n-1} a_i \sigma_1^{p^n-1}) \sigma_1^{p^n} \\ &= a_1^{1+\sigma_1+\ldots+\sigma_1^{p^n-1}} \sigma_1^{p^n} \end{aligned}$$

Claim 1.2.10. *Let $Y_0 \leqslant X_\infty$ be the $\mathbb{Z}_p$-submodule of X_∞ generated by $a_2, \ldots, a_s \in X_\infty$ and G'. Let $Y_n = \nu_n Y_0$. Then $A_n \simeq X_\infty / Y_n$ for $n \geqslant 0$.*

Proof. For $n = 0$, L_0/K_0 is the maximal unramified abelian subextension of L_∞/K_0 by construction. Hence $\mathrm{Gal}(L_\infty/L_0)$ is the closed subgroup of G generated by $I_1, \ldots, I_s$ and G', or equivalently, by $I_1, a_2, \ldots, a_s$ and G'. Hence

$$\begin{aligned} A_0 &= \mathrm{Gal}(L_0/K_0) && \text{by definition} \\ &= G/\mathrm{Gal}(L_\infty/L_0) && \text{Galois theory} \\ &= X_\infty I_1 / \mathrm{Gal}(L_\infty/L_0) && (1.5) \\ &= X_\infty / Y_0 && \text{by definition} \end{aligned}$$

For $n \geqslant 0$, our considerations above yield that Y_0 becomes $\nu_n Y_0 = Y_n$ when passing from K to K_n. □

At this point we give up our assumption that every prime is either unramified or totally ramified in K_∞/K. We generalise Claim 1.2.10 to arbitrary $\mathbb{Z}_p$-extensions K_∞/K with K_∞/K_e being a subextension as above, i.e. in which all ramifying primes of K_∞/K ramify totally.

Claim 1.2.11. *Let $\nu_{n,e} := \nu_n/\nu_e$. Then $A_n \simeq X_\infty/\nu_{n,e} Y_e$.*

Proof. This is immediate from Claim 1.2.10 and

$$\nu_{n,e} Y_e = \frac{\nu_n}{\nu_e} \nu_e Y_0 = \nu_n Y_0 = Y_n$$ □

Claim 1.2.12. *Y_e is finitely generated over Λ. (Hence the same holds for X_∞ too since $X_\infty/Y_e = A_e$ is finite.)*

Proof. Recall that Y_e is finitely generated as a Λ-module iff it is finitely generated over $\Lambda_e = \mathbb{Z}_p[\![(1+T)^{p^e} - 1]\!]$. By Nakayama's lemma (Lemma 1.1.5.1), Y_e is finitely generated over Λ_e iff $Y_e/(p, (1+T)^{p^e} - 1)Y_e$ is finite. Since $\nu_{e+1,e} \in (p, (1+T)^{p^e} - 1)$, we have

$$\# \left(Y_e \middle/ (p, (1+T)^{p^e} - 1) Y_e \right) \leqslant \# \left(Y_e / \nu_{e+1,e} Y_e \right) \leqslant \# \left(X_\infty / \nu_{e+1,e} Y_e \right) = \# A_{e+1} < \infty$$ □

By the structure theorem of finitely generated Λ-modules, Y_e is quasi-isomorphic to

$$E_e = \Lambda^{\oplus r} \oplus \bigoplus_{i=1}^{s} \Lambda/(p_i^k) \oplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j} \tag{1.7}$$

where each f_j is distinguished.

Recall that our goal is to compute e_n up to constant for n large enough where $p^{e_n} = \#A_n$. We have

$$\#A_n = \#\left(X_\infty/\nu_{n,e}Y_e\right) = \#\left(X_\infty/Y_e\right)\#\left(Y_e/\nu_{n,e}Y_e\right)$$

The first factor is some power of p independent of n, so we may focus only on $Y_e/\nu_{n,e}Y_e$. The following lemma tells us that we can work with $E_e/\nu_{n,e}E_e$ instead.

Lemma 1.2.13. *Let Y, E be Λ-modules for which $Y \sim E$ and $Y/\nu_{n,e}Y$ is finite for all $n \geqslant e$. Then there are $n_1 \geqslant e$, $c \geqslant 0$ such that for $n \geqslant n_1$*

$$\#\left(Y/\nu_{n,e}Y\right) = p^c \#\left(E/\nu_{n,e}E\right)$$

Proof. For each $n \geqslant e$ the quasi-isomorphism φ and $\nu_{n,e}$ give rise to the following commutative diagram

$$\begin{tikzcd}
 & \operatorname{Ker}(\nu_{n,e}\varphi) \arrow[r] \arrow[d] & \operatorname{Ker}\varphi \arrow[r] \arrow[d] & \operatorname{Ker}(\varphi \bmod \nu_{n,e}) \arrow[d] \arrow[r, dashed, no head] & {} \\
0 \arrow[r] & \nu_{n,e}Y \arrow[r] \arrow[d, "\nu_{n,e}\varphi"] & Y \arrow[r] \arrow[d, "\varphi"] & Y/\nu_{n,e}Y \arrow[r] \arrow[d, "\varphi \bmod \nu_{n,e}"] & 0 \\
0 \arrow[r] & \nu_{n,e}E \arrow[r] \arrow[d] & E \arrow[r] \arrow[d] & E/\nu_{n,e}E \arrow[r] \arrow[d] & 0 \\
{} \arrow[r, dashed] & \operatorname{Coker}(\nu_{n,e}\varphi) \arrow[r] & \operatorname{Coker}\varphi \arrow[r] & \operatorname{Coker}(\varphi \bmod \nu_{n,e}) &
\end{tikzcd}$$

We will show that for large enough n, the cardinality of the kernels and cokernels stabilises. This implies the statement of the Lemma.

Looking at representatives, we find

$$\#\operatorname{Coker}(\nu_{n,e}\varphi) \leqslant \#\operatorname{Coker}\varphi \tag{1.8}$$

By the snake lemma, we have an exact sequence

$$\begin{aligned}
0 \to \operatorname{Ker}(\nu_{n,e}\varphi) &\to \operatorname{Ker}\varphi \to \operatorname{Ker}(\varphi \bmod \nu_{n,e}) \\
&\to \operatorname{Coker}(\nu_{n,e}\varphi) \to \operatorname{Coker}\varphi \to \operatorname{Coker}(\varphi \bmod \nu_{n,e}) \to 0,
\end{aligned}$$

which implies the inequalities

$$\#\operatorname{Ker}(\nu_{n,e}\varphi) \leqslant \#\operatorname{Ker}\varphi \tag{1.9}$$

$$\#\operatorname{Coker}(\varphi \bmod \nu_{n,e}) \leqslant \#\operatorname{Coker}\varphi \tag{1.10}$$

$$\#\operatorname{Ker}(\varphi \bmod \nu_{n,e}) \leqslant \#\operatorname{Ker}(\varphi)\#\operatorname{Coker}(\nu_{n,e}\varphi) \overset{(1.10)}{\leqslant} \#\operatorname{Ker}(\varphi)\#\operatorname{Coker}(\varphi) \tag{1.11}$$

Now observe what happens if we let n increase. Since $\nu_{n,e} \mid \nu_{n+k,e}$ for $k \geqslant 0$,

$$\# \operatorname{Ker}(\nu_{n+k,e}\varphi) \leqslant \# \operatorname{Ker}(\nu_{n,e}\varphi) \tag{1.12}$$

$$\# \operatorname{Coker}(\varphi \bmod \nu_{n+k,e}) \geqslant \# \operatorname{Coker}(\varphi \bmod \nu_{n,e}) \tag{1.13}$$

It is easily seen that multiplying representatives for $\operatorname{Coker}(\nu_{n,e}\varphi)$ by $\nu_{n+k,e}/\nu_{n,e}$ gives representatives for $\operatorname{Coker}(\nu_{n+k,e}\varphi)$, hence

$$\# \operatorname{Coker}(\nu_{n+k,e}\varphi) \leqslant \# \operatorname{Coker}(\nu_{n,e}\varphi) \tag{1.14}$$

Putting all these inequalities together, it follows that

$$\# \operatorname{Ker}(\nu_{n,e}\varphi),\ \# \operatorname{Coker}(\nu_{n,e}\varphi),\ \text{and}\ \# \operatorname{Coker}(\varphi \bmod \nu_{n,e})$$

stabilise for $n \geqslant n_1$ where $n_1 \geqslant e$ is suitably large. The snake lemma yields

$$\# \operatorname{Ker}(\nu_{n,e}\varphi) \# \operatorname{Ker}(\varphi \bmod \nu_{n,e}) \# \operatorname{Coker}\varphi = \# \operatorname{Ker}(\varphi) \# \operatorname{Coker}(\nu_{n,e}\varphi) \# \operatorname{Coker}(\varphi \bmod \nu_{n,e})$$

Since every term except for $\# \operatorname{Ker}(\varphi \bmod \nu_{n,e})$ is constant for $n \geqslant n_1$, $\# \operatorname{Ker}(\varphi \bmod \nu_{n,e})$ must stabilise as well. This completes the proof. □

Now all that remains is to compute $\#(E/\nu_{n,e}E)$. This may be done for all three types of direct summands in (1.7) separately. In what follows, we omit the indices i and j for brevity. Note that what happens here is completely general and holds for any finitely generated torsion Λ-module for which $\#(E_e/\nu_{n,e}E_e)$ is finite (see Theorem 1.2.14).

Case 1. First consider $\Lambda/(\nu_{n,e})$. Since the polynomial $\nu_{n,e}$ is distinguished, the quotient is infinite: this follows from the p-adic Weierstrass division theorem (Theorem 1.1.2). But as $\#(Y_e/\nu_{n,e}Y_e)$ is finite, so is $\#(E_e/\nu_{n,e}E_e)$, hence E has no free part, that is, $r = 0$.

Case 2. For $\Lambda/(p^k)$, we have

$$\Lambda/(p^k)\Big/\nu_{n,e}\Lambda/(p^k) \simeq \Lambda\big/(\nu_{n,e}, p^k)$$

It is easily seen that the polynomial

$$\nu_{n,e} = \frac{(1+T)^{p^n} - 1}{(1+T)^{p^e} - 1}$$

is distinguished. Using Weierstrass division (Theorem 1.1.2), we find that the above quotient module has representatives that are polynomials mod p^k of degree at most $\deg \nu_{n,e} = p^n - p^e$, hence the order is $p^{k(p^n - p^e)} = p^{kp^n + \text{constant}}$.

Case 3. Consider $\Lambda/(f(T)^m)$. Since f is distinguished, so is f^m. Let $d = \deg f^m$. Thus for $p^n \geqslant d$,

$$(1+T)^{p^n} \equiv 1 + p \cdot (\text{polynomial}) \pmod{f^m}$$

and taking the p^{th} power yields

$$(1+T)^{p^{n+1}} \equiv 1 + p^2(\text{polynomial}) \pmod{f^m}$$

Therefore

$$\begin{aligned}(1+T)^{p^{n+2}}-1 &= \Big(1+(1+T)^{p^{n+1}}+\ldots+(1+T)^{(p-1)p^{n+1}}\Big)\Big((1+T)^{p^{n+1}}-1\Big)\\ &\equiv p(1+p\cdot(\text{polynomial}))\Big((1+T)^{p^{n+1}}-1\Big) \bmod f^m\end{aligned}$$

Since

$$\frac{\Big((1+T)^{p^{n+2}}-1\Big)}{\Big((1+T)^{p^{n+1}}-1\Big)}=\frac{\nu_{n+2,e}}{\nu_{n+1,e}}$$

and $(1+p\cdot(\text{polynomial}))\in\Lambda^\times$, we get $\nu_{n+2,e}\Lambda/(f^m)=p\nu_{n+1,e}\Lambda/(f^m)$ for all $n\geqslant n_2$ where $n_2>e$ and $p^{n_2}\geqslant d$. Therefore

$$\begin{aligned}\#\Big(\Lambda/(f^m)\Big/\nu_{n+2,e}\Lambda/(f^m)\Big) &= \#\Big(\Lambda/(f^m)\Big/p\nu_{n+1,e}\Lambda/(f^m)\Big)\\ &= \#\Big(\Lambda/(f^m)\Big/p\Lambda/(f^m)\Big)\,\#\Big(p\Lambda/(f^m)\Big/p\nu_{n+1,e}\Lambda/(f^m)\Big)\\ &= p^d\#\Big(\Lambda/(f^m)\Big/\nu_{n+1,e}\Lambda/(f^m)\Big)\end{aligned}$$

because

$$\Lambda/(f^m)\Big/p\Lambda/(f^m)\simeq\Lambda/(p,f^m)=\Lambda/(p,T^d)$$

and multiplication by p is injective on $\Lambda/(f^m)$ since $(p,f)=1$.

In conclusion, for all $n\geqslant n_2+1$ we have

$$\#\Big(\Lambda/(f^m)\Big/\nu_{n+2,e}\Lambda/(f^m)\Big)=p^{d(n-n_2-1)}\#\Big(\Lambda/(f^m)\Big/\nu_{n_2+1,e}\Lambda/(f^m)\Big)=p^{dn+\text{constant}}$$

(The quotient on the right hand side must be finite because $\#(E_e/\nu_{n,e}E_e)$ is finite.)

Combining the computations above—the k's add up to μ and the d's add up to λ—and letting $n_0:=\max(n_1,n_2+1)$ finishes the proof of Theorem 1.2.1. □

As before, let $\Gamma_n=\Gamma^{p^n}$, and let $E_{\Gamma_n}:=E/\left(\gamma^{p^n}-1\right)E$ denote the module of Γ_n-coinvariants. As already alluded to, the calculation of $\#(E/\nu_{n,e}E)$ in the end of the proof above gives us the following:

Theorem 1.2.14 (Iwasawa)**.** *Let E be a finitely generated Λ-module such that E_{Γ_n} is finite for all n. Let $\#E_{\Gamma_n}=p^{e_n}$ denote its cardinality. Then there exists $c\geqslant 0$ such that for every sufficiently large n we have $e_n=\mu p^n+\lambda n+c$.* □

1.3 Class field theory of $\mathbb{Z}_p$-extensions

In this section we collect some consequences of Iwasawa's theorem as well as other statements from the class field theory of $\mathbb{Z}_p$-extensions. These will later be used in the proof of the Iwasawa main conjecture.

Remark 1.3.1. In the $\mathbb{Z}_p$-extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$, the only prime ramifying is p, and it does so totally. This will allow us to use some results of the previous as well as this section in this setting; we will do this in the proof of the Iwasawa main conjecture.

Lemma 1.3.2. *$X_\infty := \varprojlim A_n$ is a finitely generated torsion Λ-module (called the* unramified Iwasawa module*).*

Proof. We have finitely generatedness by Claim 1.2.12, and being torsion was shown in Case 1 on page 16. □

Lemma 1.3.3. *Let K_∞/K_0 be a $\mathbb{Z}_p$-extension with only one prime ramifying, and it doing so totally. Then $A_0 = 0$ iff $A_n = 0$ for all $n \geqslant 0$, the latter being equivalent to $X_\infty = 0$ by definition.*

Proof. One direction is obvious. Suppose $A_0 = 0$. Apply Claim 1.2.10 with $s = 1$: using (1.6), this yields $A_0 \simeq X_\infty/Y_0 = X_\infty/TX_\infty$. By assumption, $X_\infty/TX_\infty = 0$, therefore $X_\infty/(p,T)X_\infty = 0$, hence $X_\infty = 0$ by Nakayama's lemma (Lemma 1.1.5.2). □

Let us consider a $\mathbb{Z}_p$-extension K_∞/K_0 where K_0 is a number field. For all $n \leqslant \infty$ let H_n be the p-Hilbert class field of K_n and Ω_n be the unique maximal p-abelian extension unramified outside p (also known as the unique maximal p-abelian p-ramified extension), with $\mathfrak{X}_n := \mathrm{Gal}(\Omega_n/K_n)$ being the Galois group. It will be convenient to use the language of idèles for the next theorem. We recall the following notation: let J_n denote the idèles of K_n, and let

$$\mathfrak{U}_n := \prod_{\mathfrak{p}\text{ a prime of }K_n} \mathfrak{U}_{n,\mathfrak{p}}$$

be the group of unit idèles where

$$\mathfrak{U}_{n,\mathfrak{p}} := \begin{cases} \mathcal{O}^\times_{K_n,\mathfrak{p}} & \text{if } \mathfrak{p} \text{ is non-archimedean} \\ K^\times_{n,\mathfrak{p}} & \text{if } \mathfrak{p} \text{ is archimedean} \end{cases}$$

Furthermore let

$$\mathfrak{U}_{n,p} := \prod_{\mathfrak{p}|p} \mathfrak{U}_{n,\mathfrak{p}}, \quad \mathfrak{U}_{n,[p]} := \prod_{\ell \neq p} \mathfrak{U}_{n,\ell} = \prod_{\lambda \nmid p} \mathfrak{U}_{n,\lambda}, \quad J_n^\infty := \prod_{\substack{v\text{ an infinite}\\ \text{prime of }K_n}} K_v^\times$$

Finally let

$$\mathfrak{E}_n := \mathcal{O}^\times_{K_n}, \quad \mathfrak{U}^{(m)}_{n,p} := \left\{ u \in \mathfrak{U}_{n,p} \,\middle|\, \forall \mathfrak{p} \mid p : u \equiv 1 \bmod p^m \right\} \text{ for } m \geqslant 0,$$

and $\sigma_{n,p} : \mathfrak{E}_n \hookrightarrow \mathfrak{U}_{n,p}$ be the diagonal embedding. Note that the sets $\mathfrak{U}^{(m)}_{n,p}, m \geqslant 0$ form a fundamental system of neighbourhoods for $\mathfrak{U}_{n,p}$.

Theorem 1.3.4. *For all $n \leqslant \infty$ one has*

$$\mathrm{Gal}(\Omega_n/H_n) \simeq \mathfrak{U}^{(1)}_{n,p} \Big/ \left(\mathfrak{U}^{(1)}_{n,p} \cap \overline{\sigma_{n,p}\mathfrak{E}_n} \right)$$

where overline means closure in $\mathfrak{U}_{n,p}$.

Proof. Let $n < \infty$; the case $n = \infty$ will follow by taking projective limits. For the sake of simplicity, we will omit the indices n (as we will be working on just one level of the $\mathbb{Z}_p$-extension in the proof, these indices would be superfluous).

Note that we have

$$\mathfrak{U}^{(1)}_{p} \Big/ \left(\mathfrak{U}^{(1)}_{p} \cap \overline{\sigma_p\mathfrak{E}} \right) \simeq \left(\mathfrak{U}_p/\overline{\sigma_p\mathfrak{E}} \right) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

Indeed, this follows from $\mathfrak{U}_p/\mathfrak{U}^{(1)}_p \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and that $\mathfrak{U}^{(1)}_p$ is a pro-p group [Neu99, Proposition 10.2]. So it remains to show

$$\mathrm{Gal}(\Omega/H) \simeq \left(\mathfrak{U}_p/\overline{\sigma_p\mathfrak{E}} \right) \otimes_{\mathbb{Z}} \mathbb{Z}_p \tag{1.15}$$

Class field theory gives us the following isomorphism (by the description of unramifying primes in terms of idèles, cf. [Lan86, Chapter XI, §4, Theorem 4] or [Was97, Appendix on Class Field Theory, Theorem 11])

$$\begin{aligned}\operatorname{Gal}(\Omega/K) &\simeq \left(J\Big/\overline{\mathfrak{U}_{[p]}J^{\infty}K^{\times}}\right)\otimes_{\mathbb{Z}}\mathbb{Z}_p\\ &\simeq \left(\left(J/\mathfrak{U}_p\mathfrak{U}_{[p]}J^{\infty}K^{\times}\right)\left(\mathfrak{U}_p\mathfrak{U}_{[p]}J^{\infty}K^{\times}\big/\overline{\mathfrak{U}_{[p]}J^{\infty}K^{\times}}\right)\right)\otimes_{\mathbb{Z}}\mathbb{Z}_p\\ &\simeq \left(\left(J/\mathfrak{U}K^{\times}\right)\left(\mathfrak{U}_p/(\mathfrak{U}_p\cap\overline{\mathfrak{U}_{[p]}J^{\infty}K^{\infty}})\right)\right)\otimes_{\mathbb{Z}}\mathbb{Z}_p\\ &\simeq \left(\operatorname{Gal}(H/K)\left(\mathfrak{U}_p/\overline{\sigma_p\mathfrak{E}}\right)\right)\otimes_{\mathbb{Z}}\mathbb{Z}_p\end{aligned}$$

In the last step we used $J/\mathfrak{U}K^{\times}\simeq\operatorname{Gal}(H/K)$ in the first term. As for the second term, it is easily seen that we have

$$\mathfrak{U}_p^{(m)}\mathfrak{U}_{[p]}J^{\infty}\cap\mathfrak{U}_p=\mathfrak{U}_p^{(m)}\mathfrak{E}$$

Taking intersections for $m\geqslant 0$ on both sides, it follows from the fact that the sets $\mathfrak{U}_p^{(m)}$ form a fundamental system of neighbourhoods that

$$\mathfrak{U}_p/\left(\mathfrak{U}_p\cap\overline{\mathfrak{U}_{[p]}J^{\infty}K^{\infty}}\right)=\mathfrak{U}_p/\overline{\sigma_p\mathfrak{E}}$$

Since H is the p-Hilbert class field of K, $\operatorname{Gal}(H/K)\otimes_{\mathbb{Z}}\mathbb{Z}_p=\operatorname{Gal}(H/K)$. Then (1.15) follows from $\operatorname{Gal}(\Omega/H)=\operatorname{Gal}(\Omega/K)/\operatorname{Gal}(H/K)$. This completes the proof. □

Corollary 1.3.5. *$\mathfrak{X}_\infty$ is a finitely generated Λ-module (called the* p-ramified Iwasawa module*).*

Proof. $\mathfrak{X}_\infty$ has a natural Λ-module structure. Since H_0/K_0 is a finite extension and $\mathfrak{X}_0$ is a pro-p-group, Theorem 1.3.4 yields a pseudo-isomorphism $\mathfrak{X}_0\sim\mathfrak{U}_{0,p}/\overline{\sigma_{0,p}\mathfrak{E}_0}$. The group $\mathfrak{U}_{0,p}$ contains a subgroup of $\mathbb{Z}_p$-rank $(K_0:\mathbb{Q})$ and finite index [Neu99, §5.3], therefore $\operatorname{rk}_{\mathbb{Z}_p}\mathfrak{U}_{0,p}=(K_0:\mathbb{Q})$, and we obtain

$$r:=\operatorname{rk}_{\mathbb{Z}_p}\mathfrak{X}_0=(K_0:\mathbb{Q})-\operatorname{rk}_{\mathbb{Z}_p}\overline{\sigma_{0,p}\mathfrak{E}_0}$$

Since $\mathfrak{X}_0$ is the Galois group of the maximal abelian extension of K_0 inside Ω_∞, we have that $\mathbb{Z}_p^r$ is pseudo-isomorphic to the commutator subgroup of $\operatorname{Gal}(\Omega_\infty/K_0)$. The commutator subgroup of $\mathfrak{X}_\infty$ is $\mathfrak{X}_\infty/T\mathfrak{X}_\infty$, so we get that $\mathfrak{X}_\infty/T\mathfrak{X}_\infty\sim\mathbb{Z}_p^{r-1}$ where the (-1) in the exponent comes from the difference between the base fields of $\mathfrak{X}_0$ and $\mathfrak{X}_\infty$: these are K_0 resp. K_∞, with the Galois group between them being $\Gamma\simeq\mathbb{Z}_p$. From $\mathfrak{X}_\infty/T\mathfrak{X}_\infty\sim\mathbb{Z}_p^{r-1}$ it follows that $\mathfrak{X}_\infty$ is finitely generated using Nakayama's lemma (Lemma 1.1.5.1). □

We will now specialise to the extension where $K_n=\mathbb{Q}(\mu_{p^{n+1}})$, with which we will be working in Chapter 3. (For more results on the above level of generality, cf. [Was97, §§13.1, 13.4–5] and [Lan90, Chapter 5, §§5–6].) Note the apparent discrepancy of indexing between K_n and $\mathbb{Q}(\mu_{p^{n+1}})$; it will stay with us in the sequel.

In this case, there is only one prime above p in K_n, namely $\mathfrak{p}=(1-\zeta_{p^{n+1}})$. The objects denoted by Fraktur letters above become the following; the Latin letters are the notation we will use in Chapter 3.

- $\mathfrak{U}_{n,p}=\mathcal{O}^{\times}_{\mathbb{Q}(\mu_{p^{n+1}}),p}$ local units,
- $\mathfrak{U}^{(1)}_{n,p}=\left\{u\in\mathcal{O}^{\times}_{\mathbb{Q}(\mu_{p^{n+1}}),p}\,\middle|\,u\equiv 1\bmod(1-\zeta_{p^{n+1}})\right\}=:U_n$ principal local units,
- $\mathfrak{E}_n=\mathcal{O}^{\times}_{\mathbb{Q}(\mu_{p^n+1})}=:E_n$ global units,
- $\mathfrak{U}^{(1)}_{n,p}\cap\overline{\sigma_{n,p}\mathfrak{E}_n}=\overline{E_n\cap U_n}=:\overline{E}_n$

Under this notation, Theorem 1.3.4 yields the following exact sequence.

Corollary 1.3.6. *There is an exact sequence*

$$0 \to U_\infty/\overline{E}_\infty \to \mathfrak{X}_\infty \to X_\infty \to 0 \qquad \square$$

We recall the notion of orthogonal idempotents of a group ring.

Definition 1.3.7. Let $\Delta := \mathrm{Gal}(K_0/\mathbb{Q})$ and let

$$e_\chi := \frac{1}{p-1}\sum_{\delta\in\Delta}\chi^{-1}(\delta)\delta \in \overline{\mathbb{Q}}[\Delta]$$

This e_χ is called the *orthogonal idempotent* associated with a character χ of Δ (such a χ is called a *character of the first kind* in the literature).

For a slightly more general definition, see [Was97, §6.3] or [KKS12, Proposition 10.12]. A thorough exposition is presented in [Sha, §2.8]. The properties of e_χ which we will use in the sequel, all of them easily verifiable, are collected in the following proposition.

Proposition 1.3.8. *For all characters $\chi \neq \chi'$ of Δ and $\sigma \in \Delta$:*

(1) $e_\chi^2 = e_\chi$ *(idempotence)*
(2) $e_\chi e_{\chi'} = 0$ *(orthogonality)*
(3) $\sum_\chi e_\chi = 1$ *(completeness)*
(4) $e_\chi\sigma = \chi(\sigma)e_\chi$ *(eigenspace property)*

From these it follows that any module M over the ring $\overline{\mathbb{Q}}[\Delta]$ admits an orthogonal decomposition $M = \bigoplus_\chi e_\chi M$. □

As the proposition suggests, one should think of $e_\chi M$ as the χ-eigenspace. In particular, summing $e_\chi M$ over just the even characters (those for which $\chi(-1) = 1$) gives the plus part M^+ of M, i.e. the largest submodule on which complex conjugation acts trivially. Summing over odd characters ($\chi(-1) = -1$), we obtain the odd part M^-, on which complex conjugation acts by (-1).

Lemma 1.3.9. *$e_\chi\mathfrak{X}_\infty$ is torsion and $(e_\chi\mathfrak{X}_\infty)/(\gamma^{p^n} - 1) \simeq e_\chi\mathfrak{X}_n$ for all $\chi \neq \mathbb{1}$ even. (Here $\mathbb{1}$ denotes the trivial Dirichlet character.)*

Proof. As above, $\mathfrak{X}_n \sim \mathbb{Z}_p^r$ for $r = (K_n : \mathbb{Q}) - \mathrm{rk}_{\mathbb{Z}_p}\overline{\sigma_{n,p}\mathfrak{E}_n}$. We have $(K_n : \mathbb{Q}) = r_1 + 2r_2$ and the second term is $r_1 + r_2 - 1$ by Leopoldt's conjecture [Was97, Corollary 5.32], so $r = r_2 + 1$. We lose one rank for the same reason as in the proof of Corollary 1.3.5, and complex embeddings are killed by taking e_χ for $\chi \neq \mathbb{1}$ even, which proves that $e_\chi\mathfrak{X}_\infty$ is torsion.

Since Ω_n is the maximal abelian extension of K_n within Ω_∞, we have

$$\mathrm{Gal}(\Omega_\infty/K_n)' = \mathfrak{X}_\infty^{\gamma^{p^n}-1}$$

It follows that $\mathrm{Gal}(\Omega_\infty/\Omega_n) = \mathfrak{X}_\infty^{\gamma^{p^n}-1}$, and therefore

$$\mathrm{Gal}(\Omega_n/K_\infty) = \mathfrak{X}_\infty/\mathfrak{X}_\infty^{\gamma^{p^n}-1}$$

The assertion will now follow from

$$e_\chi\,\mathrm{Gal}(\Omega_n/K_\infty) = e_\chi\mathfrak{X}_n \tag{1.16}$$

Since the difference between the two Galois groups $\mathrm{Gal}(\Omega_n/K_\infty)$ and $\mathfrak{X}_n = \mathrm{Gal}(\Omega_n/K_n)$, namely $\mathrm{Gal}(K_\infty/K_n)$, is in the $\mathbb{1}$-eigenspace, the assertion (1.16) holds for $\chi \neq \mathbb{1}$ by orthogonality. □

Chapter 2

p-adic L-functions

In this chapter we very briefly survey the various equivalent definitions and some basic properties of p-adic L-functions. As our goal is to discuss and prove the Iwasawa main conjecture in Chapter 3, this chapter covers only slightly more than necessary for this. In particular, we prove nothing, and won't state everything in the fullest possible generality.

Here we present two ways to define p-adic L-functions: one through p-adic interpolation, and one by using so-called Stickelberger elements. The two definitions of course yield the same object. The first method is due to Kubota and Leopoldt [KL64], while the second one was introduced by Iwasawa [Iwa69b].

The definition by Kubota and Leopoldt is more analytical, which is why the p-adic L-functions in this chapter are sometimes referred to as analytic p-adic L-functions, as opposed to algebraic p-adic L-functions which arise as generators of certain characteristic ideals, to be discussed in Chapter 3. The Iwasawa main conjecture asserts the equivalence of these two notions.

There is also a way to interpret p-adic L-functions as measures. We won't discuss this here, as we shall not need it in the sequel. We refer to [KKS12, §10.1(e–f)], [Was97, Chapter 12], [CS06, §3.1–4.2], [Lan90, Chapters 2, 10], [Kob84, Chapter II]. The thesis [Cas08] also discusses various different approaches to p-adic L-functions in detail.

2.1 Definition via p-adic interpolation

Let $\chi : \mathbb{Z} \to \overline{\mathbb{Q}}$ be a Dirichlet character of conductor $\mathfrak{f}$. By fixing an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, we may regard χ as having values in $\mathbb{C}_p$, where $\mathbb{C}_p$ denotes the field of complex p-adic numbers.

We recall the theory of Dirichlet L-functions.

Definition 2.1.1. For $s \in \mathbb{C}$, $\operatorname{Re} s > 1$, let

$$L(s, \chi) := \sum_{n=0}^{\infty} \frac{\chi(n)}{n^s}$$

be the *Dirichlet L-function.*

It admits an Euler product expansion for $\operatorname{Re} s > 1$

$$L(s,\chi) = \prod_{p \text{ prime}} \frac{1}{1-\chi(p)p^s} \tag{2.1}$$

$L(s,\chi)$ has an analytic continuation to $\mathbb{C}$; this is a meromorphic function, analytic everywhere except at $s=1$ for $\chi = \mathbb{1}$, where $\mathbb{1}$ denotes the trivial character.

The p-adic L-function $L_p(s,\chi)$ is a p-adic meromorphic function $\mathbb{Z}_p \to \mathbb{C}_p$ interpolating the values of $L(s,\chi)$ at negative integers. In fact, for the interpolation to succeed, we need to remove the Euler factor corresponding to p in (2.1). This is necessary because the p-Euler factor behaves badly when it comes to being p-adically continuous.

For $\chi = \mathbb{1}$, an avatar of this phenomenon is given by Kummer's congruences

$$\big(1-p^r\big)\zeta(1-r) \equiv \big(1-p^{r'}\big)\zeta(1-r') \bmod p^n$$

for $n, r, r' \in \mathbb{N}$, $(p-1) \nmid r$, $r \equiv r' \bmod (p-1)p^n$. This is connected to the definition of the p-adic zeta function, of which $L_p(s,\chi)$ is a generalisation.

Let $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ denote the Teichmüller character.

Theorem 2.1.2. *There exists a unique p-adic meromorphic function $L_p(-,\chi) : \mathbb{Z}_p \to \mathbb{C}_p$ such that for all $r \in \mathbb{N}$,*

$$L_p(1-r,\chi) = \big(1-\chi\omega^{-r}(p)p^{r-1}\big)\, L(1-r,\chi\omega^{-r}) \qquad \square$$

Uniqueness comes from the set $\{1-r \mid r \in \mathbb{N}\}$ being dense in $\mathbb{Z}_p$. It is easily seen that for an odd character χ, the p-adic L-function $L_p(s,\chi)$ is identically zero.

Definition 2.1.3. Let $\kappa : \operatorname{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \xrightarrow{\sim} \mathbb{Z}_p^\times$ be the *cyclotomic character*, defined by $\sigma(\zeta) = \zeta^{\kappa(\sigma)}$ for all $\sigma \in \operatorname{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$, $\zeta \in \mu_{p^n}$, $n \geqslant 1$.

Then κ respects the following direct product structures on the domain and codomain:

$$\begin{aligned}\operatorname{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) &\simeq \operatorname{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)) \times \operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) = \Gamma \times \Delta \\ \mathbb{Z}_p^\times &\simeq \mu_{p-1} \times (1+p\mathbb{Z}_p) \simeq (\mathbb{Z}/(p-1)\mathbb{Z}) \times \mathbb{Z}_p\end{aligned}$$

In particular, κ sends the fixed topological generator γ of Γ to a topological generator of $1+p\mathbb{Z}_p$.

The following theorem states that p-adic L-functions are *Iwasawa functions*, meaning that they are obtained by plugging $\kappa(\gamma)^s - 1$ into a power series. As explained in [Was97, p. 243], power series correspond to measures, thus the following statement also has a measure-theoretic interpretation, which we won't discuss here.

Theorem 2.1.4. *There exists a unique element $G_\chi(T) \in \operatorname{Frac}(\mathbb{Z}_p[\chi][\![T]\!])$ such that $L_p(s,\chi) = G_\chi(\kappa(\gamma)^s - 1)$. For $\mathfrak{f} \neq 1, p^n$ for $n \geqslant 2$, we have $G_\chi(T) \in \mathbb{Z}_p[\chi][\![T]\!]$. Here* Frac *denotes the field of fractions, and $\mathbb{Z}_p[\chi]$ is the ring extension of $\mathbb{Z}_p$ obtained by adjoining the values of χ.* $\square$

In Chapter 3, χ will be a character of $\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, thus $G_\chi(T)$ will be a power series whenever $\chi \neq \mathbb{1}$. One form of the Ferrero–Washington theorem, referenced in Remark 1.2.3, states that in this case, at least one coefficient of the power series $G_\chi(T)$ does not lie in the maximal ideal of the discrete valuation ring $\mathbb{Z}_p[\chi]$, and is therefore not divisible by p.

This section is based on [KKS12, §10.1] and [Was97, Chapters 4–5].

2.2 Definition via Stickelberger elements

Let $N \in \mathbb{N}$, and consider the cyclotomic extension $\mathbb{Q}(\mu_N)/\mathbb{Q}$. There is an isomorphism of groups

$$\begin{aligned} &\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \simeq (\mathbb{Z}/N\mathbb{Z})^\times \\ &(\sigma_a : \zeta_N \mapsto \zeta_N^a) \leftrightarrow a \end{aligned}$$

Definition 2.2.1. We define

$$\vartheta_N := \sum_{\substack{a=1 \\ (a,N)=1}}^{N} \left(\frac{1}{2} - \frac{a}{N}\right) \sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})]$$

to be the *Stickelberger element* of $\mathbb{Q}(\mu_N)$.

Remark 2.2.2. In the literature, there exist slightly different versions of this definition. This one will be convenient for defining the p-adic L-function, and also has the advantage of hinting at a connection with zeta functions: the coefficient $1/2 - a/N$ is the negative of the value of the first Bernoulli polynomial $B_1(x) = x - 1/2$ at $x = a/N$, which agrees with the value of the partial Riemann zeta function with respect to a modulo N at 0.

Definition 2.2.3. Let

$$\vartheta'_N := \sum_{\substack{a=1 \\ (a,N)=1}}^{N} \left(-\frac{a}{N}\right) \sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})],$$

also called the Stickelberger element by some authors. We call the ideal

$$I_N := \vartheta'_N \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})] \cap \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})]$$

the *Stickelberger ideal* of $\mathbb{Q}(\mu_N)$.

Theorem 2.2.4 (Stickelberger)**.** *The Stickelberger ideal I_N annihilates the ideal class group of $\mathbb{Q}(\mu_N)$.* □

Consider the tower of fields $\mathbb{Q}(\mu_{p^n})$ for $n \geqslant 0$. Fix $n \geqslant 1$ for now and let χ be a character of $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ with values in $\mathbb{C}_p$. Let $\mathbb{Q}_p(\chi)$ denote $\mathbb{Q}_p$ adjoined the values of χ. We have an action of χ on the group ring of $\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}(\mu_p)) \times \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ over $\mathbb{Q}$ given by the map

$$\begin{aligned} (-)^\chi : \mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})] &\to \mathbb{Q}_p(\chi)[\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})] \\ \sum_{\substack{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}(\mu_p)) \\ \tau \in \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})}} a_{\sigma,\tau}(\sigma,\tau) &\mapsto \sum_{\substack{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}(\mu_p)) \\ \tau \in \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})}} a_{\sigma,\tau}\chi(\sigma)\tau \end{aligned}$$

Let χ be not equal to the Teichmüller character. Then one can show that by applying the above action to Stickelberger elements, we obtain a projective system

$$\vartheta_{p^n}^\chi \in \mathbb{Z}_p[\chi][\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}(\mu_p))], \quad n \geqslant 1 \tag{2.2}$$

where $\mathbb{Z}_p[\chi]$ denotes the ring extension of $\mathbb{Z}_p$ obtained by adjoining the values of χ. This has a limit

$$\vartheta^{\chi}_{p^\infty} \in \varprojlim_n \mathbb{Z}_p[\chi][\mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}(\mu_p))] = \mathbb{Z}_p[\chi][\![\Gamma]\!]$$

where $\Gamma = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}/\mathbb{Q}(\mu_p))) \simeq \mathbb{Z}_p$.

Theorem 2.2.5. *Let $G_{\chi^{-1}\omega}(T) := \vartheta^{\chi}_{p^\infty}$. Then $L_p(s,\chi) := G_\chi(\kappa(\gamma)^s - 1)$ is the p-adic L-function, where κ denotes the cyclotomic character.* □

The above method can be generalised for arbitrary Dirichlet characters, not just those of Δ. This survey is based on [KKS12, §10.3(d)]. For details and proofs, see [Was97, Chapters 6–7], Iwasawa's original paper [Iwa69b], and his Princeton lectures [Iwa72].

Chapter 3

The Iwasawa main conjecture

In the first section of this chapter we will formulate the Iwasawa main conjecture. Assuming Vandiver's conjecture, the main conjecture admits a short proof, this will be presented in Section 3.2. In Section 3.3 we will give a brief outline of the proof of the main conjecture, going into further details in Section 3.4; in these sections we temporarily waive the mathematical rigour in order to focus on the essence of the the arguments. The proof itself will be given in Sections 3.5 to 3.8.

The aim was to give an account of the main conjecture that is as detailed and self-contained as possible, by building on the previous chapters. One exception to self-containedness is that we assume familiarity with the Iwasawa theory of local units. For this, we refer to [Lan90, Chapter 7] or [Was97, §13.8]. We will also recall the necessary statements without proofs in Propositions 3.7.2 and 3.7.4.

The proof we present is due to Rubin. Our presentation is based on the appendix [Rub90] to Lang's book and Washington's account [Was97, Chapter 15] of Rubin's proof.

3.1 Statement

We will work with the cyclotomic tower $\mathbb{Q}(\mu_{p^{n+1}})$ $(n \geqslant 0)$, and retain the notations of the preceding chapters. The statement we are about to make is the Iwasawa main conjecture for the plus part of these fields. More precisely, the statement will be about χ-eigenspaces of certain Iwasawa modules where χ is an even character of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$; the characters being even means that we are working with the plus part.

On the one hand, the characteristic ideal of an Iwasawa module kills the module by definition: in particular, this can be applied to the module X_∞ and its orthogonal components $e_\chi X_\infty$. On the other hand, we may consider the p-adic L-function $G_{\chi^{-1}\omega}(T) \in \Lambda$. As explained in Section 2.2, $G_{\chi^{-1}\omega} = \vartheta^\chi_{p^\infty} = \lim \vartheta^\chi_{p^n}$, where $\vartheta^\chi_{p^n}$ is obtained by applying a χ-action to the Stickelberger element ϑ_{p^n}. Recall that Stickelberger elements annihilate ideal class groups. The main conjecture states that these two annihilating objects are essentially the same:

Theorem 3.1.1 (Iwasawa main conjecture, 1st form)**.** *For all odd Dirichlet characters χ of the group* $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ *not equal to the Teichmüller character ω, we have* $\mathrm{Char}\,(e_\chi X_\infty) = G_{\chi^{-1}\omega}\Lambda$.

Here we see that the main conjecture relates the algebraic object X_∞ with an analytic one, the p-adic L-function. One may refer to the characteristic polynomial of $e_\chi X_\infty$ as the *algebraic p-adic L-function.* Then the main conjecture fits into the Hilbert–Pólya conjecture which asserts that zeta functions should arise as characteristic polynomials.

Recall that the p-adic L-function is identically zero for odd characters, hence the restriction to odd characters χ in the statement (χ and $\chi^{-1}\omega$ have opposite parities). Also recall that the p-adic L-function is a power series only for nontrivial even characters (Theorem 2.1.4), which is why we need to exclude the case $\chi = \omega$.

We may give an equivalent formulation for the p-ramified Iwasawa module $\mathfrak{X}_\infty$ in place of the unramified Iwasawa module X_∞. Recall that Ω_n = the maximal abelian p-extension of $\mathbb{Q}(\mu_{p^{n+1}})$ unramified outside p, and $\mathfrak{X}_n = \mathrm{Gal}(\Omega_n/\mathbb{Q}(\mu_{p^{n+1}}))$ the Galois group, with $\mathfrak{X}_\infty$ being the projective limit.

Theorem 3.1.2 (Iwasawa main conjecture, 2$^{\text{nd}}$ form)**.** *For all $\chi \neq \mathbb{1}$ even Dirichlet characters of* $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ *we have* $\mathrm{Char}(e_\chi \mathfrak{X}_\infty) = G_\chi\left(\kappa(\gamma)(1+T)^{-1} - 1\right)\Lambda$.

For the equivalence of Theorems 3.1.1 and 3.1.2 see [Rub90], where these are Theorems 8.1 and 8.9, respectively. The proof given there shows that Theorem 3.1.2 implies Theorem 3.1.1; it is easily seen that each step can be reversed, proving the equivalence. The proof actually uses Iwasawa's theory of adjoints, which is not discussed in [Rub90]; for these details, see [Was97, §§15.4–15.5]. The even/odd change comes from a Kummer duality type statement.

In this chapter we will give a proof of this theorem; for the proof, it will be more convenient to consider yet another alternate formulation, for which we need to make further definitions.

Definition 3.1.3. We recall the following notations from the theory of cyclotomic extensions.

1. $U_n := \left\{u \in \mathbb{Z}_p[\zeta_{p^{n+1}}]^\times \,\middle|\, u \equiv 1 \bmod (\zeta_{p^{n+1}} - 1)\right\}$ = the local units of $\mathbb{Q}(\mu_{p^{n+1}})$ congruent to 1 modulo the maximal ideal $(\zeta_{p^{n+1}} - 1)$, also referred to as the group of *principal local units*;
2. $E_n := \mathbb{Z}[\zeta_{p^n+1}]^\times$ = the global units of $\mathbb{Q}(\mu_{p^{n+1}})$;
3. $C_n := \langle \zeta_{p^{n+1}}, 1 - \zeta_{p^{n+1}}^a \mid 1 \leqslant a \leqslant p^n - 1\rangle \cap E_n$ = the cyclotomic units of $\mathbb{Q}(\mu_{p^{n+1}})$;
4. $\overline{E}_n$:= the closure of $E_n \cap U_n$ in U_n;
5. $\overline{C}_n$:= the closure of $C_n \cap U_n$ in U_n;
6. For all the above as well as $\mathfrak{X}_n$, we will use the index ∞ to denote the projective limit taken with respect to the relative norm maps, e.g. $\mathfrak{X}_\infty = \varprojlim \mathfrak{X}_n$. We also let $X_\infty = \varprojlim A_n$. (The notation A_∞ is usually used to denote the injective limit of the groups A_n.)

Theorem 3.1.4 (Iwasawa main conjecture, 3$^{\text{rd}}$ form)**.** *For all even Dirichlet characters χ of* $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ *we have* $\mathrm{Char}\left(e_\chi X_\infty\right) = \mathrm{Char}\left(e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty\right)$.

We postpone checking that the Iwasawa modules of which characteristic ideals are considered are indeed finitely generated torsion modules to Section 3.7.

Claim 3.1.5. *Theorem 3.1.4 implies Theorem 3.1.2 (and hence Theorem 3.1.1).*

Proof. Consider the following two exact sequences; the first one comes from Corollary 1.3.6, the second one is self-defining.

$$0 \to e_\chi U_\infty / e_\chi \overline{E}_\infty \to e_\chi \mathfrak{X}_\infty \to e_\chi X_\infty \to 0 \tag{3.1}$$

$$0 \to e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty \to e_\chi U_\infty / e_\chi \overline{C}_\infty \to e_\chi U_\infty / e_\chi \overline{E}_\infty \to 0 \tag{3.2}$$

These together with Lemma 1.1.13, which asserts the multiplicativity of characteristic ideals in exact sequences, give the following:

$$\begin{aligned}
\operatorname{Char}(e_\chi \mathfrak{X}_\infty) &= \operatorname{Char}\left(e_\chi U_\infty / e_\chi \overline{E}_\infty\right) \operatorname{Char}(e_\chi X_\infty) && \text{multiplicativity for (3.1)} \\
&= \operatorname{Char}\left(e_\chi U_\infty / e_\chi \overline{E}_\infty\right) \operatorname{Char}\left(e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty\right) && \text{Theorem 3.1.4} \\
&= \operatorname{Char}\left(e_\chi U_\infty / e_\chi \overline{C}_\infty\right) && \text{multiplicativity for (3.2)} \\
&= G_\chi\left(\kappa(\gamma)(1+T)^{-1} - 1\right)\Lambda && \text{[Lan90, Chapter 7, Theorem 5.2]}
\end{aligned}$$

This finishes the proof. □

Remark 3.1.6. Note that our 3rd formulation of the main conjecture concerns *all* even Dirichlet characters χ, including the trivial character $\mathbb{1}$. This special case, however, will be treated separately from the case $\chi \neq \mathbb{1}$ in Section 3.8.1, and has a rather straightforward proof as compared to the much more complicated $\chi \neq \mathbb{1}$ case, the proof of which occupies most of this chapter.

Remark 3.1.7. In the beginning of this section we gave a heuristic motivation via killing Iwasawa modules. A more historically correct approach is viewing the main conjecture as the analogue of the rationality of the zeta function of a curve over a finite field. This analogy is outlined in Appendix A.3.

The characteristic ideal is a rather rough invariant: for instance, the modules $\Lambda/(a) \oplus \Lambda/(b)$ and $\Lambda/(ab)$ have the same characteristic ideal. It stands to reason to raise the question whether there is a finer version of the main conjecture. Vandiver's conjecture implies a strengthening, see Section 3.2. Kato [Kat07, §2.3.5] states that Kurihara devised a method in which multiple p-adic L-functions are used simultaneously to obtain more data about the Λ-module structure. Furthermore, using p-adic modular forms, Sharifi made a conjecture that can be understood to be a refinement of the Iwasawa main conjecture [Sha18, Conjecture 5.5.2]. Finally we mention that in all known cases, the characteristic polynomial of $e_\chi X_\infty$ has no double roots, and this leads to a rather elementary proof of the main conjecture [KKS12, §10.3(d)].

3.2 Relation to Vandiver's conjecture

Conjecture 3.2.1 (Vandiver)**.** *p does not divide the class number of* $\mathbb{Q}(\mu_p)^+$.

We will now show that Vandiver's conjecture implies a stronger version of the 3rd form of Iwasawa main conjecture. The proof we present is from [CS06, Proposition 4.5.3]; for a proof of the 2nd form, see [Was97, Theorem 10.16]. In Appendix A.3 we will discuss a heuristic interpretation of the main conjecture assuming Vandiver's conjecture.

Definition 3.2.2. We define the plus parts of the global and cyclotomic units defined in Definition 3.1.3. In the direct sums, χ runs through all even characters of $\operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, and projective limits are taken with respect to relative norm maps.

1. $E_n^+ := \bigoplus e_\chi E_n = E_n \cap \mathbb{Q}(\mu_p^{n+1})^+$
2. $C_n^+ := \bigoplus e_\chi C_n = C_n \cap \mathbb{Q}(\mu_p^{n+1})^+$
3. $\overline{E}_n^+ := \bigoplus e_\chi \overline{E}_n =$ the closure of $E_n^+ \cap U_n$ in U_n
4. $\overline{C}_n^+ := \bigoplus e_\chi \overline{C}_n =$ the closure of $C_n^+ \cap U_n$ in U_n
5. $\overline{E}_\infty^+ := \bigoplus e_\chi \overline{E}_\infty = \varprojlim \overline{E}_n^+$

6. $\overline{C}_\infty^+ := \bigoplus e_\chi \overline{C}_\infty = \varprojlim \overline{C}_n^+$

Theorem 3.2.3. *Suppose Vandiver's conjecture holds. Then we have* $X_\infty = 0$ *and* $\overline{E}_\infty^+ / \overline{C}_\infty^+ = 0$.

Proof. Recall that A_n denotes the p-part of the class group of $\mathbb{Q}(\mu_{p^{n+1}})$. Vandiver's conjecture asserts that $A_0 = 0$. Then Lemma 1.3.3 states $X_\infty = \varprojlim A_n = 0$, proving the first assertion.

For the second assertion, recall the analytic class number formula, (one form of) which states that $(E_n^+ : C_n^+) = \# \operatorname{Cl} \mathbb{Q}(\mu_{p^n+1})^+$. This class number is prime to p by Vandiver's conjecture and Lemma 1.3.3. Thus we have a short exact sequence

$$0 \to C_n^+ \to E_n^+ \to (\text{finite group of order prime to } p) \to 0$$

Therefore the same is true after taking intersections with U_n:

$$0 \to C_n^+ \cap U_n \to E_n^+ \cap U_n \to (\text{finite group of order prime to } p) \to 0$$

Now tensor this exact sequence of abelian groups by $\mathbb{Z}_p$; this is an exact functor because $\mathbb{Z}_p$ is flat over $\mathbb{Z}$. The cokernel is killed, and we obtain an isomorphism

$$\left(C_n^+ \cap U_n\right) \otimes \mathbb{Z}_p \xrightarrow{\simeq} \left(E_n^+ \cap U_n\right) \otimes \mathbb{Z}_p \tag{3.3}$$

Recall that Leopoldt's conjecture holds for totally real fields and states that $\operatorname{rk}_{\mathbb{Z}_p} \overline{E}_n^+ = \operatorname{rk}_{\mathbb{Z}}(E_n^+ \cap U_n)$. It follows that $(E_n^+ \cap U_n) \otimes \mathbb{Z}_p = \overline{E}_n^+$ and $(C_n^+ \cap U_n) \otimes \mathbb{Z}_p = \overline{C}_n^+$. Therefore (3.3) proves $\overline{C}_n^+ = \overline{E}_n^+$ for all $n \geqslant 0$. Taking projective limits yields the second assertion. □

3.3 Outline of the proof

The proof of Theorem 3.1.4 will go as follows. Let $e_\chi X_\infty \sim \bigoplus_{i=1}^k \Lambda / f_i \Lambda$; then the characteristic polynomial of $e_\chi X_\infty$ is $f_\chi = f_1 \cdots f_k$ (warning: the character χ is suppressed in this notation for brevity's sake). Let h_χ be the characteristic polynomial of $e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty$. Theorem 3.1.4 states that f_χ and h_χ agree up to a unit of Λ, that is, $f_\chi \Lambda = h_\chi \Lambda$.

For $\chi = \mathbb{1}$, the proof is simple, and uses only the class number formula, Leopoldt's conjecture, and Lemma 1.3.3; this case is treated in Section 3.8.1. For $\chi \neq \mathbb{1}$, we need much more elaborate techniques, which we discuss now.

It is, in fact, sufficient to prove that $f_\chi \mid h_\chi$. The proof that this seemingly weaker statement already implies $f_\chi \Lambda = h_\chi \Lambda$ will use Iwasawa's theorem on the growth of an Iwasawa module (Theorem 1.2.14) as well as the analytic class number formula and Leopoldt's conjecture. (See the beginning of Section 3.8.)

The proof of $f_\chi \mid h_\chi$ will be done by finite induction: we will prove $f_1 \cdots f_i \mid \eta^{i+1} h_\chi$ for $i = 1, \ldots, k$ where the η-factor comes from a technical difficulty. Notice that h_χ already appears in the base case. For $i = k$, we get $f_\chi \mid \eta^{k+1} h_\chi$; luckily the η-factor can then be removed and we get $f_\chi \mid h_\chi$, as desired.

The technique used in the induction step is as follows. Using the structure theorem of finitely generated Λ-modules, we can represent f_i by an ideal class c_i (defined in Lemma 3.7.10) and h_χ by a morphism ψ (defined in (3.30) for $i = 1$ and (3.31) for $2 \leqslant i$)—we will refer to this as the *first conversion step.* Using heavy machinery from algebraic number theory, we will construct an

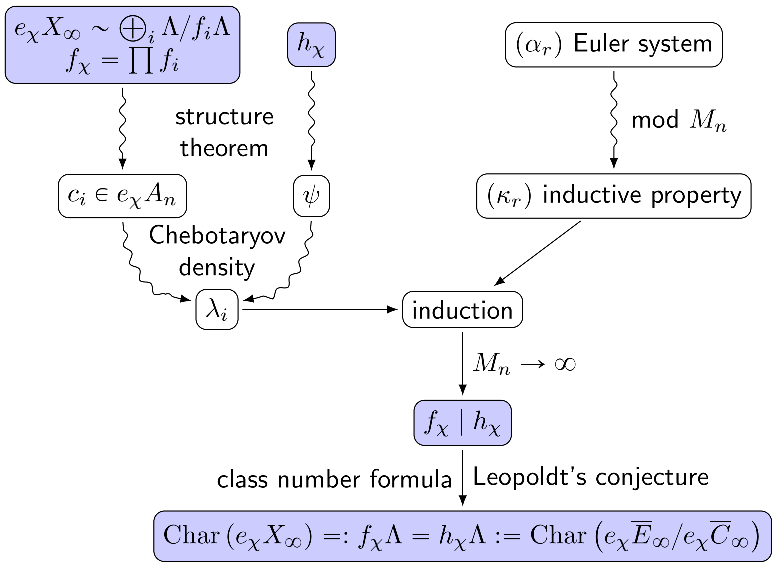
$e_\chi X_\infty \sim \bigoplus_i \Lambda/f_i\Lambda$
$f_\chi = \prod f_i$
h_χ
(α_r) Euler system
structure theorem
mod M_n
$c_i \in e_\chi A_n$
ψ
(κ_r) inductive property
Chebotaryov density
λ_i
induction
$M_n \to \infty$
$f_\chi \mid h_\chi$
class number formula
Leopoldt's conjecture
$\mathrm{Char}\,(e_\chi X_\infty) =: f_\chi\Lambda = h_\chi\Lambda := \mathrm{Char}\,\big(e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty\big)$

Figure 3.1: A simplified outline of the proof. Concepts with blue background are on the ∞-level, the rest are on finite levels.

auxiliary prime λ_i satisfying properties determined by *both* c_i and ψ (that is, f_i and h_χ); this will be our *second conversion step*. This will imply a divisibility relation like $f_1 \cdots f_i \mid \eta^{i+1} h_\chi$.

Actually, there is one more factor on the left that facilitates the induction. This has to do with cyclotomic units. We will encode the cyclotomic units in the precise formulation of the divisibility condition and in the construction of ψ in the base case. The way we do this constitutes a crucial part of the proof: we will use an Euler system (α_r) for the cyclotomic units, introduced in Section 3.5. For our purposes, one may think of the Euler system as a set of cyclotomic units admitting some nice properties that make it well fit to use in inductive arguments (Proposition 3.5.5).

Remark 3.3.1. Another proof of the main conjecture, using modular forms, was given by Mazur and Wiles. They proved the converse divisibility $h_\chi \mid f_\chi$. This underlines the point that the 'luxury' of only proving one of these divisibility relations is due to the presence of the analytic class number formula, an analogue of which is not available in more general setups, thus necessitating the usage of both Euler systems and modular forms. For an outline of the proof using the modular form method (and the necessary background), see [Sha18, §4.3].

3.4 Technical details of the proof

In this section we will elaborate further on what actually goes into the proof of the main conjecture. Figure 3.1 shows the general strategy, while Figure 3.2 details the steps in the proof. In the latter figure, in order to keep things as simple as possible, all arrows coming out of Proposition 3.7.2 are represented by just one dotted arrow. Within the Iwasawa theory part, the structure theorem of finitely generated Λ-modules is used extensively; this is also not shown in the figure.

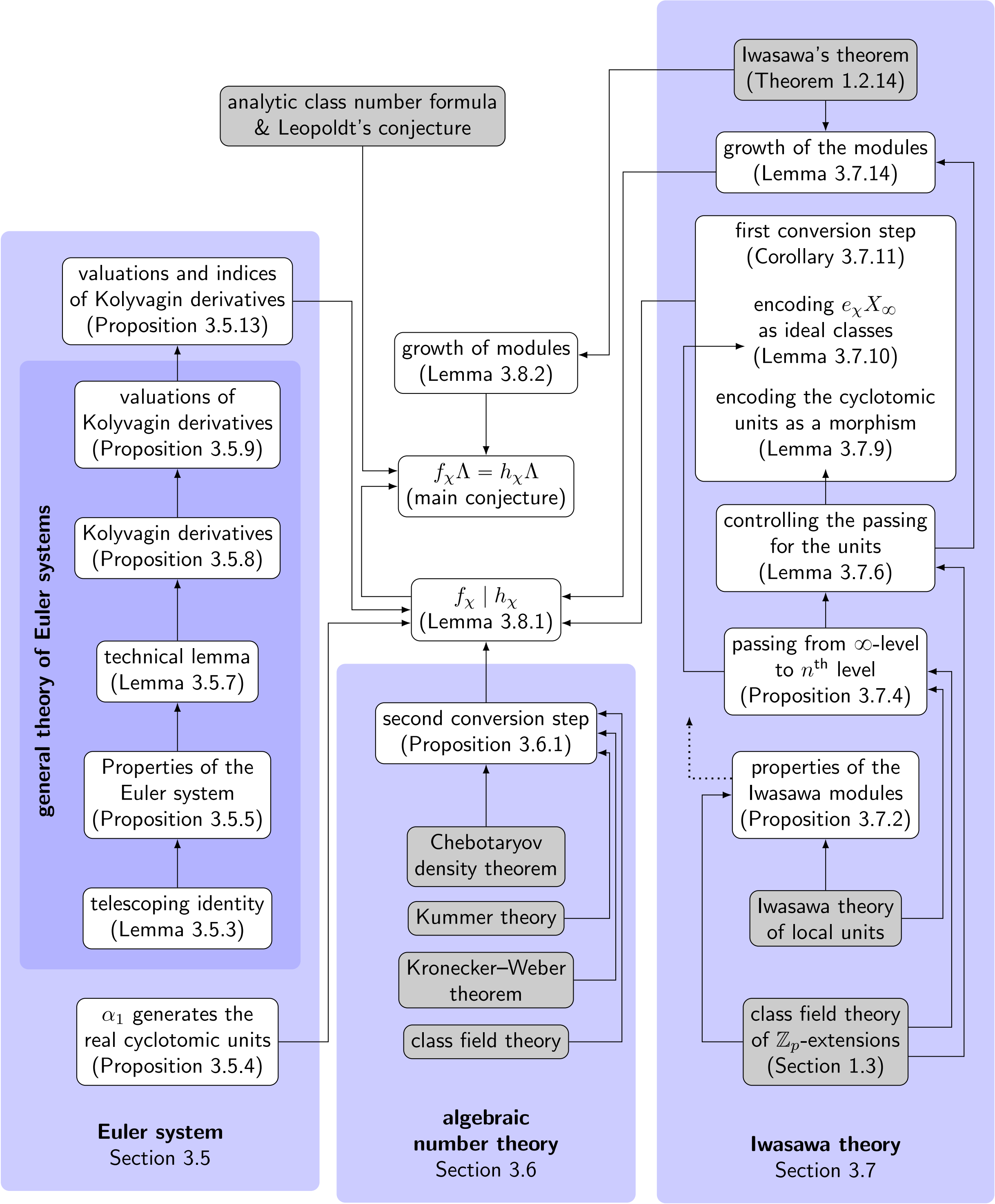
Iwasawa's theorem (Theorem 1.2.14)
analytic class number formula & Leopoldt's conjecture
growth of the modules (Lemma 3.7.14)
first conversion step (Corollary 3.7.11)
encoding $e_\chi X_\infty$ as ideal classes (Lemma 3.7.10)
encoding the cyclotomic units as a morphism (Lemma 3.7.9)
valuations and indices of Kolyvagin derivatives (Proposition 3.5.13)
growth of modules (Lemma 3.8.2)
valuations of Kolyvagin derivatives (Proposition 3.5.9)
$f_\chi \Lambda = h_\chi \Lambda$ (main conjecture)
controlling the passing for the units (Lemma 3.7.6)
Kolyvagin derivatives (Proposition 3.5.8)
general theory of Euler systems
$f_\chi \mid h_\chi$ (Lemma 3.8.1)
technical lemma (Lemma 3.5.7)
passing from ∞-level to n^{th} level (Proposition 3.7.4)
second conversion step (Proposition 3.6.1)
Properties of the Euler system (Proposition 3.5.5)
properties of the Iwasawa modules (Proposition 3.7.2)
Chebotaryov density theorem
Kummer theory
telescoping identity (Lemma 3.5.3)
Iwasawa theory of local units
Kronecker–Weber theorem
α_1 generates the real cyclotomic units (Proposition 3.5.4)
class field theory of $\mathbb{Z}_p$-extensions (Section 1.3)
class field theory
Euler system
Section 3.5
algebraic number theory
Section 3.6
Iwasawa theory
Section 3.7

Figure 3.2: A complete outline of the dependencies of steps in the main conjecture's proof. Arrows mean that one concept is used in the proof of the other. Concepts with grey background are considered to be prerequisites for the proof.

Let us first detail the part of the proof taking place on finite levels.

We begin with the **Euler system**. We will explicitly define a set of cyclotomic units (α_r) where r will run over some subset $\mathcal{S}$ of the rational integers. These (α_r) will enjoy two key properties: α_1 will generate the real cyclotomic units (Proposition 3.5.4), and the system (α_r) will satisfy the property of being an Euler system (Proposition 3.5.5). Euler systems, in general, are cohomological objects obeying a generalisation of Proposition 3.5.5, and there is a whole theory of their properties in this high generality. We will need to build up some of this theory in our case: this will be done in Lemma 3.5.7 and Propositions 3.5.8 and 3.5.9. Since these statements constitute part of a general theory, the explicit definition of (α_r) won't matter, just the fact that it is an Euler system. While all these statements have a deeper cohomological truth to them, neither the assertions nor their proofs will be done in cohomological terms, save for the proof of Proposition 3.5.8, which uses Hilbert's theorem 90.

More precisely, the part of the theory of Euler systems we need is the notion of a **Kolyvagin derivative** (κ_r) associated with (α_r). This can be thought of as modulo M_n instance of the Euler system (α_r) where the modulus M_n will be chosen later. The reason for considering these derivative classes is that this will allow us to obtain some results about their valuations over some primes (Proposition 3.5.9), which will be well suited for use in an induction. We have no such results for (α_r). We will restate these results in terms of valuations and indices (Proposition 3.5.13); this is the form we will use in proving $f_\chi \mid h_\chi$.

The second conversion step given in Proposition 3.6.1 is a rather technically loaded part of the proof: we will need the full arsenal of algebraic number theory. What happens here is that given an ideal class c_i and a morphism ψ, we want to find a prime $\lambda_i \in c_i$ satisfying some nice property with respect to ψ. The prime will be given by the Chebotaryov density theorem (so in fact, there will be infinitely many such primes) applied to some large field extension. This extension has to, on one hand, encode c_i, which can be done via class field theory. On the other hand, we also need to encode the morphism ψ, for which Kummer theory will prove to be an effective tool. During these steps, there will be several technical details to attend to; at one point we will also need to invoke the Kronecker–Weber theorem.

Now we discuss the steps that have to do with the ∞-level. The most important part **Iwasawa theory** plays is encoding f_χ and h_χ so that we may do induction on finite levels. In order to do this, we need to describe the behaviour of several Iwasawa modules. Some information has already been obtained in Chapter 1. We will also need the Iwasawa theory of local units as described in [Lan90, Chapter 7, Theorem 5.1]. These statements will be recalled in Propositions 3.7.2 and 3.7.4, and can be treated as blackboxes.

In particular, we will describe the natural maps from the ∞-level to finite levels. For all but one of the Iwasawa modules involved, these will be as simple as can be, that is, we will have natural isomorphisms. The only exception is $\overline{E}_\infty$, where all we can say is that the natural morphism has finite kernel and cokernel (Lemma 3.7.6). This will manifest in the technical difficulty that when we encode h_χ as a morphism (Lemma 3.7.9), an η-factor will emerge, which will represent the annihilator of the aforementioned kernel and cokernel. This is the η that was mentioned in the previous section.

Finally we will need a lemma about the growth of the modules involved (Lemma 3.7.14), one application of which will be choosing the modulus M_n for the Kolyvagin derivatives in terms of n. The proof of $f_\chi \mid h_\chi$ will then be done by putting all the previous results together: our first conversion step Corollary 3.7.11 turns f_χ and h_χ into objects on the n^{th} level so that our second conversion step can be applied. The fact that α_1 generates the real cyclotomic units establishes a connection between the Euler system and h_χ, and the result Proposition 3.5.13 on Kolyvagin derivatives makes the induction work. Finally letting $n \to \infty$ makes $M_n \to \infty$, making our modulo M_n results hold on the ∞-level. The η-factor can be removed either through two opportune choices of η or by invoking the Ferrero–Washington theorem.

To prove that $f_\chi \mid h_\chi$ implies $f_\chi\Lambda = h_\chi\Lambda$, we will use a simple consequence of Iwasawa's theorem (Lemma 3.8.2), which will be applicable as per the result on the growth of the modules involved. Then the analytic class number formula and Leopoldt's conjecture finish the proof.

3.5 An Euler system for the cyclotomic units

We begin by fixing some notation. As always, p will be an odd prime. We will be working on the n^{th} level of the $\mathbb{Z}_p$-extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)$, $n \in \mathbb{N}$. In order to emphasise this, most of our notation will feature the level n. In the present and the next section we will not be considering any other levels. Let $F_n = \mathbb{Q}(\mu_{p^{n+1}})^+$ and $G_n := \mathrm{Gal}(F_n/\mathbb{Q})$. In what follows, ℓ will always denote a rational prime. Let

$$\mathcal{S} := \left\{ r \in \mathbb{N} \,\middle|\, r \text{ square-free, } \ell \mid r \Rightarrow \ell \equiv \pm 1 \pmod{p^{n+1}} \right\}$$

Thus $\mathcal{S}$ is the set of positive integers that are a product of distinct primes, all of which split in $F_n/\mathbb{Q}$. Fix $M_n \in \mathbb{N}$ to be an odd integer (to be chosen later as some large power of the odd prime p, also depending on n), and define a mod M_n version of $\mathcal{S}$:

$$\mathcal{S}_{M_n} := \left\{ r \in \mathcal{S} \,\middle|\, \ell \mid r \Rightarrow \ell \equiv 1 \pmod{M_n} \right\}$$

Remark 3.5.1. The reason we will be working modulo M_n later is that this will enable us use the theorems about M_n^{th} powers and M_n^{th} roots of unity in field extensions (e.g. Kummer theory). These will play a substantial role in proving Propositions 3.6.1 and 3.5.9.

While it may seem that we lose information in the modulo M_n reduction, this is not exactly the case. At the very end of the proof of the Iwasawa main conjecture (Section 3.8.2), we will set $M_n := p^{n+N}$ (for some $N \in \mathbb{N}$), and let n range over $\mathbb{N}$. We will obtain divisibility properties modulo M_n for all n, which will together give a divisibility relation without any reduction.

Remark 3.5.2. We will sometimes use additive notation in the multiplicative group $F_n(\mu_r)^\times$, as is standard practice. While this notation may be admittedly confusing, it saves us from using several levels of exponents, thus—hopefully—making our computations easier to follow.

Let $r \in \mathcal{S}$ and $G_{n,r} := \mathrm{Gal}(F_n(\mu_r)/F_n) \simeq \mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q}) \simeq (\mathbb{Z}/r\mathbb{Z})^\times$. For $\ell \equiv \pm 1 \pmod{p^{n+1}}$, the group $G_{n,\ell}$ is cyclic; let σ_ℓ be a fixed generator. Let

$$\mathrm{N}_r := \sum_{\sigma \in G_{n,r}} \sigma \in \mathbb{Z}[G_{n,r}] \tag{3.4}$$

denote the relative norm in the extension $F_n(\mu_r)/F_n$. Further define the *derivative operators*

$$\mathrm{D}_\ell := \sum_{i=1}^{\ell-2} i\sigma_\ell^i \in \mathbb{Z}[G_{n,\ell}] \quad \text{and} \quad \mathrm{D}_r := \prod_{\ell \mid r} \mathrm{D}_\ell \in \mathbb{Z}[G_{n,r}] \tag{3.5}$$

The derivative operators will only be used later, when we start working modulo M_n; they will give rise to the Kolyvagin derivative of our Euler system.

Lemma 3.5.3 (Telescoping identity)**.** $(\sigma_\ell - 1)\mathrm{D}_\ell = (\ell - 1) - \mathrm{N}_\ell$.

Proof. This follows from the definitions (3.4) and (3.5):

$$\begin{aligned}(\sigma_\ell - 1)\mathrm{D}_\ell &= (\sigma_\ell - 1)\sum_{i=1}^{\ell-2} i\sigma_\ell^i \\ &= \sum_{i=1}^{\ell-2}\left(i\sigma_\ell^{i+1} - i\sigma_\ell^i\right) \\ &= (\ell-2)\sigma_\ell^{\ell-1} - \sum_{i=1}^{\ell-2}\sigma_\ell^i \\ &= (\ell-1) - \sum_{i=1}^{\ell-1}\sigma_\ell^i \\ &= (\ell-1) - \mathrm{N}_\ell \qquad \square\end{aligned}$$

For $r \in \mathcal{S}$ define

$$\alpha_r := \left(\zeta_{p^{n+1}}\left(\prod_{\ell \mid r}\zeta_\ell\right) - 1\right)\left(\zeta_{p^{n+1}}^{-1}\left(\prod_{\ell \mid r}\zeta_\ell\right) - 1\right)$$

where $\zeta_{p^{n+1}}$ and the ζ_ℓ's are fixed primitive $(p^{n+1})^{\mathrm{th}}$ resp. ℓ^{th} roots of unity. These numbers α_r form a so-called *Euler system.* The properties of this system will be given in Propositions 3.5.4 and 3.5.5. There is a key distinction between the natures of these two propositions. The former is about this particular Euler system; it will be used towards the end of the proof of the main conjecture. It will enable us to establish a connection between the Euler system and the Iwasawa module of cyclotomic units, and thus h_χ. This will be beneficial because it will allow us to use the general theory of Euler systems, which is what Proposition 3.5.5 and the subsequential statements of this section are about.

In general, an Euler system is a collection of cohomology classes satisfying conditions similar those in Proposition 3.5.5. Rubin [Rub00] gives a general treatment of Euler systems, and all statements in this section after Proposition 3.5.5 can be found there, albeit in vastly larger generality (and hence much longer proofs). (For a quick survey on what Euler systems represent in different settings, see [Kat07, §2.5].)

Proposition 3.5.4. *For all nontrivial even characters χ of Δ, $e_\chi\alpha_1$ generates the $e_\chi\Lambda_{\Gamma_n} := e_\chi\mathbb{Z}_p[\Gamma^{p^n}] = e_\chi\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^{n+1}}))]$-module $e_\chi\overline{C}_n$.*

Proof. By definition, $\alpha_1 = \left(\zeta_{p^{n+1}} - 1\right)\left(\zeta_{p^{n+1}}^{-1} - 1\right)$. The group C_n^+ of cyclotomic units of $\mathbb{Q}(\zeta_{p^{n+1}})^+$ is generated by -1 and the elements

$$\beta_g := \zeta_{p^{n+1}}^{(1-g)/2} \cdot \frac{1 - \zeta_{p^{n+1}}^g}{1 - \zeta_{p^{n+1}}}, \quad 1 < g < \frac{1}{2}p^{n+1},\ p \nmid g;$$

see [Was97, Lemma 8.1]. Let $\sigma_g \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ be defined by $\sigma_g(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^g$. Then we have $(\sigma_g - 1)\alpha_1 = (1 + \sigma_{-1})\beta_g$. It is easily checked that $\beta_g = \sigma_{-1}\beta_g$, thus we obtain $(\sigma_g - 1)\alpha_1 = \beta_g^2$. So far we have been working in the group C_n^+. It follows that in the Λ_{Γ_n}-module $\overline{C}_n$ we have $\frac{1}{2}(\sigma_g - 1)\alpha_1 = \beta_g$ as 2 is invertible in Λ_{Γ_n}. The assertion then follows using that χ is even. $\square$

Proposition 3.5.5 (Properties of the Euler system)**.** *For all $r \in \mathcal{S}$ and $\ell \mid r$ we have the following:*

(1) $\alpha_r \in F_n(\mu_r)^\times$.
(2) α_r *is a cyclotomic unit if* $r > 1$.
(3) $\alpha_r \equiv \alpha_{r/\ell}$ *modulo every prime above* ℓ.
(4) $\mathrm{N}_\ell \alpha_r = (\mathrm{Fr}_\ell - 1)\alpha_{r/\ell}$ *where* Fr_ℓ *denotes the Frobenius of* ℓ.

Proof. The first two assertions are easily seen. For (3) one only needs to observe that $\zeta_\ell \equiv 1$ modulo all primes above ℓ. It remains to show (4).

$$\begin{aligned}
\mathrm{N}_\ell \alpha_r &= \mathrm{N}_\ell \left(\zeta_{p^{n+1}} \left(\prod_{q \mid r} \zeta_q \right) - 1 \right) \mathrm{N}_\ell \left(\zeta_{p^{n+1}}^{-1} \left(\prod_{q \mid r} \zeta_q \right) - 1 \right) \\
&= \prod_{\tau \in G_{n,\ell}} \tau \left(\zeta_{p^{n+1}} \left(\prod_{q \mid r} \zeta_q \right) - 1 \right) \prod_{\tau \in G_{n,\ell}} \tau \left(\zeta_{p^{n+1}} \left(\prod_{q \mid r} \zeta_q \right) - 1 \right) \\
&= \prod_{i=1}^{\ell-1} \left(\zeta_\ell^i \underbrace{\zeta_{p^{n+1}} \left(\prod_{q \mid \frac{r}{\ell}} \zeta_q \right)}_{A} - 1 \right) \prod_{i=1}^{\ell-1} \left(\zeta_\ell^i \underbrace{\zeta_{p^{n+1}}^{-1} \left(\prod_{q \mid \frac{r}{\ell}} \zeta_q \right)}_{B} - 1 \right) && (3.6) \\
&= \frac{\prod_{i=0}^{\ell-1} \left(\zeta_\ell^i A - 1 \right)}{A - 1} \cdot \frac{\prod_{i=0}^{\ell-1} \left(\zeta_\ell^i B - 1 \right)}{B - 1} \\
&= \frac{A^\ell - 1}{A - 1} \cdot \frac{B^\ell - 1}{B - 1} && (3.7) \\
&= \frac{\zeta_{p^{n+1}}^\ell \prod_{q \mid \frac{r}{\ell}} \zeta_q^\ell - 1}{\zeta_{p^{n+1}} \prod_{q \mid \frac{r}{\ell}} \zeta_q - 1} \cdot \frac{\zeta_{p^{n+1}}^{-\ell} \prod_{q \mid \frac{r}{\ell}} \zeta_q^\ell - 1}{\zeta_{p^{n+1}}^{-1} \prod_{q \mid \frac{r}{\ell}} \zeta_q - 1} \\
&= (\mathrm{Fr}_\ell - 1)\alpha_{r/\ell} && (3.8)
\end{aligned}$$

In (3.6) we used that $\tau(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}$ and $\forall q \neq \ell : \tau(\zeta_q) = \zeta_q$. The last step (3.8) uses $\zeta_{p^{n+1}}^\ell = \zeta_{p^{n+1}}^{\pm 1}$ and $\zeta_{p^{n+1}}^{-\ell} = \zeta_{p^{n+1}}^{\mp 1}$ which hold since $\ell \equiv \pm 1 \bmod m$. The step (3.7) follows from the following lemma:

Lemma 3.5.6. *Let p be a prime, η a primitive p^{th} root of unity. Then in any field F containing $\mathbb{Q}(\mu_p)$, the following holds for any $X \in F$:*

$$\prod_{i=0}^{p-1} \left(\eta^i X - 1 \right) = X^p - 1$$

Proof. This is immediate from the factorisation of $X^p - 1$:

$$X^p - 1 = \prod_{i=0}^{p-1} \left(X - \eta^i \right) = \prod_{i=0}^{p-1} \left(\eta^{p-1-i} X - 1 \right) \eta^{p(p-1)/2} = \prod_{i=0}^{p-1} \left(\eta^i X - 1 \right) \cdot 1 \qquad \square$$

This finishes the proof of Proposition 3.5.5. □

From now on until the end of this section, it won't matter how our Euler system α_r was defined, just that it satisfies the properties listed in Proposition 3.5.5.

We will now start working modulo M_n (q.v. Remark 3.5.1). In Proposition 3.5.8 we will introduce mod M_n representatives κ_r of α_r. The advantage of these is that we will be able to describe their valuations mod M_n in Proposition 3.5.9.

Lemma 3.5.7. *For $r \in \mathcal{S}_{M_n}$ we have $\mathrm{D}_r\alpha_r \in \left(F_n(\mu_r)^\times / (F_n(\mu_r)^\times)^{M_n}\right)^{G_{n,r}}$, i.e. $\mathrm{D}_r\alpha_r$ is fixed under $G_{n,r}$ up to M_n^{th} powers.*

Proof. We do induction on the number of prime factors of r. For $r = 1$, the statement is trivial as $G_1 = 1$. For the induction step, let $r = \ell \cdot \frac{r}{\ell}$. Keep in mind that we are using additive notation in the multipicative group $F_n(\mu_r)^\times$.

$$\begin{aligned}
(\sigma_\ell - 1)\mathrm{D}_r\alpha_r &= (\sigma_\ell - 1)\mathrm{D}_\ell \mathrm{D}_{r/\ell}\alpha_r && \text{definition of } \mathrm{D}_r \\
&= \left((\ell - 1) - \mathrm{N}_\ell\right)\mathrm{D}_{r/\ell}\alpha_r && \text{Lemma 3.5.3} \\
&= (\ell - 1)\mathrm{D}_{r/\ell}\alpha_r - \mathrm{D}_{r/\ell}\mathrm{N}_\ell\alpha_r && \mathrm{D}_{r/\ell} \text{ and } \mathrm{N}_\ell \text{ commute}
\end{aligned}$$

The commuting of $\mathrm{D}_{r/\ell}$ and N_ℓ follows from their definition and $(r/\ell, \ell) = 1$; in particular, we use that r is square-free. Observe that the first term $(\ell - 1)\mathrm{D}_{r/\ell}\alpha_r$ is an M_n^{th} power since $\ell \equiv 1 \bmod M_n$. For the second term, we have

$$\begin{aligned}
\mathrm{D}_{r/\ell}\mathrm{N}_\ell\alpha_r &= \mathrm{D}_{r/\ell}(\mathrm{Fr}_\ell - 1)\alpha_{r/\ell} && \text{Proposition 3.5.5.4} \\
&= (\mathrm{Fr}_\ell - 1)\mathrm{D}_{r/\ell}\alpha_{r/\ell} && (\mathrm{Fr}_\ell - 1) \text{ and } \mathrm{D}_{r/\ell} \text{ commute}
\end{aligned}$$

$\mathrm{D}_{r/\ell}\alpha_{r/\ell}$ is an M_n^{th} power by induction, and M_n^{th} powers are preserved by $(\mathrm{Fr}_\ell - 1)$. Thus $(\sigma_\ell - 1)\mathrm{D}_r\alpha_r$ is an M_n^{th} power. Since $G_{n,r} = \langle G_{n,r/\ell}, \sigma_\ell \rangle$, this finishes the proof. □

Proposition 3.5.8. *For every $r \in \mathcal{S}_{M_n}$ there is a unique $\kappa_r \in F_n^\times / (F_n^\times)^{M_n}$ for which $\kappa_r \equiv$ $\mathrm{D}_r\alpha_r \bmod (F_n(\mu_r)^\times)^{M_n}$.*

Proof. This can be seen using Galois cohomology: we may define κ_r to be the image of $\mathrm{D}_r\alpha_r$ under the following composition of isomorphisms:

$$\begin{tikzcd}
\left(\dfrac{F_n(\mu_r)^\times}{(F_n(\mu_r)^\times)^{M_n}}\right)^{G_{n,r}} \arrow[r, "\simeq"] & H^1\left(\overline{F}_n/F_n(\mu_r), \mu_{M_n}\right)^{G_{n,r}} & H^1\left(\overline{F}_n/F_n, \mu_{M_n}\right) \arrow[l, "\simeq"'] & \dfrac{F_n^\times}{(F_n^\times)^{M_n}} \arrow[l, "\simeq"'] \\
\mathrm{D}_r\alpha_r \arrow[rrr, mapsto] & & & \kappa_r
\end{tikzcd}$$

The first and last isomorphisms come from Hilbert's theorem 90 [Ser02, II.§1.2]. The isomorphism in the middle comes from the inflation–restriction exact sequence (aka the Hochschild–Serre spectral sequence):

$$\begin{aligned}
0 \to H^1\left(F_n(\mu_r)/F_n, \mu_{M_n}^{\mathrm{Gal}(\overline{F}_n/F_n(\mu_r))}\right) &\to H^1\left(\overline{F}_n/F_n, \mu_{M_n}\right) \to H^1\left(\overline{F}_n/F_n(\mu_r), \mu_{M_n}\right)^{G_{n,r}} \\
\to H^2\left(F_n(\mu_r)/F_n, \mu_{M_n}^{\mathrm{Gal}(\overline{F}_n/F_n(\mu_r))}\right) &\to H^2\left(\overline{F}_n/F_n, \mu_{M_n}\right)
\end{aligned}$$

Here $H^i\left(F_n(\mu_r)/F_n, \mu_{M_n}^{\mathrm{Gal}(\overline{F}_n/F_n(\mu_r))}\right) = 0$ for $i = 1, 2$ (recall that M_n is a power of p, and r is prime to p), which gives us the isomorphism above. □

The collection of these κ_r is called the *Kolyvagin derivative* of the Euler system α_r (cf. [Rub00, §4.4]). In the upcoming Proposition 3.5.9, we will need a more explicit description of κ_r; for this, we make the construction more direct.

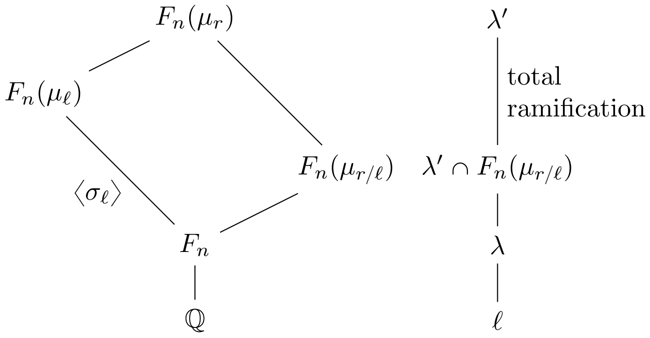

Figure 3.3: Objects in the proof of Proposition 3.5.9: fields on the left, prime ideals on the right

Proof (Second proof of Proposition 3.5.8). Consider the cochain

$$\begin{aligned} G_{n,r} = \mathrm{Gal}(F_n(\mu_r)/F_n) &\to F_n(\mu_r)^\times \\ \sigma &\mapsto ((\sigma - 1)\mathrm{D}_r\alpha_r)^{1/M_n} \end{aligned}$$

This cochain is well-defined by Lemma 3.5.7, and it is easily seen to be a 1-cocycle. As the cohomology group $H^1(F_n(\mu_r)/F_n, F_n(\mu_r)^\times) = 0$ is trivial, there is some $\beta_r \in F_n(\mu_r)^\times$ (unique up to $F_n^\times$) satisfying

$$(\sigma - 1)\beta_r = ((\sigma - 1)\mathrm{D}_r\alpha_r)^{1/M_n} \tag{3.9}$$

for all $\sigma \in G_{n,r}$. Then

$$\kappa_r := \frac{\mathrm{D}_r\alpha_r}{\beta_r^{M_n}} \tag{3.10}$$

satisfies the conditions of Proposition 3.5.8. □

The following is a key result about Kolyvagin derivatives; it corresponds to Theorems 4.5.1 and 4.5.4 in [Rub00]. (Rubin's somewhat obscure way of phrasing it [Rub90, Proposition 2.4] is made explicit in [CS06, §5.4] and in [Was97, Proposition 15.12].)

Recall that we fixed a generator σ_ℓ of $G_{n,\ell} = \mathrm{Gal}(F_n(\mu_\ell)/F_n) \simeq (\mathbb{Z}/\ell\mathbb{Z})^\times$. There is a mod ℓ primitive root x associated with σ_ℓ, meaning that $\sigma_\ell(\zeta_\ell) = \zeta_\ell^x$ where ζ_ℓ is the previously fixed primitive ℓ^{th} root of unity.

Proposition 3.5.9 (Kolyvagin)**.** *Let $r \in \mathcal{S}_{M_n}$, ℓ a rational prime, λ a prime of F_n above ℓ. Then*

(1) *If $\lambda \nmid r$ then $\mathrm{ord}_\lambda(\kappa_r) \equiv 0 \bmod M_n$ where ord_λ denotes the λ-adic valuation.*
(2) *If $\lambda \mid r$ then $\mathrm{ord}_\lambda(\kappa_r) \equiv -a \bmod M_n$ where $\kappa_{r/\ell} \equiv x^a \bmod \lambda$ for $a \in \mathbb{Z}$, and x is the mod ℓ primitive root associated with σ_ℓ.*

Remark 3.5.10. Note that this statement depends heavily on fixed choices. If we change our choice of σ_ℓ, then x changes as well, but so does the derivative operator D_r, and consequently, the image κ_r of $\mathrm{D}_r\alpha_r$. If we change our choice of ζ_ℓ, this also affects x, but it alters α_r too, and therefore $\mathrm{D}_r\alpha_r$ and thus κ_r as well.

Proof. First suppose $\lambda \nmid r$. Then by Lemma 3.5.7, $\mathrm{D}_r\alpha_r$ is a unit in $F_n(\mu_r)$ thus (3.10) yields $(\kappa_r) = (\beta_r^{-1})^{M_n}$ as ideals of $F_n(\mu_r)$. Since λ is unramified in $F_n(\mu_r)/F_n$, this proves $\mathrm{ord}_\lambda(\kappa_r) \equiv 0 \bmod M_n$.

Now let $\lambda \mid r$ and fix a mod ℓ primitive root x. Then x is a primitive root mod λ as well, so we can indeed write $\kappa_{r/\ell} \equiv x^a \bmod \lambda$ for some $a \in \mathbb{Z}$. Let λ' be a prime of $F_n(\mu_r)$ above λ; then x is still a primitive root mod λ' so we have $\mathrm{D}_{r/\ell}\alpha_{r/\ell} \equiv x^{a'} \bmod \lambda'$ for some $a' \in \mathbb{Z}$. By (3.10) we have

$$a \equiv a' \pmod{M_n} \tag{3.11}$$

Now by a calculation similar to that in the proof of Lemma 3.5.7:

$$\begin{aligned}
(\sigma_\ell - 1)\beta_r &= (\sigma_\ell - 1)\mathrm{D}_r\alpha_r^{1/M_n} && \text{by (3.9)}\\
&= (\sigma_\ell - 1)\mathrm{D}_\ell\mathrm{D}_{r/\ell}\alpha_r^{1/M_n} && \text{by (3.5)}\\
&= (\ell - 1 - \mathrm{N}_\ell)\mathrm{D}_{r/\ell}\alpha_r^{1/M_n} && \text{Lemma 3.5.3}\\
&= \mathrm{D}_{r/\ell}\alpha_r^{(\ell-1)/M_n} - \mathrm{D}_{r/\ell}\mathrm{N}_\ell\alpha_r^{1/M_n} && \mathrm{D}_{r/\ell} \text{ and } \mathrm{N}_\ell \text{ commute}
\end{aligned}$$

By Proposition 3.5.5.4 we have $\mathrm{N}_\ell\alpha_r^{1/M_n} = (\mathrm{Fr}_\ell - 1)\alpha_r^{1/M_n}$. Since $\ell \equiv 1 \bmod M_n$, this means $\mathrm{N}_\ell\alpha_r^{1/M_n} = 1$. Thus

$$\begin{aligned}
(\sigma_\ell - 1)\beta_r &= \mathrm{D}_{r/\ell}\alpha_r^{(\ell-1)/M_n}\\
&\equiv \mathrm{D}_{r/\ell}\alpha_{r/\ell}^{(\ell-1)/M_n} && \text{by Proposition 3.5.5.3}
\end{aligned}$$

mod all primes above ℓ. Hence $(\sigma_\ell - 1)\beta_r \equiv x^b \bmod \lambda'$ where

$$b := a'(\ell - 1)/M_n \tag{3.12}$$

Also let

$$c := \operatorname{ord}_{\lambda'} \beta_r \tag{3.13}$$

Since $(1 - \zeta_\ell)$ is a uniformiser, i.e. $\operatorname{ord}_{\lambda'}(1 - \zeta_\ell) = 1$, we have $\beta_r = (1 - \zeta_\ell)^c y$ for some λ'-unit $y \in F_n(\mu_r)$ (i.e. $\operatorname{ord}_{\lambda'} y = 0$). Then we have

$$x^b \equiv (\sigma_\ell - 1)\,\beta_r = \left((1 - \zeta_\ell)^{\sigma_\ell - 1}\right)^c y^{\sigma_\ell - 1} \equiv x^c \bmod \lambda' \tag{3.14}$$

To justify the last congruence in (3.14), we need to make two simple observations. First, by definitions of σ_ℓ and x

$$\begin{aligned}
(\sigma_\ell - 1)\,(1 - \zeta_\ell) &= \frac{1 - \zeta_\ell^x}{1 - \zeta_\ell}\\
&= 1 + \zeta_\ell + \zeta_\ell^2 + \ldots + \zeta_\ell^{x-1}\\
&= 1 + [\zeta_\ell - 1] + \left[\zeta_\ell^2 - 1\right] + \ldots + \left[\zeta_\ell^{x-1} - 1\right] + (x - 1)\\
&\equiv x \bmod \lambda'
\end{aligned}$$

Here the last step uses that the expressions in square brackets are all divisible by $(\zeta_\ell - 1) \in \lambda'$.

Secondly, we have $\sigma_\ell y \equiv y \bmod \lambda'$ since σ_ℓ is in the inertia group of λ' as this is totally ramified in $F_n(\mu_r)/F_n(\mu_{r/\ell})$.

Now (3.14) implies

$$b \equiv c \bmod \ell - 1 \tag{3.15}$$

Therefore

$$\begin{aligned}
\operatorname{ord}_\lambda \kappa_r &= \frac{1}{\ell-1}\operatorname{ord}_{\lambda'} \kappa_r && \lambda = (\lambda')^{\ell-1}\\
&= \frac{-1}{\ell-1}\operatorname{ord}_{\lambda'}\left(\beta_r^{M_n}\right) && (\kappa_r) = (\beta_r^{-1})^{M_n}\\
&= \frac{-M_n c}{\ell-1} && \text{definition (3.13) of } c\\
&\equiv \frac{-M_n b}{\ell-1} && \text{by (3.15)}\\
&= -a' && \text{definition (3.12) of } b\\
&\equiv -a \bmod M_n && \text{by (3.11)}
\end{aligned}$$

□

Proposition 3.5.9.2 establishes a connection between valuations and indices of Kolyvagin derivatives in the following sense.

Definition 3.5.11. As before, let x be the mod ℓ primitive root associated with σ_ℓ. Let $w \in F_n^\times$ be coprime to ℓ and λ a prime of F_n above ℓ. Then for any $\sigma \in G_n = \mathrm{Gal}(F_n/\mathbb{Q})$ define the *index* $\operatorname{ind}_{\sigma\lambda} w \in (\mathbb{Z}/(\ell-1)\mathbb{Z})$ by

$$w \equiv x^{\operatorname{ind}_{\sigma\lambda}(w)} \bmod \sigma\lambda$$

It will prove useful to extend this connection to valuations and indices of *all* Galois conjugates of a prime λ. To this end, we make the following definitions.

Definition 3.5.12. We define the collections of valuations and indices as follows:

$$\begin{aligned}
\overline{\operatorname{ord}}_\lambda(w) &:= \sum_{\sigma\in G_n} \operatorname{ord}_{\sigma\lambda}(w)\sigma \in \mathbb{Z}[G_n]\\
\overline{\operatorname{ind}}_\lambda(w) &:= \sum_{\sigma\in G_n} \operatorname{ind}_{\sigma\lambda}(w)\sigma \in (\mathbb{Z}/M_n\mathbb{Z})[G_n]
\end{aligned}$$

The operators $\overline{\operatorname{ord}}_\lambda$ and $\overline{\operatorname{ind}}_\lambda$ thus collect information about how w behaves with respect to all the primes above ℓ. We have the following proposition.

Proposition 3.5.13.

$$\overline{\operatorname{ord}}_\lambda\left(e_\chi \kappa_{\ell_1\cdots\ell_i}\right) \equiv -\,\overline{\operatorname{ind}}_\lambda\left(e_\chi \kappa_{\ell_1\cdots\ell_{i-1}}\right) \bmod M_n$$

Proof. Follows directly from Definition 3.5.11 and Proposition 3.5.9.2 and the fact that every expression involved is $\mathbb{Z}[G_n]$-linear. □

Proposition 3.5.13 is how we will ultimately make use of the nice properties of the Euler system in the proof of the main conjecture.

3.6 The second conversion step

We continue dealing with objects that live entirely on finite levels. The first conversion step, which logically precedes the topic of the present section, will be therefore discussed later, as its point is transforming objects from the ∞-level to the n^{th} level (Corollary 3.7.11).

Note that up until now we have not made any assumptions about M_n other than it being an integer. In the upcoming Proposition 3.6.1 we will already assume that M_n is a power of an odd prime, but M_n will only be explicitly chosen towards the end of the proof of the Iwasawa main conjecture (q.v. Remark 3.5.1). The following Proposition 3.6.1 will be the tool used in each inductive step in the proof of the main conjecture.

Proposition 3.6.1. *Let p be an odd prime, $A := (\mathrm{Cl}\, F_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ the p-part of the ideal class group of $F_n = \mathbb{Q}(\mu_{p^{n+1}})^+$, $c \in A$ an ideal class, M_n a power of p, W a finite $G_n = \mathrm{Gal}(F_n/\mathbb{Q})$-submodule of $F_n^\times/(F_n^\times)^{M_n}$ and*

$$\psi : W \to (\mathbb{Z}/M_n\mathbb{Z})[G_n]$$

a Galois-equivariant map. Then there exist infinitely many primes satisfying the following four properties:

(1) *$\lambda \in c$;*
(2) *$\ell \equiv \pm 1 \bmod m$ and $\ell \equiv 1 \bmod M_n$ where ℓ is the rational prime under λ;*
(3) *$\forall w \in W$: $\mathrm{ord}_\lambda w \equiv 0 \bmod M_n$;*
(4) *$\exists u \in (\mathbb{Z}/M_n\mathbb{Z})^\times : \overline{\mathrm{ind}}_\lambda(w) = u\psi(w)$.*

Remark 3.6.2. Proposition 3.6.1 will be used in the proof of the Iwasawa main conjecture to inductively choose primes λ_i (q.v. Remark 3.7.12). We won't actually need the fact that there are infinitely many such primes λ, just that there is *at least* one, but as it will be evident, the natural way of proving this already yields the existence of infinitely many λ's. The ideal class c will come from factors f_i of f_χ, the homomorphism ψ from h_χ. Properties (1) and (4) thus assert that λ_i represents *both* f_i and h_χ. The point of property (2) is that ℓ is a prime factor in the indexing set $\mathcal{S}_{M_n}$ of mod M_n Kolyvagin derivatives. Property (3) is only technical, asserting that it is valid to consider indices on W as we do in (4).

Remark 3.6.3. Proposition 3.6.1 can also be found in [Rub87], with a simpler version being present in [Tha88]. Greither [Gre92] gives a variant of Proposition 3.6.1 that is also valid for $p = 2$.

Proof. The proof is based upon Chebotaryov's density theorem, which we recall now [Lan86, Chapter VIII, §4, Theorem 10].

Theorem 3.6.4 (Chebotaryov). *Let K/k be a finite Galois extension of degree N with Galois group $\mathcal{G}$, let $\sigma \in \mathcal{G}$, and let s be the number of elements in the conjugacy class of σ. Then the primes $\mathfrak{p}$ of k which are unramified in K/k and above which there is a prime $\mathfrak{P} \mid \mathfrak{p}$ such that $\sigma = (\mathfrak{P}, K/k)$ have density s/N. In particular, there are infinitely many such primes.* □

In view of this, what we need to do is find an extension of F_n the Galois group of which encodes all the data in the setup of Proposition 3.6.1. Then the lambdas will be obtained by applying Theorem 3.6.4 to a suitably chosen element of this Galois group.

Let H be the p-Hilbert class field of F_n; then $A \simeq \mathrm{Gal}(H/F_n)$ by class field theory. Now consider Figure 3.4; $HF_n(\mu_{M_n}, W^{1/M_n})/F_n$ will play the role of K/k in Theorem 3.6.4. We now verify that this is the composite of the extensions H/F_n and $F_n(\mu_{M_n}, W^{1/M_n})/F_n$. This will allow us to choose an element of $\mathrm{Gal}(HF_n(\mu_{M_n}, W^{1/M_n})/F_n)$ that has suitable restrictions to H and $F_n(\mu_{M_n}, W^{1/M_n})$.

Claim 3.6.5. $F_n(\mu_{M_n}) \cap H = F_n$

Proof (Proof of Claim 3.6.5). The extension $F_n(\mu_{M_n}) \cap H$ of $F_n = \mathbb{Q}(\mu_m)^+$ is abelian. By the Kronecker–Weber theorem there is some N that is a multiple of p^{n+1} and $F_n(\mu_{M_n}) \cap H \subseteq$

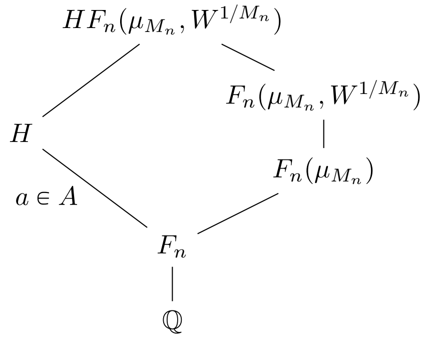

Figure 3.4: Field extensions in the proof of Proposition 3.6.1

$\mathbb{Q}(\mu_N)$. The extension $F_n(\mu_{M_n}) \cap H/F_n$ is unramified, so by the ramification theory of cyclotomic extensions, $F_n(\mu_{M_n}) \cap H$ is either $\mathbb{Q}(\mu_{p^{n+1}})$ or $\mathbb{Q}(\mu_{p^{n+1}})^+ = F_n$. Since $\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}(\mu_{p^{n+1}})^+$ has degree 2, it is not a p-extension. Hence we must have $F_n(\mu_{M_n}) \cap H = F_n$. □

Claim 3.6.6. $F_n(\mu_{M_n}, W^{1/M_n}) \cap H = F_n$

Proof (Proof of Claim 3.6.6). Let $\tau \in \mathrm{Gal}(F_n(\mu_{M_n})/F_n)$ be the complex conjugation automorphism. Since $F_n = \mathbb{Q}(\mu_{p^{n+1}})^+$, τ acts trivially on F_n and since $W \leqslant F_n^\times/(F_n^\times)^{M_n}$, the action is also trivial on W. The action on μ_{M_n} is by (-1), so it follows that τ acts by (-1) on the group $\mathrm{Gal}(F_n(\mu_{M_n}, W^{1/M_n})/F_n(\mu_{M_n}))$.

On the other hand, $\mathrm{Gal}(HF_n(\mu_{M_n})/F_n(\mu_{M_n})) \simeq \mathrm{Gal}(H/F_n)$ by Claim 3.6.5, and therefore τ acts trivially by definition of H. Hence τ acts both trivially and by (-1) on the intersection $\mathrm{Gal}(F_n(\mu_{M_n}, W^{1/M_n}) \cap HF_n(\mu_{M_n})/F_n(\mu_{M_n}))$, proving

$$F_n\left(\mu_{M_n}, W^{1/M_n}\right) \cap HF_n(\mu_{M_n}) = F_n(\mu_{M_n}) \tag{3.16}$$

Therefore

$$\begin{aligned} F_n(\mu_{M_n}, W^{1/M_n}) \cap H &= F_n(\mu_{M_n}, W^{1/M_n}) \cap HF_n(\mu_{M_n}) \cap H && HF_n(\mu_{M_n}) \supseteq H \\ &= F_n(\mu_{M_n}) \cap H && \text{by (3.16)} \\ &= F_n && \text{Claim 3.6.5} \end{aligned}$$ □

Claim 3.6.7. $\mathrm{Gal}(F_n(\mu_{M_n}, W^{1/M_n})/F_n(\mu_{M_n})) \simeq \mathrm{Hom}(W, \mu_{M_n})$.

Proof (Proof of Claim 3.6.7). Kummer theory (cf. e.g. [Mil18, Remark 5.31]) gives us a non-degenerate pairing

$$\mathrm{Gal}\left(F_n\left(\mu_{M_n}, W^{1/M_n}\right)/F_n\left(\mu_{M_n}\right)\right) \times W\Big/\mathrm{Ker}\left(W \hookrightarrow \frac{F_n^\times}{(F_n^\times)^{M_n}} \to \frac{F_n(\mu_{M_n})^\times}{(F_n(\mu_{M_n})^\times)^{M_n}}\right) \to \mu_{M_n}$$

The claim will follow once we show that the kernel above is zero, which is equivalent to proving that $F_n \hookrightarrow F_n(\mu_{M_n})$ induces

$$F_n^\times/(F_n^\times)^{M_n} \hookrightarrow F_n(\mu_{M_n})^\times/(F_n(\mu_{M_n})^\times)^{M_n}$$

This can be seen using Galois cohomology; bars will denote algebraic closure.

$$\begin{aligned}
&\operatorname{Ker}\left(F_n^\times/(F_n^\times)^{M_n} \to F_n(\mu_{M_n})^\times/(F_n(\mu_{M_n})^\times)^{M_n}\right) \\
&= \operatorname{Ker}\left(H^1\left(\overline{F}_n/F_n, \mu_{M_n}\right) \to H^1\left(\overline{F_n(\mu_{M_n})}/F_n(\mu_{M_n}), \mu_{M_n}\right)\right) && \text{from Hilbert 90 [Ser02, II.§1.2]} \\
&= H^1\left(F_n(\mu_{M_n})/F_n, \mu_{M_n}\right) && \text{inflation–restriction sequence}
\end{aligned}$$

In a cyclic extension, 1st and 0th cohomology have the same cardinality, and the latter group is trivial. □

Define the map

$$\begin{aligned}
\iota : (\mathbb{Z}/M_n\mathbb{Z})[G_n] &\to \mu_{M_n} \\
\sum_{g \in G_n} a_g g &\mapsto \zeta_{M_n}^{a_1}
\end{aligned}$$

Composing with ψ, we get a map $\iota \circ \psi \in \operatorname{Hom}(W, \mu_{M_n})$. Let $\varphi \in \operatorname{Gal}(F_n(\mu_{M_n}, W^{1/M_n})/F_n(\mu_{M_n}))$ be the associated Galois automorphism given by Claim 3.6.7; by Kummer theory this means

$$\forall w \in W : (\iota \circ \psi)(w) = \frac{\varphi(w^{1/M_n})}{w^{1/M_n}} \tag{3.17}$$

By Claim 3.6.6 we may choose an automorphism $\delta \in \operatorname{Gal}(HF_n(\mu_{M_n}, W^{1/M_n})/F_n)$ such that $\delta|_H = a$ (under the Artin map of class field theory) and $\delta|_{F_n(\mu_{M_n}, W^{1/M_n})} = \varphi$.

Let λ be a prime of F_n given by Theorem 3.6.4 with $\sigma := \delta$; we now check that it satisfies the properties above.

(1) and (2) follow directly from construction. (3) comes from λ being unramified.

For (4), we will show that

$$\exists u \in (\mathbb{Z}/M_n\mathbb{Z})^\times : \iota \circ \overline{\operatorname{ind}}_\lambda(w) = u(\iota \circ \psi)(w). \tag{3.18}$$

Then replacing g by $g^{-1}w$ and using the G_n-stability of W will prove (4). Since both sides of (3.18) are in $\mu_{M_n} \simeq \mathbb{Z}/M_n\mathbb{Z}$, it is equivalent to proving that the two sides are 1 for the same w's.

On the left hand side, we have

$$\iota \circ \overline{\operatorname{ind}}_\lambda(w) = \iota\left(\sum_{\sigma \in G_n} \operatorname{ind}_{\sigma\lambda}(w)\sigma\right) = \operatorname{ind}_\lambda(w),$$

hence the left hand side of (3.18) is 1 iff w is an M_n^{th} power mod λ.

For the right hand side, let λ' be a prime of $F_n(\mu_{M_n}, W^{1/M_n})$ above λ for which $\operatorname{Fr}_{\lambda'} = \varphi$. Then

$$\begin{aligned}
\iota \circ \psi(w) = 1 &\iff \frac{\varphi(w^{1/M_n})}{w^{1/M_n}} = 1 && \text{by (3.17)} \\
&\iff \operatorname{Fr}_{\lambda'} w^{1/M_n} = w^{1/M_n} \\
&\iff w \text{ is an } M_n^{\text{th}} \text{ power mod } \lambda' \cap F_n(\mu_{M_n}) \\
&\iff w \text{ is an } M_n^{\text{th}} \text{ power mod } \lambda
\end{aligned}$$

The last equivalence holds because ℓ splits completely in $F_n(\mu_{M_n})/F_n$ by (2). This concludes the proof of (4), and thus the proof of Proposition 3.6.1. □

3.7 Results using Iwasawa theory

So far we have focused on the field $F_n = \mathbb{Q}(\mu_{p^{n+1}})^+$. We will now make use of Iwasawa theory: to do so, we will be looking at an infinite tower of fields, use results from Iwasawa theory to obtain information about the ∞-level of this tower, and then translate this information to the finite levels.

So consider the tower consisting of the fields $\mathbb{Q}(\mu_{p^{n+1}})$ for $n \geqslant 0$. The ascending union of these is denoted by

$$\mathbb{Q}(\mu_{p^\infty}) := \bigcup_{n\geqslant 0} \mathbb{Q}(\mu_{p^{n+1}})$$

Write $\Delta := \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$, $\Gamma := \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_p)) \simeq \mathbb{Z}_p$ and $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) = \Delta \times \Gamma$ for the Galois groups. We assume familiarity with the Iwasawa theory of local units (cf. [Lan90, Chapter 7]), but will recall the relevant results in Propositions 3.7.2 and 3.7.4 below.

Definition 3.7.1. We recall the following notations from the theory of cyclotomic extensions.

1. $A_n := \mathrm{Cl}\,\mathbb{Q}(\mu_{p^{n+1}}) \otimes_{\mathbb{Z}} \mathbb{Z}_p = p$-part of the ideal class group $\mathrm{Cl}\,\mathbb{Q}(\mu_{p^{n+1}})$;
2. $U_n := \{u \in \mathbb{Z}_p[\zeta_{p^{n+1}}]^\times \mid u \equiv 1 \bmod (\zeta_{p^{n+1}} - 1)\}$ = the local units of $\mathbb{Q}(\mu_{p^{n+1}})$ congruent to 1 modulo the maximal ideal $(\zeta_{p^{n+1}} - 1)$;
3. $E_n := \mathbb{Z}[\zeta_{p^n+1}]^\times$ = the global units of $\mathbb{Q}(\mu_{p^{n+1}})$;
4. $C_n := \langle \zeta_{p^{n+1}}, 1 - \zeta_{p^{n+1}}^a \mid 1 \leqslant a \leqslant p^{n+1} - 1\rangle \cap E_n$ = the cyclotomic units of $\mathbb{Q}(\mu_{p^{n+1}})$;
5. $\overline{E}_n :=$ the closure of $E_n \cap U_n$ in U_n;
6. $\overline{C}_n :=$ the closure of $C_n \cap U_n$ in U_n;
7. $\Omega_n :=$ the maximal abelian p-extension of $\mathbb{Q}(\mu_{p^{n+1}})$ unramified outside p;
8. $\mathfrak{X}_n := \mathrm{Gal}(\Omega_n/\mathbb{Q}(\mu_{p^{n+1}}))$;
9. For all the above, we will use the index ∞ to denote the projective limit taken with respect to the relative norm maps, e.g. $\mathfrak{X}_\infty = \varprojlim \mathfrak{X}_n$, except for $X_\infty = \varprojlim A_n$. (The notation A_∞ is usually used to denote the injective limit of the groups A_n.)
10. $\Lambda := \mathbb{Z}_p[\![T]\!]$ the Iwasawa algebra.

In the proof of the main conjecture, we will need to relate the finite levels of these modules to the ∞-level. The reason for this is the general observation of Iwasawa theory that the ∞-level—which can be thought of as batching all finite levels together—behaves more nicely than the finite levels on their own. This can be traced back to having an additional tool on the ∞-level as compared to finite levels, namely the structure theorem of finitely generated Λ-modules.

Proposition 3.7.2. *In the category of Λ-modules, we have the following.*

(1) *$e_\chi X_\infty$ is finitely generated and torsion for all characters χ;*
(2) *$e_\chi \mathfrak{X}_\infty$ is finitely generated for all characters χ and torsion for $\chi \neq \mathbb{1}$ even;*
(3) *$e_\chi U_\infty$ is free of rank 1—in particular, it is finitely generated—for $\chi \neq \mathbb{1}$ even;*
(4) *$e_\chi \overline{C}_\infty$ is free of rank 1—in particular, it is finitely generated—for $\chi \neq \mathbb{1}$ even;*
(5) *$e_\chi U_\infty / e_\chi \overline{C}_\infty$ is torsion for $\chi \neq \mathbb{1}$ even;*
(6) *$e_\chi \overline{E}_\infty$ is finitely generated for all characters χ.*

Proof. We only give references to the proofs.

(1) Lemma 1.3.2
(2) Corollary 1.3.5 and Lemma 1.3.9
(3) [Lan90, Chapter 7, Theorem 2.1]

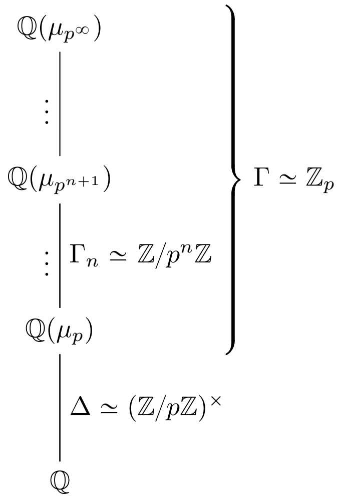
$\mathbb{Q}(\mu_{p^\infty})$
$\mathbb{Q}(\mu_{p^{n+1}})$
$\Gamma_n \simeq \mathbb{Z}/p^n\mathbb{Z}$
$\mathbb{Q}(\mu_p)$
$\Gamma \simeq \mathbb{Z}_p$
$\Delta \simeq (\mathbb{Z}/p\mathbb{Z})^\times$
$\mathbb{Q}$

Figure 3.5: The cyclotomic tower $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$

(4) [Lan90, Chapter 7, Theorem 5.1]
(5) [Lan90, Chapter 7, Theorem 5.2]
(6) $\Lambda = \mathbb{Z}_p[\![T]\!]$ is noetherian because $\mathbb{Z}_p$ is [Stacks, Tag 0306]. U_∞ is finitely generated over the noetherian ring Λ [Lan86, Chapter 7, Theorem 2.1], hence it is noetherian. Since submodules of noetherian modules are finitely generated, $\overline{E}_\infty$ is finitely generated. □

Definition 3.7.3. Let $\Gamma_n := \Gamma^{p^n} = \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^{n+1}}))$ and $\gamma \in \Gamma$ be a generator. For any Λ-module Y define the Γ_n-invariants resp. -coinvariants Y^{Γ_n} resp. Y_{Γ_n} by the exact sequence

$$0 \to Y^{\Gamma_n} \to Y \xrightarrow{\cdot(\gamma^{p^n}-1)} Y \to Y_{\Gamma_n} \to 0$$

In particular, $\Lambda_{\Gamma_n} = \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}(\mu_p))]$.

For $Y := Y_\infty \in \{X_\infty, U_\infty, \overline{E}_\infty, \overline{C}_\infty, \mathfrak{X}_\infty\}$ we obtain natural maps $(e_\chi Y_\infty)_{\Gamma_n} \to e_\chi Y_n$ which describe the relation between the ∞-level and the n^{th} level. The following Proposition 3.7.4 states that the situation is the best possible except for the module $\overline{E}_\infty$. As for $\overline{E}_\infty$, we will relate it to the more well-behaved modules in Lemma 3.7.6.

Proposition 3.7.4. *In the category of Λ-modules, we have the following.*

(1) $(e_\chi X_\infty)_{\Gamma_n} \to e_\chi A_n$ *is an isomorphism for all characters* χ*;*
(2) $(e_\chi \mathfrak{X}_\infty)_{\Gamma_n} \to e_\chi \mathfrak{X}_n$ *is an isomorphism for* $\chi \neq \mathbb{1}$ *even;*
(3) $(e_\chi \overline{U}_\infty)_{\Gamma_n} \to e_\chi \overline{U}_n$ *is an isomorphism for* $\chi \neq \mathbb{1}$*;*
(4) $(e_\chi \overline{C}_\infty)_{\Gamma_n} \to e_\chi \overline{C}_n$ *is an isomorphism for* $\chi \neq \mathbb{1}$ *even.*

Proof. Again we only give references to the proofs.

(1) Claim 1.2.11 (which can be applied since p ramifies totally in $\mathbb{Q}(\mu_p)/\mathbb{Q}$)
(2) Lemma 1.3.9
(3) [Lan90, Chapter 7, Theorem 2.2]
(4) [Lan90, Chapter 7, Theorem 5.1] □

Remark 3.7.5. Upon first glance, the diversity of conditions on χ in Propositions 3.7.2 and 3.7.4 may appear confusing. We will, in fact, only need these assertions for $\chi \neq \mathbb{1}$ even: for χ trivial, the main conjecture admits a simpler proof, discussed in Section 3.8.1.

Lemma 3.7.6. *For all $\chi \neq \mathbb{1}$ even, there is an ideal $\mathcal{A} \subseteq \Lambda$ of finite index such that for all $0 \leqslant n$:*

$$\mathcal{A}\operatorname{Ker}\left(\left(e_\chi\overline{E}_\infty\right)_{\Gamma_n} \to e_\chi\overline{E}_n\right) = 0, \quad \mathcal{A}\operatorname{Coker}\left(\left(e_\chi\overline{E}_\infty\right)_{\Gamma_n} \to e_\chi\overline{E}_n\right) = 0,$$

and the size of these kernels resp. cokernels is uniformly bounded.

Proof. First consider the following commutative diagram with exact sequences as its rows.

$$\begin{tikzcd}
 & \operatorname{Ker}\pi_{U/\overline{E},n} \arrow[dl, equal] \arrow[d] & & & \\
\operatorname{Ker}\varphi_n \arrow[r] & \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\Gamma_n} \arrow[r, "\varphi_n"] \arrow[d, "\pi_{U/\overline{E},n}"] \arrow[dr, phantom, "(\dagger)"] & \left(e_\chi\mathfrak{X}_\infty\right)_{\Gamma_n} \arrow[r] \arrow[d, "\simeq"] & \left(e_\chi X_\infty\right)_{\Gamma_n} \arrow[r] \arrow[d, "\simeq"] & 0 \\
0 \arrow[r] & e_\chi U_n/e_\chi\overline{E}_n \arrow[r] & e_\chi\mathfrak{X}_n \arrow[r] & e_\chi A_n \arrow[r] & 0
\end{tikzcd}$$

The first row is obtained by applying e_χ and $(-)_{\Gamma_n}$ to the short exact sequence

$$0 \to U_\infty/\overline{E}_\infty \to \mathfrak{X}_\infty \to X_\infty \to 0$$

which comes from Corollary 1.3.6. The vertical arrows are the natural ones, the ones in the middle resp. on the right being isos by Proposition 3.7.4.2 resp. Proposition 3.7.4.1.

Claim 3.7.7.

$$\operatorname{Ker}\varphi_n \simeq \left(e_\chi X_\infty\right)^{\Gamma_n} \Big/ \operatorname{Im}\left(\left(e_\chi\mathfrak{X}_\infty\right)^{\Gamma_n} \to \left(e_\chi X_\infty\right)^{\Gamma_n}\right)$$

Proof. Apply the snake lemma to the following diagram:

$$\begin{tikzcd}
 & \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)^{\Gamma_n} \arrow[r] \arrow[d] & \left(e_\chi\mathfrak{X}_\infty\right)^{\Gamma_n} \arrow[r] \arrow[d] & \left(e_\chi X_\infty\right)^{\Gamma_n} \arrow[r, dashed, dash] \arrow[d] & {} \\
0 \arrow[r] & e_\chi U_\infty/e_\chi\overline{E}_\infty \arrow[r] \arrow[d, "\gamma^{p^n}-1"] & e_\chi\mathfrak{X}_\infty \arrow[r] \arrow[d, "\gamma^{p^n}-1"] & e_\chi X_\infty \arrow[r] \arrow[d, "\gamma^{p^n}-1"] & 0 \\
0 \arrow[r] & e_\chi U_\infty/e_\chi\overline{E}_\infty \arrow[r] \arrow[d] & e_\chi\mathfrak{X}_\infty \arrow[r] \arrow[d] & e_\chi X_\infty \arrow[r] \arrow[d] & 0 \\
{} \arrow[r, dashed] & \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\Gamma_n} \arrow[r, "\varphi"] & \left(e_\chi\mathfrak{X}_\infty\right)_{\Gamma_n} \arrow[r] & \left(e_\chi X_\infty\right)_{\Gamma_n} &
\end{tikzcd}$$

Then it follows that

$$\begin{aligned}
\operatorname{Ker}\varphi_n &= \operatorname{Im}\left(\left(e_\chi X_\infty\right)^{\Gamma_n} \dashrightarrow \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\Gamma_n}\right) && \text{exactness at } \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\Gamma_n} \\
&\simeq \left(e_\chi X_\infty\right)^{\Gamma_n} / \operatorname{Ker}\left(\left(e_\chi X_\infty\right)^{\Gamma_n} \dashrightarrow \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\Gamma_n}\right) && 1^{\text{st}} \text{ isomorphism theorem} \\
&= \left(e_\chi X_\infty\right)^{\Gamma_n} / \operatorname{Im}\left(\left(e_\chi\mathfrak{X}_\infty\right)^{\Gamma_n} \to \left(e_\chi X_\infty\right)^{\Gamma_n}\right) && \text{exactness at } \left(e_\chi X_\infty\right)^{\Gamma_n}
\end{aligned}$$

This proves the claim. □

In particular, $\operatorname{Ker}\varphi_n$ is a quotient of $(e_\chi X_\infty)^{\Gamma_n}$. We know that $e_\chi X_\infty$ is finitely generated (Proposition 3.7.2.1). Since $(e_\chi X_\infty)_{\Gamma_n} \simeq e_\chi A_n$ (Proposition 3.7.4.1) and the latter is finite, so is $(e_\chi X_\infty)_{\Gamma_n}$. The exact sequence

$$0 \to (e_\chi X_\infty)^{\Gamma_n} \to e_\chi X_\infty \to e_\chi X_\infty \to (e_\chi X_\infty)_{\Gamma_n} \to 0$$

gives rise to a pseudo-isomorphism $e_\chi X_\infty / (e_\chi X_\infty)^{\Gamma_n} \sim e_\chi X_\infty$. Thus $(e_\chi X_\infty)^{\Gamma_n}$ must be finite as well, as the contrary would violate the structure theorem of finitely generated Λ-modules (Theorem 1.1.8). This gives a uniform bound on $\#\operatorname{Ker}\varphi_n$ as it is a quotient of the maximal finite Λ-submodule of $e_\chi X_\infty$, denoted $(e_\chi X_\infty)_{\text{fin}}$. In the square (†), the bottom and right arrows are monos, thus $\operatorname{Ker}\varphi_n = \operatorname{Ker}\pi_{U/\overline{E},n}$, so $\#\operatorname{Ker}\pi_{U/\overline{E},n}$ is also uniformly bounded.

Now consider another commutative diagram.

$$\begin{tikzcd}
 & \operatorname{Ker}\pi_{\overline{E},n} \arrow[d] & 0 \arrow[r] \arrow[d] & \operatorname{Ker}\pi_{U/\overline{E},n} \arrow[d] \arrow[dddll, dashed] & \\
\operatorname{Ker}\rho_n \arrow[r] \arrow[ur, equal] & \left(e_\chi\overline{E}_\infty\right)_{\Gamma_n} \arrow[r, "\rho_n"] \arrow[d, "\pi_{\overline{E},n}"] \arrow[dr, phantom, "(\ddagger)"] & (e_\chi U_\infty)_{\Gamma_n} \arrow[r] \arrow[d, "\simeq"] & \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\Gamma_n} \arrow[r] \arrow[d, "\pi_{U/\overline{E},n}"] & 0 \\
0 \arrow[r] & e_\chi\overline{E}_n \arrow[r] \arrow[d] & e_\chi U_n \arrow[r] \arrow[d] & e_\chi U_n/e_\chi\overline{E}_n \arrow[r] & 0 \\
 & \operatorname{Coker}\pi_{\overline{E},n} \arrow[r] & 0 & &
\end{tikzcd}$$

The diagram is induced by the short exact sequence

$$0 \to e_\chi\overline{E}_\infty \to e_\chi U_\infty \to e_\chi U_\infty/e_\chi\overline{E}_\infty \to 0$$

and it has exact sequences as its rows. The dashed arrow comes from the snake lemma and it yields $\operatorname{Ker}\pi_{U/\overline{E},n} \simeq \operatorname{Coker}\pi_{\overline{E},n}$, hence $\#\operatorname{Coker}\pi_{\overline{E},n}$ is also uniformly bounded.

By looking at the square (‡), we deduce $\operatorname{Ker}\rho_n = \operatorname{Ker}\pi_{\overline{E},n}$. Again by the snake lemma as in Claim 3.7.7, we have

$$\operatorname{Ker}\rho_n = \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)^{\Gamma_n} \Big/ \operatorname{Im}\left((e_\chi U_\infty)^{\Gamma_n} \to \left(e_\chi\overline{E}_\infty\right)^{\Gamma_n}\right)$$

The module $\left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\Gamma_n}$ is finite: its size is uniformly bounded by the product

$$\#\left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right) \cdot \#\operatorname{Ker}\pi_{U/\overline{E},n}$$

Here the first factor is finite by Proposition 3.7.2 and the second is uniformly bounded. Invoking the structure theorem of finitely generated Λ-modules (Theorem 1.1.8) as before, we deduce that $\operatorname{Ker}\rho_n$ is a quotient of $\left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\text{fin}}$ and hence $\#\operatorname{Ker}\rho_n = \#\operatorname{Ker}\pi_{\overline{E},n}$ is uniformly bounded. (In fact, one can show $\operatorname{Ker}\rho_n = 0$: this follows from $\left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\text{fin}} = 0$. The latter is a consequence of Lemma 8.7 in [Rub90], which asserts that $e_\chi\mathfrak{X}_\infty$ has no nontrivial finite submodules. The proof uses the Iwasawa main conjecture.)

It also follows that

$$\mathcal{A} := \operatorname{Ann}_\Lambda\left((e_\chi X_\infty)_{\text{fin}} \oplus \left(e_\chi U_\infty/e_\chi\overline{E}_\infty\right)_{\text{fin}}\right) \subseteq \Lambda$$

annihilates the kernel and cokernel of $\pi_{\overline{E}}$. It only remains to check that is is of finite index. Both direct summands above are finite by definition and torsion by Proposition 3.7.2, thus we may use the following lemma.

Lemma 3.7.8. *The annihilator of a finite torsion Λ-module Y is of finite index in $\Lambda = \mathbb{Z}_p[\![T]\!]$.*

Proof. We claim that for k sufficiently large, $(p,T)^k Y = 0$, thus $\operatorname{Ann}_\Lambda Y \subseteq (p,T)^k$, which will prove the lemma.

Let $y \in Y$ and $f \in (p,T)$. Since Y is finite, there exist $0 < i < j$ for which $f^i y \neq f^j y$. Thus $(1 - f^{j-i}) f^i y = 0$, but $(1 - f^{j-i})$ is a unit because f is in the maximal ideal (p,T). Therefore $f^i y = 0$. Doing this for $f := p$ and $f := T$, we obtain $p^i y = T^i y = 0$ for some i, thus $(p,T)^{2i} \subseteq (p^i, T^i)$ annihilates y. Since Y is finite we may repeat this for all y and obtain some k for which $(p,T)^k Y = 0$. □

This finishes the proof of Lemma 3.7.6. □

Now that we have all this information (Propositions 3.7.2 and 3.7.4 and Lemma 3.7.6), we can start working towards the Iwasawa main conjecture. These first steps will be done in Lemmata 3.7.9 and 3.7.10 and summarised in Corollary 3.7.11. See Remark 3.7.12 for an explanation of the role these statements play in the proof. Both lemmata are proven by using the structure theorem and some previously discussed properties of the Iwasawa modules in question.

For each character χ fix a generator h_χ of $\operatorname{Char}\left(e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty\right) \subseteq \Lambda$ (recall that characteristic ideals are principal by definition).

Lemma 3.7.9. *Let $\chi \neq \mathbb{1}$ be even and $\mathcal{A} \subseteq \Lambda$ as in Lemma 3.7.6. Then for all $\eta \in \mathcal{A}$ and $0 \leqslant n$ there is a $\vartheta_{n,\eta} : e_\chi \overline{E}_n \to \Lambda_{\Gamma_n}$ for which $\vartheta_{n,\eta}(e_\chi \overline{C}_n) = \eta h_\chi \Lambda_{\Gamma_n}$.*

Proof. $e_\chi E_\infty$ is a nonzero submodule of $e_\chi U_\infty$ which is free of rank 1 over Λ (Proposition 3.7.2), therefore $e_\chi E_\infty$ is torsion free of rank 1. By the structure theorem of finitely generated Λ-modules (Theorem 1.1.8), we obtain an injective pseudo-isomorphism $\vartheta : e_\chi \overline{E}_\infty \to \Lambda$ (injectivity comes from torsion freeness) with finite cokernel. Quotienting out by $e_\chi \overline{C}_\infty$, we obtain a pseudo-isomorphism

$$e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty \to \Lambda / e_\chi \overline{C}_\infty$$

Therefore

$$\begin{aligned}
\vartheta\left(e_\chi \overline{C}_\infty\right) &= \operatorname{Char}\left(\Lambda / \vartheta\left(e_\chi \overline{C}_\infty\right)\right) && \text{definition of Char, } e_\chi \overline{C}_\infty \text{ is free of rank 1} \\
&= \operatorname{Char}\left(e_\chi \overline{E}_\infty / e_\chi \overline{C}_\infty\right) && \text{pseudo-isomorphism preserves Char} \\
&= h_\chi \Lambda && \text{definition of } h_\chi
\end{aligned} \tag{3.19}$$

For $0 < n$ let

$$\vartheta_n := (-)_{\Gamma_n} \circ \vartheta : \left(e_\chi \overline{E}_\infty\right)_{\Gamma_n} \to \Lambda_{\Gamma_n}$$

and $\pi_{\overline{E},n} : \left(e_\chi \overline{E}_\infty\right)_{\Gamma_n} \to e_\chi \overline{E}_n$ be the same as in Lemma 3.7.6. For $\eta \in \mathcal{A}$ define

$$\begin{aligned}
\vartheta_{n,\eta} : e_\chi \overline{E}_n &\to \Lambda_{\Gamma_n} \\
u &\mapsto \vartheta_n(\pi_{\overline{E},n}^{-1}(\eta u))
\end{aligned}$$

This $\vartheta_{n,\eta}$ is well-defined: since $\eta \operatorname{Coker} \pi_{\overline{E},n} = 0$, the equation $\eta u = \pi_{\overline{E},n}(v)$ can be solved for each u. The value $\vartheta_{n,\eta}(u)$ does not depend on the choice of v because $\operatorname{Ker} \pi_{\overline{E},n} \subseteq \operatorname{Ker} \vartheta_n$. This is because since Λ_{Γ_n} has no $\mathbb{Z}_p$-torsion, ϑ_n kills all finite submodules of $e_\chi \overline{E}_\infty$, and $\operatorname{Ker} \pi_{\overline{E},n}$ is one of these by Lemma 3.7.6.

Now we may conclude the proof:

$$\begin{aligned} \vartheta_{n,\eta}\left(e_\chi \overline{C}_n\right) &= \eta \vartheta_n \left(e_\chi \overline{C}_\infty\right) && e_\chi \overline{C}_n = \pi_{\overline{E},n}\left(e_\chi \overline{C}_\infty\right) \text{ by definition} \\ &= \eta h_\chi \Lambda_{\Gamma_n} && \text{definition of } \vartheta_n \text{ and (3.19)} \end{aligned}$$

□

Lemma 3.7.10. *Suppose $e_\chi X_\infty \sim \bigoplus_{i=1}^k \Lambda/f_i\Lambda$ where the f_i are irreducible (cf. Theorem 1.1.8 and Proposition 3.7.2.1). Then there exists an ideal $\mathcal{B} \subseteq \Lambda$ of finite index and*

$$\forall n > 0 : \exists c_1, \ldots, c_k \in e_\chi A_n : \forall i = 1, \ldots, k : \mathcal{B} \operatorname{Ann}_{e_\chi A_n/(c_1\Lambda_{\Gamma_n} + \ldots + c_{i-1}\Lambda_{\Gamma_n})}(c_i) \subseteq f_i \Lambda_{\Gamma_n}$$

Proof. Since $e_\chi X_\infty$ is torsion (Proposition 3.7.2.1), the pseudo-isomorphism relation is symmetric (Lemma 1.1.10), that is, there is an exact sequence

$$0 \to Y \to \bigoplus_{i=1}^k \Lambda/f_i\Lambda \to e_\chi X_\infty \to Z \to 0$$

where Y and Z are finite. Even better, we have $Y = 0$: Y is finite and a direct sum of submodules of $\Lambda/f_i\Lambda$, but since f_i is irreducible, the submodules are only the trivial ones, and $\Lambda/f_i\Lambda$ itself is infinite (proven in Example 1.1.9), therefore Y must be the direct sum of zero modules.

Tensoring with Λ_{Γ_n} is right exact, $e_\chi X_\infty$ becomes $e_\chi A_n$ (Proposition 3.7.4.1). Apply the snake lemma:

$$\begin{tikzcd}
 & & & Z^{\Gamma_n} \arrow[d] \arrow[dddll, dashed] & \\
0 \arrow[r] & \bigoplus_{i=1}^k \Lambda/f_i\Lambda \arrow[r] \arrow[d, "\gamma^{p^n}-1"] & e_\chi X_\infty \arrow[r] \arrow[d, "\gamma^{p^n}-1"] & Z \arrow[r] \arrow[d, "\gamma^{p^n}-1"] & 0 \\
0 \arrow[r] & \bigoplus_{i=1}^k \Lambda/f_i\Lambda \arrow[r] \arrow[d] & e_\chi X_\infty \arrow[r] \arrow[d] & Z \arrow[r] \arrow[d] & 0 \\
 & \bigoplus_{i=1}^k \Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n} \arrow[r] & e_\chi A_n \arrow[r] & Z_{\Gamma_n} \arrow[r] & 0
\end{tikzcd}$$

Thus we have the following exact sequence:

$$Z^{\Gamma_n} \to \bigoplus_{i=1}^k \Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n} \to e_\chi A_n \to Z_{\Gamma_n} \to 0$$

Set $\mathcal{B} := \operatorname{Ann}_\Lambda(Z)$ and $c_i := \operatorname{Im}\left(\Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n} \to e_\chi A_n\right)$. Since Z is finite and torsion, $\mathcal{B}$ is of finite index by Lemma 3.7.8. □

Combining Lemmata 3.7.9 and 3.7.10 by setting $\mathcal{C} := \mathcal{A} \cap \mathcal{B}$, we obtain the following.

Corollary 3.7.11 (First conversion step)**.** *Let $\chi \neq \mathbb{1}$ be even. Then there exists an ideal $\mathcal{C} \subseteq \Lambda$ of finite index such that*

1. *$\forall \eta \in \mathcal{C}\ \forall n \geqslant 0\ \exists \vartheta_{n,\eta} : e_\chi \overline{E}_n \to \Lambda_{\Gamma_n}$ such that $\vartheta_{n,\eta}(e_\chi \overline{C}_n) = \eta h_\chi \Lambda_{\Gamma_n}$;*

2. $\forall n > 0\ \exists c_1, \dots, c_k \in e_\chi A_n : \mathcal{C}\,\mathrm{Ann}_{e_\chi A_n/(c_1\Lambda_{\Gamma_n}+\ldots+c_{i-1}\Lambda_{\Gamma_n})}(c_i) \subseteq f_i\Lambda_{\Gamma_n}$. □

Remark 3.7.12. The main conjecture concerns the generators h_χ resp. $f_\chi = \prod_i f_i$ of the characteristic ideals of $e_\chi\overline{E}_\infty/e_\chi\overline{C}_\infty$ resp. $e_\chi X_\infty$. What Corollary 3.7.11 does is bringing these two closer to one another. Lemma 3.7.10 lets the factors f_i of f_χ be represented by ideal classes c_i. Lemma 3.7.9 will, on the other hand, provide a map $\vartheta_{n,\eta}$. Note that in both cases, the proof used the structure theorem of finitely generated Λ-modules in an essential way.

So the first conversion step gives us objects on finite levels, thus allowing for more flexible algebraic machinery to be used. Namely, the second conversion step Proposition 3.6.1 will provide us with ideals λ_i representing both c_i and a morphism ψ which will arise from $\vartheta_{n,\eta}$. This will ultimately lead to establishing a connection between f_χ and h_χ.

Definition 3.7.13. For two sequences of positive numbers (a_n) and (b_n) we will write $a_n \sim_\Theta b_n$ and call the two sequences Big Theta-equivalent if a_n/b_n is uniformly bounded (from above and below). (We deviate from the standard notation $a_n = \Theta(b_n)$ here for the sake of convenience.)

Lemma 3.7.14. *For every even character $\chi \neq \mathbb{1}$ we have the following:*

(1) For every $n > 0$ the quotients $\Lambda_{\Gamma_n}/f_\chi\Lambda_{\Gamma_n}$ and $\Lambda_{\Gamma_n}/h_\chi\Lambda_{\Gamma_n}$ are finite.

(2) We have

$$\#e_\chi A_n \underset{\Theta}{\sim} \#\Lambda_{\Gamma_n}/f_\chi\Lambda_{\Gamma_n}, \quad \#e_\chi\overline{E}_n/e_\chi\overline{C}_n \underset{\Theta}{\sim} \#\Lambda_{\Gamma_n}/h_\chi\Lambda_{\Gamma_n}$$

Proof. Tensoring the pseudo-isomorphism

$$e_\chi X_\infty \to \bigoplus_{i=1}^k \Lambda/f_i\Lambda$$

with Λ_{Γ_n} we obtain a morphism

$$e_\chi A_n \simeq (e_\chi X_\infty)_{\Gamma_n} \to \bigoplus_{i=1}^k \Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n}$$

Since the kernel and cokernel of the original pseudo-isomorphism were finite, so are the ones of the tensored morphism, and their sizes are uniformly bounded. Therefore $\Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n}$ is finite for all n and i since the direct sum of these form the codomain of a morphism with finite domain, kernel and cokernel.

Write $f_\chi = \prod_j f_j^{a_j}$ where $a_j \geqslant 1$ and the f_j's are distinct. Then the Chinese remainder theorem states that

$$\Lambda_{\Gamma_n}/f_\chi\Lambda_{\Gamma_n} \simeq \bigoplus_j \Lambda_{\Gamma_n}/f_j^{a_j}\Lambda_{\Gamma_n}$$

Therefore

$$\begin{aligned}
\#\left(\Lambda_{\Gamma_n}/f_\chi\Lambda_{\Gamma_n}\right) &= \prod_j \#\left(\Lambda_{\Gamma_n}/f_j^{a_j}\Lambda_{\Gamma_n}\right) \\
&= \prod_j \left(\#\left(\Lambda_{\Gamma_n}/f_j\Lambda_{\Gamma_n}\right)\right)^{a_j} && \Lambda_{\Gamma_n} \text{ has no } \mathbb{Z}_p\text{-torsion} \\
&= \prod_{i=1}^k \#\left(\Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n}\right) \\
&= \#\left(\bigoplus_{i=1}^k \Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n}\right)
\end{aligned}$$

In summary, we have

$$\#e_\chi A_n = \#\left(e_\chi X_\infty\right)_{\Gamma_n} \underset{\Theta}{\sim} \#\left(\bigoplus_{i=1}^{k} \Lambda_{\Gamma_n}/f_i\Lambda_{\Gamma_n}\right) = \#\left(\Lambda_{\Gamma_n}/f_\chi\Lambda_{\Gamma_n}\right) \tag{3.20}$$

This proves the first assertions of (1) and (2).

Write $h_\chi = \prod_{i'} h_{i'}$ for the decomposition of h_χ into irreducible factors. Then as above we have a pseudo-isomorphism

$$e_\chi\overline{E}_\infty/e_\chi\overline{C}_\infty \to \bigoplus_{i'} \Lambda/h_{i'}\Lambda$$

and we obtain pseudo-isomorphisms with uniformly bounded kernels and cokernels

$$\left(e_\chi\overline{E}_\infty/e_\chi\overline{C}_\infty\right)_{\Gamma_n} \to \bigoplus_{i'} \Lambda_{\Gamma_n}/h_{i'}\Lambda_{\Gamma_n} \tag{3.21}$$

but here we don't have isomorphisms as we did for the p-part of the class group, just morphisms

$$\left(e_\chi\overline{E}_\infty/e_\chi\overline{C}_\infty\right)_{\Gamma_n} \to e_\chi\overline{E}_n/e_\chi\overline{C}_n \tag{3.22}$$

with uniformly bounded kernels and cokernels (Lemma 3.7.6). As before, we have that each $\Lambda_{\Gamma_n}/h_{i'}\Lambda_{\Gamma_n}$ is finite, and

$$\#\left(e_\chi\overline{E}_n/e_\chi\overline{C}_n\right) \underset{\Theta}{\sim} \#\left(e_\chi\overline{E}_\infty/e_\chi\overline{C}_\infty\right)_{\Gamma_n} \underset{\Theta}{\sim} \#\left(\bigoplus_{i'} \Lambda_{\Gamma_n}/h_{i'}\Lambda_{\Gamma_n}\right) = \#\left(\Lambda_{\Gamma_n}/h_\chi\Lambda_{\Gamma_n}\right) \tag{3.23}$$

proving the second halves of (1) and (2). □

Remark 3.7.15. Instead of the Chinese remainder theorem, we could also have used Iwasawa's theorem on the growth of Γ_n-coinvariants (Theorem 1.2.14). That way, the last equalities of (3.20) and (3.23) would only have been Big Theta-equivalences.

3.8 The end of the proof

Recall that $e_\chi X_\infty \sim \bigoplus_{i=1}^{k} \Lambda/f_i\Lambda$, the characteristic polynomial of $e_\chi X_\infty$ is $f_\chi = f_1 \cdots f_k$, and h_χ is the characteristic polynomial of $e_\chi\overline{E}_\infty/e_\chi\overline{C}_\infty$. We wish to prove Theorem 3.1.4, which states that $f_\chi\Lambda = h_\chi\Lambda$ for all even characters χ of Δ.

The proof will use the machinery developed in the previous sections, namely Propositions 3.6.1 and 3.5.13, Corollary 3.7.11, and Lemma 3.7.14. The heart of the proof will be the following:

Lemma 3.8.1. *For all even characters χ of Δ, $f_\chi \mid h_\chi$.*

We postpone the proof of Lemma 3.8.1 and use it to prove the main conjecture after making just one more observation:

Lemma 3.8.2. *Let $g_1, g_2 \in \Lambda$ such that $g_1 \mid g_2$ and*

$$\#\left(\Lambda/g_1\Lambda\right)_{\Gamma_n} \underset{\Theta}{\sim} \#\left(\Lambda/g_2\Lambda\right)_{\Gamma_n}$$

Then $g_1\Lambda = g_2\Lambda$.

Proof. This follows from Theorem 1.2.14. □

Proof (Proof of the main conjecture). Let $f := \prod_{\chi \text{ even}} f_\chi$ and $h := \prod_{\chi \text{ even}} h_\chi$; then the above Lemma 3.8.1 implies $f \mid h$. We now verify the condition of Lemma 3.8.2 for $g_1 := f$ and $g_2 := h$.

$$\begin{aligned}
\#\left(\Lambda/f\Lambda\right)_{\Gamma_n} &\underset{\Theta}{\sim} \prod_{\chi \text{ even}} \#\left(\Lambda/f_\chi\Lambda\right)_{\Gamma_n} && \\
&\underset{\Theta}{\sim} \prod_{\chi \text{ even}} \#\left(e_\chi A_n\right) && \text{Lemma 3.7.14.2} \\
&= \#A_n^+ && \text{orthogonality of idempotents}
\end{aligned}$$

$$\begin{aligned}
\#\left(\Lambda/h\Lambda\right)_{\Gamma_n} &\underset{\Theta}{\sim} \prod_{\chi \text{ even}} \#\left(\Lambda/h_\chi\Lambda\right)_{\Gamma_n} && \\
&\underset{\Theta}{\sim} \prod_{\chi \text{ even}} \left(e_\chi \overline{E}_n : e_\chi \overline{C}_n\right) && \text{Lemma 3.7.14.2} \\
&= \left(\overline{E}_n^+ : \overline{C}_n^+\right) && \text{orthogonality of idempotents}
\end{aligned}$$

Here $\overline{E}_n^+$ resp. $\overline{C}_n^+$ are as before the closures of $E_n^+ \cap U_n$ resp. $C_n^+ \cap U_n$ in U_n. The analytic class number formula [Lan90, Chapter 3, Theorem 5.1] states the following:

$$\#\operatorname{Cl}\mathbb{Q}(\mu_{p^{n+1}})^+ = (E_n^+ : C_n^+) \tag{3.24}$$

Claim 3.8.3. *The p-parts of* $(E_n^+ : C_n^+)$ *and* $(E_n^+ \cap U_n : C_n^+ \cap U_n)$ *agree.*

Proof. For every $x \in E_n^+$ we have that $x^{\mathrm{N}(1-\zeta_{p^{n+1}})-1}$ is in U_n where N denotes the absolute norm. (Recall that p ramifies totally in $\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}$ with $(1-\zeta_{p^{n+1}})$ being the only prime above p.) Therefore the index $(E_n^+ : E_n^+ \cap U_n)$ is finite and divides $\mathrm{N}(1-\zeta_{p^{n+1}})-1 = \Phi_{p^{n+1}}(1)-1 = p-1$ where $\Phi_{p^{n+1}}$ is the cyclotomic polynomial. In particular, we have that $(E_n^+ : E_n^+ \cap U_n)$ is prime to p. Similarly $p \nmid (C_n^+ : C_n^+ \cap U_n)$. Write $(E_n^+ : C_n^+ \cap U_n)$ in two ways:

$$\underbrace{(E_n^+ : E_n^+ \cap U_n)}_{p\nmid}(E_n^+ \cap U_n : C_n^+ \cap U_n) = (E_n^+ : C_n^+ \cap U_n) = (E_n^+ : C_n^+)\underbrace{(C_n^+ : C_n^+ \cap U_n)}_{p\nmid}$$

The assertion follows. (We could also have argued as in the proof of Theorem 1.3.4.) □

Leopoldt's conjecture $\operatorname{rk}_{\mathbb{Z}_p} \overline{E}_n^+ = \operatorname{rk}_{\mathbb{Z}}(E_n^+ \cap U_n)$ holds for real cyclotomic fields [Was97, p. 75], and it implies that $(E_n^+ \cap U_n) \otimes \mathbb{Z}_p = \overline{E}_n^+$ and $(C_n^+ \cap U_n) \otimes \mathbb{Z}_p = \overline{C}_n^+$.

Using this and Claim 3.8.3 we get that by tensoring by $\mathbb{Z}_p$ in (3.24) we obtain $\#A_n^+ = \left(\overline{E}_n^+ : \overline{C}_n^+\right)$. Therefore Lemma 3.8.2 can be applied, and we get $f = h$. Using Lemma 3.8.1 again we conclude that $f_\chi\Lambda = h_\chi\Lambda$ for all even characters χ. □

We now prove Lemma 3.8.1.

3.8.1 Proof of $f_\chi \mid h_\chi$ for $\chi = \mathbb{1}$

First assume $\chi = \mathbb{1}$. We will show that both $f_{\mathbb{1}}$ and $h_{\mathbb{1}}$ are units. (The main conjecture for $\chi = \mathbb{1}$ follows immediately, i.e. without using Lemma 3.8.1, from this.) Recall that $\Delta = \operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

Then

$$e_{\mathbb{1}} A_n = A_n^{\Delta} = \mathrm{Cl}\left(\mathbb{Q}(\mu_{p^{n+1}})^{\Delta}\right) \otimes_{\mathbb{Z}} \mathbb{Z}_p$$

In particular, for $n = 0$ we have $e_{\mathbb{1}} A_0 = (\mathrm{Cl}\,\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_p = 0$. Using (the proof of) Lemma 1.3.3 we conclude $e_{\mathbb{1}} X_\infty = 0$, and thus $f_{\mathbb{1}} = 1$.

We have $e_{\mathbb{1}} \overline{E}_n = \overline{E}_n^{\Delta}$ and $e_{\mathbb{1}} \overline{C}_n = \overline{C}_n^{\Delta}$. The analytic class number formula (3.24) is also true for the field $\mathbb{Q}(\mu_{p^{n+1}})^{\Delta}$. (This is clear from the proof given in [Lan90, Chapter 3, Theorem 5.1].) Therefore we have

$$\#\,\mathrm{Cl}\left(\mathbb{Q}(\mu_{p^{n+1}})^{\Delta}\right) = \left(E_n^{\Delta} : C_n^{\Delta}\right)$$

Upon tensoring by $\mathbb{Z}_p$, the right hand side becomes the p-part of $\mathrm{Cl}\left(\mathbb{Q}(\mu_{p^{n+1}})^{\Delta}\right)$ and on the left hand side we get the index of local units $\left(\overline{E}_n^{\Delta} : \overline{C}_n^{\Delta}\right)$. As before, tensoring by $\mathbb{Z}_p$ is valid here since the p-adic regulator does not vanish by Leopoldt's conjecture. The p-part of the class group is trivial, hence so is $\overline{E}_n^{\Delta}/\overline{C}_n^{\Delta}$ for all n. It follows that the characteristic ideal of $\overline{E}_\infty^{\Delta}/\overline{C}_\infty^{\Delta}$ is Λ, that is, h_χ is a unit. □

3.8.2 Proof of $f_\chi \mid h_\chi$ for $\chi \neq \mathbb{1}$

Now suppose $\chi \neq \mathbb{1}$. Let n be fixed for now. Let $\mathcal{C}$ and $c_1, \dots, c_k$ be as in Corollary 3.7.11, and choose $c_{k+1} \in e_\chi A_n$ arbitrarily. The reason behind this seemingly odd step is that we will be doing an inductive process, the i^{th} step of which will give us information about $f_1 \cdots f_{i-1}$ (see (3.29)). Since we are interested in $f_\chi = f_1 \cdots f_k$, the induction will need to go on for $k+1$ steps.

Let $\eta \in \mathcal{C}$ be such that

$$\text{for all } j,\ \Lambda_{\Gamma_j}/\eta\Lambda_{\Gamma_j} \text{ is finite} \tag{3.25}$$

Below we will give some possible choices for η, so we need not worry about existence here. It is now finally time to choose M_n. Choose $t \in \mathbb{N}$ such that

$$p^t \geqslant \#\Lambda_{\Gamma_n}/\eta\Lambda_{\Gamma_n} \text{ and } p^t \geqslant \#\Lambda_{\Gamma_n}/h_\chi\Lambda_{\Gamma_n} \tag{3.26}$$

Such a t exists: the first inequality can be satisfied due to our assumption on η and so can the second one by Lemma 3.7.14.1. Set $M_n := \#(e_\chi A_n) \cdot p^{n+(k+1)t}$.

Since $e_\chi \overline{C}_n$ is generated by $e_\chi \alpha_1$ (see Proposition 3.5.4), we may assume that $\vartheta_{n,\eta}$ is normalised such that

$$\vartheta_{n,\eta}(e_\chi \alpha_1) = \eta h_\chi \tag{3.27}$$

Recall that

$$\Lambda_{\Gamma_n} = \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}(\mu_p))], \quad G_n = \mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})^+/\mathbb{Q}),$$

and χ is an even character of $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. It follows that $e_\chi \mathbb{Z}_p[G_n] = e_\chi \Lambda_{\Gamma_n}$. Thus while by definition, $\overline{\mathrm{ord}}$ resp. $\overline{\mathrm{ind}}$ map to the group rings $\mathbb{Z}[G_n]$ resp. $(\mathbb{Z}/M_n\mathbb{Z})[G_n]$, we may consider $\overline{\mathrm{ord}}_{\lambda_{i-1}}(e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}})$ and $\overline{\mathrm{ind}}_{\lambda_{i-1}}(e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}})$ as elements of $\Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n}$. We shall do this from now on without further comment.

For all $i = 1, \dots, k+1$ we will construct $\lambda_i \in c_i$ such that for all $i = 1, \dots, k+1$,

$$\ell_i := (\lambda_i \cap \mathbb{Z}) \equiv 1 \bmod M_n \tag{3.28}$$

$$\overline{\mathrm{ind}}_{\lambda_i}\left(e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}\right) f_1 \cdots f_{i-1} \,\middle|\, e_\chi \eta^i h_\chi \ \text{ in } e_\chi\left(\Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n}\right) \tag{3.29}$$

where for $i = 1$, the empty products in (3.29) are understood to be 1. The construction of these λ_i's will be done by finite induction using the second conversion step Proposition 3.6.1.

Of the two properties of λ_i above, it is (3.29) that is actually important to the proof; (3.28) is just a technical necessity, asserting that it is valid to consider the Kolyvagin derivative $\kappa_{\ell_1 \cdots \ell_{i-1}}$.

Before doing the induction, we show that Lemma 3.8.1 already follows from (3.29). Indeed, consider the equation for $i = k+1$. We get

$$\overline{\operatorname{ind}}_{\lambda_{k+1}}\left(e_\chi \kappa_{\ell_1 \cdots \ell_k}\right) \underbrace{f_1 \cdots f_k}_{f_\chi} \,\Big|\, e_\chi \eta^{k+1} h_\chi \quad \text{in } e_\chi \left(\Lambda_{\Gamma_n}/M_n \Lambda_{\Gamma_n}\right)$$

It follows that $f_\chi \mid \eta^{k+1} h_\chi$ in $\Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n}$ and therefore in $\Lambda_{\Gamma_n}/p^n\Lambda_{\Gamma_n}$. Up until now n was fixed; now let it run through all of $\mathbb{N}$. We obtain that $f_\chi \mid \eta^{k+1}h_\chi$ holds in Λ. All that's left to do is to remove the η-factor. To do this, let $j \in \mathbb{N}$ be large enough so that $T^j \in \mathcal{C}$ and $p^j \in \mathcal{C}$—this is possible since $\mathcal{C}$ is of finite index in $\Lambda = \mathbb{Z}_p[\![T]\!]$—and set $\eta_1 := T^j - p^{2j}$ and $\eta_2 := T^j - p^{3j}$. These satisfy the condition (3.25). Moreover they are coprime to each other and to $(1+T)^{p^m} - 1$ (quotienting out by this polynomial is the same as taking $(-)_{\Gamma_n}$). Since Λ is a UFD (Corollary 1.1.4), it follows from $f_\chi \mid \eta_1^{k+1}h_\chi$ and $f_\chi \mid \eta_2^{k+1}h_\chi$ that

$$f_\chi \,\big|\, \left(\eta_1^{k+1}h_\chi, \eta_2^{k+1}h_\chi\right) = h_\chi$$

holds in Λ, proving Lemma 3.8.1. (Another way to get rid of the η-factor is choosing $\eta := p^j$. Then the Ferrero–Washington theorem mentioned in Remark 1.2.3 asserts that $p \nmid f_\chi$, implying $f_\chi \mid h_\chi$.)

Now we return to constructing the λ_i's. We will be using Proposition 3.6.1 a total of $k+1$ times for $F_n := \mathbb{Q}(\mu_{p^{n+1}})^+$; in each step we need to specify an ideal class c, a finite G_n-submodule W of $F_n^\times/(F_n^\times)^{M_n}$, and a Galois-equivariant map $\psi : W \to (\mathbb{Z}/M_n\mathbb{Z})[G_n]$, where $G_n = \operatorname{Gal}(F_n/\mathbb{Q})$. In the i^{th} step we will set $c := c_i$; it immediately follows that the λ_i obtained will belong to c_i and satisfy (3.28). The choices for W and ψ and the verification of (3.29) are more complicated and will take up the rest of the proof. As we previously have pointed out, h_χ already appears in (3.29) for $i = 1$; this will be reflected in the difference between the definitions of ψ for $i = 1$ and $i \geqslant 2$.

The base case $i = 1$

First note that we have a map

$$\bar{\psi} : \Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n} \xrightarrow{e_\chi} e_\chi\left(\Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n}\right) \to (\mathbb{Z}/M_n\mathbb{Z})[G_n]$$

Here the second arrow is the natural map arising from the facts that there is an isomorphism $\Lambda_{\Gamma_n} \simeq \mathbb{Z}_p[\operatorname{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}(\mu_p))]$, M_n is a power of p, $G_n = \operatorname{Gal}(\mathbb{Q}(\mu_{p^{n+1}})^+/\mathbb{Q})$, and χ is an even character of $\Delta = \operatorname{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$.

For $i = 1$, let $W := e_\chi\left(\overline{E}_n/\overline{E}_n^{M_n}\right)$ and

$$\psi : W = e_\chi\left(\overline{E}_n/\overline{E}_n^{M_n}\right) \xrightarrow{\vartheta_{n,\eta} \bmod M_n} \Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n} \xrightarrow{\bar{\psi}} (\mathbb{Z}/M_n\mathbb{Z})[G_n] \tag{3.30}$$

Recall Proposition 3.5.8 with $r = 1$: κ_1 agrees with $\mathrm{D}_1\alpha_1 = \alpha_1$ modulo M_n^{th} powers. Therefore $\vartheta_{n,\eta}(e_\chi\kappa_1) = \vartheta_{n,\eta}(e_\chi\alpha_1) = \eta h_\chi$ by our assumption (3.27) on η. Thus (3.29) follows from (3.6.1.4):

$$\overline{\operatorname{ind}}_{\lambda_1}(e_\chi\kappa_1) \,\Big|\, \psi(e_\chi\kappa_1) = e_\chi\vartheta_{n,\eta} = e_\chi\eta h_\chi$$

The cases $2 \leqslant i \leqslant k+1$

Now let $2 \leqslant i \leqslant k+1$ and assume that $\lambda_1, \dots, \lambda_{i-1}$ have already been chosen. Let

$$W := (\Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n})\, e_\chi \kappa_{\ell_1\cdots\ell_{i-1}} \subseteq F_n^\times/(F_n^\times)^{M_n}$$

Thus W is the modulo M_n reduction of the subgroup of $F_n^\times$ generated by Galois conjugates of $e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}$; in particular, it is indeed a finite G_n-submodule.

With this in mind, define the map $\psi : W \to (\mathbb{Z}/M_n\mathbb{Z})[G_n]$ by $\psi := \bar{\psi} \circ \hat{\psi}$ where

$$\begin{aligned} \hat{\psi} : W = (\Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n})\, e_\chi\kappa_{\ell_1\cdots\ell_{i-1}} &\to \Lambda_{\Gamma_n}/M_n\Lambda_{\Gamma_n} \\ \rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}} &\mapsto \rho\frac{\eta\,\overline{\mathrm{ord}}_{\lambda_{i-1}}\left(e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}\right)}{f_{i-1}} \end{aligned} \tag{3.31}$$

where $\rho \in \Lambda_{\Gamma_n}$. We need to check that $\hat{\psi}$ is well-defined, that is, dividing by f_{i-1} is valid here, and if $\rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}} = w^{M_n}$ is an M_n^{th} power for some $w \in F_n^\times = (\mathbb{Q}(\mu_{p^{n+1}})^+)^\times$, then $\hat{\psi}(\rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}})$ is also an M_n^{th} power. After this, all that will remain is verifying (3.29).

First assume that $\rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}} = w^{M_n}$. Recall the statement of Proposition 3.5.13:

$$\overline{\mathrm{ord}}_{\lambda_{i-1}}\left(e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}\right) \equiv -\,\overline{\mathrm{ind}}_{\lambda_{i-1}}\left(e_\chi\kappa_{\ell_1\cdots\ell_{i-2}}\right) \bmod M_n\Lambda_{\Gamma_n} \qquad \text{(Proposition 3.5.13)}$$

Apply the induction hypothesis (3.29) to the expression on the right hand side of Proposition 3.5.13; by our choice (3.26) of t we have $\eta \mid p^t$ and $h_\chi \mid p^t$, thus we obtain

$$-\,\overline{\mathrm{ind}}_{\lambda_{i-1}}\left(e_\chi\kappa_{\ell_1\cdots\ell_{i-2}}\right) \bigm| e_\chi p^{it} \tag{3.32}$$

Meanwhile for the left hand side of Proposition 3.5.13, we have

$$\rho\,\overline{\mathrm{ord}}_{\lambda_{i-1}}\left(e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}\right) \equiv \overline{\mathrm{ord}}_{\lambda_{i-1}}\left(\rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}\right) \equiv 0 \bmod M_n\Lambda_{\Gamma_n} \tag{3.33}$$

since $\rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}$ is an M_n^{th} power by assumption. Putting Proposition 3.5.13, (3.32) and (3.33) together yields $\rho p^{it} \equiv 0 \bmod M_n\Lambda_{\Gamma_n}$. or equivalently $\rho \equiv 0 \bmod M_n p^{-it}\Lambda_{\Gamma_n}$. Then since $M_n = \#(e_\chi A_n)\cdot p^{n+(k+1)t}$, we obtain

$$\rho e_\chi A_n = 0$$

Consider the ideal $(\rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}) = (w)^{M_n}$ of F_n. It can be decomposed as a product with three factors.

1. The first consists of the primes above ℓ_{i-1}, which are the Galois conjugates of λ_{i-1}, the contribution of which is, in additive notation,

$$\overline{\mathrm{ord}}_{\lambda_{i-1}}\left(\rho e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}\right)\lambda_{i-1}$$

2. The second factor contains prime ideals above the rational primes $\ell_1, \dots, \ell_{i-2}$.
3. The third factor consists of primes $\mathfrak{p}$ not above any of the $\ell_1, \dots, \ell_{i-1}$: in additive notation, this factor is

$$\sum_{\mathfrak{p}} \rho\,\mathrm{ord}_{\mathfrak{p}}\left(e_\chi\kappa_{\ell_1\cdots\ell_{i-1}}\right)\mathfrak{p}$$

Now consider the image of the ideal class of the ideal $(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}})$ in

$$e_\chi A_n / \left(\text{prime ideals above } \ell_1, \ldots, \ell_{i-2}\right)$$

The second factor obviously vanishes, as does the third since every term in it is divisible by ρ, which kills $e_\chi A_n$. Since $(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}) = (w)^{M_n}$ and $\lambda_{i-1} \in c_{i-1}$, it follows that

$${M_n}^{-1} \, \overline{\operatorname{ord}}_{\lambda_{i-1}} \left(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}\right)$$

annihilates c_{i-1}. Dividing by M_n is valid here for the following reason. In the above factorisation of $(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}) = (w)^{M_n}$, the second factor is killed in the quotienting, and the third factor has exponent divisible by M_n by Proposition 3.5.9.1. Since every other exponent is divisible by M_n, so must $\overline{\operatorname{ord}}_{\lambda_{i-1}} \left(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}\right)$ be as well.

From Corollary 3.7.11.2 we get that

$$f_{i-1} {M_n}^{-1} \hat{\psi}(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}) = \eta {M_n}^{-1} \, \overline{\operatorname{ord}}_{\lambda_{i-1}} \left(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}\right) \in f_{i-1} \Lambda_{\Gamma_n} \tag{3.34}$$

It follows that ${M_n}^{-1} \hat{\psi}(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}) \in \Lambda_{\Gamma_n}$, wherefore $\hat{\psi}(\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}) \in M_n \Lambda_{\Gamma_n}$. This proves well-definedness of $\hat{\psi}$ under the assumption $\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}} = w^{M_n}$.

Now set $\rho := M_n$. This in particular implies $\rho e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}} = w^{M_n}$, therefore (3.34) applies, and shows that the numerator $\eta \, \overline{\operatorname{ord}}_{\lambda_{i-1}}(e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}})$ in (3.31) is divisible by f_{i-1}. Dividing by f_{i-1} is therefore valid by Weierstrass division (Theorem 1.1.2).

This proves that $\hat{\psi}$ is well-defined for arbitrary ρ, and consequently so is ψ as well.

Remark 3.8.4. Observe that we used both the first and second conversion step for $i = 1$ as well as for $2 \leqslant i \leqslant k + 1$. For $i = 1$, this was very direct; for $2 \leqslant i \leqslant k + 1$, using the first conversion step is subtly hidden in verifying that our explicit formula for ψ gives a well-defined map.

Now we verify (3.29) for i, i.e. we prove that

$$\overline{\operatorname{ind}}_{\lambda_i} \left(e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}\right) f_1 \cdots f_{i-1} \,\middle|\, e_\chi \eta^i h_\chi \quad \text{in } e_\chi \left(\Lambda_{\Gamma_n} / M_n \Lambda_{\Gamma_n}\right)$$

This is done as follows: working mod $M_n \Lambda_{\Gamma_n}$ we have

$$\begin{aligned} \eta \, \overline{\operatorname{ind}}_{\lambda_{i-1}} \left(e_\chi \kappa_{\ell_1 \cdots \ell_i}\right) &\equiv \eta \, \overline{\operatorname{ord}}_{\lambda_{i-1}} \left(e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}\right) && \text{by Proposition 3.5.13} \\ &\equiv f_{i-1} \psi \left(e_\chi \kappa_{\ell_1 \cdots \ell_{i-1}}\right) && \text{definition (3.31) of } \psi \end{aligned}$$

This together with (3.29) for $i - 1$ proves (3.29) for i, thus completes the induction, and finishes the proof of Lemma 3.8.1. □

This completes the proof of the Iwasawa main conjecture. □

Appendix A

The function field analogy

In this chapter we elaborate on how the analogy between number fields and function fields motivated Iwasawa to develop Iwasawa theory. We will mostly follow [Iwa69a]. The various objects and statements which correspond to one another under the function field analogy will be collected in Table A.3.

We will make several statements without proof, and will focus on establishing the analogy on a heuristic level instead. One should think of the analogy as a way to motivate statements—but not proofs—in Iwasawa theory. As we have seen in previous chapters, the whole theory can be built up and also motivated without mentioning function fields. It is worth noting though that exploring the analogy further can still lead to new results, as demonstrated in the recent papers [KW10; Sha14], some of whose ideas we discuss in Appendix A.5.

As we shall see, the way this analogy is used is by taking algebro-geometric results about function fields and formulating analogous assertions about number fields; this will lead us to cyclotomic fields in a natural way. One could raise the question whether the analogy can be turned the other way around: is there a theory corresponding to cyclotomic fields in the arithmetic of function fields? The answer is positive, but won't be discussed here. We instead refer to the books [Gos96; Tha04].

Remark A.0.1. In this appendix, *number field* will mean any algebraic extension of $\mathbb{Q}$, not just a finite one. This deviates from the standard usage of the term. We will call a finite extension of $\mathbb{Q}$ a *finite number field.*

A.1 The p-part of the Jacobian

Let k be an algebraically closed field, and consider a complete, nonsingular algebraic curve $\mathcal{C}$ of genus g over k with Jacobian J. Then J is an abelian variety of genus g, and if J_ℓ denotes the ℓ-primary part where $\ell \neq \operatorname{char} k$, then

$$J_\ell(k) \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g} \tag{A.1}$$

as abelian groups. (For a quick introduction to the theory of Jacobians of curves, see §§5.3.5–5.3.6 of [MP05]. For details, see [Mil08], esp. §I.10 and §III.1.)

Proposition A.1.1. *For the endomorphism ring of $J_\ell(k)$ we have* $\operatorname{End} J_\ell(k) \simeq \mathrm{Mat}_{2g\times 2g}(\mathbb{Z}_\ell)$.

Proof. First note that $\mathbb{Q}_\ell/\mathbb{Z}_\ell = \varinjlim \mathbb{Q}_\ell/\mathbb{Z}_\ell[\ell^n]$ where $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell^n]$ is the group of elements killed by ℓ^n, and the maps are the inclusions $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell^n] \hookrightarrow (\mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell^m]$ for $0 \leqslant n \leqslant m$. Then

$$\begin{aligned}\operatorname{End}(\mathbb{Q}_\ell/\mathbb{Z}_\ell) &= \operatorname{Hom}\left(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathbb{Q}_\ell/\mathbb{Z}_\ell\right)\\ &= \operatorname{Hom}\left(\varinjlim(\mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell^n], \mathbb{Q}_\ell/\mathbb{Z}_\ell\right)\\ &\simeq \varprojlim \operatorname{Hom}\left((\mathbb{Q}_\ell/\mathbb{Z}_\ell)[\ell^n], \mathbb{Q}_\ell/\mathbb{Z}_\ell\right)\\ &\simeq \varprojlim \mathbb{Z}/\ell^n\mathbb{Z} = \mathbb{Z}_\ell\end{aligned}$$

Using $\operatorname{End}(\mathbb{Q}_\ell/\mathbb{Z}_\ell) \simeq \mathbb{Z}_\ell$ and

$$\operatorname{End}((\mathbb{Q}_\ell/\mathbb{Z}_\ell) \oplus (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^i) \simeq \begin{bmatrix}\operatorname{End}(\mathbb{Q}_\ell/\mathbb{Z}_\ell) & \operatorname{Hom}((\mathbb{Q}_\ell/\mathbb{Z}_\ell)^i, \mathbb{Q}_\ell/\mathbb{Z}_\ell)\\ \operatorname{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^i) & \operatorname{End}((\mathbb{Q}_\ell/\mathbb{Z}_\ell)^i)\end{bmatrix}$$

inductively, we deduce $\operatorname{End} J_\ell(k) \simeq \operatorname{End}(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g} \simeq \mathrm{Mat}_{2g\times 2g}(\mathbb{Z}_\ell)$. □

Our first goal is to find an object in the realm of number fields that corresponds to $J_\ell(k)$ and the endomorphisms of which can be described in a manner similar to Proposition A.1.1. Since the Jacobian is the degree zero part of the Picard group, and the ideal class group $\mathrm{Cl}\, F$ of a finite number field F is a special case of the Picard group, upon first glance it seems reasonable for the p-part $(\mathrm{Cl}\, F) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ of the ideal class group to correspond to $J_\ell(k)$ where p is any rational prime.

The group $(\mathrm{Cl}\, F) \otimes_{\mathbb{Z}} \mathbb{Z}_p$, however, turns out not to be a good analogue of $J_\ell(k)$. One fundamental difference is that the ideal class group of a finite number field is always finite, whereas $J(k)$ may be infinite (recall that k is assumed to be algebraically closed), and the same holds for the primary parts. This suggests that we should be seeking an analogue that is somehow larger.

To discover the origin of this discrepancy, we should reverse the question: why *do* we have the description in Proposition A.1.1? The proposition is clearly a direct consequence of $J_\ell(k) \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$. The proof of this isomorphism traces back to k being separably closed; more precisely, to the fact that the multiplication-by-ℓ map is surjective. (Cf. Remark 7.3 and the discussion before Proposition 10.5 in [Mil08].) Recall that we have assumed the stronger condition that k is algebraically closed.

The field of constants k is the analogue of the roots of unity in F. Indeed, in a finite field, every nonzero element is a root of unity. The field k is an algebraic closure of some finite field, thus for every element of k there is a finite subfield containing it, and therefore every nonzero element is a root of unity.

The analogy also manifests in the following form: the constants respectively the roots of unity are precisely the elements of the respective field which have absolute value 1 for every absolute value on the field. For number fields, this follows from a theorem of Kronecker [Kro57] (cf. [Gre78] for an even simpler proof). For function fields, one uses that every absolute value on K_C is a prolongation of an absolute value on $k(t)$. The latter comes either from the degree valuation or the $P(x)$-adic valuation where $P(x)$ is a monic irreducible polynomial.

Taking this into account, we set $F = K_0(\mu_{p^\infty})$ where K_0 is a finite Galois extension of $\mathbb{Q}$. Thus we have a $\mathbb{Z}_p$-extension F/K_0; we write $K_\infty = F$, and K_n for the intermediate extensions. Since $J_p(k)$ is the injective limit of the p^n-torsion points $J(k)[p^n]$, we seek its analogy in a similar

Function fields	**Number fields**
k (large enough) field of constants	(sufficiently many) roots of 1 in $F = K_\infty$
$K_{\mathcal{C}}$ function field of $\mathcal{C}$, finite extension of $k(t)$	$F = K_\infty$ number field
J Jacobian of $\mathcal{C}$	$\varinjlim \operatorname{Cl} E_i$ ideal class group
$\ell \neq \operatorname{char} k$ rational prime	p any rational prime
$J_\ell(k) = \varinjlim J(k)[\ell^n]$ ℓ-primary points	$A_\infty = \varinjlim A_n = (\varinjlim \operatorname{Cl} E_i) \otimes_{\mathbb{Z}} \mathbb{Z}_p$
$J(k)[\ell^n] = \{j \in J(k) \mid j^{\ell^n} = 0\}$	$A_n = (\operatorname{Cl} E_i) \otimes_{\mathbb{Z}} \mathbb{Z}_p$
$J_\ell(k) \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$	$A_\infty \sim (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda \oplus C(\mu_1, \ldots, \mu_s)$ $p^N A_\infty \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$
$\operatorname{End} J_\ell(k) \simeq \operatorname{Mat}_{2g\times 2g}(\mathbb{Z}_\ell)$	$\operatorname{End}(p^N A_\infty) \simeq \operatorname{Mat}_{\lambda\times\lambda}(\mathbb{Z}_p)$

Table A.2: The analogy between function fields and number fields

form. Let, as usual, A_n denote the p-part of the ideal class group of K_n, and let $A_\infty = \varinjlim A_n$ where we take the injective limit with respect to the natural maps induced by the inclusions in the tower of fields. The following theorem is the analogue of (A.1). See Table A.2 for a summary of which objects correspond to one another.

Theorem A.1.2. *There is an exact sequence*

$$0 \to (\textit{finite } p\textit{-group}) \to (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda \oplus C(\mu_1, \ldots, \mu_s) \to A_\infty \to (\textit{finite } p\textit{-group}) \to 0$$

where $C(\mu_1, \ldots, \mu_s) = \bigoplus_{i=1}^s \left(\bigoplus_{\mathbb{N}} \mathbb{Z}/p^{\mu_i}\mathbb{Z}\right)$, λ *is the* λ*-invariant of the extension, and* $\mu = \mu_1 + \ldots + \mu_s$ *is the* μ*-invariant (q.v. Definition 1.1.14). In particular,* $(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda \oplus C(\mu_1, \ldots, \mu_s)$ *is pseudo-isomorphic to* A_∞.

The proof will be given in the next section. Here we draw some conclusions to demonstrate the analogy between $J_p(k)$ and A_∞.

Corollary A.1.3. *For large enough* N*, we have* $p^N A_\infty \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$.

Proof. Choose $N \geqslant \max(\mu_1, \ldots, \mu_s)$ so that p^N is at least the order of the kernel and cokernel groups. □

Remark A.1.4. Recall that $\mu = 0$ when $K_0/\mathbb{Q}$ is abelian by the Ferrero–Washington theorem, and it is conjectured that this is also true for arbitrary K_0; q.v. Remark 1.2.3.

Corollary A.1.3 is the analogue of (A.1). Then just as for the Jacobian, we obtain:

Corollary A.1.5. $\operatorname{End} p^N A_\infty \simeq \operatorname{Mat}_{\lambda\times\lambda}(\mathbb{Z}_p)$. □

Note that the factor p^N simply means that we disregard the bottom N fields of the tower, i.e. K_N plays the role of K_0. This is the same step as in the proof of Iwasawa's theorem (Theorem 1.2.1).

Comparing Corollary A.1.3 with (A.1), one might say that $\lambda/2$ is the analogue of the genus of the function field $K_{\mathcal{C}}$. (Since λ is an invariant of the $\mathbb{Z}_p$-extension K_∞/K_0, the p^N factor makes no difference.) One might also try to relate this to the notion of the genus for a finite extension of $\mathbb{Q}$ (cf. [Neu99, p. III.3.5]). We only point out that the two are of fundamentally different nature: $\lambda/2$ is a half-integer, whereas the genus of a finite number field is in general not even rational.

Finally, we note that for certain purposes it is better to consider the minus part A_∞^-, i.e. the part where complex conjugation acts by (-1), to be the object analogous to $J_\ell(k)$. This will be illustrated in Appendix A.3 where we will sketch the motivating analogy of the main conjecture.

A.2 Proof of the pseudo-isomorphism for A_∞

In this section we give a proof of Theorem A.1.2. It will go as follows. Since $X_\infty = \varprojlim A_n$ is a finitely generated torsion Λ-module (Lemma 1.3.2), we already have a similar result for that, namely

$$0 \to (\text{finite}) \to \bigoplus_{i=1}^{s} \Lambda/p^{\mu_i}\Lambda \oplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j}\Lambda \to X_\infty \to (\text{finite}) \to 0 \tag{A.2}$$

where $\mu = \mu_1 + \ldots + \mu_s$, $\lambda = \sum_{j=1}^{t} m_j \deg f_j$ are the Iwasawa invariants. So what we need to do is relate the injective limit $A_\infty = \varinjlim A_n$ to the projective limit X_∞. We may do this by applying the following theorem of Iwasawa [Iwa73, Theorem 11].

Theorem A.2.1. *There is a pseudo-isomorphism* $\mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \sim X_\infty$. □

Given the contravariance of $\mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$, this statement is hardly surprising. We omit the proof; it uses Iwasawa's theory of adjoints (cf. [Iwa73, §1.3] for a summary, [Was97, §15.5] for details) and the standard techniques used in Section 1.2.

For finitely generated torsion Λ-modules, pseudo-isomorphism is an equivalence relation (Corollary 1.1.11), so we obtain an exact sequence for $\mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$:

$$0 \to (\text{finite}) \to \bigoplus_{i=1}^{s} \Lambda/p^{\mu_i}\Lambda \oplus \bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j}\Lambda \to \mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p) \to (\text{finite}) \to 0 \tag{A.3}$$

In the category of $\mathbb{Z}_p$-modules, $\mathbb{Q}_p/\mathbb{Z}_p$ is an injective object. Indeed, since $\mathbb{Z}_p$ is a PID, injectivity is equivalent to divisibility [Wei94, Corollary 2.3.2], and it is easily checked that $\mathbb{Q}_p/\mathbb{Z}_p$ is divisible. Thus applying $\mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ preserves the exactness of (A.3). We now verify that this yields Theorem A.1.2 by computing each term in the exact sequence in a series of claims.

Claim A.2.2 (2nd and 5th terms)**.** *If M is a finite $\mathbb{Z}_p$-module then* $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ *is also finite and of p-power order.*

Proof. Let $f \in \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ and $m \in M$. Since M is finite, $nm = 0$ for some $n \in \mathbb{N}$. Since $\mathbb{N} \subset \mathbb{Z}_p$, we also have $0 = f(0) = f(nm) = nf(m)$. Do this for all the finitely many m's, and let k be the product of the corresponding n's. Then k kills the image of f. Since this is true for every morphism f, it follows that there is a finite $\mathbb{Z}_p$-submodule N of $\mathbb{Q}_p/\mathbb{Z}_p$ such that $\mathrm{Im}\, f \subseteq N$, that is, $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}_{\mathbb{Z}_p}(M, N)$. The latter is finite since both M and N are finite.

Furthermore, since N is finite, there is a $k \in \mathbb{N}$ such that $p^k N = 0$. Therefore p^k kills $\mathrm{Hom}_{\mathbb{Z}_p}(M, N) = \mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$, hence it has order dividing p^k. □

Claim A.2.3. $\mathrm{Hom}_{\mathbb{Z}_p}(\Lambda/p^n, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \bigoplus_{i=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$

Proof. First observe that $\Lambda/p^n = \mathbb{Z}_p[\![T]\!]/p^n \simeq (\mathbb{Z}/p^n\mathbb{Z})[\![T]\!]$. Therefore any homomorphism $f \in \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda/p^n, \mathbb{Q}_p/\mathbb{Z}_p)$ is determined by its values on 1, T, T^2, ... (Remember that we are considering $(\mathbb{Z}/p^n\mathbb{Z})[\![T]\!]$ as a $\mathbb{Z}_p$-module, and forget about the ring structure of $(\mathbb{Z}/p^n\mathbb{Z})[\![T]\!]$, so there is no correspondence between the values $f(T^i)$ for different i's.) Since $p^n \in \mathbb{Z}_p$, we have $0 = f(0) = f(p^n T^i) = p^n f(T^i)$. We obtain the desired isomorphism. □

Claim A.2.4. *For $f(T) \in \Lambda$ a distinguished and irreducible polynomial:*

$$\mathrm{Hom}_{\mathbb{Z}_p}(\Lambda/f(T)^m, \mathbb{Q}_p/\mathbb{Z}_p) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^{m \deg f}$$

Proof. A morphism $f \in \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda/f(T)^m, \mathbb{Q}_p/\mathbb{Z}_p)$ is again determined by its values on T^i, $i \in \mathbb{N}$. We may choose these values freely for $0 \leqslant i < m \deg f(T)$, the rest is determined by these and the relation $f(T)^m = 0$. This yields the desired isomorphism. □

Claim A.2.5 (3rd term)**.**

$$\mathrm{Hom}_{\mathbb{Z}_p}\left(\left(\bigoplus_{i=1}^{s} \Lambda/p^{\mu_i}\Lambda\right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/f_j(T)^{m_j}\Lambda\right), \mathbb{Q}_p/\mathbb{Z}_p\right) \simeq$$

$$\simeq \left(\bigoplus_{i=1}^{s} \bigoplus_{\mathbb{N}} \mathbb{Z}/p^{\mu_i}\mathbb{Z}\right) \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^{\sum_{j=1}^{t} m_i \deg f_i} = C(\mu_1, \ldots, \mu_s) \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda}$$

Proof. Finite direct sums commute with the Hom functor, thus we may use Claims A.2.3 and A.2.4. □

Claim A.2.6 (4th term)**.** $\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Q}_p/\mathbb{Z}_p\right) \simeq A_\infty$

Proof. Since every element in A_∞ is of p-power order, the group $\mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is isomorphic to the Pontryagin dual $\mathrm{Hom}_{\mathrm{cts}}(A_\infty, \mathbb{T})$ of A_∞ where $\mathrm{Hom}_{\mathrm{cts}}(-,-)$ is the group of continuous group homomorphisms and $\mathbb{T}$ denotes the circle group. The holds for the bidual, meaning that we have

$$\mathrm{Hom}_{\mathbb{Z}_p}\left(\mathrm{Hom}_{\mathbb{Z}_p}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p), \mathbb{Q}_p/\mathbb{Z}_p\right) \simeq \mathrm{Hom}_{\mathrm{cts}}\left(\mathrm{Hom}_{\mathrm{cts}}(A_\infty, \mathbb{T}), \mathbb{T}\right)$$

The group on the right is canonically isomorphic to A_∞ by the Pontryagin duality theorem. □

Putting Claims A.2.2, A.2.5 and A.2.6 together, we see that applying $\mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ to (A.3) yields Theorem A.1.2. □

A.3 Towards the Iwasawa main conjecture

In this section we show how the Iwasawa main conjecture fits into the function field analogy.

Let τ be an algebraic correspondence on C, that is, a divisor on $C \times C$. (Cf. [Smi05, §§3.1–3.3] for a quick introduction to correspondences, or [Ful98, Chapter 16] for a more complete account.) Then τ induces an endomorphism of the Jacobian J, which restricts to the ℓ-primary part J_ℓ. Proposition A.1.1 states that this restriction can be represented by a matrix $M(\tau) \in \mathrm{Mat}_{2g\times 2g}(\mathbb{Z}_\ell)$.

In particular, let k_0 be a finite subfield of k such that $\mathcal{C}$ is also defined over k_0. Then there is a Frobenius automorphism $\varphi \in \operatorname{Gal}(k/k_0)$. Then the rationality part of the Weil conjectures states that

$$Z(\mathcal{C}/k_0, x) = \frac{\det(1 - \varphi x \mid H^1(\mathcal{C}_{/k_0}, \mathbb{Q}_\ell))}{\det(1 - \varphi x \mid H^0(\mathcal{C}_{/k_0}, \mathbb{Q}_\ell))} \tag{A.4}$$

Here the left hand side is the zeta function of the curve $\mathcal{C}$ considered as a curve over the finite field k_0, and the numerator resp. denominator on the left hand side are the characteristic polynomials of the Frobenius φ on the ℓ-adic cohomology groups. Simply put, (A.4) relates the zeta function to the eigenvalues of the Frobenius.

What is a similar result for number fields? Let σ be an automorphism of K_∞; then as before, this induces an endomorphism of $p^N A_\infty$, which can be represented by a matrix $M(\sigma) \in \operatorname{Mat}_{\lambda\times\lambda}(\mathbb{Z}_p)$.

The simplest case is the case of cyclotomic fields, i.e. when $K_\infty = \mathbb{Q}(\mu_{p^\infty})$, $K_n = \mathbb{Q}(\mu_{p^{n+1}})$. We will use the notations of Section 3.7. The different formulations of the main conjecture then relate the characteristic polynomial of an Iwasawa module to some incarnation of the p-adic L-function (Section 3.1). Since characteristic polynomials in the sense of Definition 1.1.12 describe the action of a topological generator on an Iwasawa module, this shows the analogy with (A.4).

The result $p^N A_\infty \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ can be viewed as a statement about orthogonality. In the cyclotomic tower, we have another sort of orthogonality, namely the one given by the orthogonal idempotents of $\mathbb{Z}_p[\Delta]$ (cf. [Was97, §6.3]). More explicitly, the characters of Δ are ω^i for $0 \leqslant i \leqslant p-2$ where ω denotes the Teichmüller character. To ease notation, we will write e_i for the idempotent e_{ω^i}. One might ask whether these two orthogonalities are related. The answer is positive, as demonstrated in [Iwa64, §1.3] and summarised in [Iwa69a] by Iwasawa.

We briefly sketch this relation. If we assume Vandiver's conjecture, that is, the vanishing of $e_i A_0$ for all even i, then we have that $e_i X_\infty \simeq \Lambda/G_{\omega^{1-i}}(T)\Lambda$ for all $3 \leqslant i \leqslant p-2$ odd. For a proof, consult [Was97, Theorem 10.16]; note that the proof is relatively elementary, that is, it uses little more than Iwasawa's construction of p-adic L-functions. This result should be seen as the first instance of the main conjecture; it is clear that Iwasawa considered it to be so. (See also Section 3.2 for a different perspective.)

Using p-adic Weierstrass preparation (Theorem 1.1.3), we may write

$$G_{\omega^{1-i}}(T) = p^{\mu_i} u_i(T) m_i(T)$$

where $\mu_{(i)} \geqslant 0$ is an integer, $u_i(T) \in \Lambda^\times$, and $m_i(T) \in \mathbb{Z}_p[\![T]\!]$ is a monic polynomial of degree $\lambda_{(i)}$. We have

$$\Lambda/G_{\omega^{1-i}}(T)\Lambda = \mathbb{Z}_p[\![T]\!]/\left(p^{\mu_{(i)}} u_i(T) m_i(T)\right) \simeq \left(\mathbb{Z}/p^{\mu_{(i)}}\mathbb{Z}\right)[\![T]\!]/m_i(T)$$

It follows that $\sum_{i=0}^{p-2} \lambda_{(i)} = \lambda$ and $\sum_{i=0}^{p-2} \mu_{(i)} = \mu$.

Let γ be a topological generator of Γ. This is represented by the $\lambda \times \lambda$ matrix $M(\gamma)$. By orthogonality, its action on the ω^i-component is represented by a $\lambda_{(i)} \times \lambda_{(i)}$ matrix $M_i(\gamma)$. Moreover since the topological generator γ of Γ corresponds to $1+T$, the characteristic polynomial of $M_i(\gamma)$ is $m_i(T-1)$. Let

$$G(T) := \prod_{i=0}^{p-2} G_{\omega^{1-i}}(T), \quad u(T) := \prod_{i=0}^{p-2} u_i(T), \quad m(T) := \prod_{i=0}^{p-2} m_i(T)$$

Then we have $G(T) = p^{\mu}u(T)m(T)$, and $m(T-1)$ is the characteristic polynomial of $M(\gamma)$. This is a more explicit description of how the p-adic L-function is related to the action of the topological generator.

By assuming Vandiver's conjecture above, we were essentially working with A_{∞}^{-} instead of A_{∞}, which shows that for these purposes, the former is the better analogue of $J_{\ell}(k)$.

A.4 The Weil pairing

For an abelian variety A and an algebraically closed field k, one has a non-degenerate Weil pairing $A(k)(m) \times A^{\vee}(k)(m) \to \mu_m(k)$ where m is an integer not divisible by the characteristic of k, and $A^{\vee}$ denotes the dual abelian variety [Mil08, §I.13]. Since Jacobians are autodual, in our setting we have $J[\ell^n] \times J[\ell^n] \to \mu_{\ell^n}$ for all n, which yield

$$T_{\ell}(J) \times T_{\ell}(J) \to \mu_{\ell^{\infty}} \tag{A.5}$$

Given the analogies discussed above, it is natural to raise the question whether there is an analogous pairing for $\mathbb{Z}_p$-extensions.

As indicated at the end of the previous section, we will be considering A_{∞}^{-} as the analogue of $J_{\ell}(k)$. Remembering that one of the $T_{\ell}(J)$'s in (A.5) appear in the role of a dual, in the analogous statement we will should replace one of them by X_{∞}^{+}. Instead of X_{∞}^{+}, however, the statement features the larger module $\mathfrak{X}_{\infty}^{+}$, i.e. the plus part of the Galois group of the maximal p-ramified abelian p-extension. Namely, we have a non-degenerate pairing

$$A_{\infty}^{-} \times \mathfrak{X}_{\infty}^{+} \to \mu_{p^{\infty}} \tag{A.6}$$

This is called the Iwasawa pairing, first proven by Iwasawa [Iwa64]. The pairing is constructed from a Kummer pairing [Was97, §13.5]. For elliptic curves, one may think of the Weil pairing as an instance of Kummer theory, which validates the analogy further (see [Sil09, Chapter VIII, §1] for a thorough exposition or [Sil12] for a heuristic explanation, both by Silverman). Washington makes the point that when it comes to Kummer theory, $\mathfrak{X}_{\infty}$ allows for a 'more natural theory' than X_{∞}.

Remark A.4.1. There also exists a version of the Iwasawa pairing for χ-components, see [NSW15, Theorem 11.4.3] or [Was97, Proposition 13.32].

A.5 Generalised Jacobians

In this section we will illustrate that the analogy presented above is still relevant in contemporary research as motivation. To this end, we will give a survey of the reciprocity conjecture of Khare and Wintenberger [KW10], which was strengthened and proved by Sharifi [Sha14]. For details and a proof, we refer to these papers.

As before, let C be a complete nonsingular curve over k. Let $P_1, P_2 \in C(k)$ be two distinct k-rational points. There is an exact sequence

$$0 \to \mathbb{G}_m \to J_{P_1P_2} \to J \to 0 \tag{A.7}$$

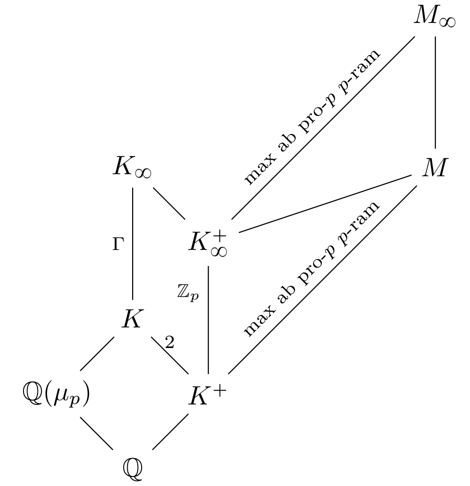

Figure A.1: The number fields involved in Appendix A.5.

where $\mathbb{G}_m$ is the multiplicative group and $J_{P_1P_2}$ denotes the generalised Jacobian [Ser88, §V.17]. In other words, $J_{P_1P_2}$ is an extension of the Jacobian J by the multiplicative group $\mathbb{G}_m$. Consider the class of (A.7) in $\mathrm{Ext}^1(J, \mathbb{G}_m)$. This can be identified with the degree zero divisor class $[P_1 - P_2] \in J(k)$ [Ser88, Theorem VII.16.6].

Taking Tate modules for a prime $\ell \neq p$, we have that $T_\ell(J_{P_1P_2})$ is also an extension:

$$0 \to \mathbb{Z}_\ell(1) \to T_\ell(J_{P_1,P_2}) \to T_\ell(J) \to 0 \tag{A.8}$$

Here $\mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}$. We have right exactness because all connecting maps between $\mathbb{G}_m[\ell^n] = \mu_{\ell^n}$ are surjective. This extension class in $\mathrm{Ext}^1_{\mathbb{Z}_\ell[\![G_k]\!]}(T_\ell J, \mathbb{Z}_\ell(1))$ is then identified with the image of $[P_1 - P_2]$ in the ℓ-primary part $J(k)[\ell^\infty]$. This identification takes place in the cohomology group $H^1(G_k, T_\ell(J))$; we end up in this group by using Weil duality [KW10, §5.3].

We seek an analogy of this statement for number fields. We begin with definitions; see Figure A.1. Let K be a CM-field containing μ_p with maximal totally real subfield K^+. Consider the cyclotomic $\mathbb{Z}_p$-extensions of K resp. K^+; these will be denoted by K_∞ resp. K_∞^+. Let M resp. M_∞ be the maximal pro-p abelian p-ramified extension of F^+ resp. F_∞^+. Let $\mathfrak{q}_1$ and $\mathfrak{q}_2$ be distinct primes of F^+ not above p which are inert in F_∞^+, and $\mathrm{Fr}_{\mathfrak{q}_1}, \mathrm{Fr}_{\mathfrak{q}_2} \in \mathrm{Gal}(M/F^+)$ be the Frobenius elements of $\mathfrak{q}_1$ resp. $\mathfrak{q}_2$.

We now construct an analogue M_Q of the ℓ-part of the degree zero divisor class $[P_1 - P_2]$. There is a short exact sequence

$$0 \to \mathrm{Gal}(M_\infty/K_\infty^+) \to \mathrm{Gal}(M_\infty/K^+) \xrightarrow{\deg} \mathbb{Z}_p \to 0$$

where we call the map to $\mathbb{Z}_p$ the *degree map*. Let $M_Q' := \langle \mathrm{Fr}_{\mathfrak{q}_1}, \mathrm{Fr}_{\mathfrak{q}_2} \rangle_{\mathbb{Z}_p}$ be the $\mathbb{Z}_p$-submodule of $\mathrm{Gal}(M_\infty/K_\infty^+)$ generated by the Frobenius elements, and M_Q its maximal $\mathbb{Z}_p$-submodule that vanishes under the degree map. Since the Frobenius elements $\mathrm{Fr}_{\mathfrak{q}_1}$, $\mathrm{Fr}_{\mathfrak{q}_2}$ represent the primes $\mathfrak{q}_1$, $\mathfrak{q}_2$, and these in turn correspond to the points P_1, P_2 under the analogy, this shows that M_Q is indeed analogous to the class $[P_1 - P_2]$.

Now for the object corresponding to the extension class. Let $A_{\infty,\mathfrak{q}_1\mathfrak{q}_2}$ denote the p-part of the ray class group of K_∞ of conductor $\mathfrak{q}_1\mathfrak{q}_2$. Using the assumptions on the primes $\mathfrak{q}_1, \mathfrak{q}_2$ we have an exact sequence

$$0 \to \mu_{p^\infty} \to A^-_{\infty,\mathfrak{q}_1\mathfrak{q}_2} \to A^-_\infty \to 0 \tag{A.9}$$

This can be considered analogous to (A.8): both generalised Jacobians and ray class groups control ramification. We define N_Q to be the subgroup of $\mathrm{Ext}^1_{\mathbb{Z}_p[\![\Gamma]\!]}(A^-_\infty, \mu_{p^\infty})$ generated by the class of (A.9).

It follows from definition that $\mathrm{Ext}^1_{\mathbb{Z}_p[\![\Gamma]\!]}(A^-_\infty, \mu_{p^\infty})$ agrees with the Γ-coinvariants of the module $\mathrm{Hom}(A^-_\infty, \mu_{p^\infty})$. The Iwasawa pairing—which, as discussed in Appendix A.4, is analogous to the Weil pairing—identifies $\mathrm{Hom}(A^-_\infty, \mu_{p^\infty})$ with $\mathrm{Gal}(M_\infty/K^+_\infty)$, the Γ-coinvariants of which is $\mathrm{Gal}(M/K^+_\infty)$. This shows $\mathrm{Ext}^1_{\mathbb{Z}_p[\![\Gamma]\!]}(A^-_\infty, \mu_{p^\infty}) \simeq \mathrm{Gal}(M/K^+_\infty)$. The latter is also isomorphic to $H^1(\Gamma, \mathrm{Gal}(M_\infty/F^+_\infty))$ via evaluation at a generator; this is in analogy with $H^1(G_k, T_\ell(J))$ above.

This allows us to relate M_Q to N_Q. Khare and Wintenberger conjectured these subgroups to be equal, in analogy with the function field case. One might notice that while the original statement is about elements, the conjecture of Khare and Wintenberger is about groups generated by corresponding elements. Sharifi later made and proved a slightly stronger version of the conjecture about generators of these groups. We decided to restrict ourselves to presenting this weaker form since most of the ways the analogy works can already be observed in this case without going into too much detail.

A.6 The analogy in tabular form

Function fields	**Number fields**
k (large enough) field of constants	(sufficiently many) roots of 1 in $F = K_\infty$
$\mathcal{C}$ complete nonsingular curve over k	—
g genus of $\mathcal{C}$	$\lambda/2$ (?)
$k(t)$	$\mathbb{Q}$
$K_{\mathcal{C}}$ function field of $\mathcal{C}$, finite extension of $k(t)$	$F = K_\infty$ number field
J Jacobian of $\mathcal{C}$	$\varinjlim \mathrm{Cl}\, E_i$ ideal class group
$\ell \neq \operatorname{char} k$ rational prime	p any rational prime
$J_\ell(k) = \varinjlim J(k)[p^n]$ ℓ-primary points	$A_\infty = \varinjlim A_n = (\varinjlim \mathrm{Cl}\, E_i) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ or A_∞^-
$J(k)[\ell^n] = \{j \in J(k) \mid j^{\ell^n} = 0\}$	$A_n = (\mathrm{Cl}\, E_i) \otimes_{\mathbb{Z}} \mathbb{Z}_p$
—	$C(\mu_1, \ldots, \mu_s) = \bigoplus_{i=1}^s (\bigoplus_{\mathbb{N}} \mathbb{Z}/p^{\mu_i}\mathbb{Z})$ $\mu = \mu_1 + \ldots + \mu_s$
$J_\ell(k) \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$	$A_\infty \sim (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda \oplus C(\mu_1, \ldots, \mu_s)$ $p^N A_\infty \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$
$\mathrm{End}\, J_p(k) \simeq \mathrm{Mat}_{2g \times 2g}(\mathbb{Z}_p)$	$\mathrm{End}(p^N A_\infty) \simeq \mathrm{Mat}_{\lambda \times \lambda}(\mathbb{Z}_p)$
$T_l(J)$ Tate module	$X_\infty = T_l(F)$ Tate module
—	$X_\infty \sim \mathrm{Hom}(A_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$
τ algebraic correspondence on $\mathcal{C}$	$\sigma \in \mathrm{Aut}(F)$
$M(\tau)$ matrix of the induced element in $\mathrm{End}\, J_p$	$M(\sigma)$ matrix of the induced element in $\mathrm{End}\, p^N A_\infty$
k_0 finite subfield of k	K_0 finite number field
$\varphi \in \mathrm{Gal}(k/k_0)$ Frobenius	$\gamma \in \Gamma$ topological generator
characteristic polynomial of φ	characteristic polynomial in the sense of Definition 1.1.12
$Z(\mathcal{C}_{/k_0}, x)$ zeta function	p-adic L-function
$T_\ell(J) \times T_\ell(J) \to \mu_{\ell^\infty}$ Weil pairing	$A_\infty^- \times \mathfrak{X}_\infty^+ \to \mu_{p^\infty}$ Iwasawa pairing
P_1, P_2 k-rational points	$\mathfrak{q}_1, \mathfrak{q}_2$ inert primes not over p
$J_{P_1 P_2}$ generalised Jacobian	ray class group

Bibliography

[Bar04] Daniel Barsky. *Sur la nullité du mu-invariant d'Iwasawa des corps totalement réels.* 2004. arXiv: `math/0405487 [math.NT]`.

[Cas08] Hugo Castillo. 'Kubota-Leopoldt p-adic L-functions'. `http://algant.eu/documents/theses/castillo.pdf`. Master's Thesis. Padova, Bordeaux: ALGANT, 2008.

[CS06] J. Coates and R. Sujatha. *Cyclotomic Fields and Zeta Values.* Springer Monographs in Mathematics. Berlin: Springer, 2006. ISBN: 978-3-540-33068-4.

[Ful98] William Fulton. *Intersection Theory.* 2nd ed. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge 2. Berlin: Springer-Verlag, 1998. ISBN: 0-387-98549-2.

[FW79] Bruce Ferrero and Lawrence C. Washington. 'The Iwasawa invariant μ_p vanishes for abelian number fields'. In: *Annals of Mathematics* 109.2 (May 1979), pp. 377–395. DOI: `10.2307/1971116`.

[Gos96] David Goss. *Basic Structures of Function Field Arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge 35. Berlin: Springer, 1996. ISBN: 3-540-61087-1.

[Gre78] G. Greiter. 'A Simple Proof for a Theorem of Kronecker'. In: *The American Mathematical Monthly* 85.9 (1978), pp. 756–757. DOI: `10.2307/2321687`.

[Gre92] Cornelius Greither. 'Class groups of abelian fields, and the main conjecture'. In: *Annales de l'Institut Fourier* 42.3 (1992), pp. 449–499.

[Iwa64] Kenkichi Iwasawa. 'On some modules in the theory of cyclotomic fields'. In: *J. Math. Soc. Japan* 16.1 (1964), pp. 42–82. DOI: `10.2969/jmsj/01610042`.

[Iwa69a] Kenkichi Iwasawa. 'Analogies between number fields and function fields'. In: *Some Recent Advances in the Basic Sciences, Proc. Annual Sci. Conf. (New York 1965–1966).* Vol. 2. Belfer Graduate School of Science, Yeshiva Univ., New York, 1969, pp. 203–208.

[Iwa69b] Kenkichi Iwasawa. 'On p-adic L-Functions'. In: *Annals of Mathematics* 89.1 (1969), pp. 198–205. ISSN: 0003486X. DOI: `10.2307/1970817`.

[Iwa72] Kenkichi Iwasawa. *Lectures on p-adic L-functions.* Annals of Mathematics Studies. Princeton University Press, 1972. ISBN: 978-0-691-08112-0.

[Iwa73] Kenkichi Iwasawa. 'On $\mathbb{Z}_l$-Extensions of Algebraic Number Fields'. In: *Annals of Mathematics* 98.2 (1973), pp. 246–326. DOI: `10.2307/1970784`.

[Kat07] Kazuya Kato. 'Iwasawa theory and generalizations'. In: *Proceedings of the International Congress of Mathematicians, Madrid, Spain, 2006.* Vol. I. European Mathematical Society, 2007, pp. 335–357.

[KKS12] Nobushige Kurokawa, Masato Kurihara and Takeshi Saito. *Number Theory 3.* Translations of Mathematical Monographs: Iwanami Series in Modern Mathematics 242. Providence, Rhode Island: American Mathematical Society, 2012. ISBN: 978-0-8218-1355-3.

[KL64] Tomio Kubota and Heinrich Wolfgang Leopoldt. 'Eine p-adische Theorie der Zetawerte. Teil I: Einführung der p-adischen Dirichletschen L-Funktionen'. In: *Journal für die reine und angewandte Mathematik* 214/215 (1964), pp. 328–339.

[Kob84] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions.* 2nd ed. Graduate Texts in Mathematics 58. New York: Springer-Verlag, 1984. ISBN: 978-0-387-96017-3.

[Kro57] Leopold Kronecker. 'Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten'. In: *Journal Für Die Reine Und Angewandte Mathematik (Crelles Journal)* 53 (1857), pp. 173–175. DOI: `10.1515/crll.1857.53.173`.

[KW10] Chandrashekhar Khare and Jean-Pierre Wintenberger. 'Ramification in Iwasawa modules'. In: *arXiv e-prints* (Nov. 2010). arXiv: `1011.6393 [math.NT]`.

[Lan86] Serge Lang. *Algebraic Number Theory.* Graduate Texts in Mathematics 110. New York: Springer-Verlag, 1986.

[Lan90] Serge Lang. *Cyclotomic Fields I and II.* Combined 2nd ed. Graduate Texts in Mathematics 121. New York: Springer-Verlag, 1990. ISBN: 0-387-96671-4.

[Lon77] Robert L. Long. *Algebraic Number Theory.* New York: Marcel Dekker, 1977. ISBN: 9780824765408.

[Mil08] James S. Milne. *Abelian Varieties (v2.00).* 2008. URL: `http://www.jmilne.org/math/CourseNotes/av.html`.

[Mil18] James S. Milne. *Fields and Galois Theory (v4.60).* 2018. URL: `http://www.jmilne.org/math/CourseNotes/ft.html`.

[MP05] Yuri Ivanovic Manin and Alexei A. Panchishkin. *Introduction to modern number theory: fundamental problems, ideas and theories.* 2. ed. Vol. 49. Encyclopaedia of Mathematical Sciences. Berlin: Springer, 2005. ISBN: 978-3-642-05797-7.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory.* Vol. 322. Grundlehren der mathematischen Wissenschaften. Berlin: Springer-Verlag, 1999. ISBN: 3-540-65399-6.

[NSW15] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg. *Cohomology of Number Fields.* 2.2 electronic edition. Available at `https://www.mathi.uni-heidelberg.de/~schmidt/NSW2e/`. Berlin: Springer, 2015.

[Rub00] Karl Rubin. *Euler Systems.* Princeton, New Jersey: Princeton University Press, 2000.

[Rub87] Karl Rubin. 'Global units and ideal class groups'. In: *Invent. math.* 89 (1987), pp. 511–526.

[Rub90] Karl Rubin. 'The Main Conjecture'. In: Serge Lang. *Cyclotomic Fields I and II.* Combined 2nd ed. Graduate Texts in Mathematics 121. New York: Springer-Verlag, 1990, pp. 397–419. ISBN: 0-387-96671-4.

[Ser02] Jean-Pierre Serre. *Galois Cohomology.* Corrected Second Printing of the First English Ed. Springer Monographs in Mathematics. Berlin: Springer-Verlag, 2002.

[Ser88] Jean-Pierre Serre. *Algebraic Groups and Class Fields.* Graduate Texts in Mathematics 117. New York: Springer, 1988. ISBN: 978-1-4612-6993-9.

[Sha] Romyar Sharifi. *Iwasawa Theory.* `http://math.ucla.edu/~sharifi/iwasawa.pdf`. Lecture notes.

[Sha14] Romyar T. Sharifi. 'The Reciprocity Conjecture of Khare and Wintenberger'. In: *International Mathematics Research Notices* 2014.5 (2014), pp. 1409–1424. DOI: `10.1093/imrn/rns259`.

[Sha18] Romyar T. Sharifi. *Modular curves and cyclotomic fields.* `http://swc.math.arizona.edu/aws/2018/2018SharifiNotes.pdf`. Lecture notes for the Arizona Winter School. 2018.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* 2nd ed. Graduate Texts in Mathematics 106. New York: Springer, 2009. ISBN: 978-0-387-09493-9.

[Sil12] Joe Silverman. *Weil pairing, Kummer theory, help to decrypt what Wikipedia says.* MathOverflow. Jan. 2012. URL: `https://mathoverflow.net/q/86655`.

[Smi05] Benjamin Smith. 'Explicit Endomorphisms and Correspondences'. PhD thesis. Australia: University of Sydney, 2005.

[Stacks] The Stacks Project Authors. *Stacks Project.* `https://stacks.math.columbia.edu`. 2018.

[Suj11] Ramdorai Sujatha. 'On the μ-invariant in Iwasawa theory'. In: *WIN—Women in Numbers: Research Directions in Number Theory.* Ed. by Alina-Carmen Cojocaru et al. Available at `http://www.math.tifr.res.in/~sujatha/win.pdf`. Mar. 2011, pp. 265–276. ISBN: 978-0-8218-5226-2. DOI: `10.1090/fic/060/15`.

[Tha04] Dinesh S. Thakur. *Function Field Arithmetic.* Singapore: World Scientific Publishing, 2004. ISBN: 981-238-839-7.

[Tha88] Francisco Thaine. 'On the ideal class groups of real abelian number fields'. In: *Annals of Mathematics* 128 (1988), pp. 1–18.

[Was97] Lawrence C. Washington. *Introduction to Cyclotomic Fields.* 2nd ed. Graduate Texts in Mathematics 83. New York: Springer-Verlag, 1997. ISBN: 0-387-94762-0.

[Wei94] Charles A. Weibel. *An introduction to homological algebra.* Vol. 38. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1994.

Nomenclature

$\mathbb{1}$	trivial Dirichlet character	20
$\sim$	pseudo-isomorphism	5
$\sim_\Theta$	Big Theta-equivalence	48
(α_r)	Euler system for the cyclotomic units	33
A_n	p-Sylow subgroup of $\mathrm{Cl}\, K_n$	8
A_∞	$\varinjlim A_n$	56
C_n	cyclotomic units of $\mathbb{Q}(\mu_{p^{n+1}})$	26
$\overline{C}_n$	closure of $C_n \cap U_n$ in U_n	26
$\overline{C}_\infty$	$\varprojlim \overline{C}_n$	26
Char	characteristic ideal	7
Cl	ideal class group	8
Δ	$\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$	20
e_χ	orthogonal idempotent	20
E_n	global units of $\mathbb{Q}(\mu_{p^{n+1}})$	26
$\overline{E}_n$	closure of $E_n \cap U_n$ in U_n	26
$\overline{E}_\infty$	$\varprojlim \overline{E}_n$	26
F_n	$\mathbb{Q}(\mu_{p^{n+1}})^+$	32
f_χ	characteristic polynomial of $e_\chi X_\infty$	28
f_i	factors of f_χ	28
$G_\chi(T)$	(quotient of of) power series associated to $L_p(s,\chi)$	22
Γ	$\mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$	8
Γ_n	Γ^{p^n}, this is $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}(\mu_{p^{n+1}}))$ in Chapter 3	11
$(-)_{\Gamma_n}$	Γ_n-coinvariants, see also Definition 3.7.3	17
γ	topological generator of Γ	11
G_n	$\mathrm{Gal}(F_n/\mathbb{Q})$	32
h_χ	characteristic polynomial of $e_\chi\overline{E}_\infty/e_\chi\overline{C}_\infty$	28
$\mathrm{ind}_{\sigma\lambda}$	index	38
$\overline{\mathrm{ind}}_\lambda$	collection of indices	38
κ	cyclotomic character	22

(κ_r)	Kolyvagin derivative of the Euler system (α_r)	35
K_∞/K	a $\mathbb{Z}_p$-extension of a number field K	8
K_n	the unique subfield with $\mathrm{Gal}(K_\infty/K_n) = p^n\Gamma$	8
Λ	the Iwasawa algebra $\mathbb{Z}_p[\![T]\!]$	4
Λ_{Γ_n}	$\mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}(\mu_p))]$	43
λ	λ-invariant	8
$L_p(s,\chi)$	p-adic L-function for the character χ	21
M_n	a large power of p, explicitly defined on page 51	32
μ	μ-invariant	8
μ_r	group of r^{th} roots of unity	2
μ_{p^∞}	group of p-power roots of unity	2
$\mathbb{N}$	positive rational integers	2
Ω_n	unique maximal p-abelian extension of K_n unramified outside p	18
ω	Teichmüller character	22
ord_λ	λ-adic valuation	36
$\overline{\mathrm{ord}}_\lambda$	collection of valuations	38
p	odd rational prime	2
U_n	principal local units: local units congruent to 1 modulo the maximal ideal	26
U_∞	$\varprojlim U_n$	26
X_∞	unramified Iwasawa module $\varprojlim A_n$	17
$\mathfrak{X}_n$	$\mathrm{Gal}(\Omega_n/K_n)$	18
$\mathfrak{X}_\infty$	p-ramified Iwasawa module $\varprojlim \mathfrak{X}_n$	18
ζ_{p^n}	primitive $(p^n)^{\mathrm{th}}$ root of unity	2