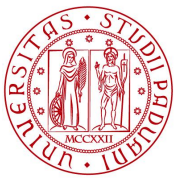


UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"

Master degree in Mathematics

Iwasawa Main conjecture and Euler systems

Supervisor:
Prof. Matteo Longo

Candidate: Lucia Onofrio
Matr. 2088650

Co-supervisor:
Prof. Guido Kings

Academic Year 2023/2024

20th September 2024

Contents

Introduction

The aim of this Master Thesis is to provide a proof of Iwasawa Main conjecture for the cyclotomic extension of a number field. In a very vague form, to be made precise later, this conjecture for the field of rational numbers $\mathbb{Q}$ (a theorem proved by Mazur-Wiles in [6], and by Rubin in [10]), predicts an equality between the ideal generated by an object of p-adic analytic nature, i.e. the p-adic L-function of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, and an object of algebraic nature, namely a subgroup of the cohomology group of the cyclotomic character, the Galois representation describing the action of the Galois group on the group of p-power roots of unity.

To be more precise, let p be an odd prime and let $K = \mathbb{Q}(\mu_p)$ be the extension obtained adjoining the p-th roots of unity to $\mathbb{Q}$.
We can consider the tower of fields $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_\infty = \bigcup K_n$, where $K_n = \mathbb{Q}(\mu_{p^{n+1}})$ and $K_\infty = \mathbb{Q}(\mu_{p^\infty})$. By Galois theory, we know that

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

If we set $\Gamma_n = \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$, then we can define the Iwasawa algebra

$$\Lambda = \varprojlim_n \mathbb{Z}_p[\Gamma_n].$$

The Iwasawa algebra Λ is isomorphic to $\mathbb{Z}_p[[T]]$, which is the ring of formal power series with coefficients in $\mathbb{Z}_p$. Moreover, in this setting we can attach to every finitely generated torsion Λ-module its characteristic ideal. We denote by C_n the p-part of the ideal class group of $K_n = \mathbb{Q}(\mu_{p^{n+1}})$, E_n the group of global units of K_n, $\mathscr{E}_n$ the group of cyclotomic units of K_n, and U_n the group of local units of the completion of K_n above p which are congruent to 1 modulo the maximal ideal. We let $\bar{E}_n$ and V_n denote the closures of $E_n \cap U_n$ and $\mathscr{E}_n \cap U_n$ in U_n. Then, the inverse limits under the norm maps

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

yield well defined Λ-modules. Now, if χ is an even p-adic character of $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, let us consider the eigenspaces $C_\infty(\chi)$, $E_\infty(\chi)$, $V_\infty(\chi)$ under χ.

Theorem (The Main conjecture) In the above notation,

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

The Main conjecture was proved following two different approaches: Mazur-Wiles, and then Wiles by himself, proved one inclusion showing that the p-adic L-function divides the characteristic ideal, constructing non zero elements in the Selmer group. In order to define the cited p-adic analytic object, we need to consider a Dirichlet character χ of conductor p, for which we can define the generalized Bernolli numbers by

$$\sum_{j=1}^{p} \frac{x(j)te^{jt}}{e^{pt}-1} = \sum_{k=0}^{\infty} B_{k,\chi}\frac{t^k}{k!}.$$

Then, the p-adic L-function is a meromorphic function $L_p(s,\chi)$ defined on $\{s \in \mathbb{C}_p \mid |s| > p^{1-\frac{1}{p-1}}\}$, such that

$$L_p(1-k,\chi) = -(1-\chi\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k},$$

with ω the Teichmüller character.

On the other side, Rubin used Euler systems to prove the opposite inclusion. Euler systems are collections of cohomology classes indexed on number fields which satisfy precise relations of compatibility with respect to corestriction maps, and they play an important role in modern number theory. Indeed, they can be used to derive several properties of Selmer groups and known results regarding the Birch–Swinnerton–Dyer conjecture. In particular, Kolyvagin's idea was to construct a system of cohomology classes derived from the Heegner points satisfying suitable norm and congruence relations; the local information about these cohomology classes were sufficient to bound the Selmer group of rank 1 elliptic curves.

Remark Note that Mazur-Wiles, Wiles and Rubin proved one divisibility; the other divisibility theorem follows from Iwasawa analytic class number formula. In particular, in [8] we can see how we can reduce to prove only one divisibility using precisely the analytic class number formula.

This work is organized as follows.

In Chapter 1, we collect preliminary notions mainly working with Iwasawa theory and Kummer theory over cyclotomic $\mathbb{Z}_p$-extensions.

With Chapter 2, we proceed with a discussion about Galois cohomology of p-adic representations, defining local and global cohomology group from which we obtain the definition of a Selmer group.

In Chapter 3, we provide the definition of Kolyvagin's Euler systems and fundamental results regarding their relation with Selmer groups.

Finally, in Chapter 4 we state and prove the Main conjecture and we provide equivalent formulations of it, focusing in particular on the role of the p-adic L-function.

Chapter 1

Preliminary notions

In the following sections one can find the preliminary notions cited in the Introduction, which constitute the basis for the next chapters. We mainly based on the book "Cyclotomic Fields I and II" by Lang [10].

1.1 Complex Analytic Class Number Formula

The class number formula relates special values, or residues, of complex L-functions attached to Dirichlet characters to units and class numbers of cyclotomic fields. We obtain these formulas by factoring the zeta function of a cyclotomic field in L-series and looking at the factorization of the residue.

1.1.1 Gauss Sums on $\mathbb{Z}/m\mathbb{Z}$

Let $m = \prod p^{n(p)}$ be the prime power product. We get the following product decompositions

$$\mathbb{Z}(m) = \prod \mathbb{Z}(p^{n(p)}) \quad \text{and} \quad \mathbb{Z}(m)^* = \prod \mathbb{Z}(p^{n(p)})^*.$$

For any character λ on $\mathbb{Z}(m)$ and any character χ on $\mathbb{Z}(m)^*$ we have product decompositions

$$\lambda = \prod_p \lambda_p \quad \text{and} \quad \chi = \prod_p \chi_p.$$

If $x \in \mathbb{Z}(m)$ is not prime to m, we define $\chi(x) = 0$. Let ζ be a primitive $m-$the root of unity and $\lambda(x) = \zeta^x$.

Let $d \mid m$. We have a natural surjective homomorphism $\mathbb{Z}(m) \to \mathbb{Z}(d)$ and a surjective homomorphism $\mathbb{Z}(m)^* \to \mathbb{Z}(d)^*$. If we do not have any $d \mid m$, $d \neq m$ such that χ factors through $\mathbb{Z}(d)^*$, then χ is said to be *primitive*. In order to determine the smallest d such that a character χ factors through $\mathbb{Z}(d)^*$, we need to look at prime powers. Indeed, let $m = p^n$

be a prime power and let χ be a character in $\mathbb{Z}(p^n)$. Let p^r be the smallest power of p such that χ is trivial on $1 + p^r\mathbb{Z}(p^n)$. We get that

$$\chi \text{ is primitive if and only if } r = n.$$

The power $p^r = p^{r(p)}$ is defined to be the *conductor* of χ. In the composite case, the *conductor* is defined by $c(\chi) = \prod_{p|m} p^{r(p)}$. Indeed, $c(\chi)$ is the smallest d such that χ factors through $\mathbb{Z}(d)^*$.

We define

$$S(\chi) = S(\chi, \lambda) = \sum_x \chi(x)\lambda(x)$$

where $x \in \mathbb{Z}(m)^*$. We obtain the product decomposition $S(\chi, \lambda) = \prod_p S_p(\chi_p, \lambda_p)$, where the sum S_p is over $\mathbb{Z}(p^{n(p)})^*$.

If d is prime to m, then

$$S(\chi, \lambda \circ d) = \overline{\chi}(d)S(\chi, \lambda)$$

by a change of variable $x \mapsto d^{-1}x$. If d is not prime to m, then

$$S(\chi, \lambda \circ d) = 0$$

[see [10] Chapter 3, §1].

1.1.2 Decomposition of L-series

Let us remark that for an integer $m > 1$ and for χ a non-trivial character on $\mathbb{Z}(m)^*$, we have that the conductor of χ is either odd or even; in particular, if it is even, it is divisible by 4. Thus, for a primitive character, m cannot be 2. If $m > 0$ is the smallest integer such that K is the field $K = \mathbb{Q}(\mu_m)$, then m is either odd or divisible by 4. In particular, if m is odd then the group of unity μ_K in K consists of $\pm\mu_m$; if m is even, $\mu_K = \mu_m$.

Now we deal with the cyclotomic field $\mathbb{Q}(\mu_m)$ for $m > 2$ and its maximal real subfield. Let K be an abelian extension of $\mathbb{Q}$ and K^+ its real subfield. Let $m > 0$ be the smallest integer such that $K \subset \mathbb{Q}(\mu_m)$, i.e. m is the *conductor* of K. We may assume $K = \mathbb{Q}(\mu_m)$ or $K = \mathbb{Q}(\mu_m)^+$. We obtain a surjective homomorphism between $\mathbb{Z}(m)^*$ and $\mathrm{Gal}(K/\mathbb{Q}) = G_{K/\mathbb{Q}}$. Note that any character χ of $G_{K/\mathbb{Q}}$ leads to a character in $\mathbb{Z}(m)^*$; $m(\chi)$ is its character.

Let

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N\mathfrak{p}}\right)^{-1}$$

be the zeta function associated with K. There is a decomposition

$$\zeta_K(s) = \prod_{\chi} L(s, \chi)$$

where χ runs through all the primitive characters induced by the characters of $G_{K/\mathbb{Q}}$.

Let r, s denote the number of real and complex conjugate embeddings of K. If K is real, then $r = [K : \mathbb{Q}]$ and $s = 0$; if K is not real, then $r = 0$ and $s = \frac{1}{2}[K : \mathbb{Q}]$.

Let n be $n = [K : \mathbb{Q}] = n_K$. Assuming the analytic continuation of the zeta function and L-series at $s = 1$ and comparing the residues, we get the *class number formula*

$$\frac{2^r(2\pi)^s hR}{w\sqrt{d}} = \prod_{\chi \neq 1} L(1, \chi)$$

where $w = w_K$ is the number of roots of unity in K, $h = h_K$ the class number of K, $R = R_K$ the regulator of K, and $d = d_K$ the absolute value of the discriminant. If K is real, then $w = 2$ and the above formula reduces to be

$$\frac{hR}{\sqrt{d}} = \prod_{\chi \neq 1} \frac{1}{2} L(1, \chi).$$

If K is not real, let h^+, R^+ and $n^+ = n/2 = s$ denote respectively the class number, the regulator and the degree of its real subfield.

Theorem 1.1 ([10], Theorem 3.1 §3, Chapter 3)**.** We have the following product expressions

(i) $\prod_{\chi \neq 1} m(\chi) = d$

(ii) $\prod_{\chi \neq 1} S(\chi) = \begin{cases} \sqrt{d} & \text{if } K \text{ is real} \\ i^s\sqrt{d} & \text{if } K \text{ is not real} \end{cases}$

Combining these product expressions with the expressions for the values of $L(1, \chi)$ for primitive characters χ, we obtain the following factorizations for the product hR, distinguishing two cases.

If K is real, we have

$$2^{n-1} hR = \prod_{\chi \neq 1} \sum_{b \bmod m(\chi)} -\chi(b) \log|1 - \zeta_{m(\chi)}^b|$$

with $n = n^+$, $h = h^+$, $R = R^+$ and even characters.

If K is not real, we have

$$\frac{2^{n/2} hR}{w} = \prod_{\substack{\chi \neq 1 \\ \text{even}}} \sum_{b \bmod m(\chi)} -\chi(b) \log|1 - \zeta_{m(\chi)}^b| \cdot \prod_{\chi \text{ odd}} -B_{1,\chi}.$$

Let us define $E = E_K$ the group of units in K, $E^+ = E_{K^+}$ the group of units in K^+, μ_K the group of roots of unity in K, and C_K the ideal class group in K.

Definition 1.2. We can define the *unit index* by

$$\mathcal{Q}_K = \mathcal{Q} := (E : \mu_K E^+) = \frac{2^{(n/2)-1} R^+}{R}.$$

Theorem 1.3 ([10] Theorem 3.2 §3, Chapter 3)**.** Let K imaginary. We have

$$h = h^+ \mathcal{Q} w 2^{-n/2} \prod_{\chi \text{ odd}} (-B_{1,\chi}).$$

Our goal is to study the decomposition $h = h^+ h^-$, where h^- is defined to be h/h^+ seen as an integer. We have the following class number formula

$$h^- = \mathcal{Q} w \prod_{\chi \text{ odd}} -\frac{1}{2} B_{1,\chi}.$$

Now, let us define the group $G := \mathbb{Z}(m)^*/\{\pm 1\}$, and for every even character χ, the group $G_\chi := \mathbb{Z}(m(\chi))^*/\{\pm 1\}$. We get a class number formula also for h^+

$$h^+ = \frac{1}{R^+} \prod_{\chi \neq 1} \sum_{b \in G_\chi} -\chi(b) \log|1 - \zeta_{m(\chi)}^b|.$$

1.1.3 The (± 1)-eigenspaces

The aim of this section is to analize the factors h^+ and h^- of the class number, i.e. the decomposition $h = h^+ h^-$. Let us assume m is odd or $m \equiv 0 \bmod 4$.

Theorem 1.4. Let $K = \mathbb{Q}(\mu_m)$. Then $\mathcal{Q}_K = \begin{cases} 1 & \text{if } m \text{ is a prime power} \\ 2 & \text{otherwise} \end{cases}$.

Theorem 1.5. Let $K = \mathbb{Q}(\mu_m)$. The natural map $C_{K^+} \to C_K$ of ideal classes in K^+ in the ideal class group of K is injective.

Theorem 1.6. Let K be an imaginary abelian extension of $\mathbb{Q}$. Then the norm map $N_{K/K^+} : C_K \to C_{K^+}$ on the ideal class group is surjective.

Lemma 1.7. Let K be an abelian extension of a number field F. Let H be the maximal abelian unramified extension of F (i.e. the Hilbert class field of F). If $K \cap H = F$, then the norm map $N_{K/F} : C_K \to C_F$ is surjective

Let τ be the complex conjugation. Let $C_K^- = \{c \in C_K \text{ such that } c^{1+\tau} = 1\}$ be the (-1)-eigenspace of C_K.

Theorem 1.8. Let $K = \mathbb{Q}(\mu_m)$. The sequence

$$1 \to C_K^- \to C_K \to C_{K^+} \to 1$$

is exact.

Corollary 1.9. The quotient h/h^+ is an integer. It coincides with the order of the group C_K^-.

1.1.4 Cyclotomic units

Let m be the conductor of $\mathbb{Q}(\mu_m)$, so that either $m > 1$, m odd, or m is divisible by 4.

Let $\zeta \in \mathbb{C}$ be a primitive m-th root of unity, i.e. $\zeta^m = 1$, such that for $b = 1, \ldots, m-1$, we have $\zeta^b \neq 1$. Along with all of its power, it is a root of the polynomial $x^m - 1$, i.e. it satisfies the equation $x^m = 1$. To find its minimal polynomial, note that the only rational m-th roots of unity is $\zeta^m = 1$. We can factor $x^m - 1 = (x-1)\phi_m(x)$, with $\phi_m(x)$ the m-th cyclotomic polynomial for ζ

$$\phi_m(x) = \frac{x^m - 1}{x - 1} = x^{m-1} + x^{m-2} + \cdots + x + 1.$$

The other m-th roots of unity are all powers of ζ and all roots of $\phi_m(x)$. In $\mathbb{C}$ we can factor

$$\phi_m(x) = \prod_{b=1}^{m-1} (x - \zeta^b) = x^{m-1} + x^{m-2} + \cdots + x + 1,$$

then both the product of the non-trivial m-th roots of unity and the sum of the non-trivial m-th roots of unity have magnitude 1, i.e. the sum of all the m-th roots of unity is 0. This implies that any m-th root of unity can be expressed as a linear sum of its power.

Definition 1.10. For $b \in \mathbb{Z}$ prime to m we define

$$g_b = \frac{\zeta^b - 1}{\zeta - 1}$$

the *cyclotomic unit*. Let g_b^+ be the *real cyclotomic unit*, uniquely determined up to sign.

Let $\mathscr{E}$, respectively $\mathscr{E}^+$ be the group of units in $\mathbb{Q}(\mu_m)$ generated by the roots of unity and the cyclotomic units, respectively the real cyclotomics units. Then $E/\mathscr{E} \cong E^+/\mathscr{E}^+$.

Definition 1.11. Let $N = [\mathbb{Q}(\mu_m) : \mathbb{Q}]$ and let $r = \frac{N}{2} - 1$ the rank of both E and E^+. If $\varepsilon_1, \ldots, \varepsilon_r$ is a basis for E^+, then the *regulator* R^+ is

$$R(E) = R^+ = \pm \det_{a,j} \log|\sigma_a \varepsilon_j|,$$

with $j = 0, \ldots, r$ and $a \in G := \mathbb{Z}(m)^*/\{\pm 1\}$, $a \not\equiv \pm 1 \bmod m$.
We can also define the *cyclotomic regulator*

$$R(\mathscr{E}) = R_{\text{cyc}} = \pm \det_{a,b \neq 1} \log|\sigma_a g_b|,$$

with $a, b \in G$.

Since we can see the regulator as the volume of a fundamental domain for the lattice generated by the log vectors of units in $\mathbb{R}^r$, we get that

$$(E : \mathscr{E}) = (E^+ : \mathscr{E}^+) = R_{\text{cyc}}/R^+.$$

Theorem 1.12. Let $K = \mathbb{Q}(\mu_m)$ and $h = h_K$. Assume $m = p^n$ is a prime power. Then

$$h^+ = (E^+ : \mathscr{E}^+) = (E : \mathscr{E})$$

1.2 The p-adic L-function

In this section we will provide Leopoldt's p-adic version of the class number formula, defining the p-adic regulator.

Let K be a totally real number field, $E = E_K$ the group of units of K, and let p be a prime number. Let $u_1, \ldots, u_r$ be a family of independent units in K, and let $\sigma_i : K \to \mathbb{C}_p$, $i = 1, \ldots, r+1$ be the embeddings of K in the p-adic complex numbers, i.e. the completion of the algebraic closure of $\mathbb{Q}_p$. Assume $\sigma_{r+1} = 1$.

Definition 1.13. We define the *p-adic regulator*, up to sign, by

$$R_p(u_1, \ldots, u_r) = \pm \det\left(\log\left(\sigma_i u_j\right)\right)_{1 \le i,j \le r}.$$

If $u_1, \ldots, u_r$ is a basis for the units, we write

$$R_p = R_{K,p} = R_p(E_K) = R_p(E).$$

If K is the real subfield of $\mathbb{Q}(\mu_m)$ and $\mathscr{E}$ is the group generated by the real cyclotomic units, we let

$$R_p(\mathscr{E}) = R_p(u_1, \ldots, u_r)$$

where $u_1, \ldots, u_r$ generate the cyclotomic units.

Theorem 1.14. Let K be the real subfield of $\mathbb{Q}(\mu_m)$. Then

$$R_p(\mathscr{E}) = (E : \mathscr{E}) R_p(E) = (E : \mathscr{E}) R_p.$$

Theorem 1.15 (Brumer)**.** For the real cyclotomic field $\mathbb{Q}(\mu_m)^+$, we have $R_p \neq 0$.

Theorem 1.16 (Leopoldt's p-adic Class Number regulator Formula)**.** Let $K^+ = \mathbb{Q}(\mu_m)^+$ and let $m = p^n$ be a prime power. Then

$$\prod_{\substack{\chi \neq 1 \\ \text{even}}} \frac{1}{2} L_p(1, \chi) = \frac{h^+}{\sqrt{d_K^+}} R_p.$$

1.3 Iwasawa Theory and Ideal Class Groups

In this section we study Iwasawa theory regarding projective limits in $\mathbb{Z}_p$-extensions. Firstly, we see algebraic notions related to projective limits and finitely generated modules over the power series ring $\mathbb{Z}_p[[X]]$ which denotes the limit of p-adic group rings of cyclic groups. Later, we deal with more arithmetic notion, considering modules over the Iwasawa algebra and the projective limit of ideal class groups which is, by class field theory, a Galois group.

1.3.1 The Iwasawa Algebra

Let Γ be a topological group isomorphic to $\mathbb{Z}_p$, multiplicatively. Let γ be a fixed generator such that the isomorphism would send x to γ^x, for $x \in \mathbb{Z}_p$. Let $\Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathbb{Z}(p^n)$. Then Γ_n is cyclic of order p^n, generated by the image of γ. On the other hand, a compatible system $\{\gamma_n\}$ of generators in a projective system $\{\Gamma_n\}$ of cyclic groups of order p^n would give a generator γ in their projective limit. We have a commutative diagram

$$\begin{array}{ccc} \mathbb{Z}_p[\Gamma_{n+1}] & \xrightarrow{\cong} & \mathbb{Z}_p[T]/(T^{p^{n+1}}-1) \\ \downarrow & & \downarrow \\ \mathbb{Z}_p[\Gamma_n] & \xrightarrow{\cong} & \mathbb{Z}_p[T]/(T^{p^n}-1) \end{array}$$

Let us note that $\mathbb{Z}_p[\Gamma_n] \cong \mathbb{Z}_p[\zeta_{p^n}]$, where ζ_{p^n} is a p^n-th root of unity, i.e. $\zeta^{p^n} - 1 = 0$. We can write the elements of $\mathbb{Z}_p[\Gamma_n]$ as $\sum_{a_i \in \Gamma_n} a_i \mathbb{Z}_p$, with each a_i of the type a_i^r with $r = 0, \ldots, p^n$. The map $\Gamma_n \to \mathbb{Z}_p[T]$ sends the coefficients a_i to T, and then $a^{p^n} \mapsto T^{p^n}$. Therefore, when we factor $Z_p[T]/(T^{p^n} - 1)$ we require $T^{p^n} - 1 = 0$ and hence $1 \mapsto 1$ by the map $f : \mathbb{Z}_p[\Gamma_n] \to \mathbb{Z}_p[T]/(T^{p^n} - 1)$. Let us show that f is an isomorphism. Indeed, it is injective since

$$\begin{aligned} a_i \mapsto 1 &\iff \text{ there exists } r = 0, \ldots, p^n \text{ such that } a_i^r \mapsto T^r - 1 \\ &\iff T^r \equiv T^{p^n} \bmod p^n \\ &\iff T^{p^n} - 1 \equiv T^r - 1 \\ &\iff r \equiv 0 \bmod p^n. \end{aligned}$$

and hence, $a_i^r = 0$. It is surjective since the map of $\mathbb{Z}_p$-modules is surjective and when we take $\langle T \rangle_{\mathbb{Z}_p} \in \mathbb{Z}_p[T]$, its image is again in $\mathbb{Z}_p$. Similarly, one can check that the map $\mathbb{Z}_p[\Gamma_{n+1}] \to \mathbb{Z}_p[T]/(T^{p^{n+1}} - 1)$ is an isomorphism. Moreover, the map $\Gamma_{n+1} \to \Gamma_n$ induces a natural map $\mathbb{Z}[\Gamma_{n+1}] \to \mathbb{Z}[\Gamma_n]$ compatible with isomorphism.

Let $X = T - 1$, so $T = X + 1$. Then $\mathbb{Z}_p[T] = \mathbb{Z}_p[X]$ and

$$\mathbb{Z}_p[T]/(T^{p^n} - 1) \cong \mathbb{Z}_p[X]/((X+1)^{p^n} - 1).$$

Let $h_n = h_n(X) = (1+X)^{p^n} - 1$. Then $h_n = X^{p^n} + \ldots$, and all coefficients, except the leading coefficient, are divisible by p. A polynomial of this type is called *distinguished*.

Our aim now is to establish an isomorphism

$$\mathbb{Z}_p[[X]] \to \lim \mathbb{Z}_p[\Gamma_n] = \lim \mathbb{Z}_p[X]/(h_n).$$

Let $\Lambda := \mathbb{Z}_p[[X]]$. If h is any distinguished polynomial, then

$$\mathbb{Z}_p[X]/(h) \cong \Lambda/h\Lambda. \tag{1.1}$$

This is true since $\Lambda/h\Lambda$ is free of rank $\deg h$ over $\mathbb{Z}_p$ and analogously, $\mathbb{Z}_p[X]/(h)$ is free of rank $\deg h$ over $\mathbb{Z}_p$. Moreover, we have that the natural map $\mathbb{Z}_p[X]/(h) \to \Lambda/h\Lambda$ is surjective, and then an isomorphism. Hence for each n we obtain a natural map $\mathbb{Z}_p[[X]] \to \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}[X]/(h_n)$ and then a homomorphism

$$\varepsilon : \Lambda = \mathbb{Z}_p[[X]] \to \lim \mathbb{Z}_p[X]/(h_n)$$

which is an isomorphism and it depends on the choice of the generator γ.

Definition 1.17. The projective limit $\varprojlim \mathbb{Z}_p[\Gamma_n]$ is called the *Iwasawa algebra*.

Now we consider modules over the Iwasawa algebra. For each n, let V_n be a module over $\mathbb{Z}_p[\Gamma_n]$ and suppose we have a homomorphism $V_{n+1} \to V_n$ compatible with the action of the group rings $\mathbb{Z}_p[\Gamma_{n+1}]$ and $\mathbb{Z}_p[\Gamma_n]$, respectively. We can define the projective limit $V = \varprojlim V_n$, which is a Λ-module. If each V_n is either a finite abelian group or compact, then the projective limit V is compact and $\mathbb{Z}_p[[X]]$ acts continuously on V, which is a topological module over $\mathbb{Z}_p[[X]]$.

Next we see some results related to finitely generated modules over the Iwasawa algebra.

Definition 1.18. Let V, V' two modules. They are *quasi-isomorphic* if there is a homomorphism $V \to V'$ with finite kernel and cokernel.

We will see that any finitely generated module V has a quasi-isomorphism with a finite product, namely we have a morphism

$$V \to \Lambda^{(r)} \oplus \prod \Lambda/(p^{m_i}) \oplus \prod \Lambda/(f_j) \tag{1.2}$$

with finite kernel and cokernel, where the f_j are distinguished, the first factor $\Lambda^{(r)}$ is the free part and the other factors are Λ-torsion modules.
Suppose that V is a torsion module such that V/h_nV is finite for all n. We want to obtain a formula for the order of V/h_nV which does not change under a quasi-isomorphism. Hence we only need to study two cases: $V = \Lambda/(p^m)$ and $V = \Lambda/(f)$, for some $m \in \mathbb{Z}$ positive and f distinguished.
In the first case $\Lambda/(p^m) = \mathbb{Z}/p^m\mathbb{Z}[[X]]$, the power series ring over $\mathbb{Z}/p^m\mathbb{Z}$. In the second case $\Lambda/(f)$ is a free module over $\mathbb{Z}_p$, with rank = deg$f$ by (1.1) with isomorphism

$$\mathbb{Z}_p[X]/(f) \cong \Lambda/(f)$$

and f irreducible, $f(X) \equiv X^{\deg(f)} \bmod p$. Since we could have that V_n, i.e. $V/(\gamma^{p^n} - 1)V$, is not finite, we need to make assumptions of finiteness to get the formula for the order. This is a power of p, hence we can say that card $V_n = p^{e_n}$, with $e_n = e_n(V)$.

Theorem 1.19. (i) If $V = \Lambda/(p^m)$ then $e_n = mp^n$.

(ii) Let $V = \Lambda/(f)$ where f is distinguished of degree d, and assume V_n finite for all n. Then there exists a constant c_0 such that for all n sufficiently large,

$$e_n = dn + c_0.$$

(iii) If V is finitely generated over Λ such that V_n is finite for all n, then there exists a constant c such that

$$e_n(V) = mp^n + dn + c$$

for all n sufficiently large. In the representation of V, as in (1.2) with $r = 0$, we have

$$m = \sum m_i \quad \text{and} \quad d = \sum \deg f_j$$

1.3.2 Modules over $\mathbb{Z}_p[[X]]$

Definition 1.20. Let $\Lambda = \mathcal{O}[[X]]$, with $\mathcal{O}$ a complete discrete valuation ring, and let p be a prime element of $\mathcal{O}$. A finitely generated module annihilated by some power p^k and some distinguished element λ is a *finite module over* $\mathcal{O}$.

We have seen that a homomorphism with finite kernel snd cokernel is called a *quasi-isomorphism*, and it is denoted by $M \sim M'$. As in (1.2), we obtain the following:

Theorem 1.21. [[10] Theorem 3.1 §3, Chapter 5] Let M be a finitely generated Λ-module. There exists a quasi isomorphism

$$M \sim \Lambda^{(r)} \oplus \prod \Lambda/(p^{n_i}) \oplus \prod \Lambda/(f_j^{m_j})$$

where f_j is a distinguished polynomial, irreducible in $\mathcal{O}[[X]]$, with i, j finite indices and $\Lambda^{(r)}$ is the product of Λ taken r times, $r \in \mathbb{Z}$.

1.3.3 $\mathbb{Z}_p$-extensions and Ideal Class Groups

Definition 1.22. Let K_0 be a number field. A $\mathbb{Z}_p$-*extension* is an abelian extension K_∞ of K_0 such that its Galois group is isomorphic to $\mathbb{Z}_p$, i.e. a tower of fields $K_\infty = \bigcup_{n=0}^{\infty} K_n \supset \cdots \supset K_n \supset \cdots \supset K_0$ such that K_n is cyclic of degree p^n over K_0.

If K is any number field, let $K^{(p)} = K(\mu^{(p)})$ be the extension of K obtained adjoining all p-power roots of unity. It is abelian, hence the fixed field of the torsion subgroup of $\mathrm{Gal}(K^{(p)}/K)$ is a $\mathbb{Z}_p$-extension, known as the cyclotomic $\mathbb{Z}_p$-extension.

Definition 1.23. An ideal $\mathfrak{p}_0$ of K_0 is *almost totally ramified* in a Galois extension K' if the inertia group of a prime $\mathfrak{p}$ in K' over $\mathfrak{p}_0$ is of finte index in $\mathrm{Gal}(K'/K_0)$. The ideal $\mathfrak{p}_0$ is *almost unramified* if its inertia group is finite.

Let us consider the following Iwasawa condition:

IW K_∞ is totally ramified over K_0 over a finite number of prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ lying above $\mathfrak{p}$; it is unramified over all other prime ideals. (1.3)

Lemma 1.24. Let K_∞/K_0 be a $\mathbb{Z}_p$-extension. Then

(i) There is only a finite number of prime ideals of K_0 which lie above p and they are almost totally ramified.

(ii) The extension K_∞/K_d is a $\mathbb{Z}_p$-extension which satisfies **IW** (1.3), for a positive integer d.

Now, assume that such **IW** condition (1.3) holds true. Analogously to Lemma 1.7, one can show that the norm map between any two successive steps in the tower is surjective on the ideal class groups. Let $C_n = C_n^{(p)}$ be the p-primary part of the ideal class group in K_n. Then we obtain a surjective sequence $C_0 \leftarrow C_1 \leftarrow \ldots$ and we let

$$C = \varprojlim C_n$$

be the projective limit, which consists of all sequences of the type $c_0, c_1, \ldots$ with $c_n \in C_n$ and c_{n+1} mapping on c_n under the norm map.

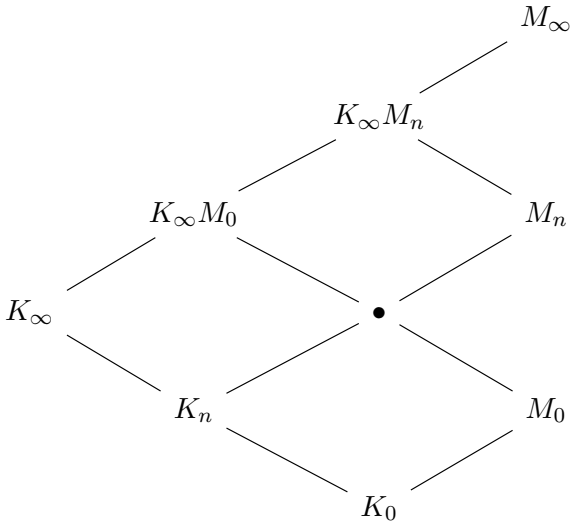
Let M_n be the maximal p-primary abelian unramified extension of K_n. By class field theory we know there is an isomorphism $C_n \cong \mathrm{Gal}(M_n/K_n)$

such that the diagram

$$\begin{array}{ccc} C_{n+1} & \longrightarrow & \mathrm{Gal}(M_{n+1}/K_{n+1}) \\ {\scriptstyle norm}\downarrow & & \downarrow{\scriptstyle restriction} \\ C_n & \longrightarrow & \mathrm{Gal}(M_n/K_n) \end{array}$$

is commutative.

Since K_∞ is totally ramified over K_n, we have that M_n is linearly disjoint from K_∞ over K_n. Let M_∞ be $\bigcup_n M_n$, G the Galois group $\mathrm{Gal}(M_\infty/K_0)$, $G_C = \mathrm{Gal}(M_\infty/K_\infty) \cong C$ and $\Gamma = \mathrm{Gal}(K_\infty/K_0)$: the lattice of fields looks as follows



Remark 1.25. If γ is a topological generator for Γ, then

$$\mathrm{Gal}(K_\infty/K_n) = \Gamma^{p^n} = \{\gamma^{p^n}\} \cong p^n\mathbb{Z}_p.$$

Theorem 1.26. Suppose that the condition **IW** (1.3) holds for $s = 1$. Let I be the inertia group of any prime above $\mathfrak{p}$ in G. Then:

(i) $G = IG_C$ is a semidirect product and the restriction of I to K_∞ gives an isomorphism of I and Γ.

(ii) The commutator group $G' = G_C^{\gamma-1}$

(iii) There is an isomorphism

$$C/C^{\gamma-1} \cong C_0 \cong \mathrm{Gal}(M_0/K_0) \cong \mathrm{Gal}(K_\infty M_0/K_\infty) \cong G_C/G_C^{\gamma-1}.$$

Theorem 1.27. Assume that **IW** (1.3) is satisfied with one prime. If $C_0 = \{1\}$, then $C_n = \{1\}$ for all n.

Theorem 1.28. For any $\mathbb{Z}_p$-extension, the module C over $\mathbb{Z}_p[[X]]$ is a finitely generated torsion module.

1.3.4 The Maximal p-abelian p-ramified Extension

The aim of this section is to describe the $\mathbb{Z}_p$-extensions of the Galois group of the maximal p-abelian p-ramified extension of a number field K for a fixed prime p. We now introduce some notation.

Let us denote with $M_p(K)$ the maximal p-abelian p-ramified extension and with $M_p^{\mathrm{unr}}(K)$ the maximal p-abelian unramified extension of K.

Let $J = J_K$ denote the ideles of K, $J^\infty = \prod_{v \in S_\infty} K_v^*$. For every $\mathfrak{p}$ prime ideal, let U be the group of unit ideles $U = \prod_{\mathfrak{p}} U_{\mathfrak{p}}$. We write

$$U_p = \prod_{\mathfrak{p}|p} U_{\mathfrak{p}} \quad \text{and} \quad U_{[p]} = \prod_{l \neq p} U_l.$$

Recall that $E = E_K$ denote the units in K. We have an embedding

$$\sigma_p : E \to U_p.$$

Let $G_p^{\mathrm{ab}}(K) = \mathrm{Gal}(M_p(K)/K)$. By class field theory, we know that an abelian extension of K is unramified at primes dividing l if and only if its associated group in the ideles contains U_l. Therefore we have an isomorphism

$$G_p^{\mathrm{ab}}(K) \cong p\text{-part of } J_K/\overline{U_{[p]} J^\infty K^*}$$

and the inclusions

$$J \supset U_p U_{[p]} J^\infty K^* \supset \overline{U_{[p]} J^\infty K^*}.$$

The factor group $J/U_p U_{[p]} J^\infty K^* = J/UK^*$ is finite and isomorphic to the Galois group of the Hilbert class field.
The other factor group is $U_p U_{[p]} J^\infty K^*/\overline{U_{[p]} J^\infty K^*} \cong U_p/U_p \cap \overline{U_{[p]} J^\infty K^*}$.

Theorem 1.29. Let H be p-Hilbert class field of K. Then there is an isomorphism

$$\mathrm{Gal}(M_p(K)/H) \cong p\text{-part of } U_p/\overline{\sigma_p E} = U_p^{(1)}/(U_p)^{(1)} \cap \overline{\sigma_p E}.$$

As p is fixed, we can only consider $U_p/\overline{E}$. A homomorphism with finite kernel and cokernel is called a *quasi-isomorphism*, denoted by $\sim$. So the theorem yields a quasi-isomorphism $G_p^{\mathrm{ab}}(K) \sim U_p/\overline{E}$.

Since U_p contains an open subgroup of finite index isomorphic to $\mathbb{Z}_p^{[K:\mathbb{Q}]}$, we have a quasi-isomorphism

$$G_p^{\mathrm{ab}}(K) \sim \mathbb{Z}_p^{[K:\mathbb{Q}]-r_p} \quad \text{with } r_p = \mathrm{rank}_{\mathbb{Z}_p} \overline{E} = r_p(E).$$

The *Leopoldt conjecture* states that $r_p = r = r_1 + r_2 - 1$.

If $Z_p(K)$ denotes the composite of all $\mathbb{Z}_p$-extensions of K, we get

$$[M_p(K) : Z_p(K)] < \infty.$$

Theorem 1.30. Assume that the Leopoldt conjecture holds true for K. Then we have a quasi-isomorphism

$$G_p^{\mathrm{ab}}(K) \sim \mathbb{Z}_p^{r_2+1} \cong \mathrm{Gal}(Z_p(K)/K).$$

1.3.5 The Galois Group as Module over the Iwasawa Algebra

Let K_0 be a number field, K_∞/K_0 any $\mathbb{Z}_p$-extension with Galois group $\Gamma = \{\gamma\}$ generated by γ. Let Ω be a p-abelian Galois extension over K_0 of K_∞. For every n, let Ω_n be the maximal subfield of Ω which is abelian over K_n.

Since Ω is Galois over K_0 and is abelian over K_∞, the commutator subgroup $\mathrm{Gal}(\Omega/K_0)^c = G^{\gamma-1}$ consists of all elements $\sigma^{\gamma-1} = \sigma\gamma\sigma^{-1}\gamma^{-1}$, with $\sigma \in G$.

It is useful to consider G as an additive module over the Iwasawa algebra: indeed, Γ_n operates by conjugation on $\mathrm{Gal}(\Omega/K_n)$ and hence on the commutator group $\mathrm{Gal}(\Omega/K_n)^{\gamma^{p^n}-1} = (\gamma^{p^n}-1)\mathrm{Gal}(\Omega/K_n)$. Therefore $\varprojlim G_n = G$ is a compact module over $\Lambda = \mathbb{Z}_p[[X]] = \varprojlim \mathbb{Z}_p[\Gamma_n]$.

Taking K_n as ground field, we have

$$\mathrm{Gal}(\Omega/\Omega_n) = (\gamma^{p^n}-1)G = ((1+X)^{p^n}-1)G$$

and in terms of Iwasawa algebra we get

$$G_n = G/(\gamma^{p^n}-1)G.$$

Theorem 1.31. Let Ω be the maximal p-abelian p-ramified extension of K_∞. Then:

(i) $G = \mathrm{Gal}(\Omega/K_\infty)$ is finitely generated over the Iwasawa algebra, indeed

$$G/G^{\gamma-1} \sim \mathbb{Z}_p^{[K_0:\mathbb{Q}]-r_p-1}$$

(ii) If K_0 satisfies the Leopoldt conjecture, then $[K_0:\mathbb{Q}]-r_p-1 = r_2$ and

$$G/XG \sim \mathbb{Z}_p^{r_2}$$

Theorem 1.32. Let K_0 be totally imaginary field. If every K_n satisfies the Leopoldt conjecture, i.e. $r_p(K_n) = r_2(K_n)$, then there is a quasi-isomorphism

$$G \sim \Lambda^{r_2} \times G_{\mathrm{tor}},$$

with G_{tor} the Λ-torsion submodule of G.

1.4 Kummer Theory over Cyclotomic $\mathbb{Z}_p$-extensions

In this section we consider the cyclotomic $\mathbb{Z}_p$-extensions of a number field and the Kummer extensions above it obtained by adjoining p^n-th roots of p-units, and the ideal classes of p-power order.

1.4.1 The Cyclotomic $\mathbb{Z}_p$-extension

Let $\mu^{(p)}$ be the group of p-power roots of unity. Then

$$\mathbb{Q}(\mu^{(p)}) = \begin{cases} \text{composite of an extension of degree } p-1 & \text{if } p \text{ is odd} \\ \mathbb{Q}(i) & \text{if } p = 2 \end{cases}$$

and a $\mathbb{Z}_p$-extension.

Definition 1.33. The above latter case is a $\mathbb{Z}_p$-extension uniquely determined as the fixed field of the torsion group of the Galois group; it is called the *cyclotomic $\mathbb{Z}_p$-extension*, denoted by $Z_p(\mathbb{Q})$.

If K is a number field, let us denote by $\mathrm{Cyc}_p(K) = KZ_p(\mathbb{Q})$ the composite of K and the cyclotomic $\mathbb{Z}_p$-extension: it is a cyclotomic $\mathbb{Z}_p$-extension of K. If K is totally real, then $\mathrm{Cyc}_p(K)$ is totally real.

Suppose that K contains the p-th roots of unity if p is odd and it contains i if $p = 2$. Let q_0 be the power of p such that the q_0-th roots of unity lie in K. Let $q_n = q_0 p^n$ and $K_n = K(\mu_{q_n})$. Then one has $[K_{n+1} : K_n] = p$ and get that $K_\infty = \bigcup_n K_n$ is a $\mathbb{Z}_p$-extension of K. Let $\Gamma = \mathrm{Gal}(K_\infty/K_0)$ and let $\chi : \Gamma \to 1 + q_0\mathbb{Z}_p$ be the canonical representation such that $\zeta^\gamma = \zeta^{\chi(\gamma)}$, for any p^n-th root of unity ζ.

Now, we describe some properties of p-abelian Galois extensions of K_∞. Let us recall that a Galois extension is said to be *p-abelian* if its Galois group is a projective limit of finite p-abelian groups, and note that in our case the p-abelian Galois extensions of K_∞ are Galois over K_0.

Let A_n be a subgroup of K_n^* and let $\Gamma_n = \mathrm{Gal}(K_n/K_0)$, $\Lambda_n = \mathbb{Z}(p^n)[\Gamma_n]$. Kummer theory yields a pairing

$$\mathrm{Gal}(K_n(A_n^{1/p^n})/K_n) \times A_n^{1/p^n}/(A_n^{1/p^n} \cap K_p^*) \to \mu_{p^n}$$

given by $(\sigma, \alpha) \mapsto \langle \sigma, \alpha \rangle_n = \frac{\sigma(\alpha)}{\alpha}$. If $\gamma \in \Gamma_n$, then

$$\langle \sigma^\gamma, \alpha^\gamma \rangle_n = \langle \sigma, \alpha \rangle_n^\gamma = \langle \sigma, \alpha \rangle_n^{\chi(\gamma)},$$

with $\sigma^\gamma = \tilde{\gamma}\sigma\tilde{\gamma}^{-1}$ and $\tilde{\gamma}$ an extension of γ to $K_n(A_n^{1/p^n})$.

The group A_n^{1/p^n} mod $A_n^{1/p^n} \cap K_n^*$ has exponent p^n and, if $\gamma^* = \gamma^{-1}\chi(\gamma)$, we can write $\langle \sigma^\gamma, \alpha \rangle_n = \langle \sigma, \alpha^{\gamma^*} \rangle_n$.

Our aim is to pass to the limit. Let us consider the Kummer pairing described above. Let $G_n = \mathrm{Gal}(K_\infty(A_n^{1/p^n})/K_\infty)$. It is a Γ_n-module and hence a Λ_n-module. Via the natural homomorphism, it is a Λ-module, where $\Lambda = \varprojlim_n \Lambda_n$ denotes the Iwasawa algebra. We know it is isomorphic to $\mathbb{Z}_p[[X]]$, where $X = \gamma_0 - 1$ and γ_0 is a generator of Γ.

If $m_i \in \mathbb{Z}_p$, let $\lambda = \sum_i m_i X^i \in \Lambda$. We can define the *Iwasawa involution* $\lambda^* = \sum_i m_i X^{*i}$, denoting by $X^* = \chi(\gamma_0)(1+X)^{-1} - 1$,. Then we can write the formula for the action of $\gamma \in \Gamma$ in terms of the Iwasawa involution $\langle \sigma^\lambda, \alpha \rangle = \langle \sigma, \alpha^{\lambda^*} \rangle$.

1.4.2 The Maximal p-abelian p-ramified Extension of the Cyclotomic $\mathbb{Z}_p$-extension

Let us fix some notation.

We have seen that a Galois extension is said to be *p-abelian* if its Galois group is a projective limit of finite p-abelian groups. It is *p-ramified* if it is unramified at all primes not dividing p.

Let K be a number field. Let us recall that $M_p(K)$ denotes the maximal p-abelian p-ramified extension of K and that $M_p^{\mathrm{unr}}(K)$ denotes the maximal p-abelian p-unramified extension of K. We can write

$$M_p(K) = \bigcup_F M_p(F),$$

where F is a family of subfields of K over $\mathbb{Q}$ whose union is K.

Let K be finite over $\mathbb{Q}$ and let K_∞ be a $\mathbb{Z}_p$-extension, then

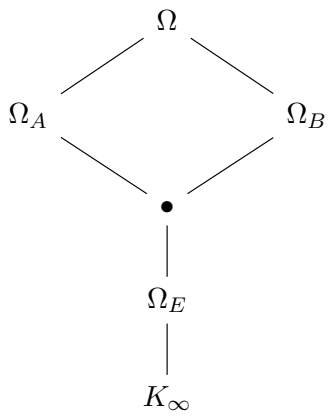
$$M_p(K_\infty) = \bigcup_n M_p(K_n).$$

Similarly,

$$M_p^{\mathrm{unr}}(K_\infty) = \bigcup_n M_p^{\mathrm{unr}}(K_n).$$

Now we recall some notation we have already set in the previous chapters. We denote with: K_∞ the cyclotomic $\mathbb{Z}_p$-extension of K_0, with K_0 containing the p-th roots of unity if p is odd, and containing i if $p = 2$; Ω the maximal p-abelian p-ramified extension of K_∞; E_n the units in K_n and $E = \bigcup_n E_n$; $\Omega_E = K_\infty\big(E^{1/p^\infty}\big)$; A_n the group of elements $\alpha \in K_n^*$ such that $(\alpha) = \mathfrak{a}^{p^n}$, where $\mathfrak{a}$ is fractional ideal prime to p and $A = \bigcup_n A_n$; $\Omega_A = \bigcup_n K_\infty\big(A_n^{1/p^n}\big)$; B_n the p-units in K_n, i.e. the group of elements whose ideal factorization consists in ideals dividing p; $\Omega_B = K_\infty\big(B^{1/p^\infty}\big)$.

In order to visualize, one can see the following diagram of fields



Remark 1.34. Clearly, Ω_A and Ω_B contain Ω_E: indeed, both A and B contain E.

Now, we want to study the structure of the extensions Ω_A/Ω_E and Ω_B/Ω_E. We have the following result.

Theorem 1.35. The Galois groups $\mathrm{Gal}(\Omega_A/\Omega_E)$ and $\mathrm{Gal}(\Omega_B/\Omega_E)$ are Λ-torsion modules. Therefore $\mathrm{Gal}(\Omega/\Omega_E)$ is a Λ-torsion module.

Proof. Firstly, let us consider $G = G_{A/E} = \mathrm{Gal}(\Omega_A/\Omega_E)$ and

$$G_n = \mathrm{Gal}(\Omega_E\big(A_n^{1/p^n}\big)/\Omega_E).$$

Clearly, G is the projective limit of G_n and G_n is a $\mathbb{Z}(p^n)[\Gamma_n]$-module, so G is a Λ-module. As in section 1.3.3, let $C_n = Cl^{(p)}(K_n)$ be the p-primary subgroup of ideal class group of K_n. Then, if $(\alpha) = \mathfrak{a}^{p^n}$ we have an homomorphism $\varphi : A_n^{1/p^n} \to C_n$, $\alpha^{1/p^n} \mapsto \mathfrak{a}$. If u is a unit in Ω such that $u^{p^n} \in A_n$, then $(u^{p^n}) = \mathfrak{a}^{p^n}$; since $A_n \subset K_n^*$ and $E_n = K_n^*$, we have that $u^{p^n} \in E_n$. Then the kernel of φ is E_n^{1/p^n} and hence we have an injective homomorphism $\psi : A_n^{1/p^n}/E_n^{1/p^n} \to C_n$, which is a Λ-homomorphism. Let us denote with $\mathscr{A}_n$ its image, i.e. we have

$$\begin{array}{ccc} G_n \times A_n^{1/p^n}/E_n^{1/p^n} & \to & \mu_{p^n} \\ \updownarrow & & \updownarrow \\ G_n \quad \times \quad \mathscr{A}_n & \longrightarrow & \mu_{p^n} \end{array}$$

where $G_n \times A_n^{1/p^n}/E_n^{1/p^n} \to \mu_{p^n}$ is the Kummer pairing

$$(\sigma, \alpha) \mapsto \langle \sigma, \alpha \rangle = \frac{\sigma(\alpha)}{\alpha}.$$

In particular, we have $\left(\frac{\sigma(\alpha)}{\alpha}\right)^{p^n} = \frac{\sigma(\alpha^{p^n})}{\alpha^{p^n}} = \frac{\alpha^{p^n}}{\alpha^{p^n}} = 1$.
We show the compatibility of the maps for n, $n+1$, i.e. we want to see

$$A_n^{1/p^n}/E_n^{1/p^n} \hookrightarrow A_{n+1}^{1/p^{n+1}}/E_{n+1}^{1/p^{n+1}}$$

Indeed,

$$\begin{aligned}
\alpha \in A_n^{1/p^n} &\iff \alpha^{p^n} \in A_n \\
&\iff (\alpha^{p^n})_{K_n} = \mathfrak{a}^{p^n} \text{ with } (\mathfrak{a}, p) = 1 \\
&\iff (\alpha^{p^{n+1}})_{K_n} = \mathfrak{a}^{p^{n+1}} \\
&\iff (\alpha^{p^{n+1}})_{K_{n+1}} = (\mathfrak{a}\mathcal{O}_{K_{n+1}})^{p^{n+1}}
\end{aligned}$$

and then $\alpha^{p^{n+1}} \in A_{n+1}$ implies that $\alpha \in A_{n+1}^{1/p^n+1}$. Moreover, if $u \in E_n^{1/p^n}$, $u^{p^n} \in E_n$, then $u^{p^{n+1}} \in E_n \subset E_{n+1}$ and hence $u \in E_{n+1}^{1/p^{n+1}}$. We get

$$\begin{array}{ccc}
A_n^{1/p^n} & \hookrightarrow & A_{n+1}^{1/p^{n+1}} \\
\uparrow & & \uparrow \\
E_n^{1/p^n} & \hookrightarrow & E_{n+1}^{1/p^{n+1}}
\end{array}$$

and hence $A_n^{1/p^n}/E_n^{1/p^n} \subset A_{n+1}^{1/p^{n+1}}/E_{n+1}^{1/p^{n+1}}$. So we can say that $\mathscr{A}_n \subset \mathscr{A}_{n+1}$.

We can then obtain the following

$$\begin{array}{ccccc}
G_{n+1} & \times & \mathscr{A}_{n+1} & \to & \mu_{p^{n+1}} \\
\downarrow & & \uparrow & & \uparrow \\
G_n & \times & \mathscr{A}_n & \longrightarrow & \mu_{p^n}
\end{array}$$

If $f_n : G_{n+1} \to G_n$, $i_n : \mathscr{A}_n \to \mathscr{A}_{n+1}$ and $j_n : \mu_{p^n} \to \mu_{p^{n+1}}$, we take $\sigma \in G_{n+1}$ and $a \in \mathscr{A}_n$. The Kummer pairing in the diagram are defined by

$$(\sigma, i_n(a)) \mapsto \langle \sigma, i_n(a) \rangle_{n+1} \quad \text{and} \quad (f_n(\sigma), a) \mapsto \langle f_n(\sigma), a \rangle_n,$$

where $\langle \sigma, i_n(a) \rangle_{n+1} = \frac{\sigma(a)}{a}$ and $\langle f_n(\sigma), a \rangle_n = \langle \sigma \mid_{K_n}, a \rangle = \frac{\sigma(a)}{a}$.

Therefore, applying the limit, we get a compact-discrete duality

$$G \times \mathscr{A} \to \mu^{(p)},$$

where $\mathscr{A}$ is the direct limit of $\mathscr{A}_n$ and G denotes the projective limit

$$\varprojlim G_n = \varprojlim \mathrm{Gal}(\Omega_E(A_n^{1/p^n})/\Omega_E) = \mathrm{Gal}(\Omega_A/\Omega_E).$$

By Theorem 1.28 there exists $\lambda \in \Lambda$ such that $C^\lambda = 1$, i.e. $C_n^\lambda = 1$ for every n and then $A_n^\lambda = 1$ for every n. By Kummer duality, for $\sigma \in G$, one has $\langle \sigma^{\lambda^*}, \alpha \rangle = \langle \sigma, \alpha^\lambda \rangle = 1$ for all $\alpha \in A_n^{1/p^n}$ and all n. Thus, $\sigma^{\lambda^*} = 1$, so λ^* annihilates G which is a torsion module over Λ.

Moreover, let us note that we have the following equivalences of direct limits $\varinjlim A_n^{1/p^n}/E_n^{1/p^n} = \varinjlim \mathscr{A}_n$ and $\varinjlim C_n = C_\infty$ since any element in C_∞ has a representative ideal prime to p. Indeed, to show that

$$\varinjlim A_n^{1/p^n}/E_n^{1/p^n} = \varinjlim \mathscr{A}_n \hookrightarrow \varinjlim C_n = C_\infty$$

we see that $\mathscr{A}_n \subset C_n$ for any n. Conversely, if we take $x \in C_\infty$, then $x \in C_n$ for some n. Hence we can write $x = [\mathfrak{a}]$ as an ideal class, with $\mathfrak{a}$ a fractional ideal in K_n prime to p. Now, C_n is a finite p-group, then there exists $N >> n$ such that $1 = x^{p^N} = [\mathfrak{a}^{p^N}]$ in C_n. Thus, $\mathfrak{a}^{p^N} = (\alpha)$, where $\alpha \in K_n^* \subset K_N^*$, and then $\alpha \in A_N$. We choose some p^N-th root $\alpha^{1/p^N} \in A_N^{1/p^N}$ and then $\varphi(\alpha^{1/p^N}) = [\mathfrak{a}] = x$ since $(\alpha) = \mathfrak{a}^{p^N}$.

This lead us to the following result.

Theorem 1.36. The Kummer pairing induces the following duality

$$\mathrm{Gal}(\Omega_A/\Omega_E) \times C_\infty \to \mu^{(p)}$$

which is non-degenerate.

Proof. To show it is non-degenerate, let us note that $\langle \sigma, a \rangle = 1$ for every $a \in \varinjlim \mathscr{A}_n$. Then, $\sigma(a) = a$ for every $a \in \bigcup_n A_n^{1/p^n}$, where A_n^{1/p^n} generates Ω_A, and thus $\sigma = \mathrm{id}$. Now, let $[a] \in \varinjlim \mathscr{A}_n$. Then, there exists n such that $[a] \in \mathscr{A}_n$. Let $a \in A_n^{1/p^n}$ be a representative. $\langle \sigma, a \rangle = 1$ if and only if $\sigma(a) = a$ for any $\sigma \in \mathrm{Gal}(\Omega_A/\Omega_E)$. Then, $a \in A_n^{1/p^n} \subset \Omega_A$ and hence, by Galois theory, $a \in \Omega_E$. Therefore, $a \in A_n^{1/p^n} \cap \Omega_E = E_n^{1/p^n}$, so $[a] = 1$. □

Now we can proceed considering the extension $G = G_{B/E} = \mathrm{Gal}(\Omega_B/\Omega_E)$. We know that if we consider a finite extension K_d, there is only a finite number of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ dividing p such that $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ are totally ramified in K_∞. If h denotes the class number of K_d, let $\mathfrak{p}_1^h = (\pi_1), \ldots, \mathfrak{p}_s^h = (\pi_s)$. Hence we have

$$\Omega_B = \Omega_E(\pi_1^{1/p^\infty}, \ldots, \pi_s^{1/p^\infty}).$$

This equivalence holds true since, from one side, we know that $\Omega_E \subset \Omega_B$, so we only need to show that the π_i^{1/p^∞} are in Ω_B for every $i = 1, \ldots, s$, i.e. it suffices to show that any p^n-th root π_i^{1/p^n} is in Ω_B for every n. By definition $(\pi_i) = \mathfrak{p}_i^h$ in K_d, hence $\pi_i \in B_d$ and then $\pi_i^{1/p^n} \in B^{1/p^\infty}$. Conversely, we want to show that $B^{1/p^\infty} \subset \Omega_E(\pi_1^{1/p^\infty}, \ldots, \pi_s^{1/p^\infty})$. Let $x \in B^{1/p^m}$ for some m. If x is a unit, then it is in Ω_E. If x is not a unit, we can write it

as $x = \pi_1^{1/p^{k_1}} \cdots \pi_t^{1/p^{k_t}} \cdot u$, where u is a unit and $\pi_1, \ldots, \pi_t$ are the only prime ideals of K_d dividing p which are totally ramified in K_∞ (this is true by condition **IW** (1.3)). Thus, the $\pi_1, \ldots, \pi_t$ are precisely some of the $\pi_1, \ldots, \pi_s$ and hence they lie in Ω_E.

It follows that

$$\mathrm{Gal}(\Omega_B/\Omega_E) \cong \mathbb{Z}_p^t \text{ with } t \leq s.$$

And hence by structure theorem for finitely generated Λ-modules, G cannot have any free part, which implies it is a Λ-torsion module, proving Theorem 1.35. □

Theorem 1.37. Let E_p be the group of units of K_∞ and $\Omega_{E_p} = \Omega(E_p^{1/p^\infty})$. If there is only one prime in K_∞ lying above p, then

$$\Omega_E = \Omega_{E_p} = \Omega_B.$$

Chapter 2

Galois cohomology of p-adic representations

In this chapter, we introduce p-adic representations of Galois groups, the cohomology groups associated and Selmer groups. We mainly refer to "Euler systems" by Rubin, [9].

2.1 Continuous group cohomology

This first section will provide the most important results about cohomology of topological groups which will be useful to deal with Galois cohomology and p-adic representations. Here we put ourselves in a general setting, where G is a profinite group.

Let G be a profinite group and A a topological G-module, i.e. a topological abelian group with a continuous action of G, compatible with the abelian group structure. For every $n \in \mathbb{N}$, 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 and their elements are called n-cochains. Let d^n be the homomorphism

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

defined by

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

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

Definition 2.1. For $n \geq 0$, the n-th *continuous cohomology group* of G with coefficients in A is the quotient group

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

where we set $\operatorname{Im}\left(d^{-1}\right) = 0$. The elements in $\ker\left(d^n\right)$ are called *cocyles*, and the elements of $\operatorname{Im}\left(d^{n-1}\right)$ are called *coboundaries*.

The cohomology groups we are interested in are $H^n(G, A)$ with $n = 0, 1$, defined as follows:

$$H^0(G, A) = \{a \in A \mid \sigma a = a \text{ for all } \sigma \in G\} = A^G,$$
$$H^1(G, A) = \frac{Z^1(G, A)}{B^1(G, A)},$$

where

$$Z^1(G, A) = \{f : G \to A \text{ continuous} \mid f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \text{ for all } \sigma, \tau \in G\}$$

and

$$B^1(G, A) = \{f : G \to A \mid f(\sigma) = \sigma a - a \text{ for a fixed } a \in A\}.$$

Remark 2.2. If the action of G on A is trivial, then $H^0(G, A) = A$ and $H^1(G, A) = \operatorname{Hom}(G, A)$, where the homomorphisms between topological groups are always assumed to be continuous.

Definition 2.3. Let A be a G-module and A' a G'-module, with G, G' profinite groups. If $\varphi : G' \to G$ and $f : A \to A'$ are two continuous homomorphisms we say that φ and f are *compatible* if

$$f\left(\varphi\left(\sigma'\right) a\right) = \sigma' f(a)$$

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

From this pair of maps, we can get canonical homomorphisms

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

We get a first example when we consider the identity Id: $G \to G$ and a G-module homomorphism $f : A \to B$, i.e. 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 wish to have a corresponding long exact sequence of cohomology groups. In order to do this for a general case, we need to add more hypothesis on the sequence.

Definition 2.4. 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).

Theorem 2.5 ([13], 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.

Now, we see important examples of compatible maps.

Example 2.6. (i) Let $\varphi : H \to G$ be the inclusion and $f : A \to A$ be the identity, where H is a subgroup of G. We have a *restriction* homomorphism:

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

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

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

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

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

This homomorphisms constitute an important exact sequence.

Proposition 2.7 ([9], Proposition 2.5, Appendix B)**.** Let H be a closed normal subgroup of G.

(i) There is an inflation-restriction exact sequence

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

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

$$\begin{aligned} 0 \to H^1\left(G/H, A^H\right) \to H^1(G, A) \to H^1(H, A)^{G/H} \to \\ \to H^2\left(G/H, A^H\right) \to H^2(G, A). \end{aligned}$$

In order to apply this result, we need to check if $H^n(G, S)$ is finite for every G-module S of finite p-power order. Before seeing a relevant result about this, we recall an important construction in group theory and number theory, mainly referring to [7].

Let A be a locally compact abelian group, i.e. an abelian topological group whose topology is Hausdorff and locally compact.

Definition 2.8. The *Pontryagin dual* of A is the group $A^\vee = \mathrm{Hom}(A, \mathbb{R}/\mathbb{Z})$, with the compact-open topology.

(i) If A is profinite or discrete torsion, then $A^\vee = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$,.

(ii) If A is pro-p or discrete p-torsion, e.g. a finitely generated $\mathbb{Z}_p$-module, then $A^\vee = \mathrm{Hom}\left(A, \mathbb{Q}_p/\mathbb{Z}_p\right)$..

(iii) If A is a topological G-module, then $A^\vee$ has a natural structure of G-module: for $g \in G$, $f \in A^\vee$ and $a \in A$, $(g \cdot f)(a) = f\left(g^{-1}a\right)$.

Theorem 2.9 (Pontryagin Duality, [7], Theorem 1.1.11)**.** If A is a locally compact abelian group, then $A^\vee$ is a locally compact abelian group with the compact-open topology. The canonical homomorphism

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

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

$$\{\text{abelian compact groups}\} \overset{\vee}{\Longleftrightarrow} \{\text{discrete abelian groups}\},$$

$$\{\text{abelian profinite groups}\} \overset{\vee}{\Longleftrightarrow} \{\text{discrete abelian torsion groups}\}.$$

Definition 2.10. A $\mathbb{Z}_p$-module is *cofinitely generated* if its Pontryagin dual is finitely generated.

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

Proposition 2.11 ([9], Proposition 2.7, Appendix B)**.** Assume that one of the following holds:

(i) K is a global field, K_S is a Galois extension unramified outside a finite set of places of K and $G = \mathrm{Gal}\left(K_S/K\right)$;

(ii) K is a local field and $G = G_K$;

(iii) K is a local field of residue characteristic different from p, and G is the inertia subgroup of G_K.

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

There is a another relevant map, but it cannot be obtained by compatible homomorphisms: the *corestriction*

$$\text{cor: } H^n(H, A) \to H^n(G, A),$$

with H open subgroup of G. Note that when $n = 0$, it is just the trace or the norm map $A^H \to A^G, a \mapsto \sum_{\sigma \in R} \sigma a$, where R is a representative of the left cosets of H in G.

Proposition 2.12 ([7], Proposition 1.5.2)**.** The corestriction map is functorial in the considered G-module, and it commutes with the connecting homomorphisms. Indeed, given a well-adjusted short exact sequence of G-modules

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

the diagram

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

is commutative.

Now, let G be a profinte group and A a G-module.

Theorem 2.13 ([13], Theorem 9.7.3)**.** If A is discrete. Then

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

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

where the limit is over all finitely generated submodules B of A;

(ii) 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 2.14 ([11], Corollary 2.2)**.** Assume $n > 0$ 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 $\mathbb{Z}_p$-module, tensoring it over $\mathbb{Z}_p$ with the exact sequence $0 \to \mathbb{Z}_p \to \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \to 0$, we have the sequence

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

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

Proposition 2.15 ([11], Proposition 2.3)**.** 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 $H^{n-1}(G, W)_{\text{div}}$, and its image is $H^n(G, A)_{\text{tors.}}$ Moreover, $H^n(G, A)$ has no divisible elements and there is an isomorphism

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

2.2 p-adic Galois representations

Let us consider a field K and a fixed separable closure $\bar{K}$. We denote by G_K the absolute Galois group $\text{Gal}(\bar{K}/K)$. Let Φ be a finite extension of $\mathbb{Q}_p$, where p is a rational prime, and $\mathcal{O}$ its ring of integers.

Definition 2.16. A *p-adic 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.

Many authors define a p-adic Galois representation to be a continuous group homomorphism $\rho : G_K \longrightarrow \text{GL}_d(\Phi) \cong \text{Aut}(V)$, where V is a d-dimensional Φ-vector space, or equivalently, a $\Phi\,[G_K]$-module which is finite-dimensional as Φ-vector space. However, given a representation, we can extend it to a representation for the Φ-vector space $V = T \otimes_{\mathcal{O}} \Phi$. If we denote by $\mathbf{D}$ the divisible module $\Phi/\mathcal{O}$, we can also define

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

so W_M is the M-torsion in W and we have the relations $W = \varinjlim W_M$ and $T = \varprojlim W_M$.

Example 2.17. Given a continuous character $\rho : G_K \to \mathcal{O}^\times$, we can consider as p-adic representation a free $\mathcal{O}$-module $\mathcal{O}_\rho$ of rank 1, on which G_K acts via ρ. Indeed, every 1-dimensional p-adic representation of G_K arises in this way. For example, let $\mathcal{O} = \mathbb{Z}_p$. If the characteristic of K is not p, we can consider the group of p-power roots of unity in $\bar{K}$, $\mu_{p^\infty} = \varinjlim \mu_{p^n}$, with $\mu_{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$ as abelian groups. The p-power maps $\mu_{p^{n+1}} \to \mu_{p^n}$, $\zeta \mapsto \zeta^p$ give rise to an inverse system of discrete groups, for which we can compute the inverse limit:

$$\mathbb{Z}_p(1) := \varprojlim \mu_{p^n}.$$

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

$$\chi_p : G_K \longrightarrow \mathrm{Aut}\,(\mu_{p^\infty}) \cong \mathbb{Z}_p^\times.$$

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

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

Definition 2.18. Let T be the p-adic representation of G_K with coefficients in $\mathcal{O}$. If the caracteristic 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 described as follows: if $\varphi \in \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}(1))$, $g \in G_K$ and $x \in T$, we have $(g\varphi)(x) = g(\varphi(g^{-1}x))$.

We can write

$$V^* = \mathrm{Hom}_{\mathcal{O}}(V, \Phi(1)) = T^* \otimes_{\mathcal{O}} \Phi \quad \text{and} \quad W^* = V^*/T^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathbf{D}(1))$$

Example 2.19. If $\mathcal{O}_\rho$ is the representation obtained by a continuous character $\rho : G_K \to \mathcal{O}^\times$ and χ_ρ is the cyclotomic character, then $T^* = \mathcal{O}_{\rho^{-1}\chi_\rho}$.

2.3 Galois cohomology

Let K be a field and A an abelian topological group with G_K action. Then we can define the continuous group cohomology: we will write $H^n(K, A)$ for $H^n(G_K, A)$ and $H^n(L/K, A)$ for $H^n(\mathrm{Gal}(L/K), A)$ if the action of G_K factors through $\mathrm{Gal}(L/K)$, for some extension L/K. In particular, if T is the p-adic representation of G_K, we can consider $H^n(K, T)$, $H^n(K, T \otimes \Phi)$ and $H^n(K, T \otimes \Phi/\mathcal{O})$.

Recall that if G_K acts trivially on A, then the first cohomology group coincides with the group of continuous homomorphisms from G_K to A. Hence, we can write

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

If L/K is a Galois extension, then $\mathrm{Gal}(L/K)$ acts naturally on the additive abelian group L and on the multiplicative abelan group $L^\times$. We assume to have the discrete topology.

Theorem 2.20 (Hilbert 90)**.** Let L/K be a Galois extension.

(i) $H^1(L/K, L) = 0$

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

Proof. See [2], Proposition 2, Chapter X, §1. □

We can see a relevant application of the above result in Kummer theory. 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 μ_n in $\bar{K}$. From the exact sequence

$$1 \to \mu_n \to \bar{K}^\times \xrightarrow{x \mapsto x^n} \bar{K}^\times \to 1$$

we obtain the exact sequence

$$1 \to K^\times/(K^\times)^n \to H^1(K, \mu_n) \to H^1(K, \bar{K}^\times) = 0.$$

Therefore, $\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \cong K^\times/(K^\times)^n$. If K contains all the n-th roots of unity, we get that $\mathrm{Hom}(G_K, \mathbb{Z}/n\mathbb{Z}) \cong K^\times/(K^\times)^n$ and therefore, we obtain that any Galois extension L/K with Galois group $\mathbb{Z}/n\mathbb{Z}$ is of the form $L = K(\alpha^{1/n})$.

Coming back to the general setting where T is a p-adic representation of G_K with coefficients in $\mathcal{O}$, $V = T \otimes \Phi$ and $W = V/T$, let us consider a non-zero $M \in \mathcal{O}$. We have the 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 2.21. If $M \in \mathcal{O} \setminus \{0\}$. Then

(i) The sequence (2.1) induces an exact sequence

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

(ii) 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. (i) Follows applying the long exact sequence in cohomology to (2.1), noting that $H^1(K,W)_M = \ker(H^1(K,W) \xrightarrow{M} H^1(K,W))$.

(ii) By Proposition 2.15, $H^1(K,T)_{\text{tors}} = \ker(H^1(K,T) \to H^1(K,V))$. □

2.4 Local cohomology groups

Let K be a finite extension of $\mathbb{Q}_l$, with l a finite rational prime. Let $\Bbbk$ be its residue field, $K^{\text{unr}} \subseteq \bar{K}$ the maximal unramified subfield of $\bar{K}$ and $\mathcal{I}$ the inertia subgroup of $\text{Gal}(\bar{K}/K^{\text{unr}})$. We have an exact sequence

$$1 \to \mathcal{I} \to G_K \to G_\Bbbk \to 1,$$

with $\text{Gal}(K^{\text{unr}}/K) \cong G_\Bbbk = \text{Gal}(\bar{\Bbbk}/\Bbbk) \cong \widehat{\mathbb{Z}}$, where $\widehat{\mathbb{Z}} \cong \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \prod_p \mathbb{Z}_p$. Here, the Frobenius element $\text{Frob} \in \text{Gal}(K^{\text{unr}}/K)$ coincides to the Frobenius automorphism in $\text{Gal}(\bar{\Bbbk}/\Bbbk)$, i.e. $x \mapsto x^{|\Bbbk|}$, which corresponds to $1 \in \widehat{\mathbb{Z}}$. In particular, $\text{Gal}(K^{\text{unr}}/K)$ is topologically generated by the element Frob.

Definition 2.22. Let A be a G_K-module. We say that A is *unramified* if $\mathcal{I}$ acts trivially on it. We define the subgroup of *unramified cohomology classes* by

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

Remark 2.23. If T is a p-adic representation of G_K, T is unramified if and only if V is unramified, hence if and only if W is unramified. If $l \neq p$, this holds true also for the dual representation.

Lemma 2.24. If $G \cong \widehat{\mathbb{Z}}$ with topological generator γ and we let A be a $\mathbb{Z}_p[G]$-module which is either a finitely generated $\mathbb{Z}_p$-module, or a finite dimensional $\mathbb{Q}_p$-vector space, or a discrete torsion $\mathbb{Z}_p$-module, then

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

where the isomorphism is induced by evaluating cocycles at γ.

Proof. It is easy to see that the evaluation of cocycles at γ induces a well defined injective homomorphism $H^1(G,A) \to A/(\gamma-1)A$. Using direct and inverse limit, and tensoring with $\mathbb{Q}_p$ as in section 2.1, we can reduce to the case in which A is finite. In this case we refer to [2], Chapter XIII, §1. □

Lemma 2.25. Let A be a G_K-module which is either a finitely generated $\mathbb{Z}_p$-module, or a finite dimensional $\mathbb{Q}_p$-vector space, or a discrete torsion $\mathbb{Z}_p$-module, then

$$H^1_{\text{unr}}(K, A) \cong H^1(K^{\text{unr}}/K, A^{\mathcal{I}}) \cong A^I/(\text{Frob} - 1)A^I.$$

If $l \neq p$, then

$$H^1(K, A)/H^1_{\text{unr}}(K, A) \cong H^1(\mathcal{I}, A)^{\text{Frob}=1},$$

where with $H^1(\mathcal{I}, A)^{\text{Frob}=1}$ we denote the elements of $H^1(\mathcal{I}, A)$ fixed by the Frobenius.

Proof. We obtain the first isomorphisms by applying the inflation-restriction exact sequence of Proposition 2.7 and Lemma 2.24. By Proposition 2.7 and Proposition 2.11, we have a Hochschild-Serre sequence

$$0 \to H^1(K^{\text{unr}}/K, A^{\mathcal{I}}) \to H^1(K, A) \to H^1(\mathcal{I}, A)^{\text{Frob}=1} \to H^2(K^{\text{unr}}/K, A^{\mathcal{I}}).$$

Since $\text{Gal}(K^{\text{unr}}/K) \cong \widehat{\mathbb{Z}}$ has cohomological dimension equal to 1 (see [13], Chapter 11), then $H^2(K^{\text{unr}}/K, A^{\mathcal{I}}) = 0$, and we get our last isomorphism. □

Example 2.26. If $K = \mathbb{Q}_l$, we can consider the trivial action of $G_{\mathbb{Q}}$ on $T = \mathcal{O} = \mathbb{Z}_p$. Hence,

$$H^1_{\text{unr}}(\mathbb{Q}_l, \mathbb{Z}_p) \cong \mathbb{Z}_p^{\mathcal{I}}/(\text{Frob} - 1)\mathbb{Z}_p^{\mathcal{I}} = \mathbb{Z}_p/(\text{Frob} - 1)\mathbb{Z}_p = \mathbb{Z}_p.$$

If V is a finite $\mathbb{Q}_p$-vector space and a p-adic representation of a group G, we can give the structure of a $\mathbb{Q}_p$-vector space to the the cohomology groups $H^n(G, V)$. In general, these are not finite dimensional. From previous section, we have $H^1(K, \mathbb{Z}_p(1)) \cong K^{\times}\widehat{\otimes}\mathbb{Z}_p$ since K has characteristic different from p. In particular, we can obtain an injection $K^{\times} \otimes \mathbb{Q}_p \hookrightarrow H^1(K, \mathbb{Q}_p(1))$ which gives us that $H^1(K, \mathbb{Q}_p(1))$ cannot have finite dimension since $K^{\times}$ has countably infinite rank. Unramified cohomology groups can help to solve this problem.

Corollary 2.27. If $l \neq p$ and V is a $\mathbb{Q}_p[G_K]$-module which is finite dimensional as $\mathbb{Q}_p$-vector space, then

$$\dim_{\mathbb{Q}_p}(H^1_{\text{unr}}(K, V)) = \dim_{\mathbb{Q}_p}(V^{G_K}) < \infty.$$

Proof. By Lemma 2.25, we have an exact sequence

$$0 \longrightarrow V^{G_K} \longrightarrow V^{\mathcal{I}} \xrightarrow[\text{Frob}-1]{} V^{\mathcal{I}} \longrightarrow H^1_{\text{unr}}(K, V) \longrightarrow 0$$

From known result about the dimension of vector spaces in exact sequences, we obtain our claim. □

Now, we consider K a finite extension of $\mathbb{Q}_l$, and we allow l to be infinity. Hence, K would be $\mathbb{R}$ or $\mathbb{C}$. Let T be a p-adic representation of G_K, let $V = T \otimes \Phi$ and $W = V/T$. Following [1], we define special subgroups $H^1_f(K, \cdot)$ of the cohomology groups $H^1(K, \cdot)$.

Definition 2.28. If $l \neq p, \infty$, we define the *finite part* of $H^1(K, v)$ by

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

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 of $H^1_f(K, V)$ under the natural maps

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

Similarly, for $M \in \mathcal{O} \smallsetminus \{0\}$, we define $H^1_f(K, W_M)$ as the inverse image of $H^1_f(K, W)$ under the map induced by the inclusion $W_M \hookrightarrow W$.
For V, T, W or W_M we define the *singular quotient* of $H^1(K, \cdot)$ by

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

and hence there is an exact sequence

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

Lemma 2.29. Let T be a p-adic representation of G_K, with $l \neq p, \infty$.

(i) $H^1_f(K, W) = H^1_{\text{unr}}(K, W)_{\text{div}}$.

(ii) $H^1_{\text{unr}}(K, T) \subseteq H^1_f(K, T)$ with finite index, and $H^1_s(K, T)$ is torsion free.

(iii) If $\mathcal{W} = W^{\mathcal{I}}/(W^{\mathcal{I}})_{\text{div}}$, then there are natural isomorphisms

$$H^1_{\text{unr}}(K, W)/H^1_f(K, W) \cong \mathcal{W}/(\text{Frob} - 1)\mathcal{W}$$

$$H^1_f(K, T)/H^1_{\text{unr}}(K, T) \cong \mathcal{W}^{\text{Frob}=1}$$

(iv) If T is unramified, then

$$H^1_f(K, T) = H^1_{\text{unr}}(K, T) \quad \text{and} \quad H^1_f(K, W) = H^1_{\text{unr}}(K, W).$$

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

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

we get $H^1_{\text{unr}}(K,T) \subseteq H^1_f(K,T)$ and $H^1_f(K,W) \subseteq H^1_{\text{unr}}(K,W)$. The rest of (i) and (ii) will follow from (iii), since $\mathcal{W}$ is finite: indeed, by Proposition 2.14, $\mathcal{W}$ is isomorphic to $H^1(K,T)_{\text{tors}}$, which is finite, being the torsion part of a finitely generated module over $\mathbb{Z}_p$.
(iii) The image of $V^{\mathcal{I}} \to W^{\mathcal{I}}$ is $\left(W^{\mathcal{I}}\right)_{\text{div}}$ again by Proposition 2.14. Therefore, taking first $\mathcal{I}$-cohomology and then $\text{Gal}\,(K^{\text{ur}}/K)$-invariants of the exact sequence $0 \to T \to V \to W \to 0$, we derive an exact sequence

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

Using Lemma 2.25, we get

$$\begin{aligned} H_f(K,T)/H_{\text{unr}}(K,T) &= \ker\left(H^1(K,T)/H^1_{\text{unr}}(K,T) \to H^1(K,V)/H^1_{\text{unr}}(K,V)\right) \\ &= \ker\left(H^1(\mathcal{I},T)^{\text{Frob}=1} \to H^1(\mathcal{I},V)^{\text{Frob}=1}\right) \\ &= (\mathcal{W})^{\text{Frob}-1} \end{aligned}$$

$$\begin{aligned} H_{\text{unr}}(K,W)/H_f(K,W) &= \text{coker}\left(H^1_{\text{unr}}(K,V)/ \to H^1_{\text{unr}}(K,W)\right) \\ &= \text{coker}\left(V^{\mathcal{I}}/(\text{Frob}-1)V^{\mathcal{I}} \to W^{\mathcal{I}}/(\text{Frob}-1)W^{\mathcal{I}}\right) \\ &= W^{\mathcal{I}}/\left(\left(W^{\mathcal{I}}\right)_{\text{div}} + (\text{Frob}-1)W^{\mathcal{I}}\right) \\ &= \mathcal{W}/(\text{Frob}-1)\mathcal{W} \end{aligned}$$

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

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

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

However, we will not enter in details; we can just fix an arbitrary subspace of $H^1(K,V)$, denoting it by $H^1_f(K,V)$. Natural choices are

$$H^1_f(K,V) = 0 \quad \text{or} \quad H^1_f(K,V) = H^1(K,V).$$

Then, we can define $H_f(K,T), H_f(K,W)$ and $H_f\left(K,W_M\right)$ as before.

Finally, if $l = \infty, K = \mathbb{R}$ or $\mathbb{C}$, we have that G_K is finite of order 1 or 2. Since V is torsion-free and divisible, then $H^1(K,V) = 0$. Again, we have:

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

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

(iii) $H^1_f(K,T) = H^1(K,T)$;

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

Remark 2.30. If we consider W_M, for $M \in \mathcal{O} \smallsetminus \{0\}$, then we see it is a subgroup of W and also a quotient of T, hence the subgroup $H^1_f(K, W_M)$ can be defined as the inverse image of $H^1_f(K, W)$ or the image of $H^1_f(K, T)$. This choice makes no difference: we see the following lemma.

Lemma 2.31. Suppose $M \in \mathcal{O}$ is non zero.

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

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

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

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

Proof. (i) From the diagram (2.2), we get a commutative diagram with exact rows

$$\begin{array}{ccccccc} H^1(K,T) & \xrightarrow{M} & H^1(K,T) & \longrightarrow & H^1(K,W_M) & \longrightarrow & H^2(K,T) \\ \| & & \downarrow{\scriptstyle M^{-1}} & & \downarrow & & \| \\ H^1(K,T) & \longrightarrow & H^1(K,V) & \longrightarrow & H^1(K,W) & \longrightarrow & H^2(K,T) \end{array} \tag{2.3}$$

Therefore, we see 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 (2.3), the image of $\mathbf{c}_V = 0$ in $H^2(K, T)$, then also the image of $\mathbf{c}_{W_M}$ has to be zero in $H^2(K, T)$. By exactness, there is 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 $H^1(K, T)$, thus it differs by an element $\mathbf{c}' \in H^1(K, T)$. Therefore, the element $\mathbf{c}_T - M\mathbf{c}'$ is in $H^1_f(K, T)$ and maps to $\mathbf{c}_{W_M}$.

(ii) If $l \neq p$ and T is unramified, then $H^1_f(H, T) = H^1_{\mathrm{unr}}$. By (i) we have

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

Conversely, if ι_M is the map $H^1(K, W_M) \to H^1(K, W_M)$, then

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

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

□

Corollary 2.32. There are natural horizontal exact sequences and 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, hence, by Proposition 2.11, the groups in the inverse limits are finite. Then, the horizontal sequences are exact. Since $T = \varprojlim W_M$ and $W = \varinjlim W_M$, we have

$$H^1(K,W) = \varinjlim H^1(K,W_M) \quad \text{and} \quad H^1(K,T) = \varprojlim H^1(K,W_M).$$

Similarly, since by definition

$$H^1_f(K,W) = \varinjlim H^1(K,W_M) \quad \text{and} \quad H^1_f(K,T) = \varprojlim H^1_f(K,W_M)$$

we have

$$H^1_s(K,W) = \varinjlim H^1_s(K,W_M) \quad \text{and} \quad H^1_s(K,T) = \varprojlim H^1_s(K,W_M).$$

□

2.5 Global cohomology and Selmer groups

Let K be a number field and T a p-adic representation of G_K with coefficients in $\mathcal{O}$. We consider $V = T \otimes \Phi$ and $W = V/T$. If v is a place of K, we can consider the decomposition group of any place of $\bar{K}$ in G_K, denoted by G_{K_v} since it is the absolute Galois group of the completion K_v of K under the prime v. We denote by $\mathcal{I}_v$ the inertia subgroup contained in G_{K_v}. We have a canonical restriction map $H^1(K,\cdot) \to H^1(K_v,\cdot)$, $\mathbf{c} \mapsto \mathbf{c}_v$. Recall that T is unramified at a place v if the inertia group $\mathcal{I}_v$ acts trivially on T. We assume that T is unramified outside a finite set of primes of K.

Remark 2.33. If v is a place of K lying over the prime l of $\mathbb{Q}$, which can be ∞, then K_v is a finite extension of $\mathbb{Q}_l$. In particular, we can repeat the construction of the previous chapter, and we can take 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 $H^1_{\mathrm{unr}}(K_v,V)$; 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. We denote by K_Σ the maximal extension of K contained in $\bar{K}$ unramified outside Σ.

We introduce some Selmer groups corresponding to Σ.

Definition 2.34. Let A be T, W or W_M for some $M \in \mathcal{O} \smallsetminus \{0\}$. Recall that $H^1_s(K_v, A) = H^1(K_v, A)/H^1_f(K_v, A)$. We define

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

by

$$\mathcal{S}^\Sigma(K, A) = \ker\left(H^1(K, A) \to \prod_{v \notin \Sigma} H^1_s(K_v, A)\right)$$

$$\mathcal{S}_\Sigma(K, A) = \ker\left(\mathcal{S}^\Sigma(K, A) \to \bigoplus_{v \in \Sigma} H^1(K_v, A)\right)$$

This means that a class $\mathbf{c} \in H^1(K, A)$ belongs to $\mathcal{S}^\Sigma(K, A)$ if, for every $v \notin \Sigma$, $\mathbf{c}_v \in H^1_f(K_v, A)$; it belongs to $\mathcal{S}_\Sigma(K, A)$ if we also have $\mathbf{c}_v = 0$ for every $v \in \Sigma$. If $\Sigma = \emptyset$, we get the *true Selmer group*

$$\mathcal{S}(K, W) = \mathcal{S}_\emptyset(K, W) = \mathcal{S}^\emptyset(K, W) = \ker\left(H^1(K, A) \to \prod_{v \text{ place of } K} H^1_s(K_v, A)\right)$$

Remark 2.35. If $A = W$, the map

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

goes to $\bigoplus_{v \notin \Sigma} H^1_s(K_v, W)$. Indeed, by discreteness of W, if $f : G_K \to W$ is a cocycle, then the preimage of $\{0\}$ has to be open in G_K, so it is $\mathrm{Gal}(\bar{K}/L)$ for some L/K finite Galois. Now, L ramifies only at finite primes, hence the inertia with respect to the others is trivial, and for almost all places v, we have $H^1_f(K_v, W) = H^1_{\mathrm{unr}}(K_v, W)$.

Remark 2.36. If Σ contains all primes above p, the Selmer groups do not depend on the choice of $H^1_f(K_v, V)$ for v lying above p.

Lemma 2.37. 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 $\bar{K}$.

Proof. The fixed field of $\mathcal{I}_{\bar{v}/v}$ is the maximal extension of K in which the restriction of $\bar{v}$ is unramified (see [4] Theorem 8.3). Hence, K_Σ is contained in the fixed field of every $\mathcal{I}_{\bar{v}/v}$. Then, since $\mathrm{Gal}\left(\bar{K}/K_\Sigma\right)$ is closed, it contains the closure of the subgroup generated by the inertia. If it strictly contains the cited closure, then the fixed field of this closure would be an extension of K unramified outside Σ strictly larger than K_Σ, and we have a contradiction. □

Lemma 2.38. If Σ contains all infinite places, all primes above p and all primes of K where T is ramified. If A is T, W or W_M, with $M \in \mathcal{O} \smallsetminus \{0\}$, then

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

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

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

where the first equality follows from Lemma 2.25, the second from Lemma 2.37 and the last from the inflation-restriction sequence (Proposition 2.7). □

Proposition 2.39. Let Σ be a finite set of primes of K.

(i) $\mathcal{S}^{\Sigma}(K, T) = \varinjlim S^{\Sigma}\left(K, W_M\right)$ and $\mathcal{S}_{\Sigma}(K, T) = \varinjlim S_{\Sigma}\left(K, W_M\right)$.

(ii) $\mathcal{S}^{\Sigma}(K, W) = \varprojlim S^{\Sigma}\left(K, W_M\right)$ and $\mathcal{S}_{\Sigma}(K, W) = \varprojlim S_{\Sigma}\left(K, W_M\right)$.

Proof. Immediate from Corollary 2.32. □

The next result describes why working with the Selmer groups is easier than working just with the global cohomology group $H^1(K, \cdot)$.

Lemma 2.40. If $M \in \mathcal{O} \smallsetminus \{0\}$ and Σ is a finite set of primes of K, then

(i) $\mathcal{S}^{\Sigma}\left(K, W_M\right)$ is finite.

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

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

Proof. Without loss of generality, we can enlarge Σ so that it contains all the infinite places, all primes above p and all primes where T is ramified. By Lemma 2.38, if $A = W_M, T$ or W, then $\mathcal{S}^{\Sigma}(K, A) = H^1\left(K_{\Sigma}/K, A\right)$, which has the desired properties by Proposition 2.11. □

Remark 2.41. In Chapter 2 of [5], we can find a more general structure 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* $\mathcal{F}$ on A is a choice of $\mathcal{O}$-submodule $H^1_{\mathcal{F}}(K_v, A) \subseteq H^1(K_v, A)$ such that, for almost all places v of K, $H^1_{\mathcal{F}}(K_v) = H^1(K_v, A)$. Then, the *Selmer group* for this collection is

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

or equivalently

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

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 our choices of $H^1_f(K_v,A)$ lead to a Selmer structure.

Now, we see an important example of this construction. Let $\mathcal{O} = \mathbb{Z}_p = T$ with trivial G_K action. Then, by Lemma 2.29 and Lemma 2.25, for every prime v of K not above p, we get

$$H^1_f\left(K_v, \mathbb{Q}_p/\mathbb{Z}_p\right) = H^1_{\mathrm{unr}}\left(K_v, \mathbb{Q}_p/\mathbb{Z}_p\right) = \mathrm{Hom}\left(\mathrm{Gal}\left(K_v^{\mathrm{unr}}/K_v\right), \mathbb{Q}_p/\mathbb{Z}_p\right).$$

As in Remark 2.35 and Lemma 2.38, if Σ is a finite set of places containing the primes above p, it follows that

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

where $H_{K,\Sigma}$ is the maximal unramified abelian extension of K in which the places in Σ splits completely. This is a subfield of the Hilbert class field of K, then $\mathrm{Gal}\left(H_{K,\Sigma}/K\right)$ is a quotient of the ideal class group A_K. It is the quotient of A_K modulo the subgroup generated by the classes of primes in Σ. If we denote by $A_{K,\Sigma}$ this quotient, we get

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

Now, we see that if Σ is empty, then there is an appropriate choice of subspaces $H^1_f\left(K_v, \mathbb{Q}_p\right)$ such that

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

In general, if $\chi : G_K \to \mathcal{O}^\times$ is a character of finite order prime to p and $T = \mathcal{O}_\chi$ is 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 $\Delta = \mathrm{Gal}(L/K)$. 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 [9],

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

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

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

and if $v \mid p$, we can take this as definition for $H^1_f\left(K_v, V\right)$ as well.

Proposition 2.42. There is an isomorphism

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

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

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

This hold true since $W \to W$ is an isomorphism, and hence

$$H^1(\Delta, W) = H^2(\Delta, W) = 0.$$

Now, since $D_w/\mathcal{I}_w$ is torsion free, $\oplus_{w|v} \mathrm{Hom}\left(D_w/\mathcal{I}_w, W\right)^\Delta$ is divisible, and we obtain an isomorphism

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

from the isomorphism

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

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

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

□

In particular, if $L = K$, we obtain the identification

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

Chapter 3

Euler systems

In this chapter we provide the definition of an Euler system and main results applying them over $\mathbb{Z}_p^d$-extensions of number fields.

3.1 Euler systems: definition

Let K be a number field and $\mathcal{O}_K$ its ring of integers. If p is a rational prime and Φ a finite extension of $\mathbb{Q}_p$, let us consider a p-adic representation T of G_K with coefficients in $\mathcal{O}$, the ring of integers of Φ. Assume that T is unramified outside a finite set of primes of K.

If $\mathfrak{q}$ is a prime of K not dividing p, let $K(\mathfrak{q})$ denote the maximal p-extension of K contained in the ray class field $K^{\mathfrak{q}}$ of K modulo $\mathfrak{q}$. If $\mathrm{Frob}_{\mathfrak{q}}$ is the Frobenius of $\mathfrak{q}$ in G_K, we define

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

Note that this determinant is well-defined. We know that the Frobenius is not uniquely determined: indeed, it depends on the choice of a prime of $\bar{K}$ lying over $\mathfrak{q}$, and it is defined modulo an inertia subgroup. Since T is unramified at $\mathfrak{q}$ and $\mathfrak{q}$ does not lie over p, T^* is unramified at $\mathfrak{q}$ and hence the determinat is well-defined.

To denote that F/K is a finite extension, we write $K \subseteq_f F$.

Definition 3.1. If $\mathcal{K}$ is an infinite abelian extension of K, let $\mathcal{N}$ be an ideal of K divisible by p and by all primes, and let T be ramified, such that

(i) $\mathcal{K}$ contains $K(\mathfrak{q})$ for every $\mathfrak{q}$ prime of K not dividing $\mathcal{N}$;

(ii) $\mathcal{K}$ contains an extension K_∞ of K such that $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p^d$ for some $d \geq 1$, and no finite prime of K splits completely in K_∞/K.

An *Euler system* for $(T, \mathcal{K}, \mathcal{N})$ is a collection of classes

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

such that

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

where $K \subseteq_f F \subseteq_f F' \subseteq \mathcal{K}$, $\Sigma(F'/F)$ is 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

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

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

A collection $\mathbf{c} = \{c_F \in H^1(F, T)\}$ is an Euler system for T if we can choose $\mathcal{K}$ and $\mathcal{N}$, as above, such that $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$.

A collection $\mathbf{c} = \{c_F \in H^1(F, T)\}$ is an Euler system for (T, K_∞), where K_∞ is a $\mathbb{Z}_p^d$-extension of K where there are no finite primes splitting completely, if, again, we can choose $\mathcal{K} \supseteq K_\infty$ and $\mathcal{N}$ such that $\mathbf{c}$ is an Euler system for $(T, \mathcal{K}, \mathcal{N})$.

Remark 3.2. Since $\mathbb{Z}_p^d$ has no proper finite subgroup, the condition for a prime to do not split completely in K_∞/K is satisfied if and only if its decomposition group is infinite. If K_∞ contains the cyclotomic $\mathbb{Z}_p$-extension of K, the condition is satisfied since no finite prime of K splits completely there. In order to simplify the notation, take $p \neq 2$. The subextension $\mathbb{Q}_n$ of $\mathbb{Q}_\infty$ of degree p^n, is obtained as the fixed field of $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mu_{p-1}$ in $\mathbb{Q}(\zeta_{p^{n+1}})$, with

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

If $l \neq p$, the Frobenius of l in $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ is isomorphic to $l \pmod{p^{n+1}}$, and then l splits completely in $\mathbb{Q}_n$ if $l^p \equiv 1 (\mathrm{mod}\ p^{n+1})$, only for finitely many n.

Since p divides $\mathcal{N}$, no Euler factors at primes dividing p are considered here. The only unramified primes in K_∞ lie above p (see Lemma 1.24), hence the Euler system classes are "univeral norms" in the direction of K_∞/K: indeed, if $K \subseteq_f F \subseteq_f F' \subseteq K_\infty$, then $\Sigma(F'/F)$ is empty and thus $\mathrm{cor}_{F'/F}(\mathbf{c}_{F'}) = \mathbf{c}_F$.

Remark 3.3. Let $K^{\mathfrak{m}}$ be the ray class field of K modulo $\mathfrak{m}$, where $\mathfrak{m}$ is an ideal of K. Given $\mathcal{K}$ and $\mathcal{N}$, we say that an Euler system for $(T, \mathcal{K}, \mathcal{N})$ is a collection $\{\tilde{\mathbf{c}}_m \in H^1(K^m \cap \mathcal{K}, T) \mid \mathfrak{m} \text{ is a modulus of } K\}$ such that

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

Indeed, given such a collection, if $K \subseteq_f F$, we define $\mathbf{c}_F = \mathrm{cor}_{K^{\mathfrak{m}} \cap \mathcal{K}/F}(\tilde{\mathbf{c}}_m)$, where $\mathfrak{m}$ is the conductor of F/K. Then, it is immediate to see that $\{\mathbf{c}_F\}$ is

an Euler system. On the other hand, given an Euler system $\mathbf{c} = \{\mathbf{c}_F\}$, for every modulus $\mathfrak{m}$ of K, we define

$$\tilde{\mathbf{c}}_m = \prod_{\substack{\mathfrak{q}|\mathfrak{m} \\ \mathfrak{q}\nmid\mathcal{N}}} P(\mathrm{Frob}_{\mathfrak{q}}^{-1} \mid T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\mathbf{c}_{K^{\mathfrak{m}}\cap\mathcal{K}},$$

where the product is over primes $\mathfrak{q}$ unramified in $(K^{\mathfrak{m}} \cap \mathcal{K})/K$.

Remark 3.4. Given $\mathcal{N}$ and K_∞/K as in Definition 3.1, let $\mathfrak{t} = \mathfrak{q}_1, \ldots, \mathfrak{q}_k$ be a squarefree product of finite primes not dividing $\mathcal{N}$. Then, we can define $K(\mathfrak{t}) = K(\mathfrak{q}_1)\cdots K(\mathfrak{q}_k)$ to be the compositum. If $K \subseteq_f F \subseteq K_\infty$, we write $F(\mathfrak{t}) = FK(\mathfrak{t})$. If we denote by $\mathcal{K}_{\min}$ the compositum of K_∞ and all $K(\mathfrak{q})$ for finite primes $\mathfrak{q}$ not dividing $\mathcal{N}$, then $\mathcal{K}_{\min}$ is the smallest extension of K which satisfies Definition 3.1. 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 $\mathcal{N}$. Therefore, an Euler system for $(T, \mathcal{K}_{\min}, \mathcal{N})$ is completely determined by a subcollection $\{\mathbf{c}_{F(\mathfrak{t})} \mid \mathfrak{t}$ is squarefree and prime to $\mathcal{N}, K \subseteq_f F \subseteq K_\infty\}$. Conversely, assume we have 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 K not dividing $\mathfrak{t}\mathcal{N}$ such that $K(\mathfrak{q}) \neq K$, then

$$\mathrm{cor}_{F(\mathfrak{tq})/F(\mathfrak{t})}(\mathbf{c}_{F(\mathfrak{tq})}) = P(\mathrm{Frob}_{\mathfrak{q}^{-1}} \mid T^*; \mathrm{Frob}_{\mathfrak{q}}^{-1})\mathbf{c}_{F(\mathfrak{t})},$$

$$\mathrm{cor}_{F'(\mathfrak{t})/F(\mathfrak{t})}(\mathbf{c}_{F'(\mathfrak{t})}) = \mathbf{c}_{F(\mathfrak{t})}.$$

Then, this collection yields an Euler system. Indeed, 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 and such that $L \subseteq F(\mathfrak{t})$. Therefore, we can view an Euler system for $(T, \mathcal{K}_{\min}, \mathcal{N})$ as the described collection $\{\mathbf{c}_{F(\mathfrak{t})}\}$.

3.2 Results over K

Let us consider the setting in which $\mathfrak{p}$ is the maximal ideal of $\mathcal{O}$ and $\Bbbk = \mathcal{O}/\mathfrak{p}$ is the residue field. Let $K(1)$ denote the maximal p-extension of K in the Hilbert class field of K. We introduce two sets of hypothesis on the Galois representation T, $\mathrm{Hyp}(K, T)$ and $\mathrm{Hyp}(K, V)$.

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

(i) There exists a $\tau \in G_K$ such that τ is trivial on μ_{p^∞}, on $(\mathcal{O}_K^\times)^{1/p^\infty}$ i.e. the p-power roots of unity in $(\mathcal{O}_K)^\times$, and on $K(1)$; $T/(\tau - 1)T$ is free of rank 1 over $\mathcal{O}$;

(ii) $T \otimes \Bbbk$ is an irreducible $\Bbbk[G_K]$-module.

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

(i) There exists a $\tau \in G_K$ such that τ is trivial on μ_{p^∞}, on $(\mathcal{O}_K^\times)^{1/p^\infty}$, and on $K(1)$; $\dim_\Phi(V/(\tau-1))V = 1$;

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

Remark 3.5. Note that the hypothesis $\mathrm{Hyp}(K,T)$ are satisfied if the image of the Galois representation on T is sufficiently large. For example, if T has rank 1 as $\mathcal{O}$-module, then the hypothesis hold when $\tau = 1$.

Definition 3.6. The *index of divisibility* of an Euler system $\mathbf{c}$ is defined as

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

In this setting, $p^{\mathrm{ind}_{\mathcal{O}}(\mathbf{c})}$ is the largest power of the maximal ideal by which $\mathbf{c}_K$ can be divided in $H^1(K,T)/H^1(K,T)_{\mathrm{tors}}$. Let A be an $\mathcal{O}$-module. We denote by $\ell_{\mathcal{O}}(A)$ the lenght of A (it can be ∞). We define

$$\Omega = K(1)K(W)K(\mu_{p^\infty}(\mathcal{O}_K^\times)^{1/p^\infty}),$$

with $K(W)$ 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 3.7. [[9], Theorem 2.2, Chapter II] 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 3.8. Our aim is to obtain the smallest possible lenght. The terms $\mathfrak{n}_W$ and $\mathfrak{n}_W^*$ are related to the extension Ω/K with which we work. If $K = \mathbb{Q}$ and $T = \mathbb{Z}_p(1)$, for example, then Ω is the known field $\mathbb{Q}(\mu_{p^\infty})$.

Theorem 3.9 ([9], Theorem 2.3, Chapter II)**.** Let $\mathbf{c}$ be an Euler system for T, where T is not the one-dimensional 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 3.10. If $T = \mathcal{O}$, then $\mathcal{S}_{\Sigma_p}(K,W^*)$ is finite if and only if Leopoldt's conjecture holds for K (see [9], Corollary 6.4, Chapter 1).

Note that Theorem 3.7 provides a bound for the size of $\mathcal{S}_{\Sigma_p}(K,W^*)$ and not for the true Selmer group $\mathcal{S}(K,W^*)$. Hence, we need an additional hypothesis concerning the subspaces $H^1_f(K_v,\cdot)$ for primes v dividing p.

Now, in the setting in which K is either a finite extension of $\mathbb{Q}_l$ for some rational prime l or $K = \mathbb{R}$ or $\mathbb{C}$, and T is a p-adic representation of G_K, we have the following result.

Theorem 3.11 (Local duality, [9], Theorem 4.1)**.** Suppose that either K is non archimedean and $i = 0, 1, 2$, or K is archimedean and $i = 1$. Then the cup product and the local invariant map induce perfect pairings

Suppose that either K is non archimedean and $i = 0, 1, 2$, or K is archimedean and $i = 1$. Then the cup product and the local invariant map induce perfect pairings

$$\begin{array}{rcccl} H^i(K,V) & \times & H^{2-i}(K,V^*) & \to & H^2(K,\Phi(1)) \xrightarrow{\sim} \Phi \\ H^i(K,W_M) & \times & H^{2-i}(K,W_M^*) & \to & H^2(K,\mathcal{O}(1)/M\mathcal{O}(1)) \xrightarrow{\sim} \mathcal{O}/M\mathcal{O} \\ H^i(K,T) & \times & H^{2-i}(K,W^*) & \to & H^2(K,\mathbf{D}(1)) \xrightarrow{\sim} \mathbf{D}. \end{array}$$

We need to require that the subspaces $H^1_f(K_v, V)$ and $H^1_f(K_v, V^*)$ are orthogonal complement under the above pairing for $v \mid p$. 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 $\mathrm{loc}^s_{\Sigma_p}$ be the localization map $\mathcal{S}^{\Sigma_p}(K,T) \to H^1_s(K_p,T)$. By Lemma 2.29 and Corollary 3.4 in Appendix B of [9], if $\mathbf{c}$ is an Euler system, then $\mathbf{c}_K \in \mathcal{S}^{\Sigma_p}(K,T) \subseteq H^1(K,T)$.

Corollary 3.12 ([9], Corollary 7.5, Chapter I)**.** 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 3.13. Let $\mathbf{c}$ be an Euler system for T and $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K) \neq 0$.

(i) 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, and then $\mathcal{S}(K,W^*)$ is finite.

(ii) 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. The idea is to use Theorems 3.7 and 3.9 in order to bound $\mathcal{S}_{\Sigma_p}(K,W^*)$, and then (3.1) to control $[\mathcal{S}(K,W^*) : \mathcal{S}_{\Sigma_p}(K,W^*)]$.

(i) For every v, $H^1_s(K_v,T)$ is torsion free since it injects into the vector space $H^1_s(K_v,V)$. Then, since $\mathrm{loc}^s_{\Sigma_p}(\mathbf{c}_K)$ is non zero then we have $\mathbf{c}_K \notin H^1(K,T)_{\mathrm{tors}}$. By Theorem 3.9, $\mathcal{S}_{\Sigma_p}(K,W^*)$ is finite and by (3.1) we obtain

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

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

$$\mathbf{c}_K \in \mathfrak{p}^n H^1(K,T) + H^1(K,T)_{\text{tors}}.$$

This implies

$$\mathbf{c}_K \in \mathfrak{p}^n \mathcal{S}^{\Sigma_p}(K,T) + H^1(K,T)_{\text{tors}}$$

and then

$$\text{loc}^s_{\Sigma_p}(\mathbf{c}_K) \in \mathfrak{p}^n \,\text{loc}^s_{\Sigma_p}\left(\mathcal{S}^{\Sigma_p}(K,T)\right).$$

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

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

and by Theorem 3.7,

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

Therefore by (3.1), we obtain our claim.

□

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

In this section we want to study the $\mathbb{Z}_p^d$-extension K_∞. In particular, we put ourselves in the setting in which $d = 1$. Let us consider $K = \mathbb{Q}$ and let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

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

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

(i) There is a $\tau \in G_K$ such that τ is trivial on μ_{p^∞}, and $T/(\tau-1)T$ is free of rank one over $\mathbb{Z}_p$;

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

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

(i) There is a $\tau \in G_K$ such that τ is trivial on μ_{p^∞}; moreover, we have that $\dim_{\mathbb{Q}_p}(V/(\tau-1))V = 1$;

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

Recall that the Iwasawa algebra of the $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ is defined by $\Lambda = \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$.

Definition 3.14. Define the following Λ-modules:

$$\mathcal{S}_{\Sigma_p}(\mathbb{Q}_\infty, W^*) = \varinjlim_n \mathcal{S}_{\Sigma_p}(\mathbb{Q}_n, W^*)$$

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

$$H^1_\infty(\mathbb{Q}, T) = \varprojlim_n H^1(\mathbb{Q}_n, T)$$

Every $\mathcal{S}_{\Sigma_p}(\mathbb{Q}_n, W^*)$ has a structure of $\mathbb{Z}_p[\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})]$-module since this holds true for $H^1(\mathbb{Q}_n, W^*)$ and for $\oplus_{v|l} H^1(\mathbb{Q}_{n,v}, W^*)$, with $l \neq p$ a fixed prime of $\mathbb{Q}$. On the Pontryagin dual, Γ acts by $\gamma f(x) = f(\gamma^{-1}x)$. Then, $\Lambda = \mathbb{Z}_p[[T]]$ acts via $g(T)f(x) = f(g((1+T)^{-1})x)$.

Definition 3.15. If $\mathbf{c}$ is an Euler system, let $\mathbf{c}_{\mathbb{Q}_\infty}$ be the corresponding element of $H^1_\infty(K, T)$. We define an ideal

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

This ideal is the analogue for Λ of the index of divisibility we introduced in Definition 3.6.

The next results are proved generalizing Theorem 3.7 for every $\mathbb{Q}_n$ and then passing to the limit.

Let $\mathbf{c}$ be an Euler system for $(T, \mathbb{Q}_\infty)$.

Theorem 3.16 ([9], Theorem 3.2, Chapter II)**.** If V satisfies $\mathrm{Hyp}(\mathbb{Q}_\infty, V)$ and $\mathbf{c}_{\mathbb{Q},\infty} \notin H^1_\infty(K, T)_{\Lambda\text{-tors}}$, then X_∞ is finitely generated as Λ-torsion module.

Theorem 3.17 ([9], Theorem 3.3, Chapter II)**.** If T satisfies $\mathrm{Hyp}(\mathbb{Q}_\infty, T)$, then $\mathrm{char}(X_\infty)$ divides $\mathrm{ind}_\Lambda(\mathbf{c})$.

Theorem 3.18 ([9], Theorem 3.4, Chapter II)**.** If V satisfies $\mathrm{Hyp}(\mathbb{Q}_\infty, V)$, then there exists a non negative integer t such that $\mathrm{char}(X_\infty)$ divides $p^t \mathrm{ind}_\Lambda(\mathbf{c})$.

These theorems give bounds for the size of $\mathcal{S}_{\Sigma_p}(\mathbb{Q}_\infty, W^*)$. Now, we want to consider the true Selmer group $\varprojlim \mathcal{S}(\mathbb{Q}_n, W^*)$. We need the following assumption:

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

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

(ii) If $m \geq n$, then

$$\mathrm{cor}_{\mathbb{Q}_{m,p}/\mathbb{Q}_{n,p}} H_f^1(\mathbb{Q}_{m,p}, V) \subseteq H_f^1(\mathbb{Q}_{n,p}, V),$$

$$\mathrm{res}_{\mathbb{Q}_{m,p}/\mathbb{Q}_{n,p}} H_f^1(\mathbb{Q}_{n,p}, V^*) \subseteq H_f^1(\mathbb{Q}_{m,p}, V^*).$$

These hypothesis imply that for $m \geq n$, the restriction and corestriction maps induce respectively

$$\mathcal{S}(\mathbb{Q}_n, W^*) \to \mathcal{S}(\mathbb{Q}_m, W^*) \quad \text{and} \quad H_s^1(\mathbb{Q}_{m,p}, T) \to H_s^1(\mathbb{Q}_{n,p}, T).$$

Then we can define the Λ-modules

$$\mathcal{S}(\mathbb{Q}_\infty, W^*) = \varinjlim_n \mathcal{S}(\mathbb{Q}_n, W^*) \quad \text{and} \quad H_{\infty,s}^1(\mathbb{Q}_p, T) = \varprojlim_n H_s^1(\mathbb{Q}_{n,p}, T).$$

Proposition 3.19. Let $\mathrm{loc}_{\Sigma_p}^s : H_\infty^1(\mathbb{Q}, T) \to H_{\infty,s}^1(\mathbb{Q}_p, T)$ be the localization map. Then there is an exact sequence

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

Proof. By Corollary 3.4 in Appendix B of [9],

$$H_\infty^1(\mathbb{Q}, T) = \varprojlim_n S^{\Sigma_p}(\mathbb{Q}_n, T).$$

Then passing to the direct limit from (3.1) and applying $\mathrm{Hom}(\cdot, \mathbb{Q}_p/\mathbb{Z}_p)$, we obtain our claim. □

Theorem 3.20. If V saitisfies $\mathrm{Hyp}(\mathbb{Q}_\infty, V)$, $\mathrm{loc}_{\Sigma_p}^s(\mathbf{c}_{\mathbb{Q},\infty}) \notin H_{\infty,s}^1(\mathbb{Q}_p, T)_{\Lambda\text{-tors}}$ and $H_{\infty,s}^1(\mathbb{Q}_p, T)/\Lambda \mathrm{loc}_{\Sigma_p}^s(\mathbf{c}_{\mathbb{Q},\infty})$ is a finitely generated Λ-torsion module, then

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

(ii) There is a non negative integer t such that $\mathrm{char}\left(\mathrm{Hom}\left(\mathcal{S}\left(\mathbb{Q}_\infty, W^*\right), \mathbb{Q}_p/\mathbb{Z}_p\right)\right)$ divides $p^t \,\mathrm{char}\left(H_{\infty,s}^1\left(\mathbb{Q}_p, T\right)/\Lambda \,\mathrm{loc}_{\Sigma_p}^s\left(\mathbf{c}_{\mathbb{Q},\infty}\right)\right)$. If T satisfies $\mathrm{Hyp}\left(\mathbb{Q}_\infty, T\right)$, then

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

Proof. (i) Since $\mathrm{loc}_{\Sigma_p}^s\left(\mathbf{c}_{\mathbb{Q},\infty}\right) \notin H_{\infty,s}^1\left(\mathbb{Q}_p, T\right)_{\Lambda\text{-tors}}$, $\mathbf{c}_{\mathbb{Q},\infty} \notin H_\infty^1(\mathbb{Q}, T)_{\Lambda\text{-tors}}$. Therefore, by Theorem 3.16, X_∞ is a finitely generated Λ-torsion module, and by Proposition 3.19, $\mathrm{Hom}\left(\mathcal{S}\left(\mathbb{Q}_\infty, W^*\right), \mathbb{Q}_p/\mathbb{Z}_p\right)$ is a finitely generated Λ-torsion module such that $\mathrm{char}\left(\mathrm{Hom}\left(\mathcal{S}\left(\mathbb{Q}_\infty, W^*\right), \mathbb{Q}_p/\mathbb{Z}_p\right)\right)$ is equal to $\mathrm{char}\left(X_\infty\right)\mathrm{char}\left(H_{\infty,s}^1\left(\mathbb{Q}_p, T\right)/\mathrm{loc}_{\Sigma_p}\left(H_\infty^1(\mathbb{Q}, T)\right)\right)$.

(ii) By our assumptions, $\mathrm{loc}^s_{\Sigma_p}\left(H^1_\infty(\mathbb{Q},T)\right)$ is a Λ-module of rank one. Then, there is a pseudo-isomorphism $\psi : \mathrm{loc}^s_{\Sigma_p}\left(H^1_\infty(\mathbb{Q},T)\right) \to \Lambda$. We have that

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

The claim then follows from the definition of $\mathrm{ind}_\Lambda(\mathbf{c})$ and by the divisibilities of Theorems 3.17 and 3.18 .

□

3.4 Twisting by characters of finite order

In this section we consider a number field K, T a p-adic representation of G_K and $\mathbf{c}$ is an Euler system for $(T,\mathcal{K},\mathcal{N})$. The results discussed in the previous sections do not depend on $\mathcal{K}$, since we can just take $\mathcal{K}=\mathcal{K}_{\min}$ because it has to contain K_∞. If $\mathcal{K}$ is not the minimal field, it contains more information.

If $\chi : G_K \to \mathcal{O}^\times$ is a character of finite order, then we can denote by $\mathcal{O}_\chi$ a free $\mathcal{O}$-module of rank 1 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 3.21. If $\mathbf{c}$ is an Euler system for $(T,\mathcal{K},\mathcal{N})$, let us consider $\chi : \mathrm{Gal}(\mathcal{K}/K)\to\mathcal{O}^\times$ a character of finite order and consider $L=\mathcal{K}^{\ker(\chi)}$, the field cut out by χ. For $K\subseteq_f F\subseteq\mathcal{K}$ we define $\mathbf{c}^\chi_F\in H^1(F,T\otimes\chi)$ 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 we get the isomorphism since G_{FL} is in the kernel of χ.

Proposition 3.22. Assume that $\mathbf{c}$ is an Euler system for $(T,\mathcal{K},\mathcal{N})$ and $\chi : \mathrm{Gal}(\mathcal{K}/K)\to\mathcal{O}^\times$ is a character of finite order. If $\mathfrak{f}$ is the conductor of χ, i.e. the conductor of the field cut out by χ, then the collection $\left\{\mathbf{c}^\chi_F \mid K\subseteq fF\subseteq\mathcal{K}\right\}$ 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

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

where $P\left(\operatorname{Frob}_{\mathfrak{q}}^{-1} \mid (T \otimes \chi)^*; x\right) = \det\left(1 - \operatorname{Frob}_{\mathfrak{q}}^{-1} x \mid (T \otimes \chi)^*\right)$, and

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

□

Lemma 3.23. 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

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

is

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

Proof. Since the conductors are equal, every prime which ramifies in L'/K ramifies also in L/K, then $\operatorname{cor}_{FL'/FL} \mathbf{c}_{FL'} = \mathbf{c}_{FL}$. We get that

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

□

Chapter 4

Iwasawa Main conjecture

4.1 Cyclotomic Euler system

The aim of this section is to see how to obtain our main result using the cyclotomic Euler system.

Let $K = \mathbb{Q}$ and let $\mathbb{Z}_p(1)$ be the cyclotomic representation induced by the cyclotomic character $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^{\times}$. We obtain the previous map taking the projections $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q})$ which induce the inverse systems of maps $G_{\mathbb{Q}} \to (\mathbb{Z}/p^n\mathbb{Z})^{\times}$. Now, since every prime different from p is unramified outside p in every $\mathbb{Q}(\mu_{p^n})/\mathbb{Q}$, it follows that the cyclotomic character is unramified outside p.

We will then require an Euler system for $T = \mathbb{Z}_p(1)$. We consider as $\mathcal{K}$ the field $\mathbb{Q}^{\mathrm{ab}}$ since it contains every abelian extension of $\mathbb{Q}$ and in particular the cyclotomic extension $\mathbb{Q}_\infty$ and all the maximal p-extensions contained in the ray class fields modulo finite primes different from p; the ideal $\mathcal{N}$ is the ideal generated by p, and we simply denote it by p. Hence, our aim is to construct an Euler system for $(\mathbb{Z}_p(1), \mathbb{Q}^{\mathrm{ab}}, p)$. If m is an integer and we denote by ∞ the unique real embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$, we have two kind of modulus for $\mathbb{Q}$, i.e. $\mathfrak{m} = m$ and $\mathfrak{m} = m\infty$. The ray class field modulo m is $\mathbb{Q}(\mu_m)^+$ and the ray class field modulo $m\infty$ is $\mathbb{Q}(\mu_m)$. Since they are both contained in $\mathbb{Q}^{\mathrm{ab}}$, by Remark 3.3 an Euler system for $(\mathbb{Z}_p(1), \mathbb{Q}^{\mathrm{ab}}, p)$ is a collection $\{\tilde{\mathbf{c}}_{m\infty}, \tilde{\mathbf{c}}_m\}$ which satisfies the compatibility conditions for

$$\tilde{\mathbf{c}}_{m\infty} \in H^1(\mathbb{Q}(\mu_m), \mathbb{Z}_p(1)) \quad \text{and} \quad \tilde{\mathbf{c}}_m \in H^1(\mathbb{Q}(\mu_m)^+, \mathbb{Z}_p(1)).$$

We know that the compatibility conditions to be satisfied are related to corestriction maps and to the Euler factor

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

for a rational prime $l \neq p$. Since $\mathrm{Hom}(\mathbb{Z}_p(1), \mathbb{Z}_p(1)) = \mathbb{Z}_p$ with trivial Galois action, we have $P(\mathrm{Frob}_l^{-1} \mid \mathbb{Z}_p(1)^*; x) = 1 - x$.

We also know that, for a number field F,

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

the p-adic completion of $F^\times$. In particular, we can use the natural injection $F^\times \hookrightarrow H^1(F, \mathbb{Z}_p(1))$ to define our cohomology classes. Let us fix a collection $\{\zeta_m \mid m \geq 1\}$ such that ζ_m is a primitive m-th root of unity and $\zeta_{mn}^n = \zeta_m$, for every m and n. If L/F is a finite Galois extension and we denote by $N_{L/K}$ the field norm, for any $\alpha \in L$ we have

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

Therefore, the collection $\{\zeta_m \mid m \geq 1\}$ is such that

$$N_{\mathbb{Q}(\mu_{ml})/\mathbb{Q}(\mu_m)}(1-\zeta_{ml}) = \begin{cases} 1-\zeta_m & \text{if } l \mid m \\ (1-\mathrm{Frob}_l^{-1})(1-\zeta_m) & \text{if } l \nmid m \text{ and } m \geq 1 \\ l & \text{if } m = 1 \end{cases}, \tag{4.1}$$

with l a prime and Frob_l the Frobenius of l in $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$. Then, for $m \geq 1$ we define

$$\tilde{\mathbf{c}}_{m\infty} = N_{\mathbb{Q}(\mu_{mp})/\mathbb{Q}(\mu_m)}(1-\zeta_{mp}) \in \mathbb{Q}(\mu_m)^\times \subseteq H^1(\mathbb{Q}(\mu_m), \mathbb{Z}_p(1)),$$

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

In order to check that $\{\tilde{\mathbf{c}}_{m\infty}, \tilde{\mathbf{c}}_m\}$ is an Euler system, we need to show the compatibility conditions. In particular, since these elements are defined at cohomological level zero, it suffices to work with corestriction at level zero. By (4.1) we have that these elements satisfy the required congruence since, for every prime $l \neq p$,

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

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

To reach our aim of proving the Main conjecture, we will use a collection of cohomology elements associated to Euler systems.

Let us fix an integer $n > 0$ and let $F = \mathbb{Q}(\mu_{p^{n+1}})^+$. Let $\mathscr{S}$ be the set of positive squarefree integers divisible only by primes l which split completely in $F/\mathbb{Q}$, i.e. $l \equiv \pm 1 (\mathrm{mod}\ p^{n+1})$. For every $r \in \mathscr{S}$, we write $G_r = \mathrm{Gal}(F(\mu_r)/F) \cong \mathrm{Gal}(\mathbb{Q}(\mu_r)/\mathbb{Q})$. Let

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

denote the norm operator. Since there is a natural isomorphism on all prime divisors of r, $G_r \cong \prod_{l|r} G_l$, we have $N_r = \prod_{l|r} N_l \in \mathbb{Z}[G_r]$. If l

is a prime not dividing r in $\mathscr{S}$, we can identify $G_l = \mathrm{Gal}(F(\mu_l)/F)$ with $\mathrm{Gal}(F(\mu_{rl})/F(\mu_r))$, where Frob_l is the Frobenius of l in G_r, i.e. the map $\mu_r \mapsto \mu_r^l$. For every prime $l \in \mathscr{S}$, the group G_l is cyclic of order $l-1$, hence we can fix a generator σ_l of G_l.

Definition 4.1. For every prime $l \in \mathscr{S}$, define

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

Then, if $r \in \mathscr{S}$, we can define the *r-th derivative element*

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

Lemma 4.2. In the above notation, for every $l \in \mathscr{S}$ we have

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

Proof. We write

$$\begin{aligned}\sigma_l D_l &= \sum_{i=1}^{l-2} i\sigma_l^{i+1} = \sum_{i=1}^{l-1}(i-1)\sigma_l^i \\ &= \sum_{i=1}^{l-1} i\sigma_l^i - \sum_{i=1}^{l-1}\sigma_l^i \\ &= (D_l + l - 1) - N_l.\end{aligned}$$

□

If we fix an odd integer M to be a large power of some prime p, we set

$$\mathscr{S}_M = \{r \in \mathscr{S} \mid r \text{ is divisible only by primes } l \equiv 1 (\mathrm{mod}\ M)\}.$$

For $r \in \mathscr{S}_M$, we will use the elements of $F(\mu_r)$ as the elements of the Euler system and we denote them by

$$\alpha_r = N_{\mathbb{Q}(\mu_{p^{n+1}r})/F(\mu_r)}(1 - \zeta_{p^{n+1}r}) = (1 - \zeta_{p^{n+1}r}\zeta_r)(1 - \zeta_{p^{n+1}}^{-1}\zeta_r) \in F(\mu_r)^\times.$$

These elements are such that $N_l(\alpha_{rl}) = (\mathrm{Frob}_l - 1)\alpha_r$ for $l \nmid r$, $l \in \mathscr{S}$, and they are such that $\alpha_{rl} \equiv \alpha_r (\mathrm{mod}\ \mathscr{L})$, for every $\mathscr{L}$ of $F(\mu_r)$ above l. Indeed, $\zeta_l \equiv 1 (\mathrm{mod}\ \mathscr{L})$ holds since the residue field mod $\mathscr{L}$ has characteristic l.

Lemma 4.3. If $r \in \mathscr{S}_M$, then the class of $D_r\alpha_r$ is in $[F(\mu_r)^\times/(F(\mu_r)^\times)^M]^{G_r}$.

Proof. We proceed by induction on the number of prime divisors of r. If $r = 1$, then $G_r = 1$ and the claim is clear. If $r = ls$ for $l, s \in \mathscr{S}_M$, l prime, then

$$\begin{aligned}(\sigma_l - 1)D_r\alpha_r &= (l - 1 - N_l)D_s\alpha_r = (l - 1 - N_l)D_s\alpha_r \\ &= (l-1)D_s\alpha_r + (1 - \mathrm{Frob}_l)D_s\alpha_s \\ &\equiv (1 - \mathrm{Frob}_l)D_s\alpha_s (\mathrm{mod}\ (F(\mu_r)^\times)^{l-1}).\end{aligned}$$

By induction hypotesis $(1-\mathrm{Frob}_l)D_s\alpha_s \in (F(\mu_s)^\times)^M$. Since $l \equiv 1(\mathrm{mod}\ M)$ and G_r is generated by all the σ_l, we obtain our assertion. □

Since M is odd and coprime with r, and F is a real field, $\mu_M \cap F = \{1\}$ and $\mu_M \cap F(\mu_r) = \{1\}$. This implies that G_r acts trivially on μ_M. We apply the Hochschild-Serre exact sequence of Proposition 2.7 to $G = G_{F(\mu_r)}$ and $H = G_F$, and we get that

$$[F(\mu_r)^\times/(F(\mu_r)^\times)^M]^{G_r} \cong H^1(F(\mu_r), \mu_M)^{G_r} \cong H^1(F, \mu_M) \cong F^\times/(F^\times)^M.$$

Definition 4.4. In the above notation, there exists a unique element κ_r in $F^\times/(F^\times)^M$ corresponding to the element $D_r\alpha_r$, called *Kolyvagin derivative* of α_r. If $\tilde{\kappa}_r$ denotes a lift of κ_r in $F^\times$, there exists an element $\beta_r \in F(\mu_r)^\times$ such that $D_r\alpha_r = \tilde{\kappa}_r\beta_r^M$. This element is such that, for every $\sigma \in G_r$

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

We denote by I_F the group of fractional ideals of F: it is the free abelain group generated by the finite primes λ of $\mathcal{O}_F$. Hence, using the additive notation, we can write $I_F = \bigoplus_\lambda \mathbb{Z}\lambda = \bigoplus_l I_l$, where $I_l = \bigoplus_{\lambda|l} \mathbb{Z}\lambda$ for every rational prime l.

Definition 4.5. If $y \in F^\times$, we denote by (y) the principal ideal generated by y and we write

$$(y)_l \in I_l, \qquad [y] \in I_F/MI_F, \qquad [y]_l \in I_l/MI_l$$

for the projections of y to I_l, I_F/MI_F, I_l/MI_l, respectively.

Recall that a map is *G-equivariant* if it is a homomorphism of G-modules.

Lemma 4.6. If l splits completely in F and $l \equiv 1(\mathrm{mod}\ M)$, then there exists a unique G-equivariant surjection $\varphi_l : (\mathcal{O}_F/l\mathcal{O}_F)^\times \to I_l/MI_l$ such that the following diagram is commutative

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

Proof. Since l splits completely in F, every prime λ of F above l is totally ramified in $F(\mu_l)$. In particular, we can identify $\mathcal{O}_{F(\mu_l)}/\lambda'$ with $\mathcal{O}_F/\lambda$, where λ' is the prime above λ. Hence we get

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

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

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

If x is in this kernel, then M divides $v_\lambda(x)$ for every $\lambda \mid l$ prime of F. Therefore x is also in the kernel of the right-hand map. This implies the commutativity of the diagram. □

For a prime l as in Lemma 4.6, we denote by φ_l the induced homomorphism

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

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

Proposition 4.7 (Kolyvagin)**.** If $r \in \mathscr{S}_M$ and l is a rational prime, then

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

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

Proof. If $\lambda' \mid l$ is a prime of $F(\mu_r)$, then $v_{\lambda'}(\beta_r) = 0$ since no primes over l ramifies in $F(\mu_r)/F$. Hence, for $l \nmid r$ prime, $\tilde{\kappa}_r$ can be chosen such that β_r is a unit at all primes above l.

(i) If $l \nmid r$, then β_r is a unit at all primes above l. This holds true also for $\tilde{\kappa}_r$ since $D_r\alpha_r$ is a unit; hence we obtain our claim.

(ii) If $r = ls$, we can find $\beta_r \in F(\mu_r)^\times$ and $\beta_s \in F(\mu_s)^\times$ such that

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

with β_s a unit at all primes above l. Since $\tilde{\kappa}_r\beta_r^M = D_r\alpha_r$, the valuation of β_r^M at every prime of $F(\mu_r)$ above l has to be a multiple of $l-1$.

Moreover, since these primes are unramified in $F(\mu_r)/F(\mu_l)$, there exists $\gamma \in F(\mu_l)^\times$ such that $\beta_r\gamma^{(l-1)/M}$ has trivial valuation, i.e. it is a unit at all primes above l. Now, $N_l(\gamma)$ and γ^{l-1} have the same valuation and hence $[N_l\gamma]_l = [\kappa_r]_l$. Hence, modulo any prime of $F(\mu_r)$ above l, we get

$$\begin{aligned}(1-\sigma_l)\gamma^{(l-1)/M} &\equiv (\sigma_l - 1)\beta_r = [((l-1) - N_l)D_s\alpha_r]^{1/M} \\ &= \frac{D_s\alpha_r^{(l-1)/M}}{[(\mathrm{Frob}_l - 1)D_s\alpha_s]^{1/M}} \equiv \frac{D_s\alpha_s^{(l-1)/M}}{(\mathrm{Frob}_l - 1)\beta_s} \\ &= \left(\frac{D_s\alpha_s}{\beta_s^M}\right)^{(l-1)/M} = \tilde{\kappa}_r^{(l-1)/M}.\end{aligned}$$

Applying the diagram of Lemma 4.6 with $\gamma \in F(\mu_l)^\times$, we have

$$[\kappa_r]_l = \varphi_l(\kappa_s).$$

□

We see now an application of the Chebotarev density theorem, a result which describes statistically the splitting of primes in a number field K. In particular, our aim is to deduce the existence of primes using a consequence of this theorem.

We fix a rational prime $p > 2$ and we denote by C the p-part of the ideal class group C_F of F.

Theorem 4.8. If $\mathfrak{c} \in C$, let $M \in \mathbb{Z}$ be a power of p and let W be a finite G-submodule of $F^\times/(F^\times)^M$. Let $\psi : W \to (\mathbb{Z}/M\mathbb{Z})[G]$ be a Galois-equivariant map. Then there are infinitely many primes λ of F such that

(i) $\lambda \in \mathfrak{c}$.

(ii) The rational prime l below λ splits completely in $F/\mathbb{Q}$, and

$$l \equiv 1 (\mathrm{mod} M).$$

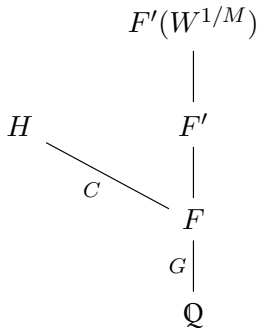
(iii) $[w]_l = 0$ for all $w \in W$, and there is a $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that

$$\varphi_l(w) = u\psi(w)\lambda$$

for all $w \in W$.

Proof. Let H be the maximal abelian unramified p-extension of F. Then by the correspondence of class field theory, we can identify C with $\mathrm{Gal}(H/F)$

and we write $F' = F(\mu_M)$. Hence, we have



Claim 1. $F' \cap H = F$. Since M is a power of p, the inertia group of p in $\mathrm{Gal}(F'/F)$ has index either 1 or 2, then there is no nontrivial unramified p-extension of F in F'.
Claim 2. $F'\left(W^{1/M}\right) \cap H = F$. Kummer theory (see Section 1.4) provides the existence of nondegenerate $\mathrm{Gal}(F'/\mathbb{Q})$-equivariant pairing

$$\mathrm{Gal}\left(F'\left(W^{1/M}\right)/F'\right) \times W/W' \to \mu_M,$$

where W' is the kernel of the map from $W \to (F')^{\times}/[(F')^{\times}]^M$. If τ is the complex conjugation in $\mathrm{Gal}(F'/F)$, then τ acts trivially on W and by -1 on μ_M, and hence also on $\mathrm{Gal}\left(F'\left(W^{1/M}\right)/F'\right)$. Since 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, τ acts trivially on $\mathrm{Gal}(H/F) \cong \mathrm{Gal}(HF'/F')$. Therefore τ acts on $\mathrm{Gal}\left(F'\left(W^{1/M}\right) \cap HF'/F'\right)$ by both 1 and -1 , so

$$F'\left(W^{1/M}\right) \cap HF = F,$$

and also $F'\left(W^{1/M}\right) \cap H = F$ by $F' \cap H = F$. M is odd, hence we obtain Claim 1 and Claim 2.
Claim 3. $F^{\times}/(F^{\times})^M \to (F')^{\times}/[(F')^{\times}]^M$ is injective, then $W' = 0$. By the inflation-restriction sequence of Galois cohomology,

$$\begin{aligned}\ker(F^{\times}/(F^{\times})^M) &= \ker(H^1(\bar{F}/F, \mu_M) \to H^1(\bar{F}/F, \mu_M) \to H^1(\bar{F}'/F', \mu_M)) \\ &= H^1(F(\mu_M)/F, \mu_M).\end{aligned}$$

Since $\mathrm{Gal}(F'/F)$ is cyclic we have

$$\#(H^1(F(\mu_M)/F, \mu_M)) = \#(H^0(F(\mu_M)/F, \mu_M)) = \#(\mu_M(F)) = 1.$$

Combining Claim 3 with the Kummer pairing decribed above, we get

$$\mathrm{Gal}\left(F'\left(W^{1/M}\right)/F'\right) \cong \mathrm{Hom}(W, \boldsymbol{\mu}_M).$$

Claim 4 Construction of λ. Fix a primitive M-th root of unity μ_M and define $\iota : (\mathbb{Z}/M\mathbb{Z})[G] \to \mu_M$ by $\iota(1_G) = \zeta_M$ and $\iota(g) = 1$ for all $g \neq 1_G$ in G. Let us denote by γ the element of $\mathrm{Gal}\left(F'\left(W^{1/M}\right)/F'\right)$ corresponding to $\iota \circ \psi \in \mathrm{Hom}(W, \mu_M)$ via the Kummer pairing. Hence, γ satisfies

$$\iota \circ \psi(w) = \gamma\left(w^{1/M}\right) w^{1/M}$$

for all $w \in W$. Since $F'\left(W^{1/M}\right) \cap H = F$, we can choose an element $\delta \in \mathrm{Gal}\left(HF'\left(W^{1/M}\right)/F\right)$ such that δ restricts to γ on $F'\left(W^{1/M}\right)$ and to $\mathfrak{c} \in C = \mathrm{Gal}(H/F)$ on H. Since W is finite, by Chebotarev theorem, there exist infinitely many primes λ such that λ has inertia degree 1 and it is unramified over $\mathbb{Q}$; it is unramified in $HF'\left(W^{1/M}\right)$, and its Frobenius in $\mathrm{Gal}\left(HF'\left(W^{1/M}\right)/F'\right)$ is the conjugacy class of G. If we fix one of those primes and let l be the rational prime below it. We check the required properties.

(i) The identification $C = \mathrm{Gal}(H/F)$ sends the class of λ to the Frobenius of λ, then $\lambda \in \mathfrak{c}$.

(ii) Since the degree of λ is 1 and it is unramified, l splits completely in F. The Frobenius of l in $\mathbb{Q}(\mu_M)$ is the restriction of the Frobenius of $HF'\left(W^{1/M}\right)$, which is the class of δ. But δ is trivial on F', so it is trivial on $\mathbb{Q}(\mu_M)$. Thus, l splits completely also in $\mathbb{Q}(\mu_M)/\mathbb{Q}$.

(iii) Since λ is unramified in $F'\left(W^{1/M}\right)/F$, then $[w]_l = 0$ for all $w \in W$. By definition, $v_\lambda(\varphi_l(w)) = 0$ if and only if w is an M-th power modulo λ. Moreover, $v_\lambda(\psi(w)\lambda) = 0$ if and only if $\iota \circ \psi(w) = 1$, i.e. $\gamma(w^{1/M})/w^{1/M} = 1$, which is true if and only if w is an M-th power modulo λ. Then there exists a unit $u \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that $v_\lambda(\varphi_l(w)) = u v_\lambda(\psi(w)\lambda)$ for all $w \in W$. Therefore, the map $w \mapsto \varphi_l(w) - u\psi(w)\lambda$ is $\mathrm{Gal}(F/K)$-equivariant homomorphism into $\bigoplus_{\lambda' | l, \lambda' \neq \lambda} (\mathbb{Z}/M\mathbb{Z})\lambda'$ which has no nonzero $\mathrm{Gal}(F/K)$-stable submodules.

□

4.2 The ideal class group of $\mathbb{Q}(\mu_p)^+$

In this section we see Kolyvagin's analysis of the ideal class group of $\mathbb{Q}(\mu_p)^+$, applying the results we obtained in the previous sections.

Let C be the p-part of the ideal class group of $F = \mathbb{Q}(\mu_p)^+$. Let E be the group of global units of F and $\mathscr{E}$ the subgroup of cyclotomic units.

Definition 4.9. If χ is a character of $G = \mathrm{Gal}(\mathbb{Q}(\mu_p)^+/\mathbb{Q})$, we define the *$\chi$-idempotent* by

$$e(\chi) = \frac{2}{p-1} \sum_{\gamma \in G} \chi^{-1}(\gamma)\gamma.$$

If Y is a $\mathbb{Z}_p[G]$-module, we write $Y(\chi) = e(\chi)Y$. We are interested in $C(\chi)$ and $(E/\mathscr{E})(\chi)$, i.e. the χ-component of the p-Sylow subgroup of the finite group $E/\mathscr{E}$.

Theorem 4.10. For every character χ of G, $\#(C(\chi)) \mid \#[(E/\mathscr{E})(\chi)]$.

Proof. Let $\chi \neq 1$, or $C(\chi) = (E/\mathscr{E})(\chi) = 0$. Let $M = \#[(E/\mathscr{E})(\chi)]p$, and let $\mathfrak{c}_1, \ldots, \mathfrak{c}_k$ be a collection of ideal classes of $C(\chi)$. Our aim is to choose inductively $\lambda_1, \ldots, \lambda_k$ primes of F such that the class of λ_i is $\mathfrak{c}_i$ and the rational prime l_i below λ_i is such that $l_i \equiv 1 (\mathrm{mod}\ M)$.

Assume we have chosen $\lambda_1, \ldots, \lambda_{i-1}$, for $1 \geq i \geq k$, lying above the rational primes $l_1, \ldots, l_{i-1}$. Write $r_i = \prod_{j<i} l_j$, and let W be the subgroup of $F^\times/(F^\times)^M$ generated by $e(\chi)\kappa_{r_i}$. Let t_i be the largest divisor of M such that

$$e(\chi)\kappa_{r_i} \in (F^\times)^{t_i}/(F^\times)^M$$

and let $\psi : W \to (\mathbb{Z}/M\mathbb{Z})[G]$ be the map defined by $\psi(e(\chi)\kappa_{r_i}) = t_i e(\chi)$. We choose λ_i to be any prime of F satisfying Theorem 4.8, an l_i to be the rational prime below λ_i. Then, $l_i \equiv 1 (\mathrm{mod}\ M)$ and there exists $u_i \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that

$$\varphi_{l_i}(e(\chi)\kappa_{r_i}) = u_i t_i e(\chi)\lambda_i.$$

We denote by E' and $\mathscr{E}'$ the image of E and $\mathscr{E}$, respectively, in $F^\times/(F^\times)^M$. Then $E'(\chi)$ and $\mathscr{E}'(\chi)$ are cyclic and $(E/\mathscr{E})(\chi) = E'(\chi)/\mathscr{E}'(\chi)$. Now, since $\kappa_1 = (1-\zeta_p)(1-\zeta_p^{-1})$, $e(\chi)\kappa_1$ generates $\mathscr{E}'(\chi)$ and hence $t_1 = \#[(E/\mathscr{E})(\chi)]$. For any $i > 1$, the principal ideal $[e(\chi)\kappa_{r_i}] \in I/MI$ is such that

$$[e(\chi)\kappa_{r_{i+1}}] = \varphi_{l_i}(e(\chi)\kappa_{r_i}) + \sum_{j<i} [e(\chi)\kappa_{r_{i+1}}]_{l_j} = u_i t_i e(\chi)\lambda_i \qquad (4.2)$$

in $I/(MI, e(\chi)\lambda_1, \ldots, e(\chi)\lambda_{i-1}$. Since $e(\chi)\kappa_{r_{i+1}} \in (F^\times)^{t_{i+1}}$, we have that $t_{i+1} \mid t_i$. In particular, $t_{i+1} \mid t_1 = \#[(E/\mathscr{E})(\chi)]$. Hence, $(M/t_{i+1})C(\chi) = 0$ and we can divide (4.2) by t_{i+1} and project into $C(\chi)$ in order to obtain $(t_i/t_{i+1})\mathfrak{c}_i = 0$ in $C(\chi)/(\mathfrak{c}_1, \ldots, \mathfrak{c}_{i-1})$. Therefore

$$\#(C(\chi)) \Big| \prod_{i=1}^{k} (t_i/t_{i+1}) = t_1/t_{k+1} = \#[(E/\mathscr{E})(\chi)]/t_{k+1}.$$

□

Theorem 4.11 (Mazur–Wiles, Kolyvagin)**.** For every character χ of G

$$\#(C(\chi)) = \#[(E/\mathscr{E})(\chi)].$$

Proof. By the analytic class number formula (see Theorem 1.12)

$$\prod_{\chi} \#(C(\chi)) = \#(C) = \#[(E/\mathscr{E}) \otimes \mathbb{Z}_p] = \prod_{\chi} \#[(E/\mathscr{E})(\chi)].$$

Applying Theorem 4.10 we obtain the claim. □

4.3 The Main conjecture

Let p be a rational odd prime. For every $n \geq 0$, we let

$$K_n = \mathbb{Q}\left(\mu_{p^{n+1}}\right) \quad \text{and} \quad K_\infty = \bigcup K_n.$$

Let

$$\Delta = \mathrm{Gal}\left(K_0/\mathbb{Q}\right) \cong (\mathbb{Z}/p\mathbb{Z})^\times \quad \text{and} \quad \Gamma = \mathrm{Gal}\left(K_\infty/K_0\right) \cong \mathbb{Z}_p$$

such that

$$\mathrm{Gal}\left(K_\infty/\mathbb{Q}\right) = \Delta \times \Gamma.$$

Recall that the Iwasawa algebra is defined by

$$\Lambda = \Lambda(\Gamma) = \varprojlim \mathbb{Z}_p\left[\mathrm{Gal}\left(K_n/K_0\right)\right].$$

Let χ be a p-adic valued character of Δ, $\chi : \Delta \to \mathbb{Z}_p^\times$.
Now, recall from Section 1.3 that:

(i) $C_\infty(\chi)$ is a finitely generated torsion Λ-module.

(ii) If χ is even, then $E_\infty(\chi)/V_\infty(\chi)$ is a finitely generated torsion Λ-module.

(iii) If χ is even and nontrivial, then $X_\infty(\chi)$ and $U_\infty(\chi)/V_\infty(\chi)$ are finitely generated torsion Λ-module.

We state now one of the several equivalent formulations of Iwasawa's Main conjecture for cyclotomic fields.

Theorem 4.12 (The Main conjecture)**.** 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 result, we need to study the structure of C_n and $\bar{E}_n$ as $\mathbb{Z}_p\left[\mathrm{Gal}\left(K_n/\mathbb{Q}\right)\right]$-modules. For any fixed n, we know that C_∞ and E_∞ are well-behaved Λ-modules by Theorem 1.21. Our aim now is to relate C_n and $\bar{E}_n$ with C_∞ and E_∞.

For every fixed n, let Γ_n denote $\mathrm{Gal}\left(K_\infty/K_n\right)$. If γ^{p^n} is its generater, let $I_n = \left(\gamma^{p^n} - 1\right)\Lambda$ and write $\Lambda_n = \Lambda/I_n\Lambda \cong \mathbb{Z}_p\left[\mathrm{Gal}\left(K_n/K_0\right)\right]$. If Y is a Λ-module, then we define

$$Y_{\Gamma_n} = Y/I_nY = Y/\left(\gamma^{p^n} - 1\right)Y = Y \otimes \Lambda_n.$$

For a Λ-module Y, Y_{Γ_n} is the maximal quotient of Y on which Γ_n acts trivially. Our goal is to study the natural maps

$$X_\infty(\chi)_{\Gamma_n} \to X_n(\chi), \quad C_\infty(\chi)_{\Gamma_n} \to C_n(\chi), \quad U_\infty(\chi)_{\Gamma_n} \to U_n(\chi),$$
$$E_\infty(\chi)_{\Gamma_n} \to \bar{E}_n(\chi) \quad \text{and} \quad V_\infty(\chi)_{\Gamma_n} \to V_n(\chi).$$

Theorem 4.13 ([10], Theorem 6.1, Appendix, §6)**.** 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

$$X_\infty(\chi)_{\Gamma_n} \to X_n(\chi), \quad U_\infty(\chi)_{\Gamma_n} \to U_n(\chi) \quad \text{and} \quad V_\infty(\chi)_{\Gamma_n} \to V_n(\chi)$$

are isomorphisms.

Lemma 4.14. If $0 \to W \to Y \to Z \to 0$ 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}. Moreover, if Z is a finitely generated Λ-module and Z_{Γ_n} is finite, then Z^{Γ_n} is finite.

Proof. If we apply the snake lemma to

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W^{\Gamma_n} & \longrightarrow & Y^{\Gamma_n} & \longrightarrow & Z^{\Gamma_n} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & W & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle (\gamma^{p^n}-1)} & & \downarrow{\scriptstyle (\gamma^{p^n}-1)} & & \downarrow{\scriptstyle (\gamma^{p^n}-1)} & & \\
0 & \longrightarrow & W & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & W_{\Gamma_n} & \longrightarrow & Y_{\Gamma_n} & \longrightarrow & Z_{\Gamma_n} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

we obtain the first assertion. Assume now that Z is finitely generated and $Z_{\Gamma_n} = Z/(\gamma^{p^n} - 1)Z$ is finite. Therefore, Z is torsion because the term $(T+1)^{p^n} - 1$ in $\mathbb{Z}_p[[T]]$ corresponding to $\gamma^{p^n} - 1$ is zero, which implies that it is not a unit in Λ and that then $\Lambda/(\gamma^{p^n} - 1)\Lambda$ is infinite. The third column and the multiplicativity imply that $\mathrm{char}(Z^{\Gamma_n}) = \mathrm{char}(Z_{\Gamma_n}) = 1$, and then Z^{Γ_n} is finite. □

Theorem 4.15. If $\chi \neq 1$ is an even 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. Let us consider the following two commutative diagrams with exact rows:

$$\begin{array}{ccccccccc}
 & & (U_\infty(\chi)/E_\infty(\chi))_{\Gamma_n} & \xrightarrow{\phi_1} & X_\infty(\chi)_{\Gamma_n} & \longrightarrow & C_\infty(\chi)_{\Gamma_n} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_{U/E}} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & U_n(\chi)/\bar{E}_n(\chi) & \longrightarrow & X_n(\chi) & \longrightarrow & C_n(\chi) & \longrightarrow & 0,
\end{array}$$

$$\begin{array}{ccccccccc} & & E_\infty(\chi)_{\Gamma_n} & \xrightarrow{\phi_2} & U_\infty(\chi)_{\Gamma_n} & \longrightarrow & (U_\infty(\chi)/E_\infty(\chi))_{\Gamma_n} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi_E} & & \downarrow & & \downarrow{\scriptstyle \pi_{U/E}} & & \\ 0 & \longrightarrow & \bar{E}_n(\chi) & \longrightarrow & U_n(\chi) & \longrightarrow & U_n(\chi)/\bar{E}_n(\chi) & \longrightarrow & 0 \end{array}$$

Since the map $U_\infty(\chi)_{\Gamma_n} \to U_n(\chi)$ is an isomorphism by Theorem 4.13, if we apply the snake lemma to the second diagram we have that

$$\operatorname{coker}(\pi_E) \cong \ker(\pi_{U/E}).$$

The map $X_\infty(\chi)_{\Gamma_n} \to X_n(\chi)$ is injective, hence

$$\ker(\pi_{U/E}) = \ker(\phi_1).$$

Since $C_\infty(\chi)_{\Gamma_n} \cong C_n(\chi)$ is finite, by Lemma 4.14 $\ker(\phi_1)$ is a quotient of $C_\infty(\chi)_{\text{finite}}$, the maximal finite Λ-submodule of $C_\infty(\chi)$. Similarly, we get $\ker(\pi_e) = \ker(\phi_2)$. By Theorem 1.15 in Section 1.2, if $\chi \neq 1$, then $[U_n(\chi) : \bar{E}_n(\chi)]$ is finite and hence

$$\#((U_\infty(\chi)/E_\infty(\chi))_{\Gamma_n}) \leq [U_n(\chi) : \bar{E}_n(\chi)]\#(\ker(\pi_{U/E}))$$

is finite. By Lemma 4.14, $\ker(\phi_2)$ is a quotient of $(U_\infty(\chi)/E_\infty(\chi))_{\text{finite}}$. If we take $\mathscr{A}$ as the annihilator in Λ of $C_\infty(\chi) \oplus (U_\infty(\chi)/E_\infty(\chi))_{\text{finite}}$, it has finite index since it annihilates a finite Λ-module. □

Let $\chi \neq 1$ be an even character of Δ. Then fix a generator $h_\chi \in \Lambda$ of $\operatorname{char}(E_\infty(\chi)/V_\infty(\chi))$.

Corollary 4.16. If $\chi \neq 1$ is an even 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

$$\theta_{n,\eta} : \bar{E}_n(\chi) \to \Lambda_n$$

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 and

$$0 \neq E_\infty(\chi) \subseteq U_\infty(\chi).$$

Hence, $E_\infty(\chi)$ is torsion free of rank one. Therefore, there is an injective homomorphism $\theta : E_\infty \to \Lambda$ with finite cokernel. This maps induces a pseudo-isomorphism

$$E_\infty(\chi)/V_\infty(\chi) \sim \Lambda/\theta(V_\infty(\chi)).$$

Since also $V_\infty(\chi)$ is free of rank one, we have

$$\theta(V_\infty(\chi)) = \operatorname{char}(\Lambda/\theta(V_\infty(\chi))) = \operatorname{char}(E_\infty(\chi)/V_\infty(\chi)) = h_\chi \Lambda.$$

Let $\mathscr{A}$ be a finite index ideal of Λ satisfying Theorem 4.15. Let us fix an n and let θ_n be the homomorphism $E_\infty(\chi)_{\Gamma_n} \to \Lambda_n$ induced by θ, and π_n the projection map $E_\infty(\chi)_{\Gamma_n} \to \bar{E}_n(\chi)$. For every $\eta \in \mathscr{A}$, we define $\theta_{n,\eta} : \bar{E}_n(\chi) \to \Lambda_n$ to be the map such that the following diagram commute:

$$\begin{array}{ccc} E_\infty(\chi)_{\Gamma_n} & \xrightarrow{\theta_n} & \Lambda \\ {\scriptstyle \pi_n}\downarrow & & \downarrow{\scriptstyle \eta} \\ \bar{E}_n(\chi) & \xrightarrow{\theta_{n,\eta}} & \Lambda_n \end{array}$$

indeed, $\theta_{n,\eta}(u) = \theta_n\left(\pi_n^{-1}(\eta u)\right)$. It is well-defined since, by Theorem 4.15, η annihilates coker (π_n) and $\ker(\pi_n)$ is finite, and thus $\ker(\pi_n) \subseteq \ker(\theta_n)$. Since $V_n(\chi) = \pi_n(V_\infty(\chi))$, we get that

$$\theta_{n,\eta}(V_n(\chi)) = \eta\theta_n(V_\infty(\chi)) = \eta h_\chi \Lambda_n.$$

□

By the classification theorem, there is a pseudo-isomorphism

$$C_\infty(\chi) \sim \bigoplus_{i=1}^{k} \Lambda/f_i\Lambda,$$

with nonzero $f_i \in \Lambda$. Therefore

$$\operatorname{char}(C_\infty(\chi)) = f_\chi\Lambda, \quad \text{where } f_\chi = \prod_{i=1}^{k} f_i$$

Corollary 4.17. Let $f_1, \ldots, f_k$ be defined as above. There is an ideal $\mathscr{B}$ of finite index in Λ and for every n there are classes $\mathfrak{c}_1, \ldots, \mathfrak{c}_k \in C_n(\chi)$ such that the annihilator $\operatorname{Ann}(\mathfrak{c}_i) \subseteq \Lambda_n$ of $\mathfrak{c}_i$ in $C_n(\chi)/(\Lambda_n\mathfrak{c}_1 + \ldots + \Lambda_n\mathfrak{c}_{i-1})$ satisfies

$$\mathscr{B}\operatorname{Ann}(c_i) \subseteq f_i\Lambda_n.$$

Proof. The pseudo-isomorphism relation 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 4.13 and Lemma 4.14, if we tensor with $\Lambda_n = \Lambda/I_n\Lambda$ we have

$$Z^{\Gamma_n} \to \bigoplus_{i=1}^{k} \Lambda_n/f_i\Lambda_n \to C_n(\chi) \to Z_{\Gamma_n} \to 0.$$

If $\mathscr{B}$ is the annihilator of the finite module Z, choose $\mathfrak{c}_i$ 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 required property. □

Lemma 4.18. Let χ be an even character of Δ, and let

$$f_\chi\Lambda = \mathrm{char}\,(C_\infty(\chi)) \quad \text{and} \quad h_\chi\Lambda = \mathrm{char}\,(E_\infty(\chi)/V_\infty(\chi))$$

as above.

(i) For every n, $\Lambda_n/f_\chi\Lambda_n$ and $\Lambda_n/h_\chi\Lambda_n$ are finite.

(ii) There is a positive constant c such that for all n,

$$c^{-1} \leq \frac{|C_n(\chi)|}{|\Lambda_n/f_\chi\Lambda_n|} \leq c, \quad c^{-1} \leq \frac{\left|\bar{E}_n(\chi)/V_n(\chi)\right|}{|\Lambda_n/h_\chi\Lambda_n|} \leq c$$

(iii) 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 finite kernel and cokernel, bounded independently of n. Therefore $\Lambda_n/f_\chi\Lambda_n$ is finite for every n, and by Theorem 1.19, the quotient

$$\#(\Lambda_n/f_\chi\Lambda_n)/\#\left(\bigoplus_{i=1}^k \Lambda_n/f_i\Lambda_n\right)$$

is bounded above and below independently of n, proving the first part of (i) and (ii). Repeating the same argument with the maps

$$(E_\infty(\chi)/V_\infty(\chi))_{\Gamma_n} \to \Lambda_n/h_\chi\Lambda_n \quad \text{and} \quad (E_\infty(\chi)/V_\infty(\chi))_{\Gamma_n} \to \bar{E}_n(\chi)/V_n(\chi)$$

we obtain then (i) and (ii) for $\chi \neq 1$. If $\chi = 1$, then h_χ is a unit and the inequalities of (ii) holds with $\chi = 1$, $c = 1$ since $\bar{E}_n(\chi)/V_n(\chi)$ and $C_n(\chi)$ are trivial. □

4.4 Proof of the Main conjecture

We proceed now to prove our main result. We fix n and we let $C = C_n$, $E = E_n$ and $V = V_n$. Our aim is to apply the results of the previous sections to $F = K_n^+$. If χ is even, we can identify $C_n(\chi)$ with the χ-component of the p-part of the ideal class group of F (see Theorems 1.5 and 1.6 in Section 1.1.3). If l is a rational prime splitting completely in F, then $I_l \otimes \mathbb{Z}_p$ is a $\mathbb{Z}_p$-module, and we consider $I_l(\chi) = e(\chi)\,(I_l \otimes \mathbb{Z}_p)$. It is free of rank one over Λ_n, generated by the element $\lambda(\chi) = e(\chi)\lambda$, with λ a prime of F above l. We can define

$$\sigma_\lambda = \sigma_{\lambda,\chi} : F^\times \to \Lambda_n$$

by $\sigma_\lambda(w)\lambda(\chi) = e(\chi)(w)_l$. We denote by $\bar{\sigma}_\lambda$ the corresponding map

$$\bar{\sigma}_\lambda : F^\times / \left(F^\times\right)^M \to \Lambda_n / M\Lambda_n$$

such that $\bar{\sigma}_\lambda(w)\lambda(\chi) = e(\chi)[w]_l$.

Recall that for $r \in \mathscr{S}_M$, we can choose an element $\kappa_r \in F^\times / \left(F^\times\right)^M$.

Lemma 4.19. If $r \in \mathscr{S}_M$, l is a prime dividing r and λ a prime of F above l, let B be the subgroup of the ideal subgroup C generated by the primes of F dividing r/l. Write $\mathfrak{c} \in C(\chi)$ for the class of $e(\chi)\lambda$ and W for the Λ_n-submodule of $F^\times / \left(F^\times\right)^M$ generated by $e(\chi)\kappa_r$. If $\eta, f \in \Lambda_n$ are such that the annihilator $\mathrm{Ann}(\mathfrak{c}) \subseteq \Lambda_n$ of $\mathfrak{c}$ in $C(\chi)/B(\chi)$ is such that $\eta \,\mathrm{Ann}(\mathfrak{c}) \subseteq f\Lambda_n$, $\Lambda_n / f\Lambda_n$ is finite and

$$M \geq \#(C(\chi))\#\left(\left(I_l(\chi)/MI_l(\chi)\right)/\Lambda_n \left[e(\chi)\kappa_r\right]_l\right),$$

then there is a Galois-equivariant map $\psi : W \to \Lambda_n / M\Lambda_n$ such that

$$f\psi\left(e(\chi)\kappa_r\right) = \eta\bar{\sigma}_\lambda\left(\kappa_r\right).$$

Proof. If β is 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 4.7, if $q \nmid r$, then $(\beta)_q \in MI_q$. Since M annihilates $C(\chi)$, we obtain that $\sigma_\lambda(\beta)\lambda(\chi)$ projects to 0 in $C(\chi)/B(\chi)$ and then $\eta\sigma_\lambda(\beta) \in f\Lambda_n$. We define $\delta = \eta\sigma_\lambda(\beta)/f$, where the division by f is uniquely defined since $\Lambda_n / f\Lambda_n$ is finite. Let $\psi : W \to \Lambda_n / M\Lambda_n$ be such that $\psi\left(\rho e(\chi)\kappa_r\right) = \rho\delta$, for all $\rho \in \mathbb{Z}\left[\mathrm{Gal}\left(K_n/K_0\right)\right]$. Hence ψ has the required property; we have to prove that it is well defined. If we assume that $\rho e(\chi)\kappa_r = 0$, we have that there exists $x \in F^\times$ such that $\rho\beta = x^M$. In particular, $\rho\left[e(\chi)\kappa_r\right]_l = 0$. If we denote by $h = \#(C(\chi))$, we have

$$(M/h)\left(I_l(\chi)/MI_l(\chi)\right) \subseteq \Lambda_n\left[e(\chi)\kappa_r\right]_l$$

by our hypotesis on M, and hence $\rho \in h\Lambda_n$. Then

$$\begin{aligned} e(\chi)(x) &= \sum_q e(\chi)(x)_q \\ &= M^{-1}e(\chi)(\rho\beta)_l + \sum_{q|(r/l)} e(\chi)(x)_q + \sum_{q|r} he(\chi)(\rho/h)\left(M^{-1}(\beta)_q\right) \\ &\equiv M^{-1}e(\chi)(\rho\beta)_l \left(\mod \bigoplus_{q|(r/l)} I_q(\chi), hI(\chi)\right) \end{aligned}$$

Since h annihilates $C(\chi)$, we get that $M^{-1}e(\chi)(\rho\beta)_l$ projects to 0 in $C(\chi)/B(\chi)$. Hence, $M^{-1}\sigma_\lambda(\rho\beta)\mathfrak{c} = 0$ in $C(\chi)/B(\chi)$ so $\rho\delta f = \eta\sigma_\lambda(\rho\beta) \in Mf\Lambda_n$ and $\psi\left(\rho e(\chi)\kappa_r\right) = \rho\delta \in M\Lambda_n$. This implies that 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 4.20. For every even character χ of Δ, $\mathrm{char}\,(C_\infty(\chi))$ divides $\mathrm{char}\,(E_\infty(\chi)/V_\infty(\chi))$.

Proof. If $\chi = 1$, both characteristic ideals are trivial by Lemma 4.18. Hence we can suppose $\chi \neq 1$. Take κ_1 represented by

$$\alpha = \alpha_1 = (\zeta_{p^n} - 1)\left(\zeta_{p^n}^{-1} - 1\right) \in F^\times$$

and notice that $\alpha(\chi) = \alpha^{e(\chi)}$ is a generator of $V_n(\chi)$. We pick $\mathfrak{c}_1, \ldots, \mathfrak{c}_k$ in $C(\chi)$ as in Corollary 4.17, and choose one more class $\mathfrak{c}_{k+1}$, which can be any element of $C(\chi)$, e.g. $\mathfrak{c}_{k+1} = 0$. Fix an ideal $\mathscr{C}$ of Λ with finite index, satisfying both Corollary 4.16 and 4.17. Let $\eta \in \mathscr{C}$ be such that $\Lambda_m/\eta\Lambda_m$ is finite for all m, i.e. η is prime to $\gamma^{p^m} - 1$, with γ generator of Γ. Let

$$\theta = \theta_{n,\eta} : \bar{E}(\chi) \to \Lambda_n$$

be the map given by Corollary 4.16 with this choice of η, and normalize it so that $\theta(\alpha(\chi)) = \eta_\chi$. If h denotes any integer such that

$$p^h \geq \#(\Lambda_n/\eta\Lambda_n) \quad \text{and} \quad p^h \geq \#(\Lambda_n/h_\chi\Lambda_n),$$

which is finite by Lemma 4.18, let $M = \#(C(\chi))p^{n+(k+1)h}$.
We want to use Theorem 4.8 to choose inductively $\lambda_i \in F$ primes lying above primes l_i of $\mathbb{Q}$ for $1 \leq i \leq k+1$ such that

$$\lambda_i \in c_i, \quad l_i \equiv 1 (\mathrm{mod}\, M) \tag{4.3}$$

$$\bar{\sigma}_{\lambda_1}(\kappa_{l_1}) = u_1\eta h_\chi, \quad f_{i-1}\bar{\sigma}_{\lambda_i}(\kappa_{r_i}) = u_i\eta\bar{\sigma}_{\lambda_{i-1}}\left(\kappa_{r_{i-1}}\right), \quad \text{for } 2 \leq i \leq k+1, \tag{4.4}$$

with $r_i = \prod_{j\leq i} l_j$ and $u_i \in (\mathbb{Z}/M\mathbb{Z})^\times$. Take $\mathfrak{c} = \mathfrak{c}_1, W = \left(E/E^M\right)(\chi)$ and

$$\psi : W \to \bar{E}(\chi) \to \bar{E}(\chi)^M \xrightarrow{\theta} \Lambda_n/M\Lambda_n \xrightarrow{e(\chi)} e(\chi)(\mathbb{Z}/M\mathbb{Z})[\mathrm{Gal}(F/\mathbb{Q})].$$

If λ_1 is a prime satisfying Theorem 4.8 with this data, and l_1 the rational prime below λ_1, then (4.3) holds. Moreover, by Theorem 4.8 and by Proposition 4.7, for some $u_1 \in (\mathbb{Z}/M\mathbb{Z})^\times$,

$$\begin{aligned}\bar{\sigma}_{\lambda_1}(\kappa_{l_1}) = e(\chi)\left[\kappa_{l_1}\right]_{l_1} &= e(\chi)\varphi_{l_1}(\kappa_1) = u_1\psi(\kappa_1)\lambda_1(\chi) \\ &= u_1\theta(\alpha(\chi))\lambda_1(\chi) = u_1\eta h_\chi\lambda_1(\chi).\end{aligned}$$

Since $\lambda_1(\chi)$ generates the free $\Lambda_n/M\Lambda_n$-module (I_{l_1}/MI_{l_1}), (4.4) holds for $i = 1$. Suppose now that $2 \leq i \leq k+1$ and we have chosen $\lambda_1, \ldots, \lambda_{i-1}$ satisfying the required properties (4.3) and (4.4). We want to define λ_i. Let

us consider $r_{i-1} = \prod_{j<i} l_j$. By (4.4), $\bar{\sigma}_{\lambda_{i-1}}\left(\kappa_{r_{i-1}}\right)$ divides $\eta^{i-1}h_\chi$, hence we have

$$\#[\left(I_{l_{1-1}}/MI_{l_{i-1}}\right)/\Lambda_n\left[\kappa_{r_{i-1}}\right]_{l_{i-1}}] \leq \#(\Lambda_n/\eta^{i-1}h_\chi\Lambda_n) \leq p^{ih}.$$

Let W_i denote the Λ_n-submodule of $F^\times/\left(F^\times\right)^M$ generated by $e(\chi)\kappa_{r_{i-1}}$. Applying Corollary 4.17, Lemma 4.18 and Lemma 4.19 with $r = r_{i-1}$ and $l = l_{i-1}$, we obtain a map $\psi_i : W_i \to \Lambda_n/M\Lambda_n$ such that

$$f_{i-1}\psi_i\left(e(\chi)\kappa_{r_{i-1}}\right) = \eta\bar{\sigma}_{\lambda_{i-1}}\left(\kappa_{r_{i-1}}\right).$$

Now, it is enough to choose λ_i satisfying Theorem 4.8 with $\mathfrak{c} = \mathfrak{c}_i$, $W = W_i$, $\psi = e(\chi)\psi_i$ and M as above, to obtain condition (4.3). Moreover, there is a $u_i \in (\mathbb{Z}/M\mathbb{Z})^\times$ such that

$$\begin{aligned} f_{i-1}\bar{\sigma}_{\lambda_i}\left(\kappa_{r_i}\right)\lambda_i(\chi) &= f_{i-1}e(\chi)\left[\kappa_{r_i}\right]_{l_i} \\ &= f_{i-1}\varphi_{l_i}\left(e(\chi)_{r_{i-1}}\right) \\ &= f_{i-1}u_i\psi_i(e(\chi)\kappa_{r_{i-1}})\lambda_i(\chi) \\ &= u_i\eta\bar{\sigma}_{\lambda_{i-1}}(\kappa_{r_{i-1}})\lambda_i(\chi). \end{aligned}$$

which proves (4.4) for i. If we proceed this induction for $k+1$ steps, then combining all the relations (4.4) we have

$$\eta^{k+1}h_\chi = u\left(\prod_{i=1}^{k} f_i\right)\bar{\sigma}_{\lambda_{k+1}}\left(\kappa_{r_{k+1}}\right) \quad \text{in } \Lambda_n/M\Lambda_n$$

for some $u \in (\mathbb{Z}/M\mathbb{Z})^\times$. Therefore, for every n, $f_\chi = \prod_{i=1}^{k} f_i$ divides $\eta^{k+1}h_\chi$ in $\Lambda_n/p^n\Lambda_n$, and then also in Λ. To conclude, we need to remove the factor η^{k+1}. Firstly, recall that $\mathscr{C}$ is an ideal of Λ of finite index and $\eta \in \mathscr{C}$ is such that for every n $\Lambda_n/\eta\Lambda_n$ is finite. Hence, we can choose η as a power of p, and say that f_χ does not divide p by Ferrero-Washington theorem ([10], Theorem 2.3, Chapter 10). If we avoid the use of this result, we can just say that it is possible to choose two different η which are relatively prime, and since Λ is a unique factorization domain, we have that f_χ divides h_χ, which concludes the proof. □

Let

$$f = \prod_{\chi \text{ even}} f_\chi \quad \text{and} \quad h = \prod_{\chi \text{ even}} h_\chi,$$

with $f_\chi = \text{char}\left(C_\infty(\chi)\right)$ and $h_\chi = \text{char}\left(E_\infty(\chi)/V_\infty(\chi)\right)$. We want to show that $f\Lambda = h\Lambda$. From this and Theorem 4.20, 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 4.21. If $g_1, g_2 \in \Lambda$, $g_1 \mid g_2$ and $\#((\Lambda/g_1\lambda)_{\Gamma_n}) \approx \#((\Lambda/g_2\lambda)_{\Gamma_n})$, then $g_1\Lambda = g_2\Lambda$.

Proof. It is an immediate consequence of Theorem 1.19. □

Now, we see the proof of our main result.

Proof of Theorem 4.12. By Theorem 1.19 and Lemma 4.18 we have

$$\#((\Lambda/f\Lambda)_{\Gamma_n}) \approx \prod_{\chi \text{ even}} \#((\Lambda/f_\chi\Lambda)_{\Gamma_n}) \approx \prod_{\chi \text{ even}} \#(C_n(\chi)),$$
$$\#((\Lambda/h\Lambda)_{\Gamma_n}) \approx \prod_{\chi \text{ even}} \#((\Lambda/h_\chi\Lambda)_{\Gamma_n}) \approx \prod_{\chi \text{ even}} \left[\bar{E}_n(\chi) : V_n(\chi)\right].$$

The analytic class number formula (Theorem 1.12) with Theorem 1.15 implies that

$$\#(C_n) = \left[\bar{E}_n : V_n\right].$$

Therefore

$$(\Lambda/f\lambda)_{\Gamma_n} \approx (\Lambda/h\lambda)_{\Gamma_n},$$

and since by Theorem 4.20 $f \mid h$, by Lemma 4.21 we obtain that $f\Lambda = h\Lambda$. By Theorem 4.20 we conclude that $f_\chi\Lambda = h_\chi\Lambda$ for all χ even, i.e.

$$\operatorname{char}\left(C_\infty(\chi)\right) = \operatorname{char}\left(E_\infty(\chi)/V_\infty(\chi)\right).$$

□

4.5 Other formulations and consequences

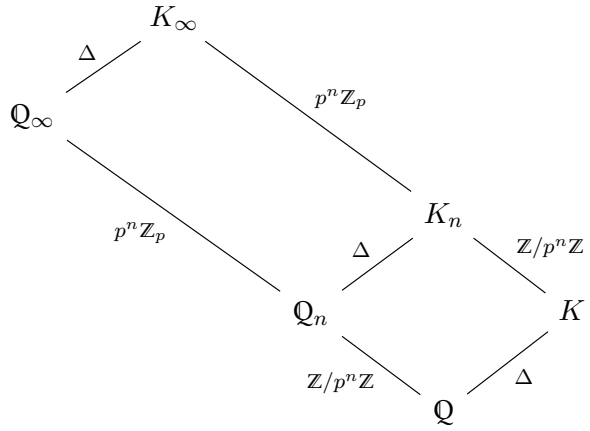
In this section we provide equivalent formulations of the Main conjecture and we deduce some relevant consequences.

Since we did not use the Selmer group and the results related to it seen in Section 3.3, we begin giving an overview about its role in this setting.

Let $\chi : \Delta \to \mathbb{Z}_p^\times$ be a non trivial even character which extends as character of $G_{\mathbb{Q}}$. If $T = (\mathbb{Z}_p)_\chi$ is the free $\mathbb{Z}_p$-module of rank 1 on which $G_{\mathbb{Q}}$ acts trivially by χ, then

$$T^* = \mathbb{Z}_p(1) \otimes \chi^{-1} = (\mathbb{Z}_p)_{\chi^{-1}\chi_p}, \quad W = (\mathbb{Q}_p/\mathbb{Z}_p)_\chi, \quad (W^*)^* = W.$$

In order to obtain an Euler system for $(T^*, \mathbb{Q}^{\text{ab}}, p)$, denoted by $\mathbf{c}^\chi$, we use the cyclotomic Euler system introduced before. This is the reason why we used the images of the Kolyvagin classes associated to the Euler system $\mathbf{c}$ under the idempotent $e(\chi)$ associated to χ. We have the following diagram



By Proposition 2.42 we have

$$\mathcal{S}(\mathbb{Q}, W) \cong \mathrm{Hom}(C(\chi), \mathbb{Q}_p/\mathbb{Z}_p), \quad \mathcal{S}(\mathbb{Q}_\infty, W) \cong \mathrm{Hom}(C_\infty(\chi), \mathbb{Q}_p/\mathbb{Z}_p).$$

This implies that $C_\infty(\chi) \cong \mathrm{Hom}(\mathcal{S}(\mathbb{Q}_\infty, W), \mathbb{Q}_p/\mathbb{Z}_p)$, i.e. $C_\infty(\chi)$ is the Pontryagin dual of $\mathcal{S}(\mathbb{Q}_\infty, W)$. Hence,

$$\mathrm{char}(C_\infty(\chi)) = \mathrm{char}(\mathrm{Hom}(\mathcal{S}(\mathbb{Q}_\infty, W), \mathbb{Q}_p/\mathbb{Z}_p))$$

and then one can deduce divisibilities for $\mathrm{char}(C_\infty(\chi))$ applying the results of Section 3.3.

Now we see other formulations of the Main conjecture, focusing in particular on the role of the p-adic L-function.

If χ is a complex Dirichlet character from $(\mathbb{Z}/p\mathbb{Z})^\times$, we can extend it to the whole $\mathbb{Z}$ and attach to it a complex L-function

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \mathrm{Re}(s) > 1.$$

We know that if $\chi \neq 1$, then $L(s, \chi)$ can be analytically continued to the complex plane; if $\chi = 1$, then $L(\chi, s)$ is a meromorphic continuation to the complex plane with a simple pole at $s = 1$. Moreover, the complex L-function admits the convergent Euler product

$$L(s, \chi) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}}, \quad \mathrm{Re}(s) > 1.$$

Definition 4.22. For a Dirichlet character χ of conductor p we can define the *generalized Bernolli numbers* by

$$\sum_{j=1}^{p} \frac{x(j)te^{jt}}{e^{pt} - 1} = \sum_{k=0}^{\infty} B_{k,\chi} \frac{t^k}{k!}.$$

These numbers are related to the L-functions as, for $m \geq 1$, we have

$$L(1-k,\chi) = -\frac{B_{k,\chi}}{k}.$$

We can generalize this construction.

Theorem 4.23 ([12], Theorem 5.11, Chapter 5)**.** Let χ be a Dirichlet character of conductor p. Then, there exists a p-adic meromorphic function $L_p(s,\chi)$, analytic if $\chi \neq 1$, defined on $\{s \in \mathbb{C}_p \mid |s| > p^{1-\frac{1}{p-1}}\}$, such that

$$L_p(1-k,\chi) = -(1-\chi\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k},$$

where ω denotes the Teichmüller character.

For χ non trivial and even character, we want now to study the relation between the p-adic L-function and the generator of $U_\infty(\chi)/V_\infty(\chi)$.

Theorem 4.24 ([12], Theorem 13.56, Chapter 13)**.** If χ is a non trivial even character of Δ, then

$$\mathrm{char}(U_\infty(\chi)/V_\infty(\chi)) = g_\chi\Lambda,$$

where g_χ, as element of $\mathbb{Z}_p[[T]]$ is such that $g_\chi((1+p)^s - 1) = L_p(1-s,\chi)$ for all $s \in \mathbb{Z}_p$.

Remark 4.25. For $k \geq 1$ we have

$$g_\chi((1+p)^k - 1) = L_p(1-k,\chi) = -(1-\chi\omega^{-k}(p)p^{k-1})\frac{B_{k,\chi\omega^{-k}}}{k}.$$

Theorem 4.26 (Main conjecture, second version)**.** For all non trivial even characters χ of Δ, we have $\mathrm{char}(X_\infty(\chi)) = g_\chi\Lambda$.

Proof. We know from class field theory that we have the exact sequence

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

By Theorem 4.12 and by multiplicativity of the characteristic ideal in exact sequences, we obtain

$$\mathrm{char}(X_\infty(\chi)) = \mathrm{char}(U_\infty(\chi)/V_\infty(\chi)) = g_\chi\Lambda.$$

□

If χ is even and non trivial we can consider $f_\chi \in \Lambda$, the element which corresponding power series is such that $f_\chi((1+p)^s - 1) = L_p(s,\chi)$ for every $s \in \mathbb{Z}_p$. We can then make the following change of variables

$$g_\chi(T) = f_\chi((1+p)(1+T)^{-1} - 1).$$

Using Kummer theory and Theorems 1.36 and 1.37 in Section 1.4.2, we obtain a non degenerate pairing $A_\infty(\chi^{-1}\omega) \times X_\infty(\chi) \to \mu_{P^\infty}$. Hence,

$$X_\infty(\chi) \cong \mathrm{Hom}(A_\infty(\chi^{-1}\omega), \mu_{p^\infty})$$

and then

$$X_\infty(\chi)^{-1} \cong \mathrm{Hom}(A_\infty(\chi^{-1}\omega), \mathbb{Q}_p/\mathbb{Z}_p),$$

where

$$X_\infty(\chi)^{-1} = X_\infty(\chi) \otimes \mathbb{Z}_p(-1) \quad \text{and} \quad \mathbb{Z}_p(-1) = \mathrm{Hom}(\mathbb{Z}_p(1), \mathbb{Z}_p) = (\mathbb{Z}_p)^{-1}_{\chi_p}.$$

Theorem 4.27 (Main conjecture, third version,[6])**.** For every non trivial even character χ of Δ, we have $\mathrm{char}(C_\infty(\chi^{-1})\omega) = f_\chi\Lambda$.

Finally, we study why the Main conjecture is useful in order to deduce results for the field $K = K_0$.

Proposition 4.28. For every odd character $\chi \neq \omega$ of Δ, we have

$$A_\infty(\chi)^{\Gamma_n} = C_n(\chi),$$

where $\Gamma_n = \mathrm{Gal}(K_n/K_0)$.

Proof. We use now some theorems seen in Chapter 1. Since $\chi \neq \omega$ is odd, by Theorem 1.4 we have that $\bar{E}_n(\chi) = \{1\}$. From Theorem 4.3, Chapter 6 in [10], the maps $C_n(\chi) \to C_m(\chi)$ are injective if $m \geq n$. Therefore, $C_n(\chi) \subseteq A_\infty(\chi)^{\Gamma_n}$. If γ_n is a generator of Γ_n, we have an exact sequence

$$0 \to C_m(\chi)^{\Gamma_n} \to C_m(\chi) \xrightarrow{\gamma-1} C_m(\chi) \to C_m(\chi)/(\gamma-1)C_m(\chi) \to 0.$$

From Theorem 1.26, we get that $C_m(\chi)/(\gamma-1)C_m(\chi) \cong C_n(\chi)$. Therefore, for $m \geq n$, $|C_m(\chi)^{\Gamma_n}| = |C_n(\chi)|$. Hence, we have our claim

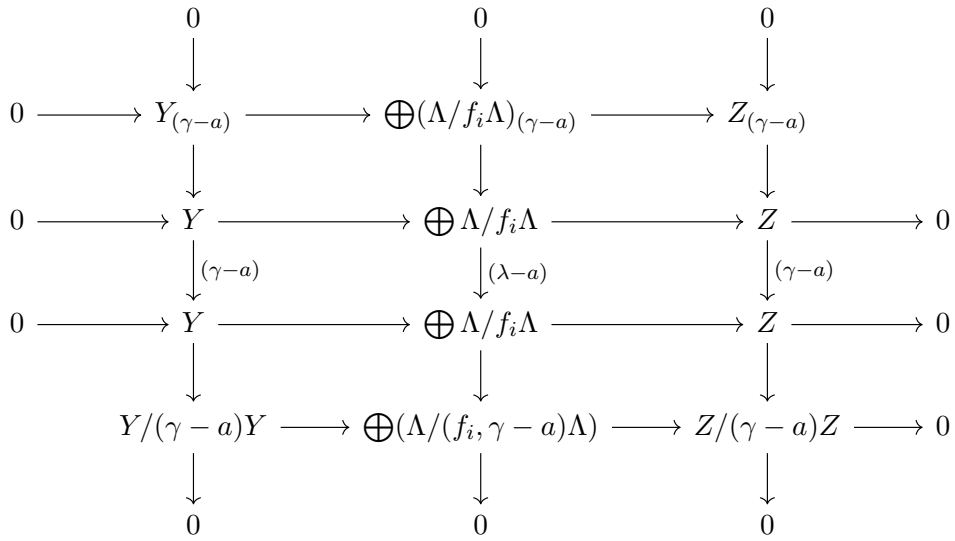
$$|A_\infty(\chi)^{\Gamma_n}| = |C_n(\chi)|.$$

□

Lemma 4.29. Let Y be a finitely generated torsion Λ-module with non zero finite Λ-submodule. Let $\gamma \in \Gamma$, $a \in 1 + p\mathbb{Z}_p$ and $Y/(\gamma - a)Y$ finite. Then

$$|Y/(\gamma - a)Y| = |\Lambda/(\mathrm{char}(Y)), (\gamma - a)\Lambda|.$$

Proof. Let $Y \to \bigoplus \Lambda/f_i\Lambda$ be a pseudo-isomorphism with finite cokernel Z. Then by assumption the kernel must be trivial. We get the exact diagram



where $Y_{(\gamma-a)}$ is the kernel of the map $(\gamma - a)$ of Y, and similarly for the other modules. We deduce then that each f_i is prime to $\gamma - a$ and $\bigoplus(\Lambda/f_i\Lambda)_{(\gamma-a)} = 0$. Moreover, we have $|Z_{(\gamma-a)}| = |Z/(\gamma - a)Z|$ since Z is finite. Applying the snake lemma we have $|Y/(\gamma-a)Y| = |\bigoplus \Lambda/(f_i, \gamma-a)\Lambda|$, and since every f_i is prime to $\gamma - a$, we obtain

$$|\bigoplus \Lambda/(f_i, \gamma - a)\Lambda\ | = |\ \Lambda/(\prod_i f_i, \gamma - a)\Lambda\ |\ .$$

□

The next result was proved by Iwasawa (see [3], Theorem 18)

Lemma 4.30. For every even character χ of Δ, $X_\infty(\chi)$ has no non zero finite Λ-submodules.

Proof. From the existence of the pairing $A_\infty(\chi^{-1}\omega) \times X_\infty(\chi) \to \mu_{p^\infty}$, it sufficies 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 of finite index p^k, then for N sufficiently large we have that $\mathrm{Gal}(K_\infty/K_N)$ acts trivially on $A_\infty(\chi^{-1}\omega)/A$. For $m \geq N$ the norm map $N_{K_{m+k}/K_m} : C_{m+k} \to C_m$ is surjective (see §4, Chapter 5), then $C_m(\chi^{-1}\omega) = N_{K_{m+k}/K_m} C_{m+k}(\chi^{-1}\omega) \subseteq A$ and $A_\infty(\chi^{-1}\omega) \subseteq A$. □

We conclude with the consequence we were searching.

Theorem 4.31 (Mazur-Wiles, Kolyvagin)**.** For every odd character $\chi \neq \omega$ of Δ $|C(\chi)| = p^{m(\chi)}$, with $m(\chi) = v_p(B_{1,\chi^{-1}})$.

Proof. Recall that a generator γ of Γ acts on μ_{p^∞} as $1+p$. By the Kummer pairing $A_\infty(\chi^{-1}\omega) \times X_\infty(\chi) \to \mu_{p^\infty}$ and by Proposition 4.28

$$\begin{aligned} C_0(\chi) &= \mathrm{Hom}(X_\infty(\chi^{-1}\omega), \mu_{p^\infty})^\Gamma \\ &= \mathrm{Hom}(X_\infty(\chi^{-1}\omega)/(\gamma - (1+p))X_\infty(\chi^{-1}\omega), \mu_{p^\infty}), \end{aligned}$$

with γ a generator of Γ. Applying the results seen in this Section, we obtain

$$\begin{aligned} |C_0(\chi)| &= |X_\infty(\chi^{-1}\omega)/(\gamma - (1+p))X_\infty(\chi^{-1}\omega)| \\ &= |\mathbb{Z}_p[[T]]/(g_{\chi^{-1}\omega}(T), 1 + T - (1+p))\mathbb{Z}_p[[T]]| \\ &= |\mathbb{Z}_p/(g_{\chi^{-1}\omega}((1+p)-1)\mathbb{Z}_p| \\ &= |\mathbb{Z}_p/B_{1,\chi^{-1}}\mathbb{Z}_p| \end{aligned}$$

□

Bibliography

[1] S. Bloch and K. Kato. "L-Functions and Tamagawa Numbers of Motives". In: 2007. URL: https://api.semanticscholar.org/CorpusID:118774981.

[2] M.J. Greenberg and J.P. Serre. Local Fields. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781475756739. URL: https://books.google.de/books?id=3LAJCAAAQBAJ.

[3] K. Iwasawa. "On Z l -Extensions of Algebraic Number Fields". In: Annals of Mathematics 98 (1973), p. 246. URL: https://api.semanticscholar.org/CorpusID:207356567.

[4] F. Lemmermeyer and H. Koch. Galois Theory of p-Extensions. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2013. ISBN: 9783662049679. URL: https://books.google.de/books?id=nqfvCAAAQBAJ.

[5] B. Mazur and K. Rubin. Kolyvagin systems. American Mathematical Society, 2004.

[6] B. Mazur and A. Wiles. "Class fields of abelian extensions of Q". In: Inventiones mathematicae 76 (1984), pp. 179–330. URL: https://api.semanticscholar.org/CorpusID:122576427.

[7] J. Neukirch, A. Schmidt, and K. Wingberg. Cohomology of Number Fields. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013. ISBN: 9783540378891. URL: https://books.google.de/books?id=ZX8CAQAAQBAJ.

[8] G. Oh. "A proof of the Iwasawa Main Conjecture for Q". In: 2018. URL: https://www.math.columbia.edu/~gyujinoh/Talk181018_Tex.pdf.

[9] K. Rubin. Euler Systems. Annals of Mathematics Studies. Princeton University Press, 2000. ISBN: 9780691050768. URL: https://books.google.de/books?id=Z1-YDwAAQBAJ.

[10] K. Rubin and S. Lang. Cyclotomic Fields I and II. Graduate Texts in Mathematics. Springer New York, 2012. ISBN: 9781461209874. URL: https://books.google.de/books?id=AFTmBwAAQBAJ.

[11] J. Tate. “Relations between K2 and Galois Cohomology.” In: Invent. Math. 36 (1976), pp. 257–274. URL: http://eudml.org/doc/142421.

[12] L.C. Washington. Introduction to Cyclotomic Fields. Graduate Texts in Mathematics. Springer New York, 1997. ISBN: 9780387947624. URL: https://books.google.de/books?id=qea_OXafBFoC.

[13] J.S. Wilson. Profinite Groups. London Mathematical Society monographs series: London Mathematical Society. Clarendon Press, 1998. ISBN: 9780198500827. URL: https://books.google.de/books?id=gcv9nQEACAAJ.