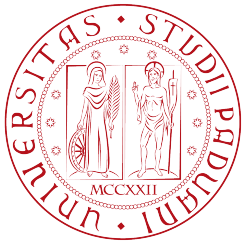


Università degli Studi di Padova

Department of Mathematics "Tullio Levi-Civita"

Master degree in Mathematics

Euler Systems and Iwasawa Theory: a Proof of the Main Conjecture

Supervisor: Prof. Matteo Longo

Candidate: Lorenzo Stefanello
Matriculation number: 1203101

16th July 2020

A Victoria e alla mia Famiglia

In these days the angel of topology and the devil of abstract algebra fight for the soul of each individual mathematical domain.

Hermann Weyl

Ringraziamenti

Quando nei mesi prima di iniziare questo lavoro, ancora senza un supervisore di riferimento, indagavo cercando varie tesi di magistrale disponibili online, ero sempre colpito, negativamente, dai ringraziamenti. Mi sono sempre sembrati impersonali, freddi, e soprattutto quelli al proprio relatore, di circostanza. Le solite frasi fatte, i soliti grazie per la pazienza, magari lontani dalla realtà. Pensavo dunque tra me e me di non fare nemmeno questa parte, ma ho dovuto presto ricredermi, avendo trovato nel professor Longo tutto quello che uno studente può chiedere in un relatore, e anche di più. Nonostante non mi conoscesse da prima, mi ha preso sotto la sua ala, stimolandomi ed aiutandomi costantemente. Le nostre chiamate duravano anche diverse ore, nelle quali non l'ho mai visto stancarsi, o perdere l'interesse. Ogni volta che ho avuto bisogno, lui c'è stato, matematicamente e personalmente. Perciò non posso fare a meno di dargli un immenso grazie, nel mio piccolo, con questa tesi.

Il mio secondo grazie va al mio compagno di avventure, Zed, con il quale ho condiviso tutto, durante questi anni patavini. Compagno di stanza, compagno di calcio, collega, amico. Ricordo con enorme gioia i lunghissimi messaggi vocali che ci siamo scambiati, aiutandoci e sostenendoci durante questo percorso difficile ma pieno di enormi soddisfazioni, della laurea e della tesi magistrale. La mia speranza è quella di continuare un percorso insieme, ritrovandoci più avanti e cominciando a collaborare con la matematica che conta veramente.

Voglio ringraziare di cuore la mia compagna di vita, la mia Vichinga, che c'è sempre per me. Il mio porto sicuro, la mia certezza quando intorno le cose magari non vanno come si spererebbe. Grazie per darmi sempre l'affetto e la tenerezza di cui ho bisogno, e soprattutto, di ricordarmi giorno per giorno le cose veramente importanti della vita.

Un enorme grazie anche ai miei parenti ed ai miei amici, che ogni giorno collaborano per rendere la vita qualcosa di più bello.

Introduction

The ideas. The final goal of this thesis is to state and prove the *Main Conjecture of Iwasawa theory* for cyclotomic fields. It is actually a theorem: its first proof was given by Barry Mazur and Andrew Wiles in [MW84]. This theorem is fundamental for multiple reasons: it is the deepest result concerning the theory of cyclotomic fields; it is related to other important results in this theory, like the converse of Herbrand-Ribet theorem, and the conjectures by Gras and Vandiver; it can be used to derive useful properties of the cyclotomic fields, for example, about the ideal class groups; it is the first and simplest of a series of conjectures that link Iwasawa theory with key objects in number theory and arithmetic geometry, like totally real fields or elliptic curves, discussing arithmetic and analytical invariants. The analytic part is played by an L-function, seen as p-adic function, while the algebraic side concerns particular ideals built from modules over the Iwasawa algebra.

The proof that appears in this thesis is due to Karl Rubin, who in the appendix of Serge Lang's book [Lan90], following the pioneering work of Francisco Thaine ([Tha88]) and Victor Kolyvagin ([Kol90]), was able to give a much more simpler proof the conjecture, making hard use of Kolyvagin's *Euler systems*. These are collections of cohomology classes indexed on number fields that play a crucial role in number theory, since they can be used to derive fundamental information about Selmer groups. For example, some of the known results regarding the Birch and Swinnerton-Dyer conjecture have been proved using the Euler systems, and also other main conjectures can be approached with these objects. This is linked to a second goal of this work, maybe less evident but surely as much fundamental: to study in detail "stylish" tools of modern number theory, such as Euler systems, Selmer group, and p-adic representations. For example, these representations are one of the most successful way to deduce information about the explicit description of absolute Galois group of $\mathbf{Q}$, probably the most important problem in algebraic number theory. Precisely because of their importance, in this thesis these objects are introduced to the most general setting possible, despite the fact that in their application to the study of cyclotomic fields they appears in a much more accessible formulation.

The mathematics. Iwasawa theory is build around (cyclotomic) $\mathbf{Z}_p$-extensions of number fields. If p is an odd prime and $K = \mathbf{Q}(\boldsymbol{\mu}_p)$, the extension obtained adding to $\mathbf{Q}$ the p-th roots of unity, then we can consider the tower of fields

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup K_n,$$

with $K_n = \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})$ and $K_\infty = \mathbf{Q}(\boldsymbol{\mu}_{p^\infty})$. By Galois theory,

$$\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p.$$

We are interested mainly in the arithmetic of K, and the previous tower can be used exactly for this goal. If $\Gamma_n = \mathrm{Gal}(K_n/K) \cong \mathbf{Z}/p^n\mathbf{Z}$, we can define the Iwasawa algebra

$$\Lambda = \varprojlim_n \mathbf{Z}_p[\Gamma_n],$$

which is isomorphic to $\mathbf{Z}_p[[T]]$, the ring of formal power series in one variable T, with coefficients in $\mathbf{Z}_p$. This follows from the identification $\gamma \to 1 + T$, where γ is a topological generator of Γ. In this setting, by a classification theorem due to Serre, we can attach to every finitely generated torsion Λ-module M a well defined invariant, the characteristic ideal, denoted by $\mathrm{char}(M)$. The study of these kind of modules is another key part of this theory. If C_n is the p-part of the ideal class group of K_n, and $\bar{E}_n$ and V_n are particular p-adic objects obtained by respectively the global and cyclotomic units of K_n, the inverse limits under the norm maps

$$C_\infty = \varprojlim_n C_n, \quad E_\infty = \varprojlim_n \bar{E}_n, \quad V_\infty = \varprojlim_n V_n$$

give rise to well defined Λ-modules. If χ is an even p-adic character of $\Delta = \mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times$, we can consider their eigenspaces $C_\infty(\chi)$, $E_\infty(\chi)$, $V_\infty(\chi)$ under χ, and the main conjecture states that

$$\mathrm{char}(C_\infty(\chi)) = \mathrm{char}(E_\infty(\chi)/V_\infty(\chi)).$$

There are several different but equivalent formulations of this important result, and moving between them is possible due to some results in class field theory and in Kummer duality. The former version does not require the intervention of a p-adic L-function, since it is specific for Euler systems. These collections of classes are related to Selmer groups, objects obtained by a p-adic representation, after the choices of some local conditions on cohomology groups. In our case, a certain Selmer group has a strict relation with $C_\infty(\chi)$, being its Pontryagin dual. The information we can get using the Euler systems are just algebraic, at least in appearance. Indeed, if T is a free $\mathbf{Z}_p$-module of finite rank on which the absolute Galois group of $\mathbf{Q}$ acts continuously, and it satisfies suitable arithmetic conditions, then a discrete Selmer group associated to T is finite, and its length as $\mathbf{Z}_p$-module can be controlled by explicit algebraic bounds.

Organization. This work is divided in four Chapters.

In Chapter 1, we give all the preliminaries notions we will need during our path. After a brief review of class field theory, we deal with cohomology of profinite groups, fundamental tool in order to understand the definition of an Euler system. Then we work with $\mathbf{Z}_p$-extensions and Λ-modules, in particular with their relation with p-adic characters. These objects are protagonists of Iwasawa theory.

The aim of Chapter 2 is to introduce p-adic Galois representations and Selmer groups. In particular, we apply the general results of Chapter 1 to Galois groups, to define local and global cohomology group, from which derive the definition of a Selmer group. We also see how a well-known Selmer group, the one associated to an elliptic curve, is part of this general setting.

In Chapter 3 we give the definition of an Euler system, in the most possible general setting, and we give fundamental theorems about their relations with Selmer groups. Some of the results here are not proved, but as always, precise references and ideas are reported.

Finally, in Chapter 4, we state and prove the main conjecture. We do not use directly the results of Chapter 3, but instead we explicitly see how the cyclotomic Euler system allows use to show one of the two divisibility of this result. After the proof, we see which is the role of the Selmer group in the conjecture, and we state equivalent formulations and important consequences.

Contents

1 Preliminary results **1**
- 1.1 Class field theory 1
- 1.2 Continuous group cohomology 5
- 1.3 Cyclotomic fields 12
- 1.4 Characters and modules 16

2 Galois cohomology of p-adic representation **21**
- 2.1 p-adic Galois representations 21
- 2.2 Galois cohomology 24
- 2.3 Local cohomology groups 26
- 2.4 Global cohomology and Selmer groups 31

3 Euler systems **39**
- 3.1 Euler systems: definition 39
- 3.2 Results over K 42
- 3.3 Results over $\mathbf{Q}_\infty$ 45
- 3.4 Twisting by characters of finite order 48

4 Main conjecture **51**
- 4.1 Cyclotomic Euler system 51
- 4.2 The Main Conjecture 60
- 4.3 The proof 66
- 4.4 Equivalent formulations and consequences 70

Chapter 1

Preliminary results

We begin this dissertation introducing some prerequisites in number theory. These are mostly elementary and well-known results, but they are basic for the sequel. Also, we provide them without proofs, but always giving precise references.

1.1 Class field theory

Class field theory is the study of abelian extensions. It can be global, concerning global fields, like number fields, or local, regarding local fields. Despite the first developments of this theory were made via ideals, the most recent approach is to study local class field theory first, and then to apply the results to global fields, via ideles. However, for the aim of this work, we will deal just with "classical" class field theory for number fields, following mainly [Jan96] and [Cox13]. The other point of view can be found in [AT90] and [Neu99], while for local class field theory we cite [Iwa86].

For this Section, we fix K a number field, and we denote by $\mathcal{O}_K$ its ring of integers.

Definition 1.1. A *prime* or *place* of K is an equivalence class of nontrivial absolute values on K. The nonarchimedean equivalence classes are called *finite primes*, while the archimedean ones are called *infinite primes*.

Finite primes coincides with ordinary prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$, with absolute value induced by the $\mathfrak{p}$-adic valuation on K, denoted by $v_\mathfrak{p}$. Infinite primes are obtained by embeddings $\sigma\colon K \to \mathbf{C}$. There are two sorts of infinite primes: *real primes*, given by real embeddings, and *complex* primes, given by a pair of conjugate nonreal embeddings (see, for example, [Jan96]).

For $\mathfrak{p}$ prime, finite or infinite, we denote by $K_\mathfrak{p}$ the completion of K with respect to the topology defined by the prime. We remark that if $\mathfrak{p}$ is a real prime, $K_\mathfrak{p} \cong \mathbf{R}$, while if $\mathfrak{p}$ is complex, $K_\mathfrak{p} \cong \mathbf{C}$.

If L/K is an algebraic extension (it can be infinite) and v is a place of K, there is a notion of place of L *lying over* v, where a place of an infinite extension of $\mathbf{Q}$ is defined in the same way. We could talk about *decomposition group*, *inertia group*, and *ramification*, but we do not enter in details here. We refer mainly to [Neu99], but also to Appendix 2 of [Was97] and Chapter 8 of [Koc02], just remarking how *unramified* coincides with *trivial inertia*.

Definition 1.2. A *modulus* (or *cycle*) for K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})}$$

taken over all primes $\mathfrak{p}$ of K, such that:

- $n(\mathfrak{p}) \geq 0$, and $n(\mathfrak{p}) = 0$ for all but finitely many primes;
- $n(\mathfrak{p}) = 0$ for $\mathfrak{p}$ complex;
- $n(\mathfrak{p}) \leq 1$ for $\mathfrak{p}$ real.

A modulus can be seen as a formal product $\mathfrak{m}_0\mathfrak{m}_\infty$, where

$$\mathfrak{m}_0 = \prod_{\mathfrak{p} \text{ finite}} \mathfrak{p}^{n(\mathfrak{p})}$$

is the *finite part* of $\mathfrak{m}$, a nonzero integral ideal of $\mathcal{O}_K$, while

$$\mathfrak{m}_\infty = \prod_{\mathfrak{p} \text{ real}} \mathfrak{p}^{n(\mathfrak{p})}$$

is the *infinite part* of $\mathfrak{m}$, a formal squarefree product of real primes.

Definition 1.3. Let $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ be a modulus for a number field K.

- Let $I_K(\mathfrak{m})$ be the free abelian group generated by the prime ideals of $\mathcal{O}_K$ not dividing $\mathfrak{m}_0$.
- For $\alpha \in K^\times$, we say that $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$ if $v_\mathfrak{p}(\alpha - 1) \geq n(\mathfrak{p})$ for every $\mathfrak{p}$ finite prime in the factorization of $\mathfrak{m}_0$, and $\alpha > 0$ under every real embedding corresponding to the archimedean primes in $\mathfrak{m}_\infty$.
- Let $P_K(\mathfrak{m})$ be the group of principal fractional ideals generated by elements $\alpha \equiv^* 1 \pmod{\mathfrak{m}}$.

The quotient $C_K(\mathfrak{m}) = I_K(\mathfrak{m})/P_K(\mathfrak{m})$ is called *ray class group* mod $\mathfrak{m}$. It is a finite group ([Jan96], Chapter IV, Corollary 1.6).

Example 1.4.

- $C_K(\mathcal{O}_K) = C_K(1) = C_K$ is just the ideal class group of K.

- If $\mathfrak{m}_0 = \mathcal{O}_K$ and $\mathfrak{m}_\infty$ is the formal product of all the real embeddings, $C_K(\mathfrak{m})$ is called *narrow ideal class group*.
- $C_{\mathbf{Q}}(n\infty) \cong (\mathbf{Z}/n\mathbf{Z})^\times$.
- $C_{\mathbf{Q}}(n) \cong (\mathbf{Z}/n\mathbf{Z})^\times/\{\pm 1\}$.

Let L/K be a Galois extension of number fields. If $\mathfrak{p}$ is an unramified prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ a prime of $\mathcal{O}_L$ above it, there is a unique element of $\mathrm{Gal}(L/K)$ (actually lying in the decomposition group $D_{\mathfrak{P}}$), called *Frobenius* and denoted by $\mathrm{Fr}_{\mathfrak{P}}$, which is identified by the condition

$$\mathrm{Fr}_{\mathfrak{P}}(\alpha) \equiv \alpha^{|\mathcal{O}_K/\mathfrak{p}|} \pmod{\mathfrak{P}}, \quad \text{for all } \alpha \in \mathcal{O}_L.$$

If the extension is abelian (that is, the Galois group is abelian), this element does not depend on the primes above $\mathfrak{p}$, therefore we call it $\mathrm{Fr}_{\mathfrak{p}}$ (see, for example, [Mar18], Chapter 4).

Definition 1.5. If L/K is an abelian extension and $\mathfrak{m}$ is a modulus divisible by all ramified primes (finite and infinite), then the map

$$\begin{aligned} \varphi_{\mathfrak{m}} \colon I_K(\mathfrak{m}) &\longrightarrow \mathrm{Gal}(L/K) \\ \prod_{i=1}^{n} \mathfrak{p}_i^{n_i} &\longmapsto \prod_{i=1}^{n} \mathrm{Fr}_{\mathfrak{p}_i}^{n_i} \end{aligned}$$

is called *Artin map*. It is a surjective map ([Jan96], Chapter IV, Theorem 5.3).

Definition 1.6. A subgroup $H \subseteq I_K(\mathfrak{m})$ is called a *congruence subgroup* for $\mathfrak{m}$ if it satisfies

$$P_K(\mathfrak{m}) \subseteq H \subseteq I_K(\mathfrak{m}).$$

The quotient $I_K(\mathfrak{m})/H$ is called *generalized ideal class group* for $\mathfrak{m}$.

The important result is that generalized ideal class groups corresponds to the Galois groups of all the abelian extension of K, and the link is provided by the Artin map. The first step is the following:

Theorem 1.7 (Artin reciprocity theorem, [Jan96], Chapter V, Theorem 5.8)**.** *Let L/K be an abelian extension and $\mathfrak{m}$ a modulus divisible by all ramified primes of K. If the exponents of the finite primes in the factorization of $\mathfrak{m}$ are sufficiently large, then the kernel of the Artin map is a congruence subgroup. In particular,* $\mathrm{Gal}(L/K)$ *is isomorphic to a generalized ideal class group.*

We sure cannot hope that the modulus $\mathfrak{m}$ for which the kernel of $\varphi_{\mathfrak{m}}$ is a congruence subgroup is unique. For instance, if $\mathfrak{n}$ is a modulus such that $\mathfrak{m} \mid \mathfrak{n}$ (in the obvious sense), then also the kernel of $\varphi_{\mathfrak{n}}$ is a congruence

subgroup. But there is one modulus which is "better" than the others. The next Theorem summarizes part of [Jan96], Chapter V, Section 6 and Theorem 11.11.

Theorem 1.8. *Let L/K be an abelian extension. Then there is a modulus $\mathfrak{f} = \mathfrak{f}(L/K)$ such that*

(a) *$\mathfrak{f}$ is divided exactly by the ramified primes of K in L.*

(b) *If $\mathfrak{m}$ is a modulus divided by all ramified primes of K in L, then the kernel of $\varphi_{\mathfrak{m}}$ is a congruence subgroup for $\mathfrak{m}$ if and only if $\mathfrak{f} \mid \mathfrak{m}$.*

This modulus, uniquely determined by $K \subseteq L$, is called *conductor*. We are ready for the classification theorem:

Theorem 1.9 (Existence theorem, [Jan96], Chapter V, Theorem 9.9)**.** *Let $\mathfrak{m}$ be a modulus of K, and let H be a congruence subgroup for $\mathfrak{m}$. Then there exists a unique abelian extension L of K, all of whose ramified primes divide $\mathfrak{m}$, such that the kernel of the Artin map $\varphi_{\mathfrak{m}}$ is precisely H.*

The importance of this result is that we can construct abelian extensions with specified Galois group and restricted ramification.

Stated the basic theorems of class field theory, we can see the most important consequences. For $K = \mathbf{Q}$ and $\mathfrak{m} = m\infty$, we easily deduce the well-know *Kronecker-Weber theorem*:

Theorem 1.10 (Kronecker-Weber theorem, [Cox13], Theorem 8.8)**.** *If L is an abelian extension of $\mathbf{Q}$, then there exists a positive integer m such that L is contained in the cyclotomic field $\mathbf{Q}(\zeta_m)$, for ζ_m primitive m-th root of unity.*

Let $\mathfrak{m} = 1$. Since $P_K(1) = P_K$ is trivially a congruence subgroup, by the existence theorem there is a unique abelian unramified extension L of K such that

$$C_K \cong \mathrm{Gal}(L/K)$$

via the Artin map. L is called *Hilbert class field*.

Theorem 1.11 ([Cox13], Theorem 8.10)**.** *The Hilbert class field is the maximal unramified abelian extension of K.*

We can generalize this construction. Given a modulus $\mathfrak{m}$, there exists a unique abelian extension $K^{\mathfrak{m}}$ of K such that

$$C_K(\mathfrak{m}) \cong \mathrm{Gal}(K^{\mathfrak{m}}/K).$$

It is called *ray class field* mod $\mathfrak{m}$, and its ramified primes divide $\mathfrak{m}$.

Example 1.12.

- For $\mathfrak{m} = 1$, the ray class group $K^{\mathfrak{m}}$ is just the Hilbert class field.
- If $K = \mathbf{Q}$ and $\mathfrak{m} = n\infty$, then $K^{\mathfrak{m}} \cong \mathbf{Q}(\zeta_n)$.
- If $K = \mathbf{Q}$ and $\mathfrak{m} = n$, then $K^{\mathfrak{m}} \cong \mathbf{Q}(\zeta_n + \zeta_n^{-1}) = \mathbf{Q}(\zeta_n)^+$, the *maximal real subfield* of $\mathbf{Q}(\zeta_n)$.

We conclude giving a useful interpretation of the conductor: if L/K is an abelian extension, the conductor $\mathfrak{f}(L/K)$ is the minimal modulus $\mathfrak{m}$ such that L is contained in the ray class field $K^{\mathfrak{m}}$.

1.2 Continuous group cohomology

We recall the most important results about cohomology of topological group. These will be very useful in the following Chapters, in order to deal with Galois cohomology and p-adic representations. In fact, for us, the group G acting will be always a Galois group. However, in this Section, we put ourself in a more general setting, where G is profinite. We mainly follow [Wil98] and the appendix B of [Rub00]. A useful review may be found in [Tat76] in the most general possible setting: G is a topological group. Finally, two cornerstones for Galois cohomology are [Ser97] and [NSW08], which focus their attention mainly on discrete Galois modules.

Let G be a profinite group and A a topological G-module, that is, a topological abelian group with a continuous action of G, compatible with the abelian group structure. For every $n \in \mathbf{N}$, let $C^n = C^n(G, A)$ be the set of continuous maps $G^n \to A$, where G^0 is the trivial group, so $C^0 = A$. These sets are abelian groups in the obvious way, and their elements are called *n-cochains*. Let d^n be the homomorphism

$$d^n : C^n \to C^{n+1}$$

defined by

$$\begin{aligned} d^n(f)(\sigma_1, \dots, \sigma_{n+1}) &= \sigma_1 f(\sigma_2, \dots, \sigma_{n+1}) \\ &\quad + \sum_{i=1}^{n} (-1)^i f(\sigma_1, \dots, \sigma_i\sigma_{i+1}, \dots, \sigma_{n+1}) \\ &\quad + (-1)^{n+1} f(\sigma_1, \dots, \sigma_n). \end{aligned}$$

For all $n \geq 1$, $d^n \circ d^{n-1} = 0$, therefore $\mathrm{Im}(d^{n-1}) \subseteq \ker(d^n)$. In this way we get a complex $C^\bullet(G, A)$.

Definition 1.13. For $n \geq 0$, the *n-th continuous cohomology group* of G with coefficients in A is the quotient group

$$H^n(G, A) = \ker(d^n)/\operatorname{Im}(d^{n-1}),$$

where we set $\operatorname{Im}(d^{-1}) = 0$. Elements in $\ker(d^n)$ are called (continuous) *cocyles*, while elements of $\operatorname{Im}(d^{n-1})$ are called (continuous) *coboundaries*.

Despite being defined for every $n \geq 0$, the cohomology groups we are interested in are usually $H^n(G, A)$ with $n = 0, 1$. We can give a more explicit description for them:

$$H^0(G, A) = \{a \in A \mid \sigma a = a \text{ for all } \sigma \in G\} = A^G;$$
$$H^1(G, A) = \frac{\{f\colon G \to A \text{ continuous} \mid f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \text{ for all } \sigma, \tau \in G\}}{\{f\colon G \to A \mid f(\sigma) = \sigma a - a \text{ for a fixed } a \in A\}}.$$

Remark 1.14. When the action of G on A is trivial, $H^0(G, A) = A$ and $H^1(G, A) = \operatorname{Hom}(G, A)$, where the homomorphisms between topological groups are always assumed to be continuous.

Let A be a G-module and A' a G'-module, with G, G' profinite groups. Given two continuous homomorphisms

$$\varphi\colon G' \to G, \qquad f\colon A \to A',$$

we say that φ and f are *compatible* if $f(\varphi(\sigma')a) = \sigma' f(a)$ for all $a \in A$, $\sigma' \in G'$. From this pair of maps, we can get canonical homomorphisms

$$H^n(G, A) \to H^n(G', A')$$

(see [Wil98], Lemma 9.2.1). The first important example occurs when we consider the identity $\mathrm{Id}\colon G \to G$ and a G-module homomorphism $f\colon A \to B$, that is a continuous group homomorphism compatible with the action of G. In this case, we get

$$H^n(G, A) \to H^n(G, B).$$

In particular, given a short exact sequence of G-modules, we would like to have a corresponding long exact sequence of cohomology groups. This is always true for discrete modules. However, for the general case, we need to add more restrictive hypothesis on the sequence:

Definition 1.15. An exact sequence $0 \to A \to B \to C \to 0$ of abelian topological groups is called *well-adjusted* if the map $A \to B$ induces an homeomorphism from A to its image, and there is a continuous section of $B \to C$ (not necessarily a homomorphism).

Clearly all short exact sequence of discrete topological groups are well-adjusted, and this is also true for short exact sequences of profinite groups ([Wil98], Lemma 0.1.2 and Proposition 1.3.3).

Theorem 1.16 ([Wil98], Theorem 9.3.3)**.** *To each well-adjusted short exact sequence*

$$0 \to A \to B \to C \to 0$$

of G-modules there corresponds a long exact sequence

$$\begin{aligned} 0 \to & A^G \to B^G \to C^G \to H^1(G, A) \to \cdots \\ & \cdots \to H^n(G, B) \to H^n(G, C) \to H^{n+1}(G, A) \to \cdots \end{aligned}$$

of cohomology groups.

We will always use cohomology groups in situations in which the hypothesis is satisfied. For example, when A is an open submodule of B and $C = B/A$ is the quotient module with the quotient topology, which is discrete.

We see other important examples of compatible maps:

- Let $\varphi\colon H \to G$ be the inclusion and $f\colon A \to A$ be the identity, where H is a subgroup of G. We get a *restriction* homomorphism:

$$\mathrm{res} : H^n(G, A) \to H^n(H, A).$$

- Let H be a normal subgroup. If $\varphi\colon G \to G/H$ is the projection and $f\colon A^H \to A$ the inclusion, we get an *inflation* homomorphism:

$$\mathrm{inf} : H^n(G/H, A^H) \to H^n(G, A).$$

- If H is a normal subgroup of G and $\sigma \in G$, we can consider $\varphi\colon H \to H$, $\tau \mapsto \sigma^{-1}\tau\sigma$ and $f\colon A \to A$, $a \to \sigma a$. We denote by $\bar{\sigma}$ the map we get:

$$\bar{\sigma}\colon H^n(H, A) \to H^n(H, A).$$

  One can show (see for example [Wil98], Lemma 10.2.4 for the discrete case) that from this map we can give to $H^n(H, A)$ the structure of G/H-module, and that the image of $\mathrm{res}\colon H^n(G, A) \to H^n(H, A)$ is in $H^n(H, A)^{G/H}$.

This homomorphisms are part of an important exact sequence:

Proposition 1.17 ([Rub00], Appendix B, Proposition 2.5)**.** *Let H be a closed, normal subgroup of G.*

(a) *There is an inflation-restriction exact sequence*

$$0 \to H^1(G/H, A^H) \to H^1(G, A) \to H^1(H, A).$$

(b) *Suppose moreover that p is a prime and for every G-module (resp. H-module) S of finite, p-power order, $H^1(G,S)$ and $H^2(G,S)$ (resp. $H^1(H,S)$) are finite. If A is discrete, or A is a finitely generated Z_p-module, or A is a finite-dimensional $\mathbf{Q}_p$-vector space, then there is a* Hochschild-Serre *exact sequence extending the previous one:*

$$0 \to H^1(G/H, A^H) \to H^1(G,A) \to H^1(H,A)^{G/H} \to$$
$$\to H^2(G/H, A^H) \to H^2(G,A).$$

In order to apply this Proposition, we need to check if a group G has the property that $H^n(G,S)$ is finite for every G-module S of finite, p-power order. Before seeing an helpful Proposition in this sense, we briefly recall an important construction in group theory and number theory, following mainly [NSW08]. Let A be a locally compact abelian group, that is, an abelian topological group whose topology is Hausdorff and locally compact (for example, a discrete group or a compact group).

Definition 1.18. The *Pontryagin dual* of A is the group

$$A^\vee = \mathrm{Hom}(A, \mathbf{R}/\mathbf{Z}),$$

with the compact-open topology.

If A is profinite or discrete torsion, then

$$A^\vee = \mathrm{Hom}(A, \mathbf{Q}/\mathbf{Z}),$$

while if A is pro-p or discrete p-torsion (for example, a finitely generated $\mathbf{Z}_p$-module), then

$$A^\vee = \mathrm{Hom}(A, \mathbf{Q}_p/\mathbf{Z}_p).$$

Finally, if A is a topological G-module, then also $A^\vee$ has a natural structure of G-module: for $g \in G$, $f \in A^\vee$ and $a \in A$,

$$(g \cdot f)(a) = f(g^{-1}a).$$

Theorem 1.19 (Pontryagin Duality, [NSW08], Theorem 1.1.11)**.** *If A is a locally compact abelian group, then the same is true for $A^\vee$ with the compact-open topology. The canonical homomorphism*

$$A \to (A^\vee)^\vee$$

is an isomorphism of groups. Therefore $\vee$ defines a contravariant functor on the category of abelian locally compact groups which commutes with limits. In addiction, $\vee$ induces equivalences of categories

$$\text{abelian compact groups} \overset{\vee}{\iff} \text{discrete abelian groups},$$
$$\text{abelian profinite groups} \overset{\vee}{\iff} \text{discrete abelian torsion groups}.$$

Definition 1.20. A $\mathbf{Z}_p$-module is *cofinitely generated* if its Pontryagin dual is finitely generated.

The following Proposition is well-known by class field theory for $n = 1$. Note that if A is a G-module which is also a $\mathbf{Z}_p$-module, then the group $H^n(G, A)$ is a $\mathbf{Z}_p$-module in a natural way.

Proposition 1.21 ([Rub00], Appendix B, Proposition 2.7)**.** *Suppose that one of the following holds:*

- *K is a global field, K_S is a Galois extension unramified outside a finite set off places of K and $G = \mathrm{Gal}(K_S/K)$;*
- *K is a local field and $G = G_K$;*
- *K is a local field of residue characteristic different from p, and G is the inertia subgroup of G_K.*

If A is a G-module which is finite (resp. finitely generated over $\mathbf{Z}_p$, resp. cofinitely generated over $\mathbf{Z}_p$) and $n \geq 0$, then $H^n(G, A)$ is finite (resp. finitely generated over $\mathbf{Z}_p$, resp. cofinitely generated over $\mathbf{Z}_p$).

There is a last relevant map, which cannot be obtained by compatible homomorphisms. It is the *corestriction*:

$$\mathrm{cor}\colon H^n(H, A) \to H^n(G, A),$$

with H open subgroup of G (recall that an open subgroup of a profinite group is closed and has finite index). For an explicit construction we refer to [Tat76] or [NSW08]. We just underline that it is a transitive map (for example, [NSW08], Chapter I), and when $n = 0$, it is just the trace or norm map:

$$\begin{aligned} \mathrm{cor}\colon A^H &\to A^G \\ a &\mapsto \sum_{\sigma \in R} \sigma a, \end{aligned}$$

where R is a representative of the left cosets of H in G. The following result, proved in [NSW08] just in the discrete case, but easily generalizable, allows us to work explicitly with corestriction also at level $n = 1$:

Proposition 1.22 ([NSW08], Proposition 1.5.2)**.** *The corestriction map is functorial in the G-module considered, and it commutes with the connecting homomorphisms. That is, given a well-adjusted short exact sequence of G-modules*

$$0 \to A \to B \to C \to 0,$$

the following diagram is commutative:

$$\begin{array}{ccc} H^n(H,C) & \longrightarrow & H^{n+1}(H,A) \\ \downarrow{\scriptstyle \mathrm{cor}} & & \downarrow{\scriptstyle \mathrm{cor}} \\ H^n(G,C) & \longrightarrow & H^{n+1}(G,A). \end{array}$$

The same result is true for every pair of compatible maps ([Wil98], Theorem 9.3.4).

Remark 1.23. If G is finite and A is discrete, we can forget about topology and we get the "classical" cohomology groups (see, for example, [Ser79]). But this is not enough for us, since the group acting will be the Galois group of an (infinite) Galois extension. Also, A will not always be discrete: it can be a finitely generated $\mathbf{Z}_p$-module or a finite-dimensional $\mathbf{Q}_p$-vector space, both with the natural p-adic topology. However, the following propositions show us how to reduce to simpler cases.

Let G be a profinite group and A a G-module.

Theorem 1.24 ([Wil98], Theorem 9.7.2 and Theorem 9.7.3)**.** *Suppose A is discrete.*

(a) *If $A = \varinjlim B$, then there is an isomorphism*

$$H^n(G,A) \cong \varinjlim H^n(G,B).$$

(b) *There is an isomorphism*

$$H^n(G,A) \cong \varinjlim_{U} H^n(G/U, A^U),$$

where U runs through the open normal subgroups of G.

Proposition 1.25 ([Tat76], Corollary 2.2 and [Rub00], Appendix B, Proposition 2.3)**.** *Suppose $n > 0$ and $A = \varprojlim A_i$, where each A_i is a finite (discrete) G-module. If $H^{n-1}(G, A_i)$ is finite for every i, then*

$$H^n(G,A) = \varprojlim_{i} H^n(G,A_i).$$

If A is a finitely generated $\mathbf{Z}_p$-module, tensoring it over $\mathbf{Z}_p$ with the exact sequence $0 \to \mathbf{Z}_p \to \mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p \to 0$, we get

$$0 \to A \to V \to W \to 0,$$

with V finite-dimensional $\mathbf{Q}_p$ vector space, A open compact subgroup and W discrete divisible torsion group. We denote by A_{div} the maximal divisible subgroup.

Proposition 1.26 ([Tat76], Proposition 2.3 and [Rub00], Appendix B, Proposition 2.4)**.** *In the long exact sequence in cohomology associated to*

$$0 \to A \to V \to W \to 0,$$

the kernel of the connecting homomorphism

$$H^{n-1}(G, W) \to H^n(G, A)$$

is $H^{n-1}(G, W)_{\mathrm{div}}$*, and its image is* $H^n(G, A)_{\mathrm{tors}}$*. In addiction,* $H^n(G, A)$ *has no divisible elements and there is an isomorphism*

$$H^n(G, A) \otimes \mathbf{Q}_p \cong H^n(G, A \otimes \mathbf{Q}_p).$$

We conclude this Section recalling an important operation between cohomology groups.

Definition 1.27. Given G-modules A, A' and B, a map

$$A \times A \xrightarrow{b} B$$

is a *G-pairing* if it is bi-additive and it respects the action of G:

$$b(\sigma a, \sigma a') = \sigma b(a, a')$$

for all $\sigma \in G$, $a \in A$, $a' \in A'$.

Such a pairing induces a map

$$\cup\colon C^r(G, A) \times C^s(G, A') \to C^{r+s}(G, B)$$

as follows: given $f \in C^r(G, A)$ and $f' \in C^r(G, A')$, the cochain

$$f \cup f' \in C^{r+s}(G, A)$$

is defined to be

$$(f \cup f')(\sigma_1, \dots, \sigma_{r+s}) = b(f(\sigma_1, \dots, \sigma_r), \sigma_1 \dots \sigma_r f'(\sigma_{r+1}, \dots, \sigma_{r+s})).$$

By the rule

$$d^{r+s}(f \cup f') = d^r(f) \cup f' + (-1)^r f \cup d^s(f'),$$

this map yields a bilinear *cup product*, again denoted by $\cup$:

$$\cup\colon H^r(G, A) \times H^s(G, A') \to H^{r+s}(G, B).$$

1.3 Cyclotomic fields

The goal of this Section is to work with cyclotomic fields, in order to have all the instruments to state and prove the main conjecture. In particular, we investigate the relation between cyclotomic fields and Iwasawa theory, introducing $\mathbf{Z}_p$-extensions and modules over the Iwasawa algebra. All these results may be found in [Was97] and in [Lan90]. Also, some results about modules are taken by [Lan02]. Finally, we have to cite the pioneering work of Iwasawa in [Iwa73].

Definition 1.28. Let K be a number field. A $\mathbf{Z}_p$-*extension* of K is a Galois extension K_∞/K with Galois group $\mathrm{Gal}(K_\infty/K)$ isomorphic to the additive group of p-adic integers $\mathbf{Z}_p$.

Every number field K has at least one $\mathbf{Z}_p$-extension, the *cyclotomic* $\mathbf{Z}_p$-*extension*. It is obtained by an appropriate subfield of $K(\boldsymbol{\mu}_{p^\infty})$, where

$$\boldsymbol{\mu}_{p^\infty} = \bigcup_n \boldsymbol{\mu}_{p^n}$$

is the union of all the p-power roots of unity contained in a fixed algebraic closure $\overline{K}$, in the following way: if p is odd (just to simplify the notation), let $\zeta_{p^{n+1}}$ be a primitive p^{n+1}-th root of unity. We consider $K = \mathbf{Q}$ first. Since

$$\mathrm{Gal}(\mathbf{Q}(\zeta_{p^{n+1}})/\mathbf{Q}) \cong (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times \cong (\mathbf{Z}/p\mathbf{Z})^\times \times \mathbf{Z}/p^n\mathbf{Z},$$

we can define $\mathbf{Q}_n$ to be the fixed field of $(\mathbf{Z}/p\mathbf{Z})^\times$ in $\mathbf{Q}(\zeta_{p^{n+1}})$, to get

$$\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \cong \mathbf{Z}/p^n\mathbf{Z}.$$

Then $\mathbf{Q}_\infty = \bigcup_n \mathbf{Q}_n$ is a field with the desired property:

$$\mathrm{Gal}(\mathbf{Q}_\infty/\mathbf{Q}) \cong \varprojlim_n \mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q}) \cong \varprojlim_n \mathbf{Z}/p^n\mathbf{Z} \cong \mathbf{Z}_p.$$

By Kronecker-Weber theorem (Theorem 1.10) and ramification considerations, this is the unique $\mathbf{Z}_p$-extension of $\mathbf{Q}$. If K is a number field, it is enough to consider $K_\infty = K\mathbf{Q}_\infty$.

Note that we can always regard a $\mathbf{Z}_p$-extension of a number field K as a tower of fields

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_n K_n,$$

with

$$\mathrm{Gal}(K_n/K) \cong \mathbf{Z}/p^n\mathbf{Z},$$

since the nontrivial closed subgroups of $\mathbf{Z}_p$ are of the form $p^n\mathbf{Z}_p$ for some n. In particular, $[K_n : K] = p^n$ for all n.

The following proposition summarizes the behaviour of primes in a $\mathbf{Z}_p$-extension.

Proposition 1.29 ([Was97], Proposition 13.2 and Lemma 13.3)**.** *Let K_∞/K be a $\mathbf{Z}_p$-extension.*

(a) *K_∞/K is* unramified outside p*, which means that it is unramified at every prime (possibly infinite) not lying above p.*

(b) *At least one prime ramifies, and there exists $n \geq 0$ such that every prime ramified in K_∞/K_n is totally ramified.*

We move now our attention to Λ-modules.

Definition 1.30. Let G be a profinite group. The *Iwasawa algebra* $\Lambda(G)$ is the inverse limit of the group rings $\mathbf{Z}_p[G/N]$, where N runs through the open normal subgroups of G:

$$\Lambda(G) = \varprojlim \mathbf{Z}_p[G/N].$$

We are interested in the case when G is isomorphic to $\mathbf{Z}_p$. We underline how this results may be extended taking, instead of $\mathbf{Z}_p$, the ring of integers $\mathcal{O}$ of a field K, with $K/\mathbf{Q}_p$ finite extension. We simplify the notation setting $\Lambda = \Lambda(G)$. If, for example, G is the Galois group of the $\mathbf{Z}_p$-extension

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup_n K_n,$$

then

$$\Lambda = \Lambda(G) = \varprojlim_n \mathrm{Gal}(K_n/K).$$

Theorem 1.31 ([Was97], Theorem 7.1)**.** *Λ is isomorphic to $\mathbf{Z}_p[[T]]$, the ring of formal power series with coefficients in $\mathbf{Z}_p$. The isomorphism is induced by $\gamma \mapsto 1 + T$, where γ is a topological generator of $G \cong \mathbf{Z}_p$.*

Our aim is to describe the ring $\Lambda = \mathbf{Z}_p[[T]]$ and to give a structure theorem for modules over it.

Definition 1.32. A nonconstant polynomial $P(T) \in \Lambda$ is called *distinguished* if $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0$ with $p \mid a_i$ for all $i \in \{0, \ldots, n-1\}$.

Using the *p-adic Weierstrass preparation theorem* ([Was97], Theorem 7.3) and a division algorithm on Λ ([Was97], Lemma 7.5), one can show that Λ is a unique factorization domain. Its irreducible elements are p and the irreducible distinguished polynomials, while units are power series with constant term in $\mathbf{Z}_p^\times$.

Proposition 1.33 ([Was97], Proposition 13.9)**.** *The prime ideals of Λ are 0, (p), (p, T) and the ideals $(P(T))$ for $P(T) \in \Lambda$ irreducible distinguished polynomial. Λ is a local ring, with unique maximal ideal (p, T).*

Since $\mathbf{Z}_p$ is Noetherian, also Λ is Noetherian ([Lan02], Chapter IV, Theorem 9.4). Summarizing, Λ is:

- an unique factorization domain;
- Noetherian;
- local.

Definition 1.34. We say that two Λ-modules M and N are *pseudo-isomorphic* (or *quasi-isomorphic*) if there exists a homomorphism $M \to N$ with finite kernel and cokernel. In other words, M and N sit in an exact sequence of Λ-modules

$$0 \to A \to M \to N \to B \to 0$$

with A and B finite Λ-modules.

We write $M \sim N$ for two pseudo-isomorphic Λ-modules M and N. Note that this relation is not symmetric in general: for example, $(p, T) \sim \Lambda$ but $\Lambda \not\sim (p, T)$. But if M and N are two finitely generated torsion Λ-modules, then $M \sim N$ if and only if $N \sim M$. Now we can state the structure theorem, due to Serre, classifying finitely generated Λ-modules up to pseudo-isomorphism.

Theorem 1.35 ([Was97], Theorem 13.12)**.** *Let M be a finitely generated Λ-module. Then*

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

where r, s, t, n_i and m_j are integers and $f_j(T)$ are distinguished and irreducible polynomial.

This factorization is uniquely determined by M ([Was97], Corollary 15.19). We observe that this result is analogue to the structure theorem for modules over principal ideal domain (see [Lan02], Chapter III, Theorems 7.2 and 7.7), except that here we work with pseudo-isomorphisms. In fact, also the proof is similar, based on row and column operations.

The following deep result, known as *Iwasawa's theorem* is proved making hard use of the structure theorem stated above.

Theorem 1.36 (Iwasawa's theorem, [Was97], Theorem 13.13)**.** *Let K_∞/K be a $\mathbf{Z}_p$-extension. For every n, let p^{e_n} be the order of the p-part of the ideal class group of K_n. There there exist integers $\lambda \geq 0$, $\mu \geq 0$ and ν, all independent of n, and an integer n_0 such that, for all $n \geq n_0$,*

$$e_n = \lambda n + \mu p^n + \nu.$$

We will work mainly with finitely generated torsion Λ-modules, which are pseudo-isomorphic to *elementary modules* of the form

$$E = \bigoplus_{i=1}^{n} \Lambda/(f_i),$$

with $f_i \in \Lambda$. A priori, these elements are not well-defined. They are if we take f_i to be powers of distinguished polynomials or powers of p. However, we can associate to every finitely generated torsion Λ-module a well-defined invariant:

Definition 1.37. The *characteristic ideal* of a finitely generated torsion Λ-module M is the ideal generated by $\prod_{i=1}^{n} f_i$, where

$$M \sim \bigoplus_{i=1}^{n} \Lambda/(f_i).$$

We denote it by $\mathrm{char}(M)$:

$$\mathrm{char}(M) = \left(\prod_{i=1}^{n} f_i \right) \Lambda.$$

Remark 1.38. This ideal is defined for torsion modules, since this is really the case in which it has great utility. However, one can extend the definition to every finitely generated Λ-modules, in two different ways: if M is a finitely generated not torsion Λ-module, then $\mathrm{char}(M) = 0$ (as in [Rub00], Section 2.3) or $\mathrm{char}(M) = \mathrm{char}(M_{\mathrm{tors}})$ (as in [Was97]). In any case, the next results hold.

Lemma 1.39 ([Was97], Lemma 15.17)**.** *Let M be a finitely generated torsion Λ-module.*

(a) $\mathrm{char}(M) \cdot M$ *is finite.*

(b) *If M is also finite, then $(p, T)^n M = 0$ for n large enough. Therefore the annihilator of a finite Λ-module has finite index in Λ.*

Proposition 1.40 ([Was97], Proposition 15.22)**.** *If*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

is an exact sequence of finitely generated (torsion) Λ-modules, then

$$\mathrm{char}(M_1) \cdot \mathrm{char}(M_3) = \mathrm{char}(M_2).$$

Note that if M is a finite Λ-module, then $M \sim 0$, so $\mathrm{char}(M) = 1$. This follows from the next useful Lemma:

Lemma 1.41 ([Was97], Lemma 13.10)**.** *If $f \in \Lambda$ is not a unit, then $\Lambda/f\Lambda$ is infinite.*

We deduce that if $M_1 \sim M_2$, then

$$\mathrm{char}(M_1) = \mathrm{char}(M_2).$$

1.4 Characters and modules

For this last part of the first Chapter, we put ourself in the setting of the main conjecture, to have all the descriptions we need to understand and prove this result. We follow again [Lan90] and [Was97].

The $\mathbf{Z}_p$-extension we will work with is the following: fix $K = K_0 = \mathbf{Q}(\boldsymbol{\mu}_p)$, for p odd prime, and $K_\infty = \mathbf{Q}(\boldsymbol{\mu}_{p^\infty})$. Then K_∞/K is a $\mathbf{Z}_p$-extension, and for all n, $K_n = \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})$. We have $\Gamma_n = \mathrm{Gal}(K_n/K)$, $\Gamma = \mathrm{Gal}(K_\infty/K) = \varprojlim \Gamma_n$. If we denote as Δ the Galois group of $K/\mathbf{Q}$, then

$$\begin{aligned} \mathrm{Gal}(K_\infty/\mathbf{Q}) &\cong \Delta \times \Gamma, \\ \mathrm{Gal}(K_n/\mathbf{Q}) &\cong \Delta \times \Gamma_n. \end{aligned}$$

This means that every $\mathrm{Gal}(K_\infty/\mathbf{Q})$-module is also a Δ-module in a natural way (and also this is true for every $\mathrm{Gal}(K_n/\mathbf{Q})$-module). The importance of this fact is that we will not work directly with Λ-modules, but with their χ-components, where χ is a p-adic Dirichlet character of Δ. We give now some information about this construction.

Let χ be a p-adic character of $\Delta \cong (\mathbf{Z}/p\mathbf{Z})^\times$: a continuous homomorphism

$$\chi \colon (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{Z}_p^\times.$$

Since $(\mathbf{Z}/p\mathbf{Z})^\times$ is cyclic of order $p-1$, there are exactly $p-1$ characters, and this makes sense since by *Hensel lemma* ([Neu99], Chapter II, Lemma 4.6), $\mathbf{Z}_p$ contains exactly $p-1$ distinct $p-1$-th roots of unity, so $\boldsymbol{\mu}_{p-1} \subseteq \mathbf{Z}_p$. There is a character which has an important role: the *Teichmüller character*, denoted by ω. It is the character defined by the condition

$$\omega(a) \equiv a \pmod{p},$$

for every $a \in (\mathbf{Z}/p\mathbf{Z})^\times$. In fact, the group of p-adic characters $\hat{\Delta}$ of $\Delta \cong (\mathbf{Z}/p\mathbf{Z})^\times$ is generated by ω:

$$\hat{\Delta} = \{\omega^i \mid i \in \{0, \dots, p-2\}\}.$$

In particular, $\omega^0 = 1$ is the trivial character, the even powers are the even characters ($\chi(-1) = 1$) and the odd powers are the odd characters ($\chi(-1) = -1$). For every $\chi \in \hat{\Delta}$, since $p-1$ in invertible in $\mathbf{Z}_p$, we can consider

$$e(\chi) = \frac{1}{p-1} \sum_{\delta \in \Delta} \chi^{-1}(\delta)\delta \in \mathbf{Z}_p[\Delta].$$

It is just a matter of computation to verify that $e(\chi)$ satisfies the following properties:

- $e(\chi)^2 = e(\chi)$;

- $e(\chi)e(\psi) = 0$ if $\chi \neq \psi$;
- $1 = \sum_{\chi \in \hat{\Delta}} e(\chi)$;
- $e(\chi)\sigma = \chi(\sigma)e(\chi)$.

These elements are called the *orthogonal idempotent* of $\mathbf{Z}_p[\Delta]$. If M is a $\mathbf{Z}_p[\Delta]$-module, then we can write

$$M = \bigoplus_{\chi \in \hat{\Delta}} M(\chi),$$

where

$$M(\chi) = e(\chi)M = \{m \in M \mid \delta m = \chi(\delta)m \text{ for all } \delta \in \Delta\}.$$

We will consider Λ-modules which are also $\mathbf{Z}_p[\Delta]$-modules, and we will take their χ-components, which will be again Λ-modules. Note that since Λ is Noetherian, every finitely generated Λ-modules is Noetherian, therefore if M is a $\mathbf{Z}_p[\Delta]$-module which is finitely generated and torsion as Λ-module, then $M(\chi)$ is also finitely generated and torsion.

In what follows, we fix γ a topological generator of Γ. Let C_n denotes the p-part of the ideal class group of K_n. Then we have surjective maps

$$C_{n+1} \to C_n$$

given by the norm maps between ideal class groups. One way to build a Λ-module is to consider the inverse limits of $\mathbf{Z}_p[\Gamma_n]$-modules M_n, with homomorphisms

$$M_{n+1} \to M_n$$

compatible with the action of the group rings $\mathbf{Z}_p[\Gamma_{n+1}]$ and $\mathbf{Z}_p[\Gamma_n]$. This is precisely the case and the next Theorem holds:

Theorem 1.42 ([Lan90], Chapter 5, Theorems 4.1 and 4.4)**.** *The Λ-module*

$$C_\infty = \varprojlim C_n$$

is a finitely generated torsion Λ-module, and there is an isomorphism

$$C_\infty/(\gamma^{p^n} - 1)C_\infty \cong C_n.$$

We will also work with $A_\infty = \varinjlim C_n$, where the limit is taken under the natural maps

$$C_n \to C_{n+1}.$$

There is a fundamental relation between these two objects:

Theorem 1.43 ([Iwa73], Theorem 11)**.** *There is a pseudo-isomorphism*

$$C_\infty \sim \mathrm{Hom}(A_\infty, \mathbf{Q}_p/\mathbf{Z}_p).$$

Let us now consider Ω_n, the maximal abelian p-extension of K_n unramified outside p. Denote by X_n the Galois group of Ω_n/K_n. We will work mostly with

$$X_\infty = \mathrm{Gal}(\Omega_\infty/K_\infty).$$

It has a natural structure of Λ-module (Γ acts via conjugation), and

Theorem 1.44 ([Lan90], Chapter 5, Theorem 6.1)**.** *The Λ-module X_∞ is finitely generated.*

When χ is even and nontrivial, $X_\infty(\chi)$ is also torsion (see the final Remark in [Lan90], Section 7.5), and one can repeat the proof of Theorem 1.42 to deduce that

$$X_\infty/(\gamma^{p^n} - 1)X_\infty \cong X_n.$$

Denote by $K_{n,p} = \mathbf{Q}_p(\boldsymbol{\mu}_{p^{n+1}})$ the completion of K_n with respect to the unique prime above p. If $\mathfrak{p}_n$ is the maximal ideal, then define U_n to be the group of units congruent to 1 modulo $\mathfrak{p}_n$, that is, the group of principal units. Then we can consider the inverse limit under the norm maps

$$U_\infty = \varprojlim U_n,$$

which is both a $\mathbf{Z}_p$-module and a Λ-module, since for every n,

$$\Gamma_n = \mathrm{Gal}(K_n/K) = \mathrm{Gal}(K_{n,p}/K_p)$$

(this is [Neu99], Proposition 7.13).

Theorem 1.45 ([Lan90], Chapter 7, Theorem 2.1)**.** *For every nontrivial character $\chi \neq \omega$ of Δ,*

$$U_\infty(\chi) \cong \Lambda,$$

that is, it is free of dimension 1 over Λ.

Theorem 1.46. *For $\chi \neq 1$, there is an isomorphism*

$$U_\infty(\chi)/(\gamma^{p^n} - 1)U_\infty(\chi) \cong U_n(\chi).$$

Before introducing the final modules, we need to recall the notion of *cyclotomic unit*. If $n \not\equiv 2 \pmod 4$ and ζ_n denotes a primitive n-th root of unity, we can consider

$$\mathcal{E}_n = E_n \cap E'_n,$$

where E_n is the group of units of $\mathbf{Q}(\zeta_n)$ and E'_n is the multiplicative group generated by

$$\{\pm\zeta_n, 1 - \zeta_n^a \mid 1 \leq a \leq n-1\}.$$

$\mathcal{E}_n$ is called the group of cyclotomic units of $\mathbf{Q}(\zeta_n)$. When K is an abelian number field with group of units E_K, we can take the minimal $n \not\equiv 2 \pmod 4$ such that $K \subseteq \mathbf{Q}(\zeta_n)$ and define $\mathcal{E}_K = \mathcal{E}_n \cap E_K$. In particular, this works well for $\mathbf{Q}(\zeta_n)^+$. When n is the power of an odd prime p, the cyclotomic units have an important property, due to Hasse:

Theorem 1.47 ([Was97], Theorem 8.2)**.** *Let p be an odd prime and $m \geq 1$. Then the cyclotomic units $\mathcal{E}^+_{p^m}$ of $\mathbf{Q}(\zeta_{p^m})^+$ have finite index in the full unit group $E^+_{p^m}$, and this index is the class number $h^+_{p^m}$ of $\mathbf{Q}(\zeta_{p^m})^+$.*

Define now E_n and $\mathcal{E}_n$ to be the global units and the cyclotomic units of K_n. Take $\bar{E}_n$ and V_n to be the closure of their intersection with U_n, in U_n. Then we can consider ([Lan90], Section 6.5) the well-defined inverse limit under the norm maps:

$$E_\infty = \varprojlim \bar{E}_n,$$
$$V_\infty = \varprojlim V_n.$$

These objects have both natural the structures of $\mathbf{Z}_p[\Delta]$ and Λ-modules. Then the following results hold.

Theorem 1.48 ([Lan90], Chapter 7, Theorem 5.1)**.** *If χ is a nontrivial even character, then $V_\infty(\chi)$ is free of rank one over Λ, and there is an isomorphism*

$$V_\infty(\chi)/(\gamma^{p^n} - 1)V_\infty(\chi) \cong V_n(\chi).$$

Theorem 1.49 ([Lan90], Chapter 7, Theorem 5.2)**.** *If χ is a nontrivial even character, then $U_\infty(\chi)/V_\infty(\chi)$ is torsion.*

We will discuss more about this fact in Section 4.4, since the generator of the characteristic ideal of $U_\infty(\chi)/V_\infty(\chi)$ has a strict relation with a p-adic L-function. In addiction, if χ is even and nontrivial, then also $E_\infty(\chi)/V_\infty(\chi)$ is torsion. The same is true for χ trivial, by the following

Proposition 1.50 ([Was97], Proposition 15.43)**.** *If $\chi = 1$ then for every n, $\bar{E}_n(\chi)/V_n(\chi)$ and $C_n(\chi)$ are trivial.*

All these modules are part of an important exact sequence, which relies in the adelic formulation of class field theory, in particular in this fundamental result:

Theorem 1.51 ([Lan90], Chapter 5, Theorem 5.1)**.** *For every n, if H_n is the p-Hilbert class field of K_n, then*

$$\mathrm{Gal}(\Omega_n/H_n) \cong U_n/\bar{E}_n.$$

From this, we get the exact sequence

$$0 \to U_n/\bar{E}_n \to X_n \to C_n \to 0,$$

and taking limits and χ-components, for χ is even and nontrivial, we derive

$$0 \to U_\infty(\chi)/E_\infty(\chi) \to X_\infty(\chi) \to C_\infty(\chi) \to 0.$$

Here we are using that finite abelian group satisfy the *Mittag-Leffler condition* (see [Wei94], Section 3.5), therefore the inverse limit functor is exact.

We shall rewrite this sequence as

$$0 \to E_\infty(\chi)/V_\infty(\chi) \to U_\infty(\chi)/V_\infty(\chi) \to X_\infty(\chi) \to C_\infty(\chi) \to 0, \qquad (1.1)$$

since the relation between $U_\infty(\chi)/V_\infty(\chi)$ and a p-adic L-function, and $E_\infty(\chi)/V_\infty(\chi)$ explicitly appears in the statement of the main conjecture. In fact, this sequence will allow us to easily move between different formulations of the principal result.

Chapter 2

Galois cohomology of p-adic representation

In this Chapter, following [Rub00], we introduce the objects we are mainly interested in: p-adic representations of Galois groups, the cohomology groups associated, and Selmer groups. After some general definitions, we apply the results of Section 1.2 for G being a Galois group, then we introduce local conditions for the cohomology groups, in order to define what a Selmer group is. One example to have clear in mind is the Tate module of an elliptic curve over a number field. We refer to [Sil09] and [Gre99] for the theory of elliptic curves.

2.1 p-adic Galois representations

Let us consider a field K and a fixed separable closure $\overline{K}$. We denote by G_K the *absolute Galois group* $\mathrm{Gal}(\overline{K}/K)$. If Φ is a finite extension of $\mathbf{Q}_p$, with p a rational prime, and $\mathcal{O}$ is its ring of integers, we can give the following

Definition 2.1. A *p-adic (Galois) representation* of G_K with coefficients in $\mathcal{O}$ is a free $\mathcal{O}$-module T of finite rank, together with a continuous $\mathcal{O}$-linear action of G_K. The *dimension* of the representation is the rank of T as $\mathcal{O}$-module.

Usually, a representation is related to vector fields, instead of modules. Many authors define a p-adic Galois representation to be a continuous group homomorphism

$$\rho\colon G_K \longrightarrow \mathrm{GL}_d(\Phi) \cong \mathrm{Aut}(V),$$

where V is a d-dimensional Φ-vector space, like in [Ser89], or equivalently, a $\Phi[G_K]$-module finite-dimensional as Φ-vector space. However, given a representation in the sense of definition 2.1, we can naturally extend it to a representation for the Φ-vector space $V = T \otimes_{\mathcal{O}} \Phi$. If we denote by $\boldsymbol{D}$ the

divisible module $\Phi/\mathcal{O}$, we also define the following objects:

$$W = V/T = T \otimes_{\mathcal{O}} \boldsymbol{D},$$
$$W_M = M^{-1}T/T \subseteq W, \quad \text{for } M \in \mathcal{O} - \{0\},$$

so W_M is the M-torsion in W, and we have the relations

$$W = \varinjlim W_M, \quad T = \varprojlim W_M.$$

A first example of representation is the trivial representation. When we consider $\mathcal{O}$, Φ and $\boldsymbol{D}$ as representations, we let G act trivially on them. We deal now with two more interesting examples.

Example 2.2. Given a continuous character

$$\rho\colon G_K \longrightarrow \mathcal{O}^\times,$$

we can consider as p-adic representation a free $\mathcal{O}$-module $\mathcal{O}_\rho$ of rank one, on which G_K acts via ρ. In fact, every one-dimensional p-adic representation of G_K arises in this way. For example, let $\mathcal{O} = \mathbf{Z}_p$. If the characteristic of K is not p, we can consider the group of p-power roots of unity in $\overline{K}$

$$\boldsymbol{\mu}_{p^\infty} = \varinjlim_n \boldsymbol{\mu}_{p^n},$$

with $\boldsymbol{\mu}_{p^n} \cong \mathbf{Z}/p^n\mathbf{Z}$ as abelian groups. The p-power maps

$$\boldsymbol{\mu}_{p^{n+1}} \xrightarrow{\zeta \mapsto \zeta^p} \boldsymbol{\mu}_{p^n}$$

give rise to an inverse system of discrete groups, for which we can compute the inverse limit:

$$\mathbf{Z}_p(1) := \varprojlim_n \boldsymbol{\mu}_{p^n}.$$

Hence this object is a free $\mathbf{Z}_p$-module of rank 1: it is isomorphic to $\mathbf{Z}_p$ as abelian groups, but the symbol (1) indicates that the action of G_K is not the trivial one, as on $\mathbf{Z}_p$, but it is induced by the *cyclotomic character*, the natural continuous homomorphism

$$\chi_p\colon G_K \longrightarrow \mathrm{Aut}(\boldsymbol{\mu}_{p^\infty}) \cong \mathbf{Z}_p^\times.$$

This representation is called the *cyclotomic representation*. We denote by $\mathbf{Q}_p(1)$ the one-dimensional $\mathbf{Q}_p$-vector space $\mathbf{Z}_p(1) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, and we have $W = (\mathbf{Q}_p/\mathbf{Z}_p)(1) = \boldsymbol{\mu}_{p^\infty}$. Again, $\mathbf{Q}_p(1)$ is isomorphic to $\mathbf{Q}_p$ as $\mathbf{Q}_p$-vector space, but the action of G_K is different.

For a general $\mathcal{O}$, we also write $\mathcal{O}(1) = \mathcal{O} \otimes \mathbf{Z}_p(1)$, $\Phi(1) = \Phi \otimes \mathbf{Q}_p(1)$, $\boldsymbol{D}(1) = \boldsymbol{D} \otimes \mathbf{Z}_p(1)$. We are *twisting* with the cyclotomic character, an operation called *Tate twist*.

Example 2.3. Let E/K be an elliptic curve, where K is a field of characteristic different from p. We denote by $E[p^n]$ the kernel of the surjective multiplication-by-p^n isogeny

$$E \xrightarrow{[p^n]} E,$$

hence $E[p^n]$ consists of the p^n-torsion points of E. Then there is an isomorphism of abstract groups $E[p^n] \cong \mathbf{Z}/p^n\mathbf{Z} \times \mathbf{Z}/p^n\mathbf{Z}$ ([Sil09], Corollary III.6.4). We can define the p-adic Tate module of E as the group

$$T_p(E) = \varprojlim_n E[p^n],$$

where the inverse limit is taken with respect to the multiplication-by-p maps:

$$E[p^{n+1}] \xrightarrow{[p]} E[p^n].$$

Every $E[p^n]$ is a free $\mathbf{Z}/p^n\mathbf{Z}$-module of rank 2, therefore $T_p(E)$ is a free $\mathbf{Z}_p$-module of rank 2:

$$T_p(E) \cong \mathbf{Z}_p \times \mathbf{Z}_p.$$

G_K acts continuously on every $E[p^n]$ in a natural way, and this action commutes with the multiplication-by-p maps, allowing us to obtain a continuous action of G_K on $T_p(E)$.

Definition 2.4. If T is a p-adic representation of G_K with coefficients in $\mathcal{O}$ and the characteristic of K is not p, we can consider the *dual representation*

$$T^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1)).$$

The action of G_K is the following: for $\varphi \in \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1))$, $g \in G_K$ and $x \in T$,

$$(g\varphi)(x) = g(\varphi(g^{-1}x)).$$

We will also write

$$V^* = \mathrm{Hom}_{\mathcal{O}}(V, \Phi(1)) = T^* \otimes_{\mathcal{O}} \Phi,$$
$$W^* = V^*/T^* = \mathrm{Hom}_{\mathcal{O}}(T, \boldsymbol{D}(1)).$$

Example 2.5. If $\mathcal{O}_\rho$ is the representation obtained by a continuous character $\rho\colon G_K \to \mathcal{O}^\times$ and χ_p is the cyclotomic character, then

$$T^* = \mathcal{O}_{\rho^{-1}\chi_p}.$$

2.2 Galois cohomology

If K is a field and A is an abelian topological group on which G_K acts, we can define the continuous group cohomology as in Section 1.2. To lighten the notation, we write $H^n(K, A)$ for $H^n(G_K, A)$, and if the action of G_K factors through $\mathrm{Gal}(L/K)$ for some extension L/K, we write $H^n(L/K, A)$ for $H^n(\mathrm{Gal}(L/K), A)$. In particular, if T is a p-adic representation of G_K, it makes sense to consider $H^n(K, T)$, $H^n(K, T \otimes \Phi)$, $H^n(K, T \otimes \Phi/\mathcal{O})$, and for these groups we will have available the long exact sequence of Theorem 1.16.

Recall that if G_K acts on A trivially, then the first cohomology group is just the group of continuous homomorphisms from G_K to A. Therefore,

$$H^1(K, \mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(G_K, \mathbf{Q}_p/\mathbf{Z}_p),$$
$$H^1(K, \mathbf{Z}_p) = \mathrm{Hom}(G_K, \mathbf{Z}_p).$$

If L/K is a Galois extension, then $\mathrm{Gal}(L/K)$ acts naturally on the additive abelian group L and on the multiplicative abelian groups $L^\times$. If nothing is specified, these are assumed to have the discrete topology.

Theorem 2.6. *Let L/K be a Galois extension.*

(a) $H^1(L/K, L) = 0$*;*

(b) $H^1(L/K, L^\times) = 0$.

For a proof, we refer to [Ser79], Chapter X. The result (b) is the well-known *Hilbert's theorem 90*.

There is an important application of this theorem in *Kummer theory* (a concise reference for this is [Bir67]). If n is a positive integer and K is a field with characteristic coprime with n, we can consider the cyclic group of the n-th roots of unity $\boldsymbol{\mu}_n$ contained in $\overline{K}$. From the exact sequence

$$1 \longrightarrow \boldsymbol{\mu}_n \longrightarrow \overline{K}^\times \xrightarrow{x \mapsto x^n} \overline{K}^\times \longrightarrow 1,$$

we derive the exact sequence

$$1 \longrightarrow K^\times/(K^\times)^n \longrightarrow H^1(K, \boldsymbol{\mu}_n) \longrightarrow H^1(K, \overline{K}^\times) = 0,$$

therefore

$$H^1(K, \boldsymbol{\mu}_n) \cong K^\times/(K^\times)^n.$$

If K already contains all the n-th roots of unity, we deduce that

$$\mathrm{Hom}(G_K, \mathbf{Z}/n\mathbf{Z}) \cong K^\times/(K^\times)^n.$$

As a consequence, one can derive that any Galois extension L/K with Galois group $\mathbf{Z}/n\mathbf{Z}$ is of the form $L = K(\alpha^{1/n})$, when K already contains all the

n-th roots of unity.

We can do more: if K is a field of characteristic different from p, we have

$$H^1(K, \boldsymbol{\mu}_{p^n}) \cong K^\times/(K^\times)^{p^n} \cong K^\times \otimes \mathbf{Z}_p/p^n\mathbf{Z}_p \cong K^\times \otimes \frac{1}{p^n}\mathbf{Z}_p/\mathbf{Z}_p,$$

therefore, by Theorem 1.24,

$$H^1(K, \boldsymbol{\mu}_{p^\infty}) \cong \varinjlim_n H^1(K, \boldsymbol{\mu}_{p^n}) \cong \varinjlim_n K^\times \otimes \frac{1}{p^n}\mathbf{Z}_p/\mathbf{Z}_p \cong K^\times \otimes \mathbf{Q}_p/\mathbf{Z}_p.$$

Similarly, by Theorem 1.25,

$$H^1(K, \mathbf{Z}_p(1)) \cong \varprojlim_n K^\times/(K^\times)^{p^n} \cong (K^\times)\widehat{\ },$$

where $(K^\times)\widehat{\ }$ denotes the p-adic completion of $K^\times$, which coincides with the p-adically completed tensor product $K^\times \hat{\otimes} \mathbf{Z}_p$.

Now we come back to the general setting: T is a p-adic representation of G_K with coefficients in $\mathcal{O}$, $V = T \otimes \Phi$ and $W = V/T$. Let $M \in \mathcal{O} - \{0\}$. There are exact sequences:

$$0 \longrightarrow W_M \longrightarrow W \xrightarrow{M} W \longrightarrow 0. \tag{2.1}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T & \xrightarrow{M} & T & \xrightarrow{M^{-1}} & W_M & \longrightarrow & 0, \\ & & \| & & \downarrow{\scriptstyle M^{-1}} & & \downarrow & & \\ 0 & \longrightarrow & T & \longrightarrow & V & \longrightarrow & W & \longrightarrow & 0. \end{array} \tag{2.2}$$

Lemma 2.7. *Suppose $M \in \mathcal{O} - \{0\}$.*

(a) *The sequence* (2.1) *induces an exact sequence*

$$0 \to W^{G_K}/MW^{G_K} \to H^1(K, W_M) \to H^1(K, W)_M \to 0.$$

(b) *The bottom row of* (2.2) *induces an exact sequence*

$$V^{G_K} \to W^{G_K} \to H^1(K, T)_{\text{tors}} \to 0.$$

Proof.

(a) This follows from applying the long exact sequence in cohomology to (2.1), noting that

$$H^1(K, W)_M = \ker(H^1(K, W) \xrightarrow{M} H^1(K, W)).$$

(b) As before, since from Proposition 1.26

$$H^1(K, T)_{\text{tors}} = \ker(H^1(K, T) \to H^1(K, V)). \qquad \square$$

2.3 Local cohomology groups

Let K be a finite extension of $\mathbf{Q}_l$, for some rational prime l. We denote by $\mathbf{F}$ its residue fields, by $K^{\mathrm{ur}} \subseteq \overline{K}$ the maximal unramified subfield of $\overline{K}$ and by $\mathcal{I}$ the inertia subgroup $\mathrm{Gal}(\overline{K}/K^{\mathrm{ur}})$. There is an exact sequence

$$1 \to \mathcal{I} \to G_K \to G_{\mathbf{F}} \to 1,$$

where

$$\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong G_{\mathbf{F}} = \mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F}) \cong \hat{\mathbf{Z}},$$

with $\hat{\mathbf{Z}} \cong \varprojlim \mathbf{Z}/n\mathbf{Z} \cong \prod_p \mathbf{Z}_p$ the profinite completion of $\mathbf{Z}$. Here the Frobenius element $\mathrm{Fr} \in \mathrm{Gal}(K^{\mathrm{ur}}/K)$ corresponds to the Frobenius automorphism in $\mathrm{Gal}(\overline{\mathbf{F}}/\mathbf{F})$, namely $x \mapsto x^{|\mathbf{F}|}$, which corresponds to $1 \in \hat{\mathbf{Z}}$. In particular, $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ is topologically generated by the element Fr.

Definition 2.8. We say that a G_K-module A is *unramified* if $\mathcal{I}$ acts trivially on it. We define the subgroup of *unramified cohomology classes* by

$$H^1_{\mathrm{ur}}(K, A) = \ker(H^1(K, A) \to H^1(\mathcal{I}, A)) \subseteq H^1(K, A).$$

Remark 2.9. If T is a p-adic representation of G_K, T is unramified if and only if V is unramified if and only if W is unramified, and if $l \neq p$, this is true also for the dual representations.

Lemma 2.10. *If $G \cong \hat{\mathbf{Z}}$ with topological generator γ and A is a $\mathbf{Z}_p[G]$-module with is either a finitely generated $\mathbf{Z}_p$-module, or a finite-dimensional $\mathbf{Q}_p$-vector space, or a discrete torsion $\mathbf{Z}_p$-module, then*

$$H^1(G, A) \cong A/(\gamma - 1)A,$$

where the isomorphism is induced by evaluating cocycles at γ.

Proof. The fact that the evaluation of cocycles at γ induces a well-defined injective homomorphism

$$H^1(G, A) \to A/(\gamma - 1)A$$

is easy to prove. Using direct and inverse limits and tensoring with $\mathbf{Q}_p$, as seen in Section 1.2, we can reduce to the case where A is finite. In this case, this result is well known: we refer to [Ser79], Section XIII.1. □

Lemma 2.11. *Suppose that A is a G_K-module which is either a finitely generated $\mathbf{Z}_p$-module, or a finite-dimensional $\mathbf{Q}_p$-vector space, or a discrete torsion $\mathbf{Z}_p$-module. Then*

$$H^1_{\mathrm{ur}}(K, A) \cong H^1(K^{\mathrm{ur}}/K, A^{\mathcal{I}}) \cong A^{\mathcal{I}}/(\mathrm{Fr} - 1)A^{\mathcal{I}}.$$

If $l \neq p$, then

$$H^1(K, A)/H^1_{\mathrm{ur}}(K, A) \cong H^1(\mathcal{I}, A)^{\mathrm{Fr}=1},$$

where with $H^1(\mathcal{I}, A)^{\mathrm{Fr}=1}$ are the elements of $H^1(\mathcal{I}, A)$ fixed by the Frobenius.

Proof. The first isomorphisms easily follows by applying the inflation-restriction exact sequence (Proposition 1.17) and Lemma 2.10. By Propositions 1.17 and 1.21, we have a Hochschild-Serre spectral sequence

$$0 \to H^1(K^{\mathrm{ur}}/K, A^{\mathcal{I}}) \to H^1(K, A) \to H^1(\mathcal{I}, A)^{\mathrm{Fr}=1} \to H^2(K^{\mathrm{ur}}/K, A^{\mathcal{I}}).$$

Since $\mathrm{Gal}(K^{\mathrm{ur}}/K) \cong \hat{\mathbf{Z}}$ has cohomological dimension 1 (see [Wil98], Chapter 11), $H^2(K^{\mathrm{ur}}/K, A^{\mathcal{I}}) = 0$, and this yields the last isomorphism. □

Example 2.12. If $K = \mathbf{Q}_l$, we can consider the trivial action of $G_{\mathbf{Q}_l}$ on $T = \mathcal{O} = \mathbf{Z}_p$. In this case,

$$H^1_{\mathrm{ur}}(\mathbf{Q}_l, \mathbf{Z}_p) \cong \mathbf{Z}_p^{\mathcal{I}}/(\mathrm{Fr} - 1)\mathbf{Z}_p^{\mathcal{I}} = \mathbf{Z}_p/(\mathrm{Fr} - 1)\mathbf{Z}_p = \mathbf{Z}_p.$$

Remark 2.13. If V is a finite $\mathbf{Q}_p$-vector space and a p-adic representation of a group G, then we can naturally give the structure of a $\mathbf{Q}_p$-vector space to the cohomology groups $H^n(G, V)$. Despite having great properties, these groups are not finite-dimensional in general. Recall from last section that since K has characteristic different from p,

$$H^1(K, \mathbf{Z}_p(1)) \cong K^{\times} \hat{\otimes} \mathbf{Z}_p.$$

In particular, we can build an injection

$$K^{\times} \otimes \mathbf{Q}_p \hookrightarrow H^1(K, \mathbf{Q}_p(1))$$

which shows that $H^1(K, \mathbf{Q}_p(1))$ cannot be finite-dimensional, since $K^{\times}$ has countably infinite rank. Unramified cohomology groups come to the aid to solve this problem:

Corollary 2.14. *If $l \neq p$ and V is a $\mathbf{Q}_p[G_k]$-module, finite-dimensional as $\mathbf{Q}_p$-vector space, then*

$$\dim_{\mathbf{Q}_p}(H^1_{\mathrm{ur}}(K, V)) = \dim_{\mathbf{Q}_p}(V^{G_K}) < \infty.$$

Proof. By Lemma 2.11, we have an exact sequence

$$0 \to V^{G_K} \to V^{\mathcal{I}} \xrightarrow{\mathrm{Fr}-1} V^{\mathcal{I}} \to H^1_{\mathrm{ur}}(K, V) \to 0.$$

From a well-known result regarding the dimension of vector spaces in exact sequences, we derive our thesis. □

We now broaden our view: K will be a finite extension of $\mathbf{Q}_l$, but we allow $l = \infty$. This means that K can be $\mathbf{R}$ or $\mathbf{C}$. Let T be a p-adic representation of G_K, $V = T \otimes \Phi$ and $W = V/T$ as usual. We define special subgroups $H^1_f(K, \cdot)$ of the cohomology groups $H^1(K, \cdot)$, following the work of Bloch and Kato in [BK90]. There is a natural choice for $l \neq p, \infty$:

Definition 2.15. Suppose $l \neq p, \infty$. We define the *finite* part of $H^1(K,V)$ by

$$H^1_f(K,V) = H^1_{\mathrm{ur}}(K,V).$$

We define $H^1_f(K,T) \subseteq H^1(K,T)$ and $H^1_f(K,W) \subseteq H^1(K,W)$ to be the inverse image and image, respectively, of $H^1_f(K,V)$ under the natural maps

$$H^1(K,T) \to H^1(K,V) \to H^1(K,W).$$

In the same way, for $M \in \mathcal{O} - \{0\}$ we define $H^1_f(K,W_M)$ to be the inverse image of $H^1_f(K,W)$ under the map induced by the inclusion $W_M \hookrightarrow W$. Finally, for V, T, W or W_M we define the *singular quotient* of $H^1(K,\cdot)$ by

$$H^1_s(K,\cdot) = H^1(K,\cdot)/H^1_f(K,\cdot),$$

therefore there is an exact sequence

$$0 \to H_f(K,\cdot) \to H^1(K,\cdot) \to H^1_s(K,\cdot) \to 0.$$

The next Lemma includes important features of these cohomology subgroups and quotients.

Lemma 2.16. *Let T be a p-adic representation of G_K, with $l \neq p, \infty$.*

(a) $H^1_f(K,W) = H^1_{\mathrm{ur}}(K,W)_{\mathrm{div}}$.

(b) $H^1_{\mathrm{ur}}(K,T) \subseteq H^1_f(K,T)$ *with finite index, and* $H^1_s(K,T)$ *is torsion free.*

(c) *Denote by $\mathcal{W}$ the quotient $W^{\mathcal{I}}/(W^{\mathcal{I}})_{\mathrm{div}}$. There are natural isomorphisms*

$$H^1_{\mathrm{ur}}(K,W)/H^1_f(K,W) \cong \mathcal{W}/(\mathrm{Fr}-1)\mathcal{W},$$
$$H^1_f(K,T)/H^1_{\mathrm{ur}}(K,T) \cong \mathcal{W}^{\mathrm{Fr}=1}.$$

(d) *If T is unramified, then*

$$H^1_f(K,T) = H^1_{\mathrm{ur}}(K,T) \quad \textit{and} \quad H^1_f(K,W) = H^1_{\mathrm{ur}}(K,W).$$

Proof. By their definitions, $H^1_f(K,W)$ is divisible and $H^1_s(K,T)$ is torsion free. From the exact commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1_{\mathrm{ur}}(K,T) & \longrightarrow & H^1(K,T) & \longrightarrow & H^1(\mathcal{I},T) \\
 & & & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1_f(K,V) & \longrightarrow & H^1(K,V) & \longrightarrow & H^1(\mathcal{I},V) \\
 & & & & \downarrow & & \downarrow \\
0 & \longrightarrow & H^1_{\mathrm{ur}}(K,W) & \longrightarrow & H^1(K,W) & \longrightarrow & H^1(\mathcal{I},W)
\end{array}$$

we get $H^1_{\mathrm{ur}}(K,T) \subseteq H^1_f(K,T)$ and $H^1_f(K,W) \subseteq H^1_{\mathrm{ur}}(K,W)$. The rest of (a) and (b) will follow from (c), since $\mathcal{W}$ is finite: by Proposition 1.25, $\mathcal{W}$ is isomorphic to $H^1(K,T)_{\mathrm{tors}}$, which is finite, being the torsion part of a finitely generated module over $\mathbf{Z}_p$.

(c) The image of $V^{\mathcal{I}} \to W^{\mathcal{I}}$ is $(W^{\mathcal{I}})_{\mathrm{div}}$ (again Proposition 1.25), therefore, taking first $\mathcal{I}$-cohomology and then $\mathrm{Gal}(K^{\mathrm{ur}}/K)$-invariants of the exact sequence $0 \to T \to V \to W \to 0$, we derive an exact sequence

$$0 \to (\mathcal{W})^{\mathrm{Fr}=1} \to H^1(\mathcal{I},T)^{\mathrm{Fr}=1} \to H^1(\mathcal{I},V)^{\mathrm{Fr}=1}.$$

Using Lemma 2.11, we get

$$\begin{aligned} H_f(K,T)/H_{\mathrm{ur}}(K,T) &= \ker(H^1(K,T)/H^1_{\mathrm{ur}}(K,T) \to H^1(K,V)/H^1_{\mathrm{ur}}(K,V)) \\ &= \ker(H^1(\mathcal{I},T)^{\mathrm{Fr}=1} \to H^1(\mathcal{I},V)^{\mathrm{Fr}=1}) \\ &= (\mathcal{W})^{\mathrm{Fr}\,-1}, \end{aligned}$$

$$\begin{aligned} H_{\mathrm{ur}}(K,W)/H_f(K,W) &= \mathrm{coker}(H^1_{\mathrm{ur}}(K,V)/ \to H^1_{\mathrm{ur}}(K,W)) \\ &= \mathrm{coker}(V^{\mathcal{I}}/(\mathrm{Fr}\,-1)V^{\mathcal{I}} \to W^{\mathcal{I}}/(\mathrm{Fr}\,-1)W^{\mathcal{I}}) \\ &= W^{\mathcal{I}}/((W^{\mathcal{I}})_{\mathrm{div}} + (\mathrm{Fr}\,-1)W^{\mathcal{I}}) \\ &= \mathcal{W}/(\mathrm{Fr}\,-1)\mathcal{W}. \end{aligned}$$

(d) If T is unramified then $W^{\mathcal{I}} = W$ is divisible, hence (d) follows immediately from (c). □

When $l = p$, the choice of a subspace is $H^1_f(K,V)$ is more complicated. In [BK90], the authors use a ring defined by Fontaine in [Fon82], namely the ring B_{cris}:

$$H^1_f(K,V) = \ker(H^1(K,V) \to H^1(K, V \otimes B_{\mathrm{cris}})).$$

However, for our purposes, it will be not necessary to enter in details, and we can just fix an arbitrary subspace of $H^1(K,V)$, denoting it by $H^1_f(K,V)$. Natural choices are $H^1_f(K,V) = 0$ or $H^1_f(K,V) = H^1(K,V)$. Once this choice is made, we can define $H_f(K,T)$, $H_f(K,W)$ and $H_f(K,W_M)$ as before.

Finally, when $l = \infty$, $K = \mathbf{R}$ or $\mathbf{C}$, we have G_K finite of order 1 or 2. One can easily show that since V is torsion-free and divisible, then $H^1(K,V) = 0$ (for example, using the fact that $|G_K|\colon V \to V$ is an isomorphism). As before:

- $H^1_f(K,V) = 0$;
- $H^1_f(K,W) = 0$;

- $H^1_f(K,T) = H^1(K,T)$;
- $H^1_f(K,W_M) = \ker(H^1(K,W_M) \to H^1(K,W)) = W^{G_K}/MW^{G_K}$.

Remark 2.17. Let us consider W_M, for $M \in \mathcal{O} - \{0\}$. It is a subgroup of W but also a quotient of T, hence the subgroup $H_f(K,W_M)$ can be defined to be inverse image of $H^1_f(K,W)$ (as we did) or the image of $H^1_f(K,T)$. The next result shows that there is no difference.

Lemma 2.18. *Suppose $M \in \mathcal{O} - \{0\}$.*

(a) *$H^1_f(K,W_M)$ is the image of $H^1_f(K,T)$ under the map*

$$H^1(K,T) \to H^1(K,W_M)$$

induced by $T \twoheadrightarrow M^{-1}T/T = W_M$.

(b) *If $l \neq p, \infty$ and T is unramified, then $H^1_f(K,W_M) = H^1_{\mathrm{ur}}(K,W_M)$.*

Proof.

(a) The diagram (2.2) gives rise to a commutative diagram with exact rows

$$\begin{array}{ccccccc} H^1(K,T) & \xrightarrow{M} & H^1(K,T) & \longrightarrow & H^1(K,W_M) & \longrightarrow & H^2(K,T) \\ \| & & \downarrow{\scriptstyle M^{-1}} & & \downarrow & & \| \\ H^1(K,T) & \longrightarrow & H^1(K,V) & \longrightarrow & H^1(K,W) & \longrightarrow & H^2(K,T), \end{array}$$

from which we easily deduce that the image of $H^1_f(K,T)$ is contained in $H^1_f(K,W_M)$.

Conversely, if $\mathbf{c}_{W_M} \in H^1_f(K,W_M)$, then its image in $H^1(K,W)$ is the image of some $\mathbf{c}_V \in H^1_f(K,V)$. Since, by the previous diagram, the image of $\mathbf{c}_V$ is 0 in $H^2(K,T)$, also the image of $\mathbf{c}_{W_M}$ has to be 0 in $H^2(K,T)$. By exactness, there exists an element $\mathbf{c}_T \in H^1(K,T)$ which maps to $\mathbf{c}_{W_M}$. Its image in $H^1(K,V)$ under the map induced by M^{-1} differs from $\mathbf{c}_V$ by an element in the kernel of $H^1(K,V) \to H^1(K,W)$, which is the image of $H^1(K,T)$, so it differs by an element $\mathbf{c}' \in H^1(K,T)$. We conclude that the element $\mathbf{c}_T - M\mathbf{c}'$ belongs to $H^1_f(K,T)$ and maps to $\mathbf{c}_{W_M}$.

(b) If $l \neq p$ and T is unramified, then $H^1_f(H,T) = H^1_{\mathrm{ur}}(H,T)$, and by (a)

$$H^1_f(K,W_M) = \mathrm{Im}(H^1_f(K,T)) = \mathrm{Im}(H^1_{\mathrm{ur}}(K,T)) \subseteq H^1_{\mathrm{ur}}(K,W_M).$$

Conversely, denoted by ι_M the map $H^1(K,W_M) \to H^1(K,W)$, we have

$$H_f(K,W_M) = \iota_M^{-1}(H^1_f(K,W)) = \iota_M^{-1}(H^1_{\mathrm{ur}}(K,W)) \supseteq H^1_{\mathrm{ur}}(K,W_M),$$

since $H^1_f(H,W) = H^1_{\mathrm{ur}}(H,W)$. □

Corollary 2.19. *There are natural horizontal exact sequences with vertical isomorphisms*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_f(K,W) & \longrightarrow & H^1(K,W) & \longrightarrow & H^1_s(K,W) & \longrightarrow & 0 \\ & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\ 0 & \longrightarrow & \varinjlim H^1_f(K,W_M) & \longrightarrow & \varinjlim H^1(K,W_M) & \longrightarrow & \varinjlim H^1_s(K,W_M) & \longrightarrow & 0 \end{array}$$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_f(K,T) & \longrightarrow & H^1(K,T) & \longrightarrow & H^1_s(K,T) & \longrightarrow & 0 \\ & & \downarrow\wr & & \downarrow\wr & & \downarrow\wr & & \\ 0 & \longrightarrow & \varprojlim H^1_f(K,W_M) & \longrightarrow & \varprojlim H^1(K,W_M) & \longrightarrow & \varprojlim H^1_s(K,W_M) & \longrightarrow & 0. \end{array}$$

Proof. Every W_M is finite, therefore, by Proposition 1.21, the groups inside the inverse limits are finite. It follows that the horizontal sequences are exact, by the Mittag-Leffler condition.

Since $T = \varprojlim W_M$ and $W = \varinjlim W_M$, we have

$$\begin{aligned} H^1(K,W) &= \varinjlim H^1(K,W_M), \\ H^1(K,T) &= \varprojlim H^1(K,W_M). \end{aligned}$$

Similarly, by their definitions,

$$\begin{aligned} H^1_f(K,W) &= \varinjlim H^1_f(K,W_M), \\ H^1_f(K,T) &= \varprojlim H^1_f(K,W_M), \end{aligned}$$

we derive

$$\begin{aligned} H^1_s(K,W) &= \varinjlim H^1_s(K,W_M), \\ H^1_s(K,T) &= \varprojlim H^1_s(K,W_M) \end{aligned}$$

(note that we are using Lemma 2.18 (a) for the second set of isomorphisms). □

2.4 Global cohomology and Selmer groups

Let K be a number field and T a p-adic representation of G_K with coefficients in $\mathcal{O}$. As usual, we take $V = T \otimes \Phi$ and $W = V/T$. If v is a place of K, we can consider the decomposition group of any place of $\overline{K}$ in G_K, and we denote it by G_{K_v}, since it is the absolute Galois group of the completion K_v of K under the prime v ([Neu99], Chapter II, Proposition 9.6). We write $\mathcal{I}_v$ for the inertia subgroup contained in G_{K_v}. We have a canonical restriction map

$$H^1(K,\cdot) \to H^1(K_v,\cdot),$$

denoted by $\mathbf{c} \mapsto \mathbf{c}_v$. As before, we say that T is *unramified* at a place v if the inertia group $\mathcal{I}_v$ acts trivially on T (note that this does not depend on the choice of the prime over v, since all inertia subgroups are conjugated). We assume that T is unramified outside a finite set of primes of K.

Remark 2.20. If v is a place of K lying over the prime l (it can be ∞) of $\mathbf{Q}$, then K_v is a finite extension of $\mathbf{Q}_l$. In particular, it makes sense to repeat the construction of the previous Section, and we are able to pick a subspace $H^1_f(K_v, V)$ of $H^1(K_v, V)$. If v is a finite place not lying over p, then it is the unramified cohomology group $H^1_{\mathrm{ur}}(K_v, V)$; if v lies over p, then $H^1_f(K_v, V)$ is an arbitrary subspace of $H^1(K_v, V)$; if v is archimedean, then $H^1_f(K_v, V) = 0$.

Let Σ be a finite set of places of K. K_Σ will denote the maximal extension of K contained in $\overline{K}$ unramified outside Σ.

Definition 2.21. We introduce some *Selmer groups* corresponding to Σ as follows. If A is T, W or W_M for some $M \in \mathcal{O} - \{0\}$, recalling that

$$H^1_s(K_v, A) = H^1(K_v, A)/H_f(K_v, A),$$

we define

$$\mathcal{S}_\Sigma(K, A) \subseteq \mathcal{S}^\Sigma(K, A) \subseteq H^1(K, A)$$

by

$$\mathcal{S}^\Sigma(K, A) = \ker\Big(H^1(K, A) \to \prod_{v \notin \Sigma} H^1_s(K_v, A)\Big),$$
$$\mathcal{S}_\Sigma(K, A) = \ker\Big(\mathcal{S}^\Sigma(K, A) \to \bigoplus_{v \in \Sigma} H^1(K_v, A)\Big).$$

In other words, a class $\mathbf{c} \in H^1(K, A)$ belongs to $\mathcal{S}^\Sigma(K, A)$ if, for every $v \notin \Sigma$,

$$\mathbf{c}_v \in H^1_f(K_v, A),$$

while it belongs to $\mathcal{S}_\Sigma(K, A)$ if in addiction

$$\mathbf{c}_v = 0$$

for every $v \in \Sigma$. When $\Sigma = \emptyset$, we get the *true Selmer group*

$$\begin{aligned}\mathcal{S}(K, W) &= \mathcal{S}_\emptyset(K, W) = \mathcal{S}^\emptyset(K, W) \\ &= \ker\Big(H^1(K, A) \to \prod_{v \text{ place of } K} H^1_s(K_v, A)\Big).\end{aligned}$$

This group was firstly introduced by Bloch e Kato in [BK90], Section 5.

Remark 2.22. When $A = W$, the map

$$H^1(K, W) \to \prod_{v \notin \Sigma} H^1_s(K_v, W)$$

actually lands in

$$\bigoplus_{v \notin \Sigma} H^1_s(K_v, W).$$

This is true by discreteness of W. Indeed, if $f\colon G_K \to W$ is a cocycle, then the preimage of $\{0\}$ has to be open in G_K, so it is $\mathrm{Gal}(\overline{K}/L)$ for some L/K finite Galois. But L ramifies only at finite primes, so the inertia with respect to the others is trivial, and for almost all places v, $H^1_f(K_v, W) = H^1_{\mathrm{ur}}(K_v, W)$.

Remark 2.23. A priori the Selmer groups depend on the choice of $H^1_f(K_v, V)$ for v lying above p, but this is not the case when Σ contains all the finite primes above p. We will usually get rid of the "bad" primes, making them belong to Σ.

Lemma 2.24. *The absolute Galois group of K_Σ is the closure of the subgroup generated by all the possible inertia $\mathcal{I}_{\bar{v}/v}$, for all possible places v of K, and for all possible extensions $\bar{v}$, places of $\overline{K}$.*

Proof. It is well-known ([Koc02], Theorem 8.3) that the fixed field of $\mathcal{I}_{\bar{v}/v}$ is the maximal extension of K in which the restriction of $\bar{v}$ is unramified. Therefore K_Σ is contained in the fixed field of every $\mathcal{I}_{\bar{v}/v}$, and this means that $\mathrm{Gal}(\overline{K}/K_\Sigma)$, being closed (by infinite Galois correspondence), contains the closure of the subgroup generated by the inertia. If this containment is strict, then the fixed field of this closure would be an extension of K unramified outside Σ strictly larger then K_Σ, and this is a contradiction. □

Lemma 2.25. *If Σ contains all infinite places, all primes above p and all primes of K where T is ramified, then*

$$\mathcal{S}^\Sigma(K, A) = H^1(K_\Sigma/K, A),$$

where A can be T, W or W_M, with $M \in \mathcal{O} - \{0\}$.

Proof. For every place $v \notin \Sigma$, $H^1_f(K_v, A) = H^1_{\mathrm{ur}}(K_v, A)$. Therefore

$$\begin{aligned}\mathcal{S}^\Sigma(K, A) &= \ker\Big(H^1(K, A) \to \prod_{v \in \Sigma} \mathrm{Hom}(\mathcal{I}_v, A)\Big) \\ &= \ker\Big(H^1(K, A) \to H^1(K_\Sigma, A)\Big) = H^1(K_\Sigma/K, A),\end{aligned}$$

where the first equality follows from Lemma 2.11 (enlarging the codomain), the second from Lemma 2.24 and the last from the inflation-restriction sequence (Proposition 1.17). □

Proposition 2.26. *Let Σ be a finite set of primes of K.*

(a) $\mathcal{S}^\Sigma(K,T) = \varprojlim S^\Sigma(K,W_M)$ *and* $\mathcal{S}_\Sigma(K,T) = \varprojlim S_\Sigma(K,W_M)$.

(b) $\mathcal{S}^\Sigma(K,W) = \varinjlim S^\Sigma(K,W_M)$ *and* $\mathcal{S}_\Sigma(K,W) = \varinjlim S_\Sigma(K,W_M)$.

Proof. Immediate consequence of Corollary 2.19. □

The next Lemma is one of the reasons for which working with the Selmer groups is easier than working just with the global cohomology group $H^1(K,\cdot)$:

Lemma 2.27. *If $M \in \mathcal{O} - \{0\}$ and Σ is a finite set of primes of K, then*

(a) $\mathcal{S}^\Sigma(K,W_M)$ *is finite.*

(b) $\mathcal{S}^\Sigma(K,T)$ *is a finitely generated $\mathcal{O}$-module.*

(c) *The Pontryagin dual of $\mathcal{S}^\Sigma(K,W)$ is a finitely generated $\mathcal{O}$-module.*

Proof. Without loss of generality, we may enlarge Σ so that it containing all the infinite places, all primes above p and all primes where T is ramifies By Lemma 2.25, if $A = W_M$, T or W, then

$$\mathcal{S}^\Sigma(K,A) = H^1(K_\Sigma/K, A),$$

which has the desired properties by Proposition 1.21. □

Remark 2.28. In [MR04], Chapter 2, the authors introduce a more general setup for Selmer groups: if A is a topological $\mathcal{O}$-module with a continuous $\mathcal{O}$-linear action of G_K unramified outside a finite set of places, a *Selmer structure* for A is a choice, for every place v of K, of $\mathcal{O}$-submodules

$$H_{\mathcal{F}}(K_v,A) \subseteq H^1(K_v,A),$$

such that for almost all places v,

$$H_{\mathcal{F}}(K_v,A) = H^1_{\mathrm{ur}}(K_v,A).$$

Then a *Selmer group* for this collection is

$$\mathcal{S}(K,A) = \ker\Big(H^1(K,A) \to \prod_{v \text{ place of } K} H^1(K_v,A)/H^1_{\mathcal{F}}(K_v,A)\Big),$$

or equivalently (as in Lemma 2.25),

$$\mathcal{S}(K,A) = \ker\Big(H^1(K_\Sigma,A) \to \prod_{v\in\Sigma} H^1(K_v,A)/H^1_{\mathcal{F}}(K_v,A)\Big),$$

where Σ is a finite set of places containing all primes for which A is unramified and the primes for which $H^1_{\mathcal{F}}(K_v,A) \neq H^1_f(K_v,A)$. Then it is clear that our choices of $H^1_f(K_v,A)$ give rise to a Selmer structure, and Definition 2.21 is just an application of this more general description.

We deal now with important examples of this construction. Firstly, take $\mathcal{O} = \mathbf{Z}_p = T$ with trivial G_K action. Then, by Lemma 2.16 and Lemma 2.11, for every prime v of K not above p, we get

$$H^1_f(K_v, \mathbf{Q}_p/\mathbf{Z}_p) = H^1_{\mathrm{ur}}(K_v, \mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(\mathrm{Gal}(K_v^{\mathrm{ur}}/K_v), \mathbf{Q}_p/\mathbf{Z}_p).$$

As in Remark 2.22 and Lemma 2.25, if Σ is a finite set of places containing the ones above p, it follows that

$$\begin{aligned} H^1(K, \mathbf{Q}_p/\mathbf{Z}_p) &= \mathrm{Hom}(G_K, \mathbf{Q}_p/\mathbf{Z}_p), \\ \mathcal{S}^\Sigma(K, \mathbf{Q}_p/\mathbf{Z}_p) &= \mathrm{Hom}(\mathrm{Gal}(K_\Sigma/K), \mathbf{Q}_p/\mathbf{Z}_p), \\ \mathcal{S}_\Sigma(K, \mathbf{Q}_p/\mathbf{Z}_p) &= \mathrm{Hom}(\mathrm{Gal}(H_{K,\Sigma}/K), \mathbf{Q}_p/\mathbf{Z}_p), \end{aligned}$$

where $H_{K,\Sigma}$ is the maximal unramified abelian extension of K in which the places in Σ splits completely. This is clearly a subfield of the Hilbert class field of K, therefore $\mathrm{Gal}(H_{K,\Sigma}/K)$ is a quotient of the ideal class group A_K. By the correspondence we built in Section 1.1, it is the quotient of A_K modulo the subgroup generated by the classes of primes in Σ. Denoted by $A_{K,\Sigma}$ this quotient, we get

$$\mathcal{S}_\Sigma(K, \mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(A_{K,\Sigma}, \mathbf{Q}_p/\mathbf{Z}_p).$$

We see now that when Σ is empty there is an appropriate choice of subspaces $H^1_f(K_v, \mathbf{Q}_p)$ such that

$$\mathcal{S}(K, \mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(A_K, \mathbf{Q}_p/\mathbf{Z}_p).$$

More in general, if $\chi\colon G_K \to \mathcal{O}^\times$ is a character of finite, prime-to-p order (recall that the order of a character is the order of its image) and $T = \mathcal{O}_\chi$, a free rank-one $\mathcal{O}$-module on which G_K acts via χ, then there exists an abelian extension L of K, of degree prime to p, such that χ factors through $\Delta = \mathrm{Gal}(L/K)$, by an easy topological argument. We write $\mathbf{D}_\chi = \mathbf{D} \otimes \mathcal{O}_\chi$ and $\Phi_\chi = \Phi \otimes \mathcal{O}_\chi$. Given a place v of K, if w a place of L lying over v, we denote by D_w and $\mathcal{I}_w$ the decomposition group ad the inertia group of w. By the restriction map and Corollary 5.3 in the Appendix B of [Rub00],

$$H^1(K_v, V) \cong (\oplus_{w|v} \mathrm{Hom}(D_w, V))^\Delta = (\oplus_{w|v} \mathrm{Hom}(D_w, \Phi_\chi))^\Delta.$$

Therefore, if $v \nmid p$, this identifies

$$H^1_f(K_v, V) = H^1_{\mathrm{ur}}(K_v, V) = (\oplus_{w|v} \mathrm{Hom}(D_w/\mathcal{I}_w, V))^\Delta,$$

and if $v \mid p$, we can take this as definition for $H^1_f(K_v, V)$ as well; this agree with the definition of Bloch-Kato ([BK90]).

Proposition 2.29. *There is an isomorphism*

$$\mathcal{S}(K, W) \cong \mathrm{Hom}(A_L, \mathbf{D}_\chi)^\Delta.$$

Proof. Since $[L:K]$ is prime to p, the restriction map gives an isomorphism

$$H^1(K,W) \cong H^1(L,W)^{\Delta} = \mathrm{Hom}(G_L, \mathbf{D}_\chi)^{\Delta}.$$

This follows from the fact that $[L:K]\colon W \to W$ is an isomorphism, and so $H^1(\Delta,W) = H^2(\Delta,W) = 0$.

Also, since $D_w/\mathcal{I}_w$ is torsion free, $\oplus_{w|v} \mathrm{Hom}(D_w/\mathcal{I}_w, W)^{\Delta}$ is divisible, and from the isomorphism

$$H^1(K_v,W) \cong (\oplus_{w|v} \mathrm{Hom}(D_w,W))^{\Delta},$$

we get an isomorphism

$$H^1_f(K_v,W) \cong (\oplus_{w|v} \mathrm{Hom}(D_w/\mathcal{I}_w,W))^{\Delta}.$$

If L^1 denotes the Hilbert class field of L, we conclude that

$$\begin{aligned} S(K,W) &\cong \{\phi \in \mathrm{Hom}(G_l,\mathbf{D}_\chi)^{\Delta} \mid \phi(\mathcal{I}_w) = 0 \text{ for every } w\} \\ &= \mathrm{Hom}(\mathrm{Gal}(L^1/L),\mathbf{D}_\chi)^{\Delta} = \mathrm{Hom}(A_L,\mathbf{D}_\chi)^{\Delta}. \end{aligned}$$ □

In particular, for $L = K$, we deduce the important identification

$$\mathcal{S}(K,\mathbf{Q}_p/\mathbf{Z}_p) = \mathrm{Hom}(A_K,\mathbf{Q}_p/\mathbf{Z}_p).$$

The second example concerns elliptic curves. Let us consider an elliptic curve E/K, where K is a number field. Fix p an odd prime and denote by $[p^n]$ the multiplication-by-p^n isogeny, where $n \geq 1$. Then from the exact sequence

$$0 \to E[p^n] \to E \xrightarrow{[p^n]} E \to 0,$$

we get the exact sequence

$$0 \to E(K)/p^nE(K) \xrightarrow{\delta} H^1(K,E[p^n]) \to H^1(K,E)_{p^n} \to 0,$$

where δ is the Kummer map. The same reasoning can be repeated after localizing with a place v of K, and denoted by δ_v the Kummer map

$$\delta_v\colon E(K_v)/p^nE(K_v) \hookrightarrow H^1(K_v,E[p^n]),$$

we get a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/p^nE(K) & \longrightarrow & H^1(K,E[p^n]) & \longrightarrow & H^1(K,E)_{p^n} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(K_v)/p^nE(K_v) & \longrightarrow & \prod_v H^1(K_v,E[p^n]) & \longrightarrow & \prod_v H^1(K_v,E)_{p^n} & \longrightarrow & 0. \end{array}$$

The p^n-Selmer group of E/K is defined by

$$S^{(p^n)}(E/K) = \ker\Big(H^1(K,E[p^n]) \to \prod_v H^1(K_v,E)\Big).$$

The *Shafarevich-Tate group* of E/K is defined by

$$Ш(E/K) = \ker\Big(H^1(K,E) \to \prod_v H^1(K_v,E)\Big).$$

Finally, the p-power Selmer group of E/K is

$$S^{(p^\infty)}(E/K) = \varinjlim_n S^{(p^n)}(E/K).$$

The relation with the Bloch-Kato Selmer group is the following: take $T = T_p(E)$, the Tate module. The action of G_K on T is unramified at every prime v not lying over p for which E has good reduction ([Sil09], Chapter VII, Proposition 4.1). We have

$$\begin{aligned} V &= V_p(E) = T_p(E) \otimes \mathbf{Q}_p, \\ W &= V_p(E)/T_p(E) = E[p^\infty]. \end{aligned}$$

From the injection

$$E(K_v)/p^n E(K_v) \hookrightarrow H^1(K_v, E[p^n]),$$

we also derive the following Kummer maps, again denoted by δ_v:

$$\begin{aligned} E(K_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p &\hookrightarrow H^1(K_v, E[p^\infty]), \\ \widehat{E(K_v)} &\hookrightarrow H^1(K_v, T_p(E)), \\ \widehat{E(K_v)} \otimes \mathbf{Q}_p &\hookrightarrow H^1(K_v, V_p(E)). \end{aligned}$$

Note that by commutativity,

$$\mathcal{S}^{(p^n)}(E/K) = \ker\Big(H^1(K,E[p^n]) \to \prod_v H^1(K_v,E[p^n])/\operatorname{Im}(\delta_v)\Big),$$

and also

$$S^{(p^\infty)}(E/K) = \ker\Big(H^1(K,E[p^\infty]) \to \prod_v H^1(K_v,E[p^\infty])/\operatorname{Im}(\delta_v)\Big).$$

If v is a prime above p we can define $H^1_f(K_v, V_p(E))$ as the image of the Kummer map, and this coincide with the Bloch-Kato definition, by the renowned Example 3.11 of [BK90].

Remark 2.30. By the *Weil pairing* ([Sil09], Section III.8), $V \cong V^*$, $T \cong T^*$, and $W \cong W^*$. Therefore $H^1_f(K_v, V^*) = H^1_f(K_v, V)$, and they are orthogonal complements under the local pairing, as one requires.

Proposition 2.31 ([Gre99], Proposition 2.1)**.** *If $v \nmid p$, then the image of the Kummer map*

$$E(K_v) \otimes \mathbf{Q}_p/\mathbf{Z}_p \hookrightarrow H^1(K_v, E[p^\infty])$$

is trivial.

Proposition 2.32. *The Selmer group $\mathcal{S}(K, E[p^\infty])$ is the p-power Selmer group of E/K, and it sits in an exact sequence*

$$0 \to E(K) \otimes \mathbf{Q}_p/\mathbf{Z}_p \to \mathcal{S}(K, E[p^\infty]) \to Ш(E/K)_{p^\infty} \to 0,$$

where $Ш(E/K)_{p^\infty}$ is the p-part of the Shafarevich-Tate group.

Proof. If $v \nmid p$, then by [Sil09], Chapter VII, Proposition 6.3, $E(K_v)$ contains a subgroup of finite index which is a pro-l-group, with l rational prime below v. In particular, $E(K_v)\widehat{\ }$ is finite, and so $H^1_f(K_v, V_p(E)) = 0$. Therefore, for every v, $H^1_f(K_v, V_p(E))$ is the image of $E(K_v)\widehat{\ }\otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ under the Kummer map. We conclude that for every v, $H^1_f(K_v, E[p^\infty])$ is the image of $E(K_v)\widehat{\ }\otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p$ under the Kummer map, that is, the two definitions coincide. □

Chapter 3

Euler systems

In this Chapter, we deal with the main results. Firstly, we introduce the powerful instrument of the Euler systems, in the most possible general setting. Then we see how it relates with Selmer groups, stating fundamental Theorems in order to control their sizes. The proof of some Theorems requires difficult and deep techniques, developed in Chapters IV, V and VII of [Rub00], and in this case we just provide precise references. In particular, the Kolyvagin derivatives play a special role in the proofs, and in Chapter 4 we will introduce them and explicitly see their importance in our setting: the main conjecture. We follow again [Rub00], remarking how similar results can be found in [Kol90], [Kat99] and [MR04].

3.1 Euler systems: definition

Let K be a number field. As usual, $\mathcal{O}_K$ will be the ring of integers of K. We consider a p-adic representation T of G_K with coefficients in $\mathcal{O}$, where p is a rational prime and $\mathcal{O}$ is the ring of integers of Φ, a finite extension of $\mathbf{Q}_p$. We assume that T is unramified outside a finite set of primes of K.

If $\mathfrak{q}$ is a finite prime of K non dividing p where T is unramified, then we can take the ray class field modulo $\mathfrak{q}$, $K^{\mathfrak{q}}$. Denote by $K(\mathfrak{q})$ the maximal p-extension of K contained in $K^{\mathfrak{q}}$. We define

$$P(\mathrm{Fr}_{\mathfrak{q}}^{-1} \mid T^*; x) = \det(1 - \mathrm{Fr}_{\mathfrak{q}}^{-1}\, x \mid T^*) \in \mathcal{O}[x],$$

where $\mathrm{Fr}_{\mathfrak{q}}$ is a Frobenius of $\mathfrak{q}$ in G_K.

Remark 3.1. The Frobenius is not uniquely defined: it depends on a choice of a prime of $\overline{K}$ lying over $\mathfrak{q}$, but only up to conjugation, and it is defined modulo an inertia subgroup. However, since T is unramified at $\mathfrak{q}$ and $\mathfrak{q}$ does not lie over p, also T^* is unramified at $\mathfrak{q}$, hence this determinant is well-defined.

We write

$$K \subseteq_f F$$

to indicate that F/K is a finite extension.

Definition 3.2. Let $\mathcal{K}$ be an (infinite) abelian extension of K and $\mathcal{N}$ be an ideal of K divisible by p and by all primes where T is ramified, such that:

- K contains $K(\mathfrak{q})$ for every finite prime $\mathfrak{q}$ of K not dividing $\mathcal{N}$.
- K contains an extension K_∞ of K such that $\mathrm{Gal}(K_\infty/K) \cong \mathbf{Z}_p^d$ for some $d \geq 1$, and no finite prime of K splits completely in K_∞/K.

A collection of classes

$$\mathbf{c} = \{\mathbf{c}_F \in H^1(K,T) \mid K \subseteq_f F \subseteq \mathcal{K}\}$$

is called an *Euler system* for $(T, \mathcal{K}, \mathcal{N})$ if, whenever $K \subseteq_f F \subseteq_f F' \subseteq \mathcal{K}$, we have

$$\mathrm{cor}_{F'/F}(\mathbf{c}_{F'}) = \left(\prod_{\mathfrak{q} \in \Sigma(F'/F)} P(\mathrm{Fr}_\mathfrak{q}^{-1} \mid T^*; \mathrm{Fr}_\mathfrak{q}^{-1}) \right) \mathbf{c}_f,$$

where $\Sigma(F'/F)$ denotes the set of finite primes of K, not dividing $\mathcal{N}$, which ramify in F' but not in F, and $\mathrm{cor}_{F'/F}$ is the corestriction map

$$\mathrm{cor}_{F'/F} \colon H^1(F', T) \to H^1(F, T),$$

induced by the inclusion $\mathrm{Gal}(\overline{K}/F') \subseteq \mathrm{Gal}(\overline{K}/F)$.

We say that a collection $\mathbf{c} = \{\mathbf{c}_F \in H^1(F,T)\}$ is an Euler systems for T if we can choose, as before, $\mathcal{K}$ and $\mathcal{N}$ such that $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$.

Finally, if $\mathcal{K}_\infty$ is a $\mathbf{Z}_p^d$-extension of K in which no finite prime splits completely, we say that a collection $\mathbf{c} = \{\mathbf{c}_F \in H^1(F,T)\}$ is an Euler systems for (T, K_∞) if we can choose, as before, $\mathcal{K} \supseteq K_\infty$ and $\mathcal{N}$ such that $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$.

Since $\mathbf{Z}_p^d$ has no proper finite subgroup, a prime does not split completely in K_∞/K if and only if its decomposition group is infinite. For example, K_∞ may be the cyclotomic $\mathbf{Z}_p$-extension of K, because no finite prime of K splits completely there: by $K_\infty = K\mathbf{Q}_\infty$, without loss of generality, we can show this for $K = \mathbf{Q}$. Also, to simplify the notation, take $p \neq 2$. As we have seen in Section 1.3, $\mathbf{Q}_n$, the degree p^n subextension of $\mathbf{Q}_\infty$, is obtained as the fixed field of $(\mathbf{Z}/p\mathbf{Z})^\times \cong \boldsymbol{\mu}_{p-1}$ in $\mathbf{Q}(\zeta_{p^{n+1}})$, with $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^{n+1}})/\mathbf{Q}) \cong (\mathbf{Z}/p^{n+1}\mathbf{Z})^\times$. If $l \neq p$, the Frobenius of l in $\mathrm{Gal}(\mathbf{Q}(\zeta_{p^{n+1}})/\mathbf{Q})$ is (isomorphic to) l mod p^{n+1}, therefore l splits completely in $\mathbf{Q}_n$ if $l^{p-1} \equiv 1 \pmod{p^{n+1}}$, and this clearly can happen only for finitely many n.

Since p divides $\mathcal{N}$, no Euler factor at primes dividing p are considered. The only unramified primes in K_∞ lies above p (Proposition 1.29), therefore the Euler systems classes are "universal norms" in the K_∞/K direction: if $K \subseteq_f F \subseteq_f F' \subseteq K_\infty$, $\Sigma(F'/F)$ is empty, thus

$$\mathrm{cor}_{F'/F}(\mathbf{c}_{F'}) = \mathbf{c}_F.$$

Remark 3.3. Given $\mathcal{K}$ and $\mathcal{N}$ as before, an Euler system for $(T, \mathcal{K}, \mathcal{N})$ is equivalent to a collection

$$\{\tilde{\mathbf{c}}_{\mathfrak{m}} \in H^1(K^{\mathfrak{m}} \cap \mathcal{K}, T) \mid \mathfrak{m} \text{ is a modulus of } K\}$$

satisfying

$$\mathrm{cor}_{K^{\mathfrak{m}\mathfrak{q}} \cap \mathcal{K}/K^{\mathfrak{m}} \cap \mathcal{K}}(\tilde{\mathbf{c}}_{\mathfrak{m}\mathfrak{q}}) = \begin{cases} P(\mathrm{Fr}_{\mathfrak{q}}^{-1} \mid T^*; \mathrm{Fr}_{\mathfrak{q}}^{-1})\tilde{\mathbf{c}}_{\mathfrak{m}} & \text{if } \mathfrak{q} \nmid \mathfrak{m}\mathcal{N} \\ \tilde{\mathbf{c}}_{\mathfrak{m}} & \text{if } \mathfrak{q} \mid \mathfrak{m}\mathcal{N}. \end{cases}$$

Indeed, given such a collection, if $K \subseteq_f F$, we define

$$\mathbf{c}_F = \mathrm{cor}_{K^{\mathfrak{m}} \cap \mathcal{K}/F}(\tilde{\mathbf{c}}_{\mathfrak{m}}),$$

where $\mathfrak{m} = \mathfrak{f}(F/K)$ is the conductor of F/K. Then it is straightforward to check that the collection $\{\mathbf{c}_F\}$ is an Euler system. Conversely, given an Euler system $\mathbf{c} = \{\mathbf{c}_F\}$, for every modulus $\mathfrak{m}$ of K we define

$$\tilde{\mathbf{c}}_{\mathfrak{m}} = \prod P(\mathrm{Fr}_{\mathfrak{q}}^{-1} \mid T^*; \mathrm{Fr}_{\mathfrak{q}}^{-1})\mathbf{c}_{K^{\mathfrak{m}} \cap \mathcal{K}},$$

where the product is taken over primes $\mathfrak{q}$ dividing $\mathfrak{m}$, not dividing $\mathcal{N}$, unramified in $(K^{\mathfrak{m}} \cap \mathcal{K})/K$.

Remark 3.4. If we are given $\mathcal{N}$ and K_∞/K as in Definition 3.2 and $\mathfrak{t} = \mathfrak{q}_1 \cdots \mathfrak{q}_k$ is a squarefree product of finite primes not dividing $\mathcal{N}$, we can define $K(\mathfrak{t})$ to be the compositum

$$K(\mathfrak{t}) = K(\mathfrak{q}_1) \cdots K(\mathfrak{q}_k).$$

If $K \subseteq_f F \subseteq K_\infty$, we write $F(\mathfrak{t}) = FK(\mathfrak{t})$. Denoted by $K_{\min}$ the compositum of $\mathcal{K}_\infty$ and all $K(\mathfrak{q})$ for finite primes $\mathfrak{q}$ not dividing $\mathcal{N}$, then $\mathcal{K}_{\min}$ is the smallest extension of K satisfying Definition 3.2. Every finite extension of K in $\mathcal{K}_{\min}$ is contained in $F(\mathfrak{t})$ for some $K \subseteq_f F \subseteq K_\infty$ and some squarefree ideal τ prime to $\mathcal{N}$. It follows that an Euler system for $(T, \mathcal{K}_{\min}, \mathcal{N})$ is completely determined by the subcollection

$$\{\mathbf{c}_{F(\mathfrak{t})} \mid \mathfrak{t} \text{ is squarefree and prime to } \mathcal{N},\ K \subseteq_f F \subseteq K_\infty\}.$$

Conversely, suppose that we are given a collection $\{\mathbf{c}_{F(\mathfrak{t})}\}$ such that if

$$K \subseteq_f F \subseteq_f F' \subseteq K_\infty,$$

$\mathfrak{t}$ is a squarefree ideal of K prime to $\mathcal{N}$, and $\mathfrak{q}$ is a finite prime of $\mathcal{K}$ not dividing $\mathfrak{t}\mathcal{N}$ such that $K(\mathfrak{q}) \neq K$, then

$$\begin{aligned} \mathrm{cor}_{F(\mathfrak{t}\mathfrak{q})/F(\mathfrak{t})}(\mathbf{c}_{F(\mathfrak{t}\mathfrak{q})}) &= P(\mathrm{Fr}_{\mathfrak{q}}^{-1} \mid T^*; \mathrm{Fr}_{\mathfrak{q}}^{-1})\mathbf{c}_{F(\mathfrak{t})}, \\ \mathrm{cor}_{F'(\mathfrak{t})/F(\mathfrak{t})}(\mathbf{c}_{F'(\mathfrak{t})}) &= \mathbf{c}_{F(\mathfrak{t})} \end{aligned}$$

(if $K(\mathfrak{q}) = K$, then $F(\mathfrak{tq}) = F(\mathfrak{t})$). Then this collection determines an Euler system: for $K \subseteq_f L \subseteq \mathcal{K}_{\min}$, we can set

$$\mathbf{c}_L = \mathrm{cor}_{F(\mathfrak{t})/L}(\mathbf{c}_{F(\mathfrak{t})}),$$

where $\mathfrak{t}$ and F are minimal such that $L \subseteq F(\mathfrak{t})$. We conclude that we can view an Euler system for $(T, \mathcal{K}_{\min}, \mathcal{N})$ as such a collection $\{\mathbf{c}_{F(\mathfrak{t})}\}$.

Remark 3.5. Kolyvagin's original definition of Euler systems in [Kol90] required also an additional "congruence" condition, with which we will deal explicitly during the developing of the main conjecture. However, by the assumption that $\mathcal{K}$ contains K_∞, we can bypass the need for this condition, since it follows easily from the techniques used in Chapter IV of [Rub00].

3.2 Results over K

In the usual setting, we denote by $\mathfrak{p}$ the maximal ideal of $\mathcal{O}$ and $\mathbb{F} = \mathcal{O}/\mathfrak{p}$ the residue field. Following the notation above, let $K(1)$ be the maximal p-extension of K inside the Hilbert class field of K. We introduce two different sets of hypothesis on the Galois representation T: $\mathrm{Hyp}(K, T)$ and $\mathrm{Hyp}(K, V)$. The fomer is stronger than the latter, therefore it will allow us to get stronger conclusions.

$\mathrm{Hyp}(K, T)$:

(a) There is a $\tau \in G_K$ such that:

- τ is trivial on $\boldsymbol{\mu}_{p^\infty}$, on $(\mathcal{O}_K^\times)^{1/p^\infty}$ (the p-power roots of units in $(\mathcal{O}_K)^\times$) and on $K(1)$;
- $T/(\tau - 1)T$ is free of rank one over $\mathcal{O}$.

(b) $T \otimes \mathbb{F}$ is an irreducible $\mathbb{F}[G_K]$-module.

$\mathrm{Hyp}(K, V)$:

(a) There is a $\tau \in G_K$ such that:

- τ is trivial on $\boldsymbol{\mu}_{p^\infty}$, on $(\mathcal{O}_K^\times)^{1/p^\infty}$ and on $K(1)$;
- $\dim_\Phi(V/(\tau - 1))V = 1$.

(b) V is an irreducible $\Phi[G_K]$-module.

Remark 3.6. The hypotheses $\mathrm{Hyp}(K, T)$ are satisfied if the image of the Galois representation on T is "sufficiently large". They often hold in practice. For example, if the rank of T as $\mathcal{O}$-module is one, then they hold with $\tau = 1$.

Definition 3.7. The *index of divisibility* of an Euler system $\mathbf{c}$ is

$$\mathrm{ind}_{\mathcal{O}}(\mathbf{c}) = \sup\{n \mid \mathbf{c}_K \in \mathfrak{p}^n H^1(K, T) + H^1(K, T)_{\mathrm{tors}}\} \leq \infty.$$

This means that $\mathfrak{p}^{\mathrm{ind}_{\mathcal{O}}(\mathbf{c})}$ is the largest power of the maximal ideal by which $\mathbf{c}_K$ can be divided in $H^1(K,T)/H^1(K,T)_{\mathrm{tors}}$.

Given an $\mathcal{O}$-module A, we denote by $\ell_{\mathcal{O}}(A)$ the length of A, which can be ∞.

Define $\Omega = K(1)K(W)K(\boldsymbol{\mu}_{p^\infty}, (\mathcal{O}_K^\times)^{1/p^\infty})$, where $K(W)$ is the smallest extension of K such that its absolute Galois group acts trivially on W.

We denote by Σ_p the set of primes of K above p.

Theorem 3.8 ([Rub00], Chapter II, Theorem 2.2)**.** *Let* $\mathbf{c}$ *be an Euler system for* T*, with* T *satisfying* $\mathrm{Hyp}(K,T)$*. If* $p > 2$*, then*

$$\ell_{\mathcal{O}}(\mathcal{S}_{\Sigma_p}(K,W^*)) \leq \mathrm{ind}_{\mathcal{O}}(\mathbf{c}) + \mathfrak{n}_W + \mathfrak{n}_W^*,$$

where

$$\mathfrak{n}_W = \ell_{\mathcal{O}}(H^1(\Omega/K,W) \cap \mathcal{S}^{\Sigma_p}(K,W)),$$
$$\mathfrak{n}_W^* = \ell_{\mathcal{O}}(H^1(\Omega/K,W^*) \cap \mathcal{S}_{\Sigma_p}(K,W^*)).$$

Remark 3.9. Clearly our aim is to have this length as small as possible. The terms $\mathfrak{n}_W$ and $\mathfrak{n}_W^*$ are relate to the extension Ω/K, a nice extension we hope we can control. For example, if $K = \mathbf{Q}$ and $T = \mathbf{Z}_p(1)$, then Ω is just the well-behaved field $\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})$. Also, frequently, these "error terms" are zero.

Theorem 3.10 ([Rub00], Chapter II, Theorem 2.3)**.** *Let* $\mathbf{c}$ *be an Euler system for* T*, where* T *is not the one-dimensional trivial representation. If* V *satisfies* $\mathrm{Hyp}(K,V)$ *and* $\mathbf{c}_K \notin H^1(K,T)_{\mathrm{tors}}$*, then* $\mathcal{S}_{\Sigma_p}(K,W^*)$ *is finite.*

Remark 3.11. If $T = \mathcal{O}$, then $\mathcal{S}_{\Sigma_p}(K,W^*)$ is finite if and only if *Leopoldt's conjecture* holds for K (see [Rub00], Chapter I, Corollary 6.4).

Remark 3.12. For the trivial Euler system defined by $\mathbf{c}_{F(\mathfrak{t})} = 0$ for all F and $\mathfrak{t}$, Theorems 3.8 and 3.10 say nothing, since $\mathrm{ind}_{\mathcal{O}}(\mathbf{c}) = \infty$.

Remark 3.13. Despite all the Euler system $\mathbf{c}$ is needed in the proofs of these Theorems, only the class $\mathbf{c}_K$ appears in the statements. Also, these Theorems depend directly on the choice of the subspaces $H_f^1(K,V)$.

Note that Theorem 3.8 gives a bound for the size of $\mathcal{S}_{\Sigma_p}(K,W^*)$, not of the true Selmer group $\mathcal{S}(K,W^*)$. To get some information about $\mathcal{S}(K,W^*)$, we need to add an hypothesis regarding the choice of the subspaces $H_f^1(K_v,\cdot)$ for primes v dividing p. If L is a finite extension of $\mathbf{Q}_l$ for some prime l of $\mathbf{Q}$, $n = 0,1,2$ if l is finite, $n = 1$ if l is infinite, then the cup product and the bilinear map

$$V \times V^* \to \Phi(1),$$

given by the fact that $V^* = \mathrm{Hom}_{\mathcal{O}}(V, \Phi(1))$, induce a perfect pairing

$$H^n(K,V) \times H^{2-n}(K,V^*) \to H^2(K,\Phi(1)) \cong \Phi,$$

denoted by $\langle\ ,\ \rangle_{K_v}$. For a proof, we can just apply Propositions 1.25 and 1.26 to [Ser97], Section II.5.2.

To get our thesis, we have to require that the subspaces $H^1_f(K_v, V)$ and $H^1_f(K_v, V^*)$ are orthogonal complement under this pairing, for $v \mid p$. This is always true for $v \nmid p$ ([Rub00], Chapter I, Proposition 4.2). We write

$$H^1(K_p, \cdot\,) = \bigoplus_{v|p} H^1(K_v, \cdot\,)$$

and the same for H^1_f and H^1_s. Let $\mathrm{loc}^s_{\Sigma_p}$ denote the localization map

$$\mathrm{loc}^s_{\Sigma_p} \colon \mathcal{S}^{\Sigma_p}(K, T) \to H^1_s(K_p, T).$$

By Lemma 2.16 and [Rub00], Appendix B, Corollary 3.4, if $\mathbf{c}$ is an Euler system, then $\mathbf{c}_K \in \mathcal{S}^{\Sigma_p}(K, T) \subseteq H^1(K, T)$.

Corollary 3.14 ([Rub00], Chapter I, Corollary 7.5)**.** *There is an isomorphism*

$$\mathcal{S}(K, W^*)/\mathcal{S}_{\Sigma_p}(K, W^*) \cong \mathrm{Hom}_{\mathcal{O}}(\mathrm{coker}(\mathrm{loc}^s_{\Sigma_p}), \mathbf{D}). \tag{3.1}$$

Theorem 3.15. *Let* $\mathbf{c}$ *be an Euler system for* T *and suppose that*

$$\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K) \neq 0.$$

(a) *If* T *is not the one-dimensional trivial representation,* V *satisfies* $\mathrm{Hyp}(K, V)$*, and* $[H^1_s(K_p, T) : \mathcal{O}\,\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)]$ *is finite, then also* $\mathcal{S}(K, W^*)$ *is finite.*

(b) *If* $p > 2$ *and* T *satisfies* $\mathrm{Hyp}(K, T)$*, then*

$$\ell_{\mathcal{O}}(\mathcal{S}(K, W^*)) \leq \ell_{\mathcal{O}}(H^1_s(K_p, T)/\mathcal{O}\,\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)) + \mathfrak{n}_W + \mathfrak{n}^*_W.$$

Proof. We use Theorems 3.8 and 3.10 to bound $\mathcal{S}_{\Sigma_p}(K, W^*)$, and then (3.1) to control $[\mathcal{S}(K, W^*) : \mathcal{S}_{\Sigma_p}(K, W^*)]$.

(a) For every v, $H^1_s(K_v, T)$ is torsion free, since it injects into the vector space $H^1_s(K_v, V)$. Therefore, the hypothesis $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K) \neq 0$ implies that $\mathbf{c}_K \notin H^1(K, T)_{\mathrm{tors}}$. By Theorem 3.10, $\mathcal{S}_{\Sigma_p}(K, W^*)$ is finite and since, by (3.1),

$$\begin{aligned}[\mathcal{S}(K, W^*) : \mathcal{S}_{\Sigma_p}(K, W^*)] &= [H^1_s(K_p, T) : \mathrm{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K, T))] \\ &\leq [H^1_s(K_p, T) : \mathcal{O}\,\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)]\end{aligned}$$

we derive our first assertion.

(b) Also $H^1(K,T)/\mathcal{S}^{\Sigma_p}(K,T)$ is torsion free, since it injects in $\oplus_{v\nmid p} H^1_s(K_v,T)$. Therefore, for every n,

$$\begin{aligned}\mathbf{c}_k \in \mathfrak{p}^n H^1(K,T) + H^1(K,T)_{\text{tors}} &\Rightarrow \mathbf{c}_k \in \mathfrak{p}^n \mathcal{S}^{\Sigma_p}(K,T) + H^1(K,T)_{\text{tors}} \\ &\Rightarrow \text{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K,T)).\end{aligned}$$

Since $\text{loc}^s_{\Sigma_p}(\mathbf{c}_K) \neq 0$,

$$\text{ind}_{\mathcal{O}}(\mathbf{c}) \leq \ell_{\mathcal{O}}(\text{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K,T))/\mathcal{O}\,\text{loc}^s_{\Sigma_p}(\mathbf{c}_K)),$$

and by Theorem 3.8,

$$\ell_{\mathcal{O}}(\mathcal{S}_{\Sigma_p}(K,W^*)) \leq \ell_{\mathcal{O}}(\text{loc}^s_{\Sigma_p}(\mathcal{S}^{\Sigma_p}(K,T))/\mathcal{O}\,\text{loc}^s_{\Sigma_p}(\mathbf{c}_K)) + \mathfrak{n}_W + \mathfrak{n}^*_W.$$

Then again by (3.1), we derive our result.

□

3.3 Results over $\mathbf{Q}_\infty$

After the results for the base field K, we want to explore the $\mathbf{Z}_p^d$-extension K_∞. However, since our final goal is to prove theorems regarding the arithmetic of the cyclotomic extension of $\mathbf{Q}$, and since in Section 1.3 we gave properties in the particular case $d = 1$ for $\mathbf{Q}$, for this Section, we consider $K = \mathbf{Q}$ and we let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. These results can be found in the most general setting in [Rub00].

Let T be a p-adic representation of $G_{\mathbf{Q}}$ with coefficients in $\mathbf{Z}_p$ unramified outside a finite set of places. We write $\text{Hyp}(\mathbf{Q}_\infty, T)$ (resp. $\text{Hyp}(\mathbf{Q}_\infty, V)$) for $\text{Hyp}(\mathbf{Q}, T)$ (resp. $\text{Hyp}(\mathbf{Q}, V)$) with $G_{\mathbf{Q}}$ replaced by $G_{\mathbf{Q}_\infty}$:

$\text{Hyp}(\mathbf{Q}_\infty, T)$:

(a) There is a $\tau \in G_K$ such that:

- τ is trivial on $\boldsymbol{\mu}_{p^\infty}$;
- $T/(\tau - 1)T$ is free of rank one over $\mathbf{Z}_p$.

(b) T/pT is an irreducible $\mathbb{F}_p[G_{\mathbf{Q}_\infty}]$-module, where $\mathbb{F}_p$ is the field with p elements.

$\text{Hyp}(\mathbf{Q}_\infty, V)$:

(a) There is a $\tau \in G_K$ such that:

- τ is trivial on $\boldsymbol{\mu}_{p^\infty}$;
- $\dim_{\mathbf{Q}_p}(V/(\tau - 1))V = 1$.

(b) V is an irreducible $\mathbf{Q}_p[G_{\mathbf{Q}_\infty}]$-module.

Recall the Iwasawa algebra of the $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$:

$$\Lambda = \varprojlim_n \mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})].$$

Definition 3.16. We define the following Λ-modules:

$$\begin{aligned} \mathcal{S}_{\Sigma_p}(\mathbf{Q}_\infty, W^*) &= \varinjlim_n \mathcal{S}_{\Sigma_p}(\mathbf{Q}_n, W^*), \\ X_\infty &= \mathrm{Hom}(\mathcal{S}_{\Sigma_p}(\mathbf{Q}_\infty, W^*), \mathbf{Q}_p/\mathbf{Z}_p), \\ H^1_\infty(\mathbf{Q}, T) &= \varprojlim_n H^1(\mathbf{Q}_n, T), \end{aligned}$$

where the limits are taken respectively under restriction and corestriction maps.

Here, every $\mathcal{S}_{\Sigma_p}(\mathbf{Q}_n, W^*)$ has a structure of $\mathbf{Z}_p[\mathrm{Gal}(\mathbf{Q}_n/\mathbf{Q})]$-module, since this is true for $H^1(\mathbf{Q}_n, W^*)$ and also, fixed a prime $l \neq p$ of $\mathbf{Q}$, for $\oplus_{v|l} H^1(\mathbf{Q}_{n,v}, W^*)$, by [Rub00], Section B.5. On the Pontryagin dual, Γ acts by $\gamma f(x) = f(\gamma^{-1}x)$, therefore the action of $\Lambda = \mathbf{Z}_p[[T]]$ is the following:

$$g(T)f(x) = f(g((1+T)^{-1} - 1)x).$$

Definition 3.17. If $\mathbf{c}$ is an Euler system, we let $\mathbf{c}_{\mathbf{Q},\infty}$ denote the corresponding element of $H^1_\infty(K, T)$. Define an ideal

$$\mathrm{ind}_\Lambda(\mathbf{c}) = \{\phi(\mathbf{c}_{\mathbf{Q},\infty}) \mid \phi \in \mathrm{Hom}_\Lambda(H^1_\infty(K, T), \Lambda)\} \subseteq \Lambda.$$

The ideal ind_Λ is the analogue for Λ of the index of divisibility $\mathrm{ind}_{\mathbf{Z}_p}(\mathbf{c})$ we introduced before. The next three Theorems are proved generalizing Theorem 3.8 for every $\mathbf{Q}_n$, and then passing to the limit. The first, is usually known as *weak Leopoldt conjecture* for T. Consider an Euler system $\mathbf{c}$ for $(T, \mathbf{Q}_\infty)$.

Theorem 3.18 ([Rub00], Chapter II, Theorem 3.2)**.** *If V satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$ *and $\mathbf{c}_{\mathbf{Q},\infty} \notin H^1_\infty(K, T)_{\Lambda-\mathrm{tors}}$, then X_∞ is finitely generated a torsion Λ-module.*

Theorem 3.19 ([Rub00], Chapter II, Theorem 3.3)**.** *If T satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$*, then*

$$\mathrm{char}(X_\infty) \text{ divides } \mathrm{ind}_\Lambda(\mathbf{c}).$$

Theorem 3.20 ([Rub00], Chapter II, Theorem 3.4)**.** *If V satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$*, then there exists a nonnegative integer t such that*

$$\mathrm{char}(X_\infty) \text{ divides } p^t \,\mathrm{ind}_\Lambda(\mathbf{c}).$$

Remark 3.21. Again, these Theorems give bounds for the size of $\mathcal{S}_{\Sigma_p}(\mathbf{Q}_\infty, W^*)$. We see now how to deduce results concerning the true Selmer group $\varinjlim \mathcal{S}(\mathbf{Q}_n, W^*)$.

We need some assumptions about the choices of subspaces $H^1_f(\mathbf{Q}_{n,p}, V) \subseteq H^1(\mathbf{Q}_{n,p}, V)$ and $H^1_f(\mathbf{Q}_{n,p}, V^*) \subseteq H^1(\mathbf{Q}_{n,p}, V^*)$:

- $H^1_f(\mathbf{Q}_{n,p}, V)$ and $H^1_f(\mathbf{Q}_{n,p}, V^*)$ are orthogonal complements under the cup product pairing

$$H^1(\mathbf{Q}_{n,p}, V) \times H^1(\mathbf{Q}_{n,p}, V^*) \to H^2(\mathbf{Q}_{n,p}, \mathbf{Q}_p(1)) = \mathbf{Q}_p.$$

- If $m \geq n$, then

$$\begin{aligned} \mathrm{cor}_{\mathbf{Q}_{m,p}/\mathbf{Q}_{n,p}} H^1_f(\mathbf{Q}_{m,p}, V) &\subseteq H^1_f(\mathbf{Q}_{n,p}, V), \\ \mathrm{res}_{\mathbf{Q}_{m,p}/\mathbf{Q}_{n,p}} H^1_f(\mathbf{Q}_{n,p}, V^*) &\subseteq H^1_f(\mathbf{Q}_{m,p}, V^*). \end{aligned}$$

These requirements ensure that for $m \geq n$, the restriction and corestriction maps induces respectively

$$\begin{aligned} S(\mathbf{Q}_n, W^*) &\to \mathcal{S}(\mathbf{Q}_m, W^*), \\ H^1_s(\mathbf{Q}_{m,p}, T) &\to H^1_s(\mathbf{Q}_{n,p}, T), \end{aligned}$$

and so we can define the following Λ-modules:

$$\begin{aligned} \mathcal{S}(\mathbf{Q}_\infty, W^*) &= \varinjlim_n \mathcal{S}(\mathbf{Q}_n, W^*), \\ H^1_{\infty,s}(\mathbf{Q}_p, T) &= \varprojlim_n H^1_s(\mathbf{Q}_{n,p}, T). \end{aligned}$$

Proposition 3.22. *Denote by* $\mathrm{loc}^s_{\Sigma_p}$ *the localization map*

$$\mathrm{loc}^s_{\Sigma_p} \colon H^1_\infty(\mathbf{Q}, T) \to H^1_{\infty,s}(\mathbf{Q}_p, T).$$

Then there is an exact sequence

$$0 \to H^1_{\infty,s}(\mathbf{Q}_p, T)/\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(\mathbf{Q}, T)) \to \mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W^*), \mathbf{Q}_p/\mathbf{Z}_p) \to X_\infty \to 0.$$

Proof. Again by [Rub00], Appendix B, Corollary 3.4,

$$H^1_\infty(\mathbf{Q}, T) = \varprojlim_n \mathcal{S}^{\Sigma_p}(\mathbf{Q}_n, T).$$

Then the assertion follows passing to direct limit from (3.1) and then applying $\mathrm{Hom}(\,\cdot\,, \mathbf{Q}_p/\mathbf{Z}_p)$. □

Theorem 3.23. *If* V *satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, V)$, $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty}) \notin H^1_{\infty,s}(\mathbf{Q}_p, T)_{\Lambda-\mathrm{tors}}$ *and* $H^1_{\infty,s}(\mathbf{Q}_p, T)/\Lambda\,\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty})$ *is a finitely generated torsion* Λ*-module, then*

(a) $\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W^*), \mathbf{Q}_p/\mathbf{Z}_p)$ *is a finitely generated torsion* Λ*-module.*

(b) *There is a nonnegative integer* t *such that*

$$\mathrm{char}(\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W^*), \mathbf{Q}_p/\mathbf{Z}_p)) \text{ divides } p^t \,\mathrm{char}(H^1_{\infty,s}(\mathbf{Q}_p, T)/\Lambda \,\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty})).$$

If in addiction T *satisfies* $\mathrm{Hyp}(\mathbf{Q}_\infty, T)$*, then*

$$\mathrm{char}(\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W^*), \mathbf{Q}_p/\mathbf{Z}_p)) \text{ divides } \mathrm{char}(H^1_{\infty,s}(\mathbf{Q}_p, T)/\Lambda \,\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty})).$$

Proof.

(a) Since $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty}) \notin H^1_{\infty,s}(\mathbf{Q}_p, T)_{\Lambda-\mathrm{tors}}$, $\mathbf{c}_{\mathbf{Q},\infty} \notin H^1_\infty(\mathbf{Q}, T)_{\Lambda-\mathrm{tors}}$. Therefore, by 3.18, X_∞ is a finitely generated torsion Λ-module, and by 3.22, also

$$\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W^*), \mathbf{Q}_p/\mathbf{Z}_p)$$

is a finitely generated torsion Λ-module such that

$$\mathrm{char}(\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W^*), \mathbf{Q}_p/\mathbf{Z}_p)) = \mathrm{char}(X_\infty)\,\mathrm{char}(H^1_{\infty,s}(\mathbf{Q}_p, T)/\,\mathrm{loc}_{\Sigma_p}(H^1_\infty(\mathbf{Q}, T))).$$

(b) By our assumptions, $\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(\mathbf{Q}, T))$ is a rank one Λ-module, therefore there is a pseudo-isomorphism

$$\psi\colon\ \mathrm{loc}^s_{\Sigma_p}(H^1_\infty(\mathbf{Q}, T)) \to \Lambda.$$

We deduce that

$$\begin{aligned}\psi(\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty}))\Lambda &= \mathrm{char}(\psi(\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(\mathbf{Q}, T)))/\psi(\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty}))\Lambda) \\ &\supset \mathrm{char}(\mathrm{loc}^s_{\Sigma_p}(H^1_\infty(\mathbf{Q}, T)))/(\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_{\mathbf{Q},\infty}))\Lambda).\end{aligned}$$

The assertions then follow from the definition of $\mathrm{ind}_\Lambda(\mathbf{c})$ and by the divisibilities of Theorems 3.19 and 3.20.

□

3.4 Twisting by characters of finite order

For this Section, we come back to a more general situation: K is a number field, T is a p-adic representation of G_K and $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$. We discuss a little more about the field $\mathcal{K}$: the results described in the previous Sections does not depend on $\mathcal{K}$, except that it has to contain K_∞, therefore generally we can ignore it, taking just $\mathcal{K} = \mathcal{K}_{\min}$. However, if $\mathcal{K}$ is not the minimal field, it contains more information, and now we see a way to use this extra information, using characters.

If $\chi\colon G_K \to \mathcal{O}^\times$ is a character of finite order, then we can denote by $\mathcal{O}_\chi$ a free, rank-one $\mathcal{O}$-module on which G_K acts via χ, fixing a generator ξ_χ. We write $T \otimes \chi$ for the representation $T \otimes_{\mathcal{O}} \mathcal{O}_\chi$.

Definition 3.24. If $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$ and

$$\chi\colon \mathrm{Gal}(\mathcal{K}/K) \to \mathcal{O}^\times$$

is a character of finite order, then consider $L = \mathcal{K}^{\ker(\chi)}$, the field cut out by χ. For $K \subseteq_f F \subseteq \mathcal{K}$ we define $\mathbf{c}_F^\chi \in H^1(F, T \otimes \chi)$ to be the image of $\mathbf{c}_{FL}$ under the composition

$$H^1(FL, T) \xrightarrow{\otimes \xi_\chi} H^1(FL, T) \otimes \mathcal{O}_\chi \cong H^1(FL, T \otimes \chi) \xrightarrow{\mathrm{cor}} H^1(F, T \otimes \chi),$$

where the isomorphism depends on the fact that G_{FL} is in the kernel of χ.

Proposition 3.25. *Suppose* $\mathbf{c}$ *is an Euler system for* $(T, \mathcal{K}, \mathcal{N})$ *and*

$$\chi\colon \mathrm{Gal}(\mathcal{K}/K) \to \mathcal{O}^\times$$

is a character of finite order. If $\mathfrak{f}$ *is the conductor of* χ *(that is, the conductor of the field cut out by* χ*), then the collection*

$$\{\mathbf{c}_F^\chi \mid K \subseteq_f F \subseteq \mathcal{K}\}$$

defined above is an Euler system for $(T \otimes \chi, \mathcal{K}, \mathfrak{f}\mathcal{N})$.

Proof. If $K \subseteq_f F \subseteq_f F' \subseteq \mathcal{K}$, then

$$\begin{aligned}
\mathrm{cor}_{F'/F}(\mathbf{c}_{F'}^\chi) &= \mathrm{cor}_{F'L/F}(\mathbf{c}_{F'L} \otimes \xi_\chi) \\
&= \mathrm{cor}_{FL/L}((\mathrm{cor}_{F'L/FL}\, \mathbf{c}_{F'L}) \otimes \xi_\chi) \\
&= \mathrm{cor}_{FL/F}\left(\Big(\prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1} \mid T^*; \mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{c}_{FL}\Big) \otimes \xi_\chi\right) \\
&= \mathrm{cor}_{FL/F}\left(\prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1} \mid T^*; \chi(\mathrm{Fr}_\mathfrak{q})\,\mathrm{Fr}_\mathfrak{q}^{-1})(\mathbf{c}_{FL} \otimes \xi_\chi)\right) \\
&= \prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1} \mid T^*; \chi(\mathrm{Fr}_\mathfrak{q})\,\mathrm{Fr}_\mathfrak{q}^{-1})\,\mathrm{cor}_{FL/F}(\mathbf{c}_{FL} \otimes \xi_\chi) \\
&= \prod_{\mathfrak{q} \in \Sigma(F'L/FL)} P(\mathrm{Fr}_\mathfrak{q}^{-1} \mid (T \otimes \chi)^*; \mathrm{Fr}_\mathfrak{q}^{-1})\mathbf{c}_F^\chi,
\end{aligned}$$

where

$$P(\mathrm{Fr}_\mathfrak{q}^{-1} \mid (T \otimes \chi)^*; x) = \det(1 - \mathrm{Fr}_\mathfrak{q}^{-1}\, x \mid (T \otimes \chi)^*),$$

and

$$\begin{aligned}
\Sigma(F'L/FL) &= \{\text{primes } \mathfrak{q} \text{ not dividing } \mathcal{N} \text{ that ramify in } F'L \text{ but not in } FL\} \\
&= \{\text{primes } \mathfrak{q} \text{ not dividing } \mathfrak{f}\mathcal{N} \text{ that ramify in } F' \text{ but not in } F\}.
\end{aligned}$$

This proves our result. □

Lemma 3.26. *If $K \subseteq_f F \subseteq K_\infty$, $L \subseteq L' \subseteq \mathcal{K}$ and the conductor of L'/K is equal to the conductor of L/K, then the image of $\mathbf{c}_F^\chi$ under the composition*

$$H^1(F, T \otimes \chi) \xrightarrow{\text{res}} H^1(FL', T \otimes \chi) \xrightarrow{\otimes \xi_\chi^{-1}} H^1(FL', T)$$

is

$$\sum_{\delta \in \mathrm{Gal}(FL'/F)} \chi(\delta)\delta(\mathbf{c}_{FL'}).$$

Proof. Since the conductors are equal, every prime which ramifies in L'/K ramifies also in L/K, therefore

$$\mathrm{cor}_{FL'/FL}\, \mathbf{c}_{FL'} = \mathbf{c}_{FL}.$$

We deduce that

$$\begin{aligned}(\mathrm{res}_{FL'/F}\, \mathrm{cor}_{FL/F}(\mathbf{c}_{FL} \otimes \xi_\chi)) \otimes \xi_\chi^{-1} &= (\mathrm{res}_{FL'/F}\, \mathrm{cor}_{FL'/F}(\mathbf{c}_{FL'} \otimes \xi_\chi)) \otimes \xi_\chi^{-1} \\ &= \left(\sum_{\delta \in \mathrm{Gal}(FL'/F)} \delta(\mathbf{c}_{FL'} \otimes \xi_\chi) \right) \otimes \xi_\chi^{-1} \\ &= \sum_{\delta \in \mathrm{Gal}(FL'/F)} \chi(\delta)\delta(\mathbf{c}_{FL'}). \qquad \square\end{aligned}$$

Chapter 4

Main conjecture

4.1 Cyclotomic Euler system

Take $K = \mathbf{Q}$, and consider the cyclotomic representation $\mathbf{Z}_p(1)$, induced by the cyclotomic character

$$\chi_p \colon G_{\mathbf{Q}} \to \mathbf{Z}_p^{\times}.$$

An equivalent description of the character is the following: for every n, the projections

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^n})/\mathbf{Q})$$

give rise to an inverse systems of maps

$$G_{\mathbf{Q}} \to (\mathbf{Z}/p^n\mathbf{Z})^{\times},$$

from which we get the desired map

$$G_{\mathbf{Q}} \to \mathbf{Z}_p^{\times}.$$

In particular, from this construction, it follows easily that the cyclotomic character is unramified outside p, since every prime different from p is unramified in every $\mathbf{Q}(\boldsymbol{\mu}_{p^n})/\mathbf{Q}$, and so it has trivial inertia.

This means that it makes sense to ask for an Euler system for $T = \mathbf{Z}_p(1)$. As "big" field $\mathcal{K}$ we can consider $\mathbf{Q}^{\mathrm{ab}}$, which contains every abelian extension of $\mathbf{Q}$, so in particular the cyclotomic extension $\mathbf{Q}_\infty$ and all the maximal p-extensions contained in the ray class fields modulo finite primes different from p. As ideal, $\mathcal{N}$ will be the ideal generated by p; we will call it simply p. Therefore we are looking for an Euler system for $(\mathbf{Z}_p(1), \mathbf{Q}^{\mathrm{ab}}, p)$.

There are two sorts of modulus for $\mathbf{Q}$: $\mathfrak{m} = m$ and $\mathfrak{m} = m\infty$, where m is an integer and ∞ is the unique real embedding $\mathbf{Q} \hookrightarrow \mathbf{R}$. The ray class field modulo m is $\mathbf{Q}(\boldsymbol{\mu}_m)^+$, while the ray class field modulo $m\infty$ is $\mathbf{Q}(\boldsymbol{\mu}_m)$. Both are already contained in $\mathbf{Q}^{\mathrm{ab}}$, thus, by Remark 3.3, an Euler system for

$(\mathbf{Z}_p(1), \mathbf{Q}^{\mathrm{ab}}, p)$ consists in a collection $\{\tilde{\mathbf{c}}_{m\infty}, \tilde{\mathbf{c}}_m\}$ satisfying the compatibility conditions, where

$$\begin{aligned} \tilde{\mathbf{c}}_{m\infty} &\in H^1(\mathbf{Q}(\boldsymbol{\mu}_m), \mathbf{Z}_p(1)), \\ \tilde{\mathbf{c}}_m &\in H^1(\mathbf{Q}(\boldsymbol{\mu}_m)^+, \mathbf{Z}_p(1)). \end{aligned}$$

The conditions to be satisfied are related to corestriction maps and to the Euler factor

$$P(\mathrm{Fr}_l^{-1} \mid \mathbf{Z}_p(1)^*; x) = \det(1 - \mathrm{Fr}_l^{-1}\, x \mid \mathbf{Z}_p(1)^*),$$

for $l \neq p$ rational prime. But

$$\mathbf{Z}_p(1)^* = \mathrm{Hom}(\mathbf{Z}_p(1), \mathbf{Z}_p(1)) = \mathbf{Z}_p$$

with trivial $G_{\mathbf{Q}}$ action, therefore

$$P(\mathrm{Fr}_l^{-1} \mid \mathbf{Z}_p(1)^*; x) = 1 - x.$$

For every number field F, we have seen that

$$H^1(F, \mathbf{Z}_p(1)) = \varprojlim_n F^\times/(F^\times)^{p^n} = (F^\times)\widehat{\ },$$

the p-adic completion of $F^\times$. In particular, there is a natural injection

$$F^\times \hookrightarrow H^1(F, \mathbf{Z}_p(1)),$$

which we can use to define the classes. With this in mind, we fix a collection $\{\zeta_m \mid m \geq 1\}$, where every ζ_m is a primitive m-th root of unity such that $\zeta_{mn}^n = \zeta_m$ for every m and n. For example, we can embed $\overline{\mathbf{Q}}$ in $\mathbf{C}$ and pick $\zeta_m = e^{2\pi i/m}$. If L/F is a finite Galois extension, denote by $N_{L/K}$ the field norm: for any $\alpha \in L$,

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha) \in K.$$

Then the collection $\{\zeta_m \mid m \geq 1\}$ satisfy the following relations:

$$N_{\mathbf{Q}(\boldsymbol{\mu}_{ml})/\mathbf{Q}(\boldsymbol{\mu}_m)}(1-\zeta_{ml}) = \begin{cases} 1 - \zeta_m & \text{if } l \mid m \\ (1 - \mathrm{Fr}_l^{-1})(1 - \zeta_m) & \text{if } l \nmid m \text{ and } m > 1\,, \\ l & \text{if } m = 1 \end{cases} \quad (4.1)$$

where l is a prime and Fr_l is the Frobenius of l in $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q})$.

Remark 4.1. From now on, despite working with multiplicative groups, we will use additive notation for $\mathbf{Q}(\boldsymbol{\mu}_m)^\times$.

This (pleasant) computation can be found in Section 6.3 of [Lan90]. Then for $m \geq 1$ we can define

$$\tilde{\mathbf{c}}_{m\infty} = N_{\mathbf{Q}(\boldsymbol{\mu}_{mp})/\mathbf{Q}(\boldsymbol{\mu}_m)}(1-\zeta_{mp}) \in \mathbf{Q}(\boldsymbol{\mu}_m)^\times \subseteq H^1(\mathbf{Q}(\boldsymbol{\mu}_m), \mathbf{Z}_p(1)),$$
$$\tilde{\mathbf{c}}_m = N_{\mathbf{Q}(\boldsymbol{\mu}_m)/\mathbf{Q}(\boldsymbol{\mu}_m)^+}(\tilde{\mathbf{c}}_{m\infty}) \in (\mathbf{Q}(\boldsymbol{\mu}_m)^+)^\times \subseteq H^1(\mathbf{Q}(\boldsymbol{\mu}_m)^+, \mathbf{Z}_p(1)).$$

To check that this is an Euler system, we need to verify the compatibility conditions; since these elements are defined at cohomological level zero, by the structure of $H^1(F, \mathbf{Z}_p(1))$ for every number field F and by Proposition 1.22, it is enough to study the corestriction at level zero, where it is just the field norm. The Equation 4.1 precisely tells us that these elements verify the needed congruence, since for every prime $l \neq p$,

$$P(\mathrm{Fr}_l^{-1} \mid \mathbf{Z}_p(1)^*; \mathrm{Fr}_l^{-1}) = 1 - \mathrm{Fr}_l^{-1},$$

and therefore $\{\tilde{\mathbf{c}}_{m\infty}, \tilde{\mathbf{c}}_m\}$ is an Euler system for $(\mathbf{Z}_p(1), \mathbf{Q}^{\mathrm{ab}}, p)$.

To get the information we need to prove the main conjecture, we do not use directly the Euler system, but a collection of cohomology elements associated to them. Also, not all the system is needed: fix an integer $n > 0$ and let $F = \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})^+$. Define $\mathscr{P}$ to be the set of positive squarefree integers divisible only by primes l splitting completely in $F/\mathbf{Q}$, that is,

$$l \equiv \pm 1 \pmod{p^{n+1}}.$$

Every $r \in \mathscr{P}$ is coprime with p, therefore we write

$$G_r = \mathrm{Gal}(F(\boldsymbol{\mu}_r)/F) \cong \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_r)/\mathbf{Q}).$$

We denote by N_r the norm operator

$$N_r = \sum_{\tau \in G_r} \tau \in \mathbf{Z}[G_r],$$

and since, by Theorem 1.14 of Chapter VI in [Lan02], there is a natural isomorphism $G_r \cong \prod_{l|r} G_l$ (implicitly taken on all the prime divisors), we have

$$N_r = \prod_{l|r} N_l \in \mathbf{Z}[G_r].$$

When $l \in \mathscr{P}$ is a prime not dividing r, we can identify $G_l = \mathrm{Gal}(F(\boldsymbol{\mu}_l)/F)$ with $\mathrm{Gal}(F(\boldsymbol{\mu}_{rl})/F(\boldsymbol{\mu}_r))$, and Fr_l will denote the Frobenius of l in G_r, the automorphism sending each r-th root of unity to its l-th power. Since for every prime $l \in \mathscr{P}$ the group G_l is cyclic of order $l-1$, we can fix a generator σ_l.

Definition 4.2. If $r \in \mathscr{P}$, the *r-th derivative element* is

$$D_r = \prod_{l|r} D_l \in \mathbf{Z}[G_r],$$

where for every prime $l \in \mathscr{P}$,

$$D_l = \sum_{i=1}^{l-2} i\sigma_l^i \in \mathbf{Z}[G_l].$$

This operator satisfies an important relation:

Lemma 4.3. *For every $l \in \mathscr{P}$ prime, we have*

$$(\sigma_l - 1)D_l = (l-1) - N_l.$$

Proof.

$$\sigma_l D_l = \sum_{i=1}^{l-2} i\sigma_l^{i+1} = \sum_{i=1}^{l-1}(i-1)\sigma_l^i = \sum_{i=1}^{l-1} i\sigma_l^i - \sum_{i=1}^{l-1}\sigma_l^i = (D_l + l - 1) - N_l. \quad \square$$

Fix now an odd integer M, which will be a large power of some prime p. We set

$$\mathscr{P}_M = \{r \in \mathscr{P} \mid r \text{ is divisible by only primes } l \equiv 1 \pmod{M}\}.$$

The elements of the Euler system we will use are the ones of $F(\boldsymbol{\mu}_r)$, for $r \in \mathscr{P}_M$. We denote them by α_r:

$$\alpha_r = N_{\mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}r})/F(\boldsymbol{\mu}_r)}(1 - \zeta_{p^{n+1}r}) = (1 - \zeta_{p^{n+1}}\zeta_r)(1 - \zeta_{p^{n+1}}^{-1}\zeta_r) \in F(\boldsymbol{\mu}_r)^\times.$$

Remark 4.4. We are using a little abuse of notation here, since it is not true that $\zeta_{p^{n+1}r} = \zeta_{p^{n+1}}\zeta_r$, but instead $\zeta_{p^{n+1}r} = \zeta'_{p^{n+1}}\zeta'_r$, for some other primitive roots of unity.

These elements satisfy, for $l \nmid r$, $l \in \mathscr{P}$:

$$N_l(\alpha_{rl}) = (\mathrm{Fr}_l - 1)\alpha_r.$$

Remark 4.5. These units also satisfy

$$\alpha_{rl} \equiv \alpha_r \pmod{\mathscr{L}},$$

for every prime $\mathscr{L}$ of $F(\boldsymbol{\mu}_r)$ above l, since $\zeta_l \equiv 1 \pmod{\mathscr{L}}$, which is true since the residue field modulo $\mathscr{L}$ has characteristic l. This is exactly the Kolyvagin additional congruence we cited in Remark 3.5.

Lemma 4.6. *If $r \in \mathscr{P}_M$, then the class of $D_r\alpha_r$ belongs to*

$$[F(\boldsymbol{\mu}_r)^\times/(F(\boldsymbol{\mu}_r)^\times)^M]^{G_r}.$$

Proof. We work by induction of the number of prime divisors of r. If $r = 1$, $G_r = 1$, so the result is clear. If $r = ls$ with $l, s \in \mathscr{P}_M$, l prime, then

$$(\sigma_l - 1)D_r\alpha_r = (l - 1 - N_l)D_s\alpha_r = (l-1)D_s\alpha_r + (1 - \mathrm{Fr}_l)D_s\alpha_s,$$

using the Euler system relation. The last term is congruent to $(1 - \mathrm{Fr}_l)D_s\alpha_s$ modulo $(F(\boldsymbol{\mu}_r)^\times)^{l-1}$. By inductive hypothesis,

$$(1 - \mathrm{Fr}_l)D_s\alpha_s \in (F(\boldsymbol{\mu}_s)^\times)^M,$$

and since $l \equiv 1 \pmod{M}$ and G_r is generated by all the σ_l for $l \mid r$ prime, the assertion follows. □

Note that since M is odd and F is real, $\boldsymbol{\mu}_M \cap F = \{1\}$, and also $\boldsymbol{\mu}_M \cap F(\boldsymbol{\mu}_r) = \{1\}$, because M and r are coprime. This means that G_r acts trivially on $\boldsymbol{\mu}_M$, and applying the Hochschild-Serre exact sequence (Proposition 1.17) to $G = G_{F(\boldsymbol{\mu}_r)}$ and $H = G_F$, we deduce that

$$[F(\boldsymbol{\mu}_r)^\times/(F(\boldsymbol{\mu}_r)^\times)^M]^{G_r} \cong H^1(F(\boldsymbol{\mu}_r), \boldsymbol{\mu}_M)^{G_r} \cong H^1(F, \boldsymbol{\mu}_M) \cong F^\times/(F^\times)^M.$$

In particular, there is a unique element $\kappa_r \in F^\times/(F^\times)^M$, called *Kolyvagin derivative* of α_r, corresponding to the element $D_r\alpha_r$. Denoted by $\tilde{\kappa}_r$ a lift of κ_r in $F^\times$, there exists an element $\beta_r \in F(\boldsymbol{\mu}_r)^\times$ such that

$$D_r\alpha_r = \tilde{\kappa}_r\beta_r^M.$$

If we make things explicit, this element satisfies

$$(\sigma - 1)\beta_r = [(\sigma - 1)D_r\alpha_r]^{1/M},$$

for every $\sigma \in G_r$.

Denote by I_F the group of fractional ideals of F. It is the free abelian group generated by the finite primes λ of $\mathcal{O}_F$, so using additive notation we write

$$I_F = \bigoplus_\lambda \mathbf{Z}\lambda = \bigoplus_l I_l,$$

where for every rational prime l we set

$$I_l = \bigoplus_{\lambda \mid l} \mathbf{Z}\lambda.$$

If $y \in F^\times$, we write:

- (y) for the principal ideal generated by y;
- $(y)_l$ for its projection in I_l;

- $[y]$ for its projection in I_F/MI_F;
- $[y]_l$ for its projection in I_l/MI_l,

We remark how $[y]$ and $[y]_l$ are well-defined also for $y \in F^\times/(F^\times)^M$. Let $G = \mathrm{Gal}(F/\mathbf{Q})$. Recall that a map is *$G$-equivariant* if it is a homomorphism of G-modules.

Lemma 4.7. *If l splits completely in F and $l \equiv 1 \pmod{M}$, then there exists an unique G-equivariant surjection*

$$\varphi_l \colon (\mathcal{O}_F/l\mathcal{O}_F)^\times \to I_l/MI_l$$

such that the following diagram is commutative:

$$\begin{array}{ccc} & F(\boldsymbol{\mu}_l)^\times & \\ {\scriptstyle x\mapsto(1-\sigma_l)x}\swarrow & & \searrow{\scriptstyle x\mapsto[N_l x]_l} \\ (\mathcal{O}_F/l\mathcal{O}_F)^\times & \xrightarrow[\varphi_l]{} & I_l/MI_l \end{array}$$

Proof. First, note that since l splits completely in F, every prime λ of F above is totally ramified in $F(\boldsymbol{\mu}_l)$. In particular, we can identify $\mathcal{O}_{F(\boldsymbol{\mu}_l)}/\lambda'$ with $\mathcal{O}_F/\lambda$, where λ' is the prime above λ. We have

$$\mathcal{O}_F/l\mathcal{O}_F \cong \prod_{\lambda|l} \mathcal{O}_F/\lambda \cong \prod_{\lambda'|l} \mathcal{O}_{F(\boldsymbol{\mu}_l)}/\lambda'.$$

Since for every $x \in F(\boldsymbol{\mu}_l)^\times$ and for every prime $\lambda' \mid l$ of $F(\boldsymbol{\mu}_l)$, $v_{\lambda'}(\sigma_l x) = v_{\lambda'}(x)$, $x/\sigma_l x$ is a unit in the completion of $F(\boldsymbol{\mu}_l)$ with respect to λ'. In particular, we get a the well-defined G-equivariant vertical map on the left, which is surjective since every prime of F above l is also tamely ramified. Also the G-equivariant map on the right is surjective, because the primes of F above l are totally ramified. The kernel of the left-hand map is the subgroup

$$\{x \in F(\boldsymbol{\mu}_l)^\times \mid x \text{ has valuation divisible by } l-1 \text{ at all primes above } l\}.$$

If x is in this kernel, then M, which divides $l-1$, divides $v_\lambda(x)$ for every $\lambda \mid l$ prime of F, thus x is also in the kernel of the right-hand map. The assertion then follows. □

For a prime l as in Lemma 4.7, we denote by φ_l also the induced homomorphism

$$\varphi_l \colon \{y \in F^\times/(F^\times)^M \mid [y]_l = 0\} \to I_l/MI_l :$$

every $y \in F^\times/(F^\times)^M$ such that $[y]_l = 0$ can be seen as element of $\mathcal{O}_F/l\mathcal{O}_F$, and then send to I_l/MI_l as in the Lemma. Also, it follows that the kernel of φ_l consists of the elements which are M-th power modulo λ, for all λ above l.

Proposition 4.8 (Kolyvagin)**.** *Suppose $r \in \mathscr{P}_M$ and l is a rational prime.*

(a) *If $l \nmid r$, then $[\kappa_r]_l = 0$.*

(b) *If $l \mid r$, then $[\kappa_r]_l = \varphi_l(\kappa_{r/l})$.*

Proof. First, we remark how if a prime l does not divide $r \in \mathscr{P}_M$, then $\tilde{\kappa}_r$ can be chosen so that β_r is a unit at all primes above l, that is, if $\lambda' \mid l$ is a prime of $F(\boldsymbol{\mu}_r)$, then $v_{\lambda'}(\beta_r) = 0$. This easily follows from the fact that no primes over l ramifies in $F(\boldsymbol{\mu}_r)/F$.

(a) If $l \nmid r$, then β_r is a unit at all primes above l, and this is also true for $\tilde{\kappa}_r$, since $D_r\alpha_r$ is a unit. Therefore the result follows.

(b) If $r = ls$, then we can find $\beta_r \in F(\boldsymbol{\mu}_r)^\times$ and $\beta_s \in F(\boldsymbol{\mu}_s)^\times$ such that

$$(\sigma - 1)\beta_r = [(\sigma - 1)D_r\alpha_r]^{1/M},$$
$$(\sigma - 1)\beta_s = [(\sigma - 1)D_s\alpha_s]^{1/M},$$

where we can assume that β_s is a unit at all the primes above l. By

$$\tilde{\kappa}_r\beta_r^M = D_r\alpha_r,$$

we deduce that the valuation of β_r^M at every prime of $F(\boldsymbol{\mu}_r)$ above l has to be a multiple of $l - 1$, the ramification index. Also, since for these primes there is no ramification in $F(\boldsymbol{\mu}_r)/F(\boldsymbol{\mu}_r)$ (so the completions have the same uniformizer), we deduce that we can find an element $\gamma \in F(\boldsymbol{\mu}_l)^\times$ such that $\beta_r\gamma^{(l-1)/M}$ has trivial valuation, so is a unit, at all primes above l. Clearly $N_l(\gamma)$ and γ^{l-1} have the same valuation, and again by the previous equality, we get

$$[N_l\gamma]_l = [\kappa_r]_l.$$

Therefore, modulo any prime above l of $F(\boldsymbol{\mu}_r)$ (which is totally ramified over F), using the properties introduced in this Section, we find

$$\begin{aligned}(1 - \sigma_l)\gamma^{(l-1)/M} &\equiv (\sigma_l - 1)\beta_r = [((l-1) - N_l)D_s\alpha_r]^{1/M} \\ &= \frac{D_s\alpha_r^{(l-1)/M}}{[(\mathrm{Fr}_l - 1)D_s\alpha_s]^{1/M}} \equiv \frac{D_s\alpha_s^{(l-1)/M}}{(\mathrm{Fr}_l - 1)\beta_s} \\ &\equiv \left(\frac{D_s\alpha_s}{\beta_s^M}\right)^{(l-1)/M} = \tilde{\kappa}_r^{(l-1)/M}.\end{aligned}$$

We conclude applying the diagram of Lemma 4.7 with $\gamma \in F(\boldsymbol{\mu}_l)^\times$:

$$[\kappa_r]_l = \varphi_l(\kappa_s). \qquad \square$$

We conclude this Section with an application of the *Chebotarev density theorem*, a well-known result in algebraic number theory, describing the splitting of primes in a number field K statistically. We refer to [Neu99], Section VII.13 for this Theorem, without entering in details. Here we see how to use (a consequence of) this result to deduce the existence of primes with useful properties.

Fix a rational prime $p > 2$ and we denote by C the p-part of C_F, the ideal class group of F.

Theorem 4.9. *If $c \in C$, $M \in \mathbf{Z}$ is a power of p, W is a finite Δ-submodule of $F^\times/(F^\times)^M$, and ψ is a Galois-equivariant map*

$$\psi\colon W \to (\mathbf{Z}/M\mathbf{Z})[G],$$

then there are infinitely many primes λ of F such that

(a) $\lambda \in c$.

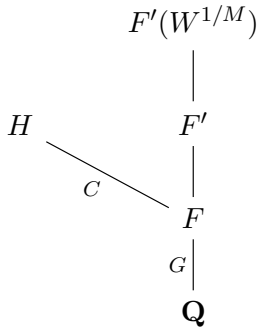
(b) *The rational prime l below λ splits completely in $F/\mathbf{Q}$, and $l \equiv 1 \pmod{M}$.*

(c) $[w]_l = 0$ *for all $w \in W$, and there is a $u \in (\mathbf{Z}/M\mathbf{Z})^\times$ such that*

$$\varphi_l(w) = u\psi(w)\lambda$$

for all $w \in W$.

Proof. If H denotes the maximal abelian unramified p-extension of F, then by the correspondence of class field theory, we can identify C with $\mathrm{Gal}(H/F)$. Write $F' = F(\boldsymbol{\mu}_M)$. Then we have



Since M is a power of p, the inertia group of p in $\mathrm{Gal}(F'/F)$ has index either 1 or 2, therefore there is no nontrivial unramified p-extension of F in F' (p is odd). We deduce that $F' \cap H = F$. We claim that also $F'(W^{1/M}) \cap H = F$. There is a Kummer nondegenerate $\mathrm{Gal}(F'/\mathbf{Q})$-equivariant pairing

$$\mathrm{Gal}(F'(W^{1/M})/F') \times W/W' \to \boldsymbol{\mu}_M,$$

where W' is the kernel of the map from W into $(F')^\times/[(F')^\times]^M$ (see, for example, Chapter 6 of [Lan90], or Section 10.2 of [Was97]). If τ denotes the complex conjugation in $\mathrm{Gal}(F'/F)$, then τ acts trivially on W and by -1 on $\boldsymbol{\mu}_M$, and therefore also on $\mathrm{Gal}(F'(W^{1/M})/F')$. On the other side, F is totally real and H is an abelian extension with Galois group isomorphic to the p-part of the ideal class group of F, hence τ acts trivially on $\mathrm{Gal}(H/F) \cong \mathrm{Gal}(HF'/F')$. This means that τ acts on $\mathrm{Gal}(F'(W^{1/M})\cap HF'/F')$ by both 1 and -1, so $F'(W^{1/M})\cap HF = F$, and also $F'(W^{1/M})\cap H = F$ by $F'\cap H = F$. M is odd, hence $\boldsymbol{\mu}_M \cap F = \{1\}$ and $H^0(\mathrm{Gal}(F'/F), \boldsymbol{\mu}_M) = 0$. But $\mathrm{Gal}(F'/F)$ is cyclic, therefore also $H^1(\mathrm{Gal}(F'/F), \boldsymbol{\mu}_M) = 0$ (this follows applying *Tate cohomology* to the finite cyclic group, and then considering its *Herbrand quotient*. We just refer to [Ser79] for this). By the inflation-restriction sequence, this implies that the map

$$F^\times/(F^\times)^M \to (F')^\times/[(F')^\times]^M$$

is injective, and so from the previous pairing we get an isomorphism:

$$\mathrm{Gal}(F'(W^{1/M})/F') \cong \mathrm{Hom}(W, \boldsymbol{\mu}_M).$$

Now we start the construction of λ. Fixed a primitive M-th root of unity $\boldsymbol{\mu}_M$, define $\iota\colon (\mathbf{Z}/M\mathbf{Z})[G] \to \boldsymbol{\mu}_M$ by $\iota(1_G) = \zeta_M$ and $\iota(g) = 1$ for all $g \neq 1_G$ in G. Denote as γ the element of $\mathrm{Gal}(F'(W^{1/M})/F')$ corresponding to $\iota \circ \psi \in \mathrm{Hom}(W, \boldsymbol{\mu}_M)$ via the Kummer pairing. Therefore γ satisfies

$$\iota \circ \psi(w) = \gamma(w^{1/M})w^{1/M}$$

for all $w \in W$.

By $F'(W^{1/M}) \cap H = F$, we can choose $\delta \in \mathrm{Gal}(HF'(W^{1/M})/F)$ such that δ restricts to γ on $F'(W^{1/M})$ and to $c \in C = \mathrm{Gal}(H/F)$ on H. Now we apply the Chebotarev theorem: since W is finite, there exist infinitely many primes λ such that λ has inertia degree 1 and is unramified over $\mathbf{Q}$, is unramified in $HF'(W^{1/M})$, and its Frobenius in $\mathrm{Gal}(HF'(W^{1/M})/F')$ is the conjugacy class of G. Fix one of those and l be the rational prime below it. We check the three desired properties.

(a) The identification $C = \mathrm{Gal}(H/F)$ sends the class of λ to the Frobenius of λ, hence $\lambda \in c$.

(b) l splits completely in F, since the degree of λ is 1 and it is unramified. The Frobenius of l in $\mathbf{Q}(\boldsymbol{\mu}_M)$ is the restriction of the Frobenius of $HF'(W^{1/M})$, which is the class of δ. But δ is trivial on F', so on $\mathbf{Q}(\boldsymbol{\mu}_M)$, hence l splits completely also in $\mathbf{Q}(\boldsymbol{\mu}_M)/\mathbf{Q}$.

(c) $[w]_l = 0$ for all $w \in W$ holds because λ is unramified in $F'(W^{1/M})/F$. By definition, $v_\lambda(\varphi_l(w)) = 0$ if and only if w is an M-th power modulo

λ. But we also have

$$\begin{aligned} v_\lambda(\psi(w)\lambda) = 0 &\iff i \circ \psi(w) = 1 \iff \gamma(w^{1/M})/w^{1/M} = 1 \\ &\iff w \text{ is an } M\text{-th power modulo } \lambda. \end{aligned}$$

Thus there exists an unit $u \in (\mathbf{Z}/M\mathbf{Z})^\times$ such that

$$v_\lambda(\varphi_l(w)) = u v_\lambda(\psi(w)\lambda)$$

for all $w \in W$. Then the map $w \mapsto \varphi_l(w) - u\psi(w)\lambda$ is a $\mathrm{Gal}(F/K)$-equivariant homomorphism into $\oplus_{\lambda' | l,\ \lambda' \neq \lambda} (\mathbf{Z}/M\mathbf{Z})\lambda'$, which has no nonzero $\mathrm{Gal}(F/K)$-stable submodules. The assertion then follows. $\square$

4.2 The Main Conjecture

Let p be a rational odd prime. For every $n \geq 0$, we let

$$\begin{aligned} K_n &= \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}}), \\ K_\infty &= \bigcup K_n. \end{aligned}$$

Write

$$\begin{aligned} \Delta &= \mathrm{Gal}(K_0/\mathbf{Q}) \cong (\mathbf{Z}/p\mathbf{Z})^\times, \\ \Gamma &= \mathrm{Gal}(K_\infty/K_0) \cong \mathbf{Z}_p, \end{aligned}$$

so that

$$\mathrm{Gal}(K_\infty/\mathbf{Q}) = \Delta \times \Gamma.$$

Recall the Iwasawa algebra

$$\Lambda = \Lambda(\Gamma) = \varprojlim \mathbf{Z}_p[\mathrm{Gal}(K_n/K_0)].$$

From now on, we write *character* to indicate a p-adic valued character of Δ. So let χ be a character

$$\chi \colon \Delta \to {\mathbf{Z}_p}^\times.$$

Recall that (Section 1.4):

- $C_\infty(\chi)$ is a finitely generated torsion Λ-module.
- If χ is even, then $E_\infty(\chi)/V_\infty(\chi)$ is a finitely generated torsion Λ-module.
- If χ is even and nontrivial, then $X_\infty(\chi)$ and $U_\infty(\chi)/V_\infty(\chi)$ are finitely generated torsion Λ-module.

We can finally state (one of the several equivalent formulations of) the Iwasawa's *main conjecture* for cyclotomic fields.

Theorem 4.10 (Main conjecture, version 1)**.** *For all even characters χ of Δ,*

$$\mathrm{char}(C_\infty(\chi)) = \mathrm{char}(E_\infty(\chi)/V_\infty(\chi)).$$

In order to prove this Theorem, we need to analize the structure of C_n and $\bar{E}_n$ as $\mathbf{Z}_p[\mathrm{Gal}(K_n/\mathbf{Q})]$-modules. For any fixed n, we do not have many information; what we know is that C_∞ and E_∞ are well-behaved Λ-modules. Therefore we need to relate C_n and $\bar{E}_n$ with C_∞ and E_∞.

For every n, consider $\Gamma_n = \mathrm{Gal}(K_\infty/K_n)$. It is the subgroup of index p^n in Γ, and it is generated by γ^{p^n}. Take

$$I_n = (\gamma^{p^n} - 1)\Lambda,$$

and write

$$\Lambda_n = \Lambda/I_n\Lambda \cong \mathbf{Z}_p[\mathrm{Gal}(K_n/K_0)].$$

If Y is a Λ-module, then define

$$Y_{\Gamma_n} = Y/I_nY = Y/(\gamma^{p^n} - 1)Y = Y \otimes \Lambda_n.$$

We want to study the following natural maps, induced by the projections:

$$X_\infty(\chi)_{\Gamma_n} \to X_n(\chi), \qquad C_\infty(\chi)_{\Gamma_n} \to C_n(\chi), \qquad U_\infty(\chi)_{\Gamma_n} \to U_n(\chi),$$
$$E_\infty(\chi)_{\Gamma_n} \to \bar{E}_n(\chi) \qquad \text{and} \qquad V_\infty(\chi)_{\Gamma_n} \to V_n(\chi).$$

These projections are in fact well-defined, since for a Λ-module Y, Y_{Γ_n} is the maximal quotient of Y on which Γ_n acts trivially. We discussed the following Theorem in Section 1.4:

Theorem 4.11. *For every character χ, the map $C_\infty(\chi)_{\Gamma_n} \to C_n(\chi)$ is an isomorphism. If χ is even and $\chi \neq 1$, then the maps*

$$X_\infty(\chi)_{\Gamma_n} \to X_n(\chi), \qquad U_\infty(\chi)_{\Gamma_n} \to U_n(\chi) \qquad \textit{and} \qquad V_\infty(\chi)_{\Gamma_n} \to V_n(\chi)$$

are isomorphisms.

Lemma 4.12. *Suppose*

$$0 \to W \to Y \to Z \to 0$$

is an exact sequence of Λ-modules. Then for every n the kernel of the induced map $W_{\Gamma_n} \to Y_{\Gamma_n}$ is a quotient of Z^{Γ_n}. If Z is a finitely generated Λ-module and Z_{Γ_n} is finite, then also Z^{Γ_n} is finite.

Proof. Applying the *snake lemma* to

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W^{\Gamma_n} & \longrightarrow & Y^{\Gamma_n} & \longrightarrow & Z^{\Gamma_n} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle (\gamma^{p^n}-1)} & & \downarrow{\scriptstyle (\gamma^{p^n}-1)} & & \downarrow{\scriptstyle (\gamma^{p^n}-1)} & & \\
0 & \longrightarrow & W & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & W_{\Gamma_n} & \longrightarrow & Y_{\Gamma_n} & \longrightarrow & Z_{\Gamma_n} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

the first assertion follows. Now suppose that Z is finitely generated and $Z_{\Gamma_n} = Z/(\gamma^{p^n}-1)Z$ is finite. Note that this implies that Z is torsion, since the constant term $(T+1)^{p^n}-1$, the element of $\mathbf{Z}_p[[T]]$ corresponding to $\gamma^{p^n}-1$, is zero, so it is not a unit in Λ, and therefore by 1.41, $\Lambda/(\gamma^{p^n}-1)\Lambda$ is infinite. The third column and the multiplicativity imply that $\mathrm{char}(Z^{\Gamma_n}) = \mathrm{char}(Z_{\Gamma_n}) = 1$, so Z^{Γ_n} is finite by Lemma 1.39. □

Theorem 4.13. *If χ is an even nontrivial character, then there is an ideal $\mathscr{A}$ of finite index in Λ such that for every n, $\mathscr{A}$ annihilates the kernel and the cokernel of the map $E_\infty(\chi)_{\Gamma_n} \to \bar{E}_n(\chi)$. In particular, the kernel and cokernel are finite with order bounded independently of n.*

Proof. Consider the following two commutative diagrams with exact rows, the first obtained similarly as (1.1):

$$\begin{array}{ccccccccc}
 & & (U_\infty(\chi)/E_\infty(\chi))_{\Gamma_n} & \xrightarrow{\phi_1} & X_\infty(\chi)_{\Gamma_n} & \longrightarrow & C_\infty(\chi)_{\Gamma_n} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_{U/E}} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_n(\chi)/\bar{E}_n(\chi) & \longrightarrow & X_n(\chi) & \longrightarrow & C_n(\chi) & \longrightarrow & 0,
\end{array}$$

$$\begin{array}{ccccccccc}
 & & E_\infty(\chi)_{\Gamma_n} & \xrightarrow{\phi_2} & U_\infty(\chi)_{\Gamma_n} & \longrightarrow & (U_\infty(\chi)/E_\infty(\chi))_{\Gamma_n} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_E} & & \downarrow & & \downarrow{\scriptstyle \pi_E} & & \\
0 & \longrightarrow & \bar{E}_n(\chi) & \longrightarrow & U_n(\chi) & \longrightarrow & U_n(\chi)/\bar{E}_n(\chi) & \longrightarrow & 0.
\end{array}$$

Since the map $U_\infty(\chi)_{\Gamma_n} \to U_n(\chi)$ is an isomorphism, applying the snake lemma to the second diagram we get

$$\mathrm{coker}(\pi_E) \cong \ker(\pi_{U/E}).$$

Also, the map $X_\infty(\chi)_{\Gamma_n} \to X_n(\chi)$ is injective, so

$$\ker(\pi_{U/E}) = \ker(\phi_1).$$

Since $C_\infty(\chi)_{\Gamma_n} \cong C_n(\chi)$ is finite, by Lemma 4.12, $\ker(\phi_1)$ is a quotient of $C_\infty(\chi)_{\text{finite}}$, the maximal finite Λ-submodule of $C_\infty(\chi)$. Similarly, we have $\ker(\pi_E) = \ker(\phi_2)$. By [Lan90], Chapter 4, Theorem 4.2, if $\chi \neq 1$, then

$$[U_n(\chi) : \bar{E}_n(\chi)]$$

is finite, so

$$|(U_\infty(\chi)/E_\infty(\chi))_{\Gamma_n}| \leq [U_n(\chi) : \bar{E}_n(\chi)]|\ker(\pi_{U/E})|$$

is finite as well. Therefore, again by Lemma 4.12, $\ker(\phi_2)$ is a quotient of $(U_\infty(\chi)/E_\infty(\chi))_{\text{finite}}$. If we take as $\mathscr{A}$ the annihilator in Λ of

$$C_\infty(\chi)_{\text{finite}} \bigoplus (U_\infty(\chi)/E_\infty(\chi))_{\text{finite}},$$

it has finite index, since it annihilates a finite Λ-module (Lemma 1.39). Then the assertion follows. □

If χ is a even nontrivial character of Δ, fix a generator $h_\chi \in \Lambda$ of $\text{char}(E_\infty(\chi)/V_\infty(\chi))$.

Corollary 4.14. *If χ is an even nontrivial character, then there is an ideal $\mathscr{A}$ of finite index in Λ such that for every $\eta \in A$ and every n, there is a map*

$$\theta_{n,\eta} \colon \bar{E}_n(\chi) \to \Lambda_n$$

with

$$\theta_{n,\eta}(V_n(\chi)) = \eta h_\chi \Lambda_n.$$

Proof. The module $U_\infty(\chi)$ is free of rank one over Λ (Theorem 1.45) and $0 \neq E_\infty(\chi) \subseteq U_\infty(\chi)$, thus $E_\infty(\chi)$ is torsion free and has rank one. This means that there is an injective homomorphism

$$\theta \colon E_\infty \to \Lambda$$

with finite cokernel. This maps clearly induces a pseudo-isomorphism

$$E_\infty(\chi)/V_\infty(\chi) \sim \Lambda/\theta(V_\infty(\chi)).$$

But also $V_\infty(\chi)$ is free of rank one (Theorem 1.48), therefore

$$\theta(V_\infty(\chi)) = \text{char}(\Lambda/\theta(V_\infty(\chi))) = \text{char}(E_\infty(\chi)/V_\infty(\chi)) = h_\chi \Lambda.$$

Let $\mathscr{A}$ be a finite index ideal of Λ satisfying Theorem 4.13. Fix an n and let θ_n denote the homomorphism from $E_\infty(\chi)_{\Gamma_n}$ to Λ_n induced by θ, and π_n the projection map from $E_\infty(\chi)_{\Gamma_n}$ to $\bar{E}_n(\chi)$. For every $\eta \in \mathscr{A}$, we define

$$\theta_{n,\eta} \colon \bar{E}_n(\chi) \to \Lambda_n$$

to be the map making the following diagram commute:

$$\begin{array}{ccc} E_\infty(\chi)_{\Gamma_n} & \xrightarrow{\theta_n} & \Lambda \\ {\scriptstyle \pi_n}\downarrow & & \downarrow{\scriptstyle \eta} \\ \bar{E}_n(\chi) & \xrightarrow{\theta_{n,\eta}} & \Lambda_n, \end{array}$$

that is,

$$\theta_{n,\eta}(u) = \theta_n(\pi_n^{-1}(\eta u)).$$

The well-definition follows from the fact that by Theorem 4.13, η annihilates $\operatorname{coker}(\pi_n)$ and $\ker(\pi_n)$ is finite, so $\ker(\pi_n) \subseteq \ker(\theta_n)$. Since $V_n(\chi) = \pi_n(V_\infty(\chi))$, we conclude that

$$\theta_{n,\eta}(V_n(\chi)) = \eta\theta_n(V_\infty(\chi)) = \eta h_\chi \Lambda_n. \qquad \square$$

By the classification theorem, there is a pseudo-isomorphism

$$C_\infty(\chi) \sim \bigoplus_{i=1}^{k} \Lambda/f_i\Lambda,$$

with nonzero $f_i \in \Lambda$. Then

$$\operatorname{char}(C_\infty(\chi)) = f_\chi \Lambda,$$

with

$$f_\chi = \prod_{i=1}^{k} f_i.$$

Corollary 4.15. *There is an ideal $\mathscr{B}$ of finite index in Λ and for every n there are classes $c_1, \ldots, c_k \in C_n(\chi)$ such that the annihilator $\operatorname{Ann}(c_i) \subseteq \Lambda_n$ of c_i in $C_n(\chi)/(\Lambda_n c_1 + \ldots + \Lambda_n c_{i-1})$ satisfies $\mathscr{B} \operatorname{Ann}(c_i) \subseteq f_i \Lambda_n$.*

Proof. The pseudo-isomorphism relation, a priori not reflexive, is reflexive on torsion Λ-modules. Therefore there is an exact sequence

$$0 \to \bigoplus_{i=1}^{k} \Lambda/f_i\Lambda \to C_\infty(\chi) \to Z \to 0,$$

with Z finite Λ-module. By Theorem 4.11 and Lemma 4.12, if we tensor with $\Lambda_n = \Lambda/I_n\Lambda$ we get

$$Z^{\Gamma_n} \to \bigoplus_{i=1}^{k} \Lambda_n/f_i\Lambda_n \to C_n(\chi) \to Z_{\Gamma_n} \to 0.$$

Let $\mathscr{B}$ be the annihilator of the finite module Z and choose c_i to be the image of 1 in the i-th summand $\Lambda_n/f_i\Lambda_n$ under this map. Then $\mathscr{B}$ satisfies the desired property. □

We conclude this series of results with a final Lemma.

Lemma 4.16. *Let χ be an even character of Δ, and let*

$$f_\chi\Lambda = \mathrm{char}(C_\infty(\chi))$$
$$h_\chi\Lambda = \mathrm{char}(E_\infty(\chi)/V_\infty(\chi))$$

as above.

(a) *For every n, $\Lambda_n/f_\chi\Lambda_n$ and $\Lambda_n/h_\chi\Lambda_n$ are finite.*

(b) *There is a positive constant c such that for all n,*

$$c^{-1} \leq \frac{|C_n(\chi)|}{|\Lambda_n/f_\chi\Lambda_n|} \leq c, \qquad c^{-1} \leq \frac{|\bar{E}_n(\chi)/V_n(\chi)|}{|\Lambda_n/h_\chi\Lambda_n|} \leq c$$

(c) *If $\chi = 1$, then f_χ and h_χ are units in Λ.*

Proof. From the pseudo-isomorphism

$$C_\infty(\chi) \sim \bigoplus_{i=1}^{k} \Lambda/f_i\Lambda$$

we get, for every n, a map

$$C_n(\chi) \cong C_\infty(\chi)_{\Gamma_n} \to \bigoplus_{i=1}^{k} \Lambda_n/f_i\Lambda_n$$

with kernel and cokernel finite and bounded independently of n. Therefore also $\Lambda_n/f_\chi\Lambda_n$ is finite for every n, and by [Lan90], Chapter 5, Theorem 1.2, the quotient

$$|\Lambda_n/f_\chi\Lambda_n|/|\bigoplus_{i=1}^{k} \Lambda_n/f_i\Lambda_n|$$

is bounded above and below independently of n. Repeating the same argument with the maps

$$(E_\infty(\chi)/V_\infty(\chi))_{\Gamma_n} \to \Lambda_n/h_\chi\Lambda_n,$$
$$(E_\infty(\chi)/V_\infty(\chi))_{\Gamma_n} \to \bar{E}_n(\chi)/V_n(\chi),$$

we deduce that we have proved (a) and (b) with $\chi \neq 1$.

If $\chi = 1$, then h_χ is a unit and the inequalities of (b) holds with $\chi = 1$, $c = 1$ by Proposition 1.50. □

4.3 The proof

We can finally come to the main result. We fix n, and we let $C = C_n$, $E = E_n$ and $V = V_n$. We want to apply the results of the previous sections to $F = K_n^+$. When χ is even, we can identify $C_n(\chi)$ with the χ-component of the p-part of the ideal class group of F (this follows from [Lan90], Chapter 3, Theorems 4.2 and 4.3). If l is a rational prime splitting completely in F, then $I_l \otimes \mathbf{Z}_p$ is a $\mathbf{Z}_p$-module, and it makes sense to consider $I_l(\chi) = e(\chi)(I_l \otimes \mathbf{Z}_p)$. This is free of rank one over Λ_n, generated by the element $\lambda(\chi) = e(\chi)\lambda$, where λ is a prime of F above, and we can define

$$\sigma_\lambda = \sigma_{\lambda,\chi} \colon F^\times \to \Lambda_n$$

by

$$\sigma_\lambda(w)\lambda(\chi) = e(\chi)(w)_l.$$

We denote by $\bar{\sigma}_\lambda$ the corresponding map

$$\bar{\sigma}_\lambda \colon F^\times/(F^\times)^M \to \Lambda_n/M\Lambda_n,$$

satisfying

$$\bar{\sigma}_\lambda(w)\lambda(\chi) = e(\chi)[w]_l.$$

Recall that for $r \in \mathscr{P}_M$, we can choose an element $\kappa_r \in F^\times/(F^\times)^M$.

Lemma 4.17. *Suppose we have $r \in \mathscr{P}_M$, l prime dividing r and λ prime of F above l. Let B the subgroup of the ideal subgroup C generated by the primes of F dividing r/l. Write $c \in C(\chi)$ for the class of $e(\chi)\lambda$ and W for the Λ_n-submodule of $F^\times/(F^\times)^M$ generated by $e(\chi)\kappa_r$. If $\eta, f \in \Lambda_n$ have the properties that the annihilator $\mathrm{Ann}(c) \subseteq \Lambda_n$ of c in $C(\chi)/B(\chi)$ satisfies $\eta\,\mathrm{Ann}(c) \subseteq f\Lambda_n$, $\Lambda_n/f\Lambda_n$ is finite and*

$$M \geq |C(\chi)| \cdot |(I_l(\chi)/MI_l(\chi))/\Lambda_n[e(\chi)\kappa_r]_l|,$$

then there is a Galois-equivariant map $\psi \colon W \to \Lambda_n/M\Lambda_n$ such that

$$f\psi(e(\chi)\kappa_r) = \eta\bar{\sigma}_\lambda(\kappa_r).$$

Proof. We denote by β any lift of $e(\chi)\kappa_r$ to $F^\times$. We have

$$e(\chi)(\beta) = e(\chi)(\beta)_l + \sum_{q \neq l} e(\chi)(\beta)_q = \sigma_\lambda(\beta)\lambda(\chi) + \sum_{q \neq l} e(\chi)(\beta)_q.$$

By Proposition 4.8, if $q \neq r$, then $(\beta)_q \in MI_q$. Since M annihilates $|C(\chi)|$, we deduce that $\sigma_\lambda(\beta)\lambda(\chi)$ projects to 0 in $C(\chi)/B(\chi)$ and thus $\eta\sigma_\lambda(\beta) \in f\Lambda_n$. We define

$$\delta = \frac{\eta\sigma_\lambda(\beta)}{f},$$

where the division by f is uniquely-defined since $\Lambda_n/f\Lambda_n$ is finite. We define $\psi\colon W \to \Lambda_n/M\Lambda_n$ by

$$\psi(\rho e(\chi)\kappa_r) = \rho\delta,$$

for all $\rho \in \mathbf{Z}[\mathrm{Gal}(K_n/K_0)]$. Then this map has by construction the desired property, but we have to show that it is well defined. So, suppose $\rho e(\chi)\kappa_r = 0$. This means that there exists $x \in F^\times$ such that $\rho\beta = x^M$. In particular, $\rho[e(\chi)\kappa_r]_l = 0$. Writing $h = |C(\chi)|$, we have by assumption

$$(M/h)(I_l(\chi)/MI_l(\chi)) \subseteq \Lambda_n[e(\chi)\kappa_r]_l,$$

so $\rho \in h\Lambda_n$. Then

$$\begin{aligned} e(\chi)(x) &= \sum_q e(\chi)(x)_q \\ &= M^{-1}e(\chi)(\rho\beta)_l + \sum_{q|(r/l)} e(\chi)(x)_q + \sum_{q\nmid r} he(\chi)(\rho/h)(M^{-1}(\beta)_q) \\ &\equiv M^{-1}e(\chi)(\rho\beta)_l \pmod{\bigoplus_{q|(r/l)} I_q(\chi), hI(\chi)}. \end{aligned}$$

From the fact that h annihilates $C(\chi)$, we conclude that $M^{-1}e(\chi)(\rho\beta)_l$ projects to 0 in $C(\chi)/B(\chi)$. Therefore $M^{-1}\sigma_\lambda(\rho\beta)c = 0$ in $C(\chi)/B(\chi)$ so $\rho\delta f = \eta\sigma_\lambda(\rho\beta) \in Mf\Lambda_n$ and

$$\psi(\rho e(\chi)\kappa_r) = \rho\delta \in M\Lambda_n.$$

This means that the map ψ is well-defined. □

Recall that $\mathrm{char}(E_\infty(\chi)/V_\infty(\chi)) = h_\chi\Lambda$ and $\mathrm{char}(C_\infty(\chi)) = f_\chi\Lambda$, with $f_\chi = \prod_{i=1}^k f_i$.

Theorem 4.18. *For every even character χ of Δ,* $\mathrm{char}(C_\infty(\chi))$ *divides* $\mathrm{char}(E_\infty(\chi)/V_\infty(\chi))$.

Proof. If $\chi = 1$, then both characteristic ideals are trivial by Lemma 4.16, so the assertion is clear.

Suppose $\chi \neq 1$. Consider κ_1, which we can represent by $\alpha = \alpha_1 = (\zeta_{p^n} - 1)(\zeta_{p^n}^{-1} - 1) \in F^\times$. As we already said, $\alpha(\chi) = \alpha^{e(\chi)}$ is a generator of $V_n(\chi)$. We pick $c_1, \ldots, c_k \in C(\chi)$ as in Corollary 4.15, and we also choose one more class c_{k+1}, which can be any element of $C(\chi)$, like $c_{k+1} = 0$. Fix an ideal $\mathscr{C}$ of Λ with finite index, satisfying both Corollary 4.14 and 4.15. Let $\eta \in \mathscr{C}$ be such that $\Lambda_m/\eta\Lambda_m$ is finite for all m, that is, η is prime to $\gamma^{p^m} - 1$, with γ generator of Γ. Consider

$$\theta = \theta_{n,\eta}\colon \bar{E}(\chi) \to \Lambda_n,$$

the map given by Corollary 4.14, and normalize it to have

$$\theta(\alpha(\chi)) = \eta h_\chi.$$

Denote by h an integer such that $p^h \geq |\Lambda_n/\eta\Lambda_n|$ and $p^h \geq |\Lambda_n/h_\chi\Lambda_n|$ (this is finite by Lemma 4.16), and let

$$M = |C(\chi)| \cdot p^{n+(k+1)h}.$$

Our goal is to use Theorem 4.9 to choose inductively primes λ_i of F lying above primes l_i of $\mathbf{Q}$ for $1 \leq i \leq k+1$, satisfying:

$$\lambda_i \in c_i, \qquad l_i \equiv 1 \pmod{M}, \tag{4.2}$$

$$\bar{\sigma}_{\lambda_1}(\kappa_{l_1}) = u_1\eta h_\chi, \quad f_{i-1}\bar{\sigma}_{\lambda_i}(\kappa_{r_i}) = u_i\eta\bar{\sigma}_{\lambda_{i-1}}(\kappa_{r_{i-1}}), \quad \text{for } 2 \leq i \leq k+1, \tag{4.3}$$

with $r_i = \prod_{j\leq i} l_j$ and $u_i \in (\mathbf{Z}/M\mathbf{Z})^\times$.

Firstly, take $c = c_1$, $W = (E/E^M)(\chi)$ and

$$\psi\colon W \to \bar{E}(\chi) \to \bar{E}(\chi)^M \xrightarrow{\theta} \Lambda_n/M\Lambda_n \xrightarrow{e(\chi)} e(\chi)(\mathbf{Z}/M\mathbf{Z})[\mathrm{Gal}(F/\mathbf{Q})].$$

If λ_1 is a prime satisfying Theorem 4.9 with this data, then (4.2) also is satisfied. Also, again by Theorem 4.9 and by Proposition 4.8, for some $u_1 \in (\mathbf{Z}/M\mathbf{Z})^\times$,

$$\begin{aligned}\bar{\sigma}_{\lambda_1}(\kappa_{l_1}) = e(\chi)[\kappa_{l_1}]_{l_1} &= e(\chi)\varphi_{l_1}(\kappa_1) = u_1\psi(\kappa_1)\lambda_1(\chi)\\ &= u_1\theta(\alpha(\chi))\lambda_1(\chi) = u_1\eta h_\chi\lambda_1(\chi).\end{aligned}$$

Since $\lambda_1(\chi)$ is a generator of the free $\Lambda_n/M\Lambda_n$-module (I_{l_1}/MI_{l_1}), also (4.3) is proved for $i = 1$.

Suppose now that $2 \leq i \leq k+1$ and we have chosen $\lambda_1, \ldots, \lambda_{i-1}$ satisfying the desired properties. We define λ_i. Consider $r_{i-1} = \prod_{j<i} l_j$. By (4.3), $\bar{\sigma}_{\lambda_{i-1}}(\kappa_{r_{i-1}})$ divides $\eta^{i-1}h_\chi$, thus

$$|(I_{l_{i-1}}/MI_{l_{i-1}})/\Lambda_n[\kappa_{r_{i-1}}]_{l_{i-1}}| \leq |\Lambda_n/\eta^{i-1}h_\chi\Lambda_n| \leq p^{ih}.$$

Denote by W_i the Λ_n-submodule of $F^\times/(F^\times)^M$ generated by $e(\chi)\kappa_{r_{i-1}}$. We apply Corollary 4.15, Lemma 4.16 and Lemma 4.17 with $r = r_{i-1}$ and $l = l_{i-1}$, to get a map

$$\psi_i\colon W_i \to \Lambda_n/M\Lambda_n$$

such that

$$f_{i-1}\psi_i(e(\chi)\kappa_{r_{i-1}}) = \eta\bar{v}_{\lambda_{i-1}}(\kappa_{r_{i-1}}).$$

It is enough now to pick λ_i satisfying Theorem 4.9 with $c = c_i$, $W = W_i$, $\psi = e(\chi)\psi_i$ and M as above, to have (4.2). Also, there is a $u_i \in (\mathbf{Z}/M\mathbf{Z})^\times$ such that

$$\begin{aligned}f_{i-1}\bar{\sigma}_{\lambda_i}(\kappa_{r_i})\lambda_i(\chi) &= f_{i-1}e(\chi)[\kappa_{r_i}]_{l_i} = f_{i-1}\varphi_{l_i}(e(\chi)_{r_{i-1}})\\ &= f_{i-1}u_i\psi_i(e(\chi)\kappa_{r_{i-1}}\lambda_i(\chi) = u_i\eta\bar{v}_{\lambda_{i-1}}(\kappa_{r_{i-1}})\lambda_i(\chi),\end{aligned}$$

so also (4.3) is true for i.

If we continue this induction for $k+1$ steps, then combining all the relations (4.3) we get

$$\eta^{k+1} h_\chi = u \left(\prod_{i=1}^{k} f_i \right) \bar{\sigma}_{\lambda_{k+1}}(\kappa_{r_{k+1}}) \quad \text{in } \Lambda_n / M\Lambda_n$$

for some $u \in (\mathbf{Z}/M\mathbf{Z})^\times$. We deduce that $f_\chi = \prod_{i=1}^{k} f_i$ divides $\eta^{k+1} h_\chi$ in $\Lambda_n / p^n \Lambda_n$ for all n, and so also in Λ. To conclude, we need to remove the factor η^{k+1}. There are two ways. Firstly, recall that $\mathscr{C}$ is an ideal of Λ with finite index and $\eta \in \mathscr{C}$ has the property that $\Lambda_n / \eta \Lambda_n$ is finite for every n. Therefore, we can choose η as a power of p, and f_χ does not divide p by *Ferrero-Washington* theorem ([Lan90], Chapter 10, Theorem 2.3). But we can also avoid the use of this result, just saying that it is possible to choose two different η which are relatively prime, and since Λ is a unique factorization domain, we conclude that f_χ divides h_χ.

□

Let

$$f = \prod_{\chi \text{ even}} f_\chi,$$
$$h = \prod_{\chi \text{ even}} h_\chi,$$

where again $f_\chi = \mathrm{char}(C_\infty(\chi))$ and $h_\chi = \mathrm{char}(E_\infty(\chi)/V_\infty(\chi))$. We want to show that $f\Lambda = h\Lambda$. From this and Theorem 4.18, it will follow that for every χ, $f_\chi \Lambda = h_\chi \Lambda$. If a_n, b_n are two sequences of positive integers, we write $a_n \approx b_n$ to mean that a_n / b_n is bounded above and below independently of n.

Lemma 4.19. *If $g_1, g_2 \in \Lambda$ such that $g_1 \mid g_2$ and $|(\Lambda/g_1\lambda)_{\Gamma_n}| \approx |(\Lambda/g_2\lambda)_{\Gamma_n}|$, then $g_1\Lambda = g_2\Lambda$.*

Proof. Immediate consequence of Theorem 1.2 of Chapter 5 in [Lan90]. □

Finally, the proof we were looking for.

Proof of Theorem 4.10. By Theorem 1.2 of Chapter 5 in [Lan90] and Lemma 4.16,

$$|(\Lambda/f\Lambda)_{\Gamma_n}| \approx \prod_{\chi \text{ even}} |(\Lambda/f_\chi\Lambda)_{\Gamma_n}| \approx \prod_{\chi \text{ even}} |C_n(\chi)|,$$
$$|(\Lambda/h\Lambda)_{\Gamma_n}| \approx \prod_{\chi \text{ even}} |(\Lambda/h_\chi\Lambda)_{\Gamma_n}| \approx \prod_{\chi \text{ even}} [\bar{E}_n(\chi) : V_n(\chi)].$$

The analytic class number formula ([Lan90], Chapter 3, Theorem 5.1) and Theorem 4.2 of Chapter 4 in [Lan90] implies that

$$|C_n| = [\bar{E}_n : V_n].$$

Thus

$$|(\Lambda/f\lambda)_{\Gamma_n}| \approx |(\Lambda/h\lambda)_{\Gamma_n}|,$$

and since by Theorem 4.18 we have $f \mid h$, by Lemma 4.19 we derive $f\Lambda = h\Lambda$. Again by Theorem 4.18 we conclude that $f_\chi\Lambda = h_\chi\Lambda$ for all χ even, that is,

$$\operatorname{char}(C_\infty(\chi)) = \operatorname{char}(E_\infty(\chi)/V_\infty(\chi)). \qquad \square$$

4.4 Equivalent formulations and consequences

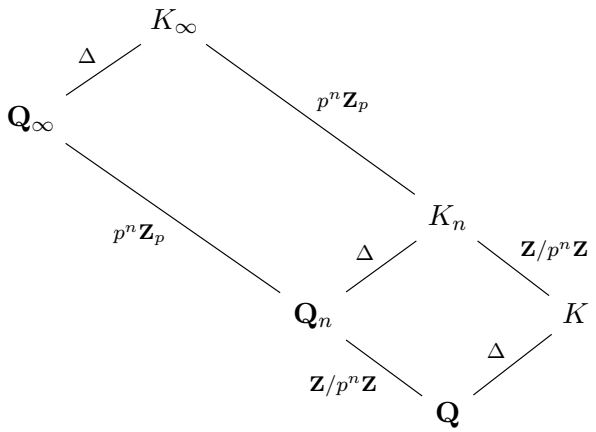
We conclude by seeing other formulations of the main conjecture, and deducing some important consequences. But first, we briefly describe the role of the Selmer group in this setting, since in the last Sections we explicitly used the cyclotomic Euler system to construct annihilators and deduce one divisibility of the main conjecture, without using Theorems of Section 3.3. Here we follow [Rub00], [Was97] and [Lan90].

Consider then a nontrivial even character $\chi\colon \Delta \to \mathbf{Z}_p^\times$, which we can extend as character of $G_{\mathbf{Q}}$. Denote by $T = (\mathbf{Z}_p)_\chi$ the free $\mathbf{Z}_p$-module of rank one on which $G_{\mathbf{Q}}$ acts by χ. Therefore

$$\begin{aligned} T^* &= \mathbf{Z}_p(1) \otimes \chi^{-1} = (\mathbf{Z}_p)_{\chi^{-1}\chi_p}, \\ W &= (\mathbf{Q}_p/\mathbf{Z}_p)_\chi, \\ (W^*)^* &= W. \end{aligned}$$

We have to take the character χ into consideration, thus we use the cyclotomic Euler system introduced in Section 4.1 to get an Euler system for $(T^*, \mathbf{Q}^{\mathrm{ab}}, p)$, which we denote by $\mathbf{c}^\chi$, exactly as in Section 3.4. This fact, during the proof we gave in the last Sections, is reflected in the use of the images of the Kolyvagin classes associated to the Euler system $\mathbf{c}$ under the idempotent $e(\chi)$ associated to the character χ.

We have the following field diagram:



By Proposition 2.29, if $C = C_0$ denotes the p-part of the ideal class group of $K = K_0$, then

$$\mathcal{S}(\mathbf{Q}, W) \cong \mathrm{Hom}(C(\chi), \mathbf{Q}_p/\mathbf{Z}_p),$$
$$\mathcal{S}(\mathbf{Q}_\infty, W) \cong \mathrm{Hom}(C_\infty(\chi), \mathbf{Q}_p/\mathbf{Z}_p)$$

This implies the following key fact:

$$C_\infty(\chi) \cong \mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W), \mathbf{Q}_p/\mathbf{Z}_p),$$

that is, $C_\infty(\chi)$ is the Pontryagin dual of $\mathcal{S}(\mathbf{Q}_\infty, W)$. Therefore

$$\mathrm{char}(C_\infty(\chi)) = \mathrm{char}(\mathrm{Hom}(\mathcal{S}(\mathbf{Q}_\infty, W), \mathbf{Q}_p/\mathbf{Z}_p)),$$

and we can apply Theorems of Section 3.3 to deduce divisibilities for $\mathrm{char}(C_\infty(\chi))$ (see [Rub00], Section III.2).

We move now our attention to other formulations of the conjecture, and in particular, we investigate the role of the p-adic L-function.

Recall that if χ is a (complex) Dirichlet character from $(\mathbf{Z}/p\mathbf{Z})^\times$, we can extend it naturally to all $\mathbf{Z}$, and attach to it a complex *L-function*

$$L(s, \chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}, \quad \mathrm{Re}(s) > 1.$$

It is well-known that if $\chi \neq 1$, $L(s, \chi)$ can be analytically continued to the entire complex plane, while if $\chi = 1$, then $L(s, \chi)$ has a meromorphic continuation to all the complex plane, with a simple pole at $s = 1$. Also, $L(s, \chi)$ admits the following convergent Euler product:

$$L(s, \chi) = \prod_{p \text{ prime}} (1 - \chi(p) p^{-s})^{-1}, \quad \mathrm{Re}(s) > 1.$$

Definition 4.20. If χ is a Dirichlet character of conductor p, then the can define the *generalized Bernoulli numbers* by

$$\sum_{j=1}^{p} \frac{\chi(j) t e^{jt}}{e^{pt} - 1} = \sum_{k=0}^{\infty} B_{k,\chi} \frac{t^k}{k!}.$$

These numbers are related to the L-functions as the "classical" Bernoulli numbers to the *Riemann zeta function*:

Theorem 4.21 ([Was97], Theorem 4.2)**.** *For $m \geq 1$, we have*

$$L(1 - k, \chi) = -\frac{B_{k,\chi}}{k}.$$

We can generalize this construction. Recall that ω denotes the Teichmüller character.

Theorem 4.22 ([Was97], Theorem 5.11)**.** *Let χ be a Dirichlet character of conductor p. Then there exists a p-adic meromorphic function $L_p(s,\chi)$, analytic for $\chi \neq 1$, defined on $\{s \in \mathbf{C}_p \mid |s| > p^{1-1/(p-1)}\}$, such that for $k \geq 1$,*

$$L_p(1-k,\chi) = -(1-\chi\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k}.$$

One way to see this p-adic function is as p-adic interpolation of the complex function $L(s,\chi)$. For $k \geq 1$,

$$L_p(1-k,\chi) = (1-\chi\omega^{-k}(p)p^{k-1})L(1-k,\chi\omega^{-k}).$$

As promised in Section 1.4, we can now discuss about the relation between the p-adic L-function and the generator of $U_\infty(\chi)/V_\infty(\chi)$, for χ nontrivial and even.

Theorem 4.23 ([Was97], Theorem 13.56)**.** *If χ is a nontrivial even character of Δ, then*

$$\mathrm{char}(U_\infty(\chi)/V_\infty(\chi)) = g_\chi\Lambda,$$

where if seen as element of $\mathbf{Z}_p[[T]]$, g_χ satisfies, for all $s \in \mathbf{Z}_p$,

$$g_\chi((1+p)^s - 1) = L_p(1-s,\chi).$$

In particular, for $k \geq 1$,

$$g_\chi((1+p)^k - 1) = L_p(1-k,\chi) = -(1-\chi\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k}.$$

We deduce the second equivalent version of the main conjecture:

Theorem 4.24 (Main conjecture, version 2)**.** *For all nontrivial even characters χ of Δ,*

$$\mathrm{char}(X_\infty(\chi)) = g_\chi\Lambda.$$

Proof. Recall the exact sequence (1.1):

$$0 \to E_\infty(\chi)/V_\infty(\chi) \to U_\infty(\chi)/V_\infty(\chi) \to X_\infty(\chi) \to C_\infty(\chi) \to 0.$$

By the first formulation of the conjecture and multiplicativity, we immediately conclude that

$$\mathrm{char}(X_\infty(\chi)) = \mathrm{char}(U_\infty(\chi)/V_\infty(\chi)) = g_\chi\Lambda. \qquad \square$$

If χ is even and nontrivial, now consider the element $f_\chi \in \Lambda$ which corresponding power series satisfying, for all $s \in \mathbf{Z}_p$,

$$f_\chi((1+p)^s - 1) = L_p(s, \chi).$$

Then the following change of variables holds:

$$g_\chi(T) = f_\chi((1+p)(1+T)^{-1} - 1).$$

We can use Kummer theory and Theorems 2.2 and 2.3 of [Lan90], Chapter 6, to get a nondegenerate pairing

$$A_\infty(\chi^{-1}\omega) \times X_\infty(\chi) \to \boldsymbol{\mu}_{p^\infty}.$$

Therefore,

$$X_\infty(\chi) \cong \mathrm{Hom}(A_\infty(\chi^{-1}\omega), \boldsymbol{\mu}_{p^\infty}).$$

It follows that

$$X_\infty(\chi)^{-1} \cong \mathrm{Hom}(A_\infty(\chi^{-1}\omega), \mathbf{Q}_p/\mathbf{Z}_p),$$

where

$$X_\infty(\chi)^{-1} = X_\infty(\chi) \otimes \mathbf{Z}_p(-1)$$

and

$$\mathbf{Z}_p(-1) = \mathrm{Hom}(\mathbf{Z}_p(1), \mathbf{Z}_p) = (\mathbf{Z}_p)_{\chi_p^{-1}}.$$

Using this fact, the pseudo-isomorphism $C_\infty(\chi) \sim \mathrm{Hom}(A_\infty(\chi), \mathbf{Q}_p/\mathbf{Z}_p)$ (Theorem 1.43), and the theory of *Adjoints* (see [Was97], Section 15.5), one can deduce the following

Proposition 4.25 ([Was97], Proposition 15.37)**.** *If the characteristic ideal of $X_\infty(\chi)$ is generated by g_χ, then the characteristic ideal of $C_\infty(\chi^{-1}\omega)$ is generated by*

$$g_\chi((1+p)(1+T)^{-1} - 1).$$

This implies the formulation of the main conjecture proved in [MW84]:

Theorem 4.26 (Main conjecture, version 3)**.** *For every nontrivial even character χ of Δ,*

$$\mathrm{char}(C_\infty(\chi^{-1}\omega)) = f_\chi\Lambda.$$

Remark 4.27. When $\chi = \omega$, $C_\infty(\chi) = 0$. This is Corollary 2, Section 1.3 of [Lan90].

Finally, we see how the main conjecture can be used to deduce results for the field $K = K_0$. Recall that $\Gamma_n = \mathrm{Gal}(K_n/K_0)$.

Proposition 4.28. *For every odd character $\chi \neq \omega$ of Δ, $A_\infty(\chi)^{\Gamma_n} = C_n(\chi)$.*

Proof. We need to use some results from [Lan90]. The first is Theorem 4.1 of Chapter 3, for which, since $\chi \neq \omega$ is odd, $\bar{E}_n(\chi) = \{1\}$. The second is Theorem 4.3, Chapter 6, for which the maps $C_n(\chi) \to C_m(\chi)$ are injective whenever $m \geq n$. We deduce that

$$C_n(\chi) \subseteq A_\infty(\chi)^{\Gamma_n}.$$

Denoted by γ_n a generator of Γ_n, we have an exact sequence

$$0 \to C_m(\chi)^{\Gamma_n} \to C_m(\chi) \xrightarrow{\gamma-1} C_m(\chi) \to C_m(\chi)/(\gamma-1)C_m(\chi) \to 0.$$

Using Theorem 4.1 of Chapter 5, we get

$$C_m(\chi)/(\gamma-1)C_m(\chi) \cong C_n(\chi),$$

and so we conclude that, whenever $m \geq n$,

$$|C_m(\chi)^{\Gamma_n}| = |C_n(\chi)|.$$

Therefore

$$|A_\infty(\chi)^{\Gamma_n}| = |C_n(\chi)|,$$

and the assertion follows. □

Lemma 4.29. *If Y is a finitely generated torsion Λ-module with no nonzero finite Λ-submodules, $\gamma \in \Gamma$, $a \in 1 + p\mathbf{Z}_p$ and $Y/(\gamma-a)Y$ is finite, then*

$$|Y/(\gamma-a)Y| = |\Lambda/(\mathrm{char}(Y), (\gamma-a)\Lambda)|.$$

Proof. Consider a pseudo-isomorphism

$$Y \to \bigoplus \Lambda/f_i\Lambda,$$

with finite cokernel Z. Then by hypothesis the kernel must be trivial. We have the following commutative exact diagram:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Y_{(\gamma-a)} & \longrightarrow & \bigoplus(\Lambda/f_i\Lambda)_{(\gamma-a)} & \longrightarrow & Z_{(\gamma-a)} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & Y & \longrightarrow & \bigoplus \Lambda/f_i\Lambda & \longrightarrow & Z & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle(\gamma-a)} & & \downarrow{\scriptstyle(\gamma-a)} & & \downarrow{\scriptstyle(\gamma-a)} & & \\
0 & \longrightarrow & Y & \longrightarrow & \bigoplus \Lambda/f_i\Lambda & \longrightarrow & Z & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & Y/(\gamma-a)Y & \longrightarrow & \bigoplus(\Lambda/(f_i, \gamma-a)\Lambda) & \longrightarrow & Z/(\gamma-a)Z & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where $Y_{(\gamma-a)}$ means the kernel of the map $(\gamma - a)$ of Y, and same for the other modules. Then we deduce that each f_i is prime to $\gamma - a$ and $\oplus(\Lambda/f_i\Lambda)_{(\gamma-a)} = 0$. Also, since Z is finite, we have

$$|Z_{(\gamma-a)}| = |Z/(\gamma - a)Z|.$$

Applying the snake lemma, we get

$$|Y/(\gamma - a)Y| = |\bigoplus \Lambda/(f_i, \gamma - a)\Lambda|.$$

Finally, since every f_i is prime to $\gamma - a$, the equality

$$|\bigoplus \Lambda/(f_i, \gamma - a)\Lambda| = |\Lambda/(\prod f_i, \gamma - a)\Lambda|$$

follows. □

The next result is due to Iwasawa([Iwa73], Theorem 18).

Lemma 4.30. *For every even character χ of Δ, $X_\infty(\chi)$ ha no nonzero finite Λ-submodules.*

Proof. By the previous Kummer pairing, it is enough to show that $A_\infty(\chi^{-1}\omega)$ has no proper Λ-submodules of finite index. If $A \subseteq A_\infty(\chi^{-1}\omega)$ is stable and has finite index p^k, then we can choose N large enough to that $\mathrm{Gal}(K_\infty/K_N)$ acts trivially on $A_\infty(\chi^{-1}\omega)/A$. For every $m \geq N$ the map $N_{K_{m+k}/K_m} : C_{m+k} \to C_m$ is surjective ([Lan90], Section 5.4), thus

$$C_m(\chi^{-1}\omega) = N_{K_{m+k}/K_m} C_{m+k}(\chi^{-1}\omega) \subseteq A,$$

and $A_\infty(\chi^{-1}\omega) \subseteq A$. □

Finally, the consequence we were looking for.

Theorem 4.31 (Mazur-Wiles, Kolyvagin)**.** *For every odd character $\chi \neq \omega$ of Δ, if $m(\chi) = v_p(B_{1,\chi^{-1}})$, then*

$$|C(\chi)| = p^{m(\chi)}.$$

Proof. Recall that a generator γ of Γ acts on $\boldsymbol{\mu}_{p^\infty}$ as $1 + p$. By the Kummer pairing and Proposition 4.28,

$$\begin{aligned} C_0(\chi) &= \mathrm{Hom}(X_\infty(\chi^{-1}\omega), \boldsymbol{\mu}_{p^\infty})^\Gamma \\ &= \mathrm{Hom}(X_\infty(\chi^{-1}\omega)/(\gamma - (1+p))X_\infty(\chi^{-1}\omega), \boldsymbol{\mu}_{p^\infty}), \end{aligned}$$

where as usual γ is a generator of Γ. Using the results of this Section, we get

$$\begin{aligned} |C_0(\chi)| &= |X_\infty(\chi^{-1}\omega)/(\gamma - (1+p))X_\infty(\chi^{-1}\omega)| \\ &= |\mathbf{Z}_p[[T]]/(g_{\chi^{-1}\omega}(T), 1 + T - (1+p))\mathbf{Z}_p[[T]]| \\ &= |\mathbf{Z}_p/g_{\chi^{-1}\omega}((1+p) - 1)\mathbf{Z}_p| \\ &= |\mathbf{Z}_p/B_{1,\chi^{-1}}\mathbf{Z}_p|. \end{aligned}$$

□

Bibliography

[AT90] E. Artin and J. Tate. *Class field theory*. Second. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1990.

[Bir67] B. J. Birch. "Cyclotomic fields and Kummer extensions". In: *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*. Thompson, Washington, D.C., 1967, pp. 85–93.

[BK90] S. Bloch and K. Kato. "L-functions and Tamagawa numbers of motives". In: *The Grothendieck Festschrift, Vol. I*. Vol. 86. Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[Cox13] D. A. Cox. *Primes of the form x^2+ny^2*. Second. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[CS06] J. Coates and R. Sujatha. *Cyclotomic fields and zeta values*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[Fon82] J.-M. Fontaine. "Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate". In: *Ann. of Math. (2)* 115.3 (1982), pp. 529–577.

[Gre99] R. Greenberg. "Iwasawa theory for elliptic curves". In: *Arithmetic theory of elliptic curves (Cetraro, 1997)*. Vol. 1716. Lecture Notes in Math. Springer, Berlin, 1999, pp. 51–144.

[Iwa73] K. Iwasawa. "On $\mathbf{Z}_l$-extensions of algebraic number fields". In: *Ann. of Math. (2)* 98 (1973), pp. 246–326.

[Iwa86] K. Iwasawa. *Local class field theory*. Oxford Science Publications. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1986.

[Jan96] G. J. Janusz. *Algebraic number fields*. Second. Vol. 7. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1996.

[Kat99] K. Kato. "Euler systems, Iwasawa theory, and Selmer groups". In: *Kodai Math. J.* 22.3 (1999), pp. 313–372.

[Koc02] H. Koch. *Galois theory of p-extensions*. Springer Monographs in Mathematics. With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer. Springer-Verlag, Berlin, 2002.

[Kol90] V. A. Kolyvagin. "Euler systems". In: *The Grothendieck Festschrift, Vol. II*. Vol. 87. Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[Lan02] S. Lang. *Algebra*. third. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002.

[Lan90] S. Lang. *Cyclotomic fields I and II*. second. Vol. 121. Graduate Texts in Mathematics. With an appendix by Karl Rubin. Springer-Verlag, New York, 1990.

[Mar18] D. A. Marcus. *Number fields*. Universitext. Second edition of [MR0457396], With a foreword by Barry Mazur. Springer, Cham, 2018.

[MR04] B. Mazur and K. Rubin. "Kolyvagin systems". In: *Mem. Amer. Math. Soc.* 168.799 (2004), pp. viii+96.

[MW84] B. Mazur and A. Wiles. "Class fields of abelian extensions of $\mathbf{Q}$". In: *Invent. Math.* 76.2 (1984), pp. 179–330.

[Neu99] J. Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of number fields*. Second. Vol. 323. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2008.

[Rub00] K. Rubin. *Euler systems*. Vol. 147. Annals of Mathematics Studies. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton, NJ, 2000.

[Rub87] K. Rubin. "Global units and ideal class groups". In: *Invent. Math.* 89.3 (1987), pp. 511–526.

[Ser79] J.-P. Serre. *Local fields*. Vol. 67. Graduate Texts in Mathematics. Translated from the French by Marvin Jay Greenberg. Springer-Verlag, New York-Berlin, 1979.

[Ser89] J.-P. Serre. *Abelian l-adic representations and elliptic curves*. Second. Advanced Book Classics. With the collaboration of Willem Kuyk and John Labute. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989.

[Ser97] J.-P. Serre. *Galois cohomology*. Translated from the French by Patrick Ion and revised by the author. Springer-Verlag, Berlin, 1997.

[Sil09] J. H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009.

[Tat76] J. Tate. "Relations between K_2 and Galois cohomology". In: *Invent. Math.* 36 (1976), pp. 257–274.

[Tha88] F. Thaine. "On the ideal class groups of real abelian number fields". In: *Ann. of Math. (2)* 128.1 (1988), pp. 1–18.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*. Second. Vol. 83. Graduate Texts in Mathematics. Springer-Verlag, New York, 1997.

[Wei94] C. A. Weibel. *An introduction to homological algebra*. Vol. 38. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1994.

[Wil98] J. S. Wilson. *Profinite groups*. Vol. 19. London Mathematical Society Monographs. New Series. The Clarendon Press, Oxford University Press, New York, 1998.