Università degli Studi di Padova

Dipartimento di Matematica“Tullio Levi-Civita”
Corso di Dottorato di Ricerca in Scienze Matematiche
Curricolo Matematica
Ciclo XXXV

Vanishing of the $\mathfrak{p}$-part of the Shafarevich-Tate group of a modular form and its consequences for Anticyclotomic Iwasawa Theory

Coordinatore
Chiar.mo Prof. Giovanni Colombo

Supervisore
Chiar.mo Prof. Matteo Longo

Dottorando
Luca Mastella

Abstract

In this thesis we prove a generalization, for the self-dual twist V of the representation attached to a modular forms f of even weight $k > 2$, of a recent result [MN19] of A. Matar and J. Nekovar in the anticyclotomic Iwasawa Theory for elliptic curves. More precisely we give a definition for the ($\mathfrak{p}$-part of the) Shafarevich-Tate groups $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K)$ and $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty)$ of f over an imaginary quadratic field K satisfying the *Heegner hypothesis* and over its *anticyclotomic* $\mathbb{Z}_p$*-extension* K_∞ and we show that if the *basic generalized Heegner cycle* $z_{f,K}$ is non-torsion and not divisible by p, then $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K) = \widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty) = 0$; moreover the Pontryagin dual of the Bloch-Kato Selmer group of the representation $A = V/T$, where T is the $G_\mathbb{Q}$-stable lattice inside V constructed by Nekovar in [Nek92], is free of rank 1 over the Iwasawa algebra.

Sommario

In questa tesi dimostriamo una generalizzazione, per il twist autoduale V della rappresentazione associata ad una forma modulare f di peso $k > 2$, di un recente risultato [MN19] di teoria di Iwasawa anticiclotomica per curve ellittiche di A. Matar and J. Nekovar. Più precisamente diamo una definizione della ($\mathfrak{p}$-parte dei) gruppi di Shafarevich-Tate $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K)$ e $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty)$ di f sopra un campo quadratico immaginario K che soddifi l'*ipotesi di Heegner* e sopra la sua $\mathbb{Z}_p$*-estensione anticiclotomica* K_∞ e mostriamo che se il *ciclo di Heegner generalizzato di base* $z_{f,K}$ non è di torsione e non è divisibile per p, allora $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K) = \widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty) = 0$; inoltre il duale di Pontryagin del gruppo di Selmer di Bloch-Kato della rappresentazione $A = V/T$, dove T è il reticolo $G_\mathbb{Q}$-stabile dentro V costruito da Nekovar in [Nek92], è libero di rango 1 sull'algebra di Iwasawa.

Contents

Introduction

In his seminal series of papers [KL89; Kol90; Kol91], Kolyvagin introduced a new method in order to bound the size of the Shafarevich-Tate group $\text{Ш}(E/K)$ of an elliptic curve $E/\mathbb{Q}$ over an imaginary quadratic field K of discriminant d_K, provided that all the prime factors of the conductor N of E split in K (assuming in other words the so called *Heegner hypothesis*) and that the basic Heegner point $y_K \in E(K)$ has infinite order. This method involves the construction of a so called (anticyclotomic) *Euler system* from the Heegner points $y_n \in E(K[n])$: fixed a rational prime number p, these are points of E defined for integers n such that $(n, pNd_K) = 1$, coming from CM points on $X_0(N)$ via a modular parametrization

$$\varphi\colon X_0(N) \to E,$$

that always exists thanks to Wiles Modularity theorem. Each y_n turns out to be rational over the ring class field $K[n]$ of conductor n and there is a sort of *norm compatibility* among them: if ℓ is a prime factor of n inert in K and we write $n = \ell \cdot m$, then

$$\mathrm{Tr}_{K[n]/K[m]}(y_n) = a_\ell y_m,$$

where $l + 1 - a_\ell$ is the number of $\mathbb{F}_\ell$-rational points of the reduction $\tilde{E}/\mathbb{F}_\ell$ of E at ℓ. For this reason in the following we will restrict our attention to squarefree integers n such that any prime $\ell \mid n$ is inert in K.

A special case of these results is the following theorem, that one can find in the expository article [Gro91] of Gross.

Theorem (Kolyvagin)**.** *Assume that the curve E does not have complex multiplication and let p be a prime number coprime with N and the discriminant of K (that is assumed to be $\neq -3, -4$ by simplicity) and such that*

$$\mathrm{Gal}\big(\mathbb{Q}(E[p])/\mathbb{Q}\big) \cong \mathrm{GL}_2(\mathbb{F}_p).$$

If $p \nmid y_K$ in $E(K)$, then

(a) the group $E(K)$ has rank 1,

(b) the p-primary subgroup $\text{Ш}(E/K)[p^\infty] = 0$.

In fact one proves that the p-primary part of the Selmer group $\mathrm{Sel}_{p^\infty}(E/K)$ is generated by the image δy_K via the Kummer map

$$\delta\colon E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/K) \subseteq \mathrm{H}^1(K, E[p^\infty])$$

of the basic Heegner point.

In a recent paper [MN19] Matar and Nekovar showed, using an abstract Iwasawa theoretical method, that the vanishing of the Shafarevich-Tate group extends over the anticyclotomic extension K_∞ of K, i.e. the unique $\mathbb{Z}_p$-extension of K that is pro-dihedral over $\mathbb{Q}$.

Theorem ([MN19, Th. 4.8]). *If $p \neq 2$ is a prime number such that*

(a) $E(K)[p] = 0$,

(b) $p \nmid N \cdot a_p \cdot (a_p - 1) \cdot \prod_{\ell | N} c_{\mathrm{Tam},\ell}(E/\mathbb{Q})$,

(c) y_K *is non-torsion,*

(d) $\mathrm{rk}_{\mathbb{Z}} E(K) = 1$ *and* $\text{Ш}(E/K)[p^\infty] = 0$,

then $\text{Ш}(E/K_\infty)[p^\infty] = 0$ *and the Pontryagin dual of* $E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{Sel}_{p^\infty}(E/K_\infty)$ *is a free module of rank* 1 *over the Iwasawa algebra* $\Lambda = \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty/K)]\!]$.

Combining it with the classical result of Kolyvagin one has the following corollary

Corollary ([MN19, Th. 6.9]). *Let* $p \neq 2$, *assume that* $E[p]$ *is an irreducible* $\mathbb{F}_p[G_{\mathbb{Q}}]$*-module and that*

$$p \nmid N \cdot a_p \cdot (a_p - 1) \cdot \prod_{\ell | N} c_{\mathrm{Tam},\ell}(E/\mathbb{Q}).$$

If y_K *is non torsion and* $y_K \notin pE(K)$, *then the group* $E(K)$ *has rank* 1 *and*

$$\text{Ш}(E/K)[p^\infty] = \text{Ш}(E/K_\infty)[p^\infty] = 0$$

and the Pontryagin dual of $E(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{Sel}_{p^\infty}(E/K_\infty)$ *is a free* Λ*-module of rank* 1.

The goal of this thesis is to generalize these results to modular forms of weight $k > 2$. Indeed several parts of the above picture already have a counterpart in the literature for modular forms.

The work of Kolyvagin in particular has been extended in huge generality: the notion of Selmer group and of Euler system can be given in general for p-adic representations following the axiomatizations of [Rub00] and [MR04]. Let K be a number field, if V is a p-adic representation of G_K (i.e. a finite dimensional vector space over a p-adic field $\mathcal{K}$ endowed with a continuous $\mathcal{K}$-linear action of G_K) and T is a G_K-stable lattice (finite free $\mathcal{O}$-module such that $V = T \otimes_{\mathcal{O}} \mathcal{K}$, where $\mathcal{O}$ is the ring of integers of $\mathcal{K}$), let $A = V/T = T \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O}$. A Selmer group for $X = T, V, A$ is a subset of the cohomology group $\mathrm{H}^1(K, X)$ whose cohomology class satisfy a bounch of *local conditions*; this means that the localization c_v of a class c at any place v of K lie in a chosen subgroup of $\mathrm{H}^1(K_v, X)$. In the case where $T = T_pE$ is the p-adic Tate module of an elliptic curve, there is a canonical choice of local conditions such that $\mathrm{Sel}_{p^\infty}(E/K)$ is a Selmer group for the representation A in this sense.

Deligne [Del71] attached to a cusp-newform $f \in S_k\big(\Gamma_0(N)\big)$ of even weight $k \geq 2$ a p-adic representation $W_{\mathfrak{p}}$ of $G_{\mathbb{Q}}$, that is a vector space over the completion $\mathcal{K} := F_{\mathfrak{p}}$ of the Hecke field F of f (i.e. the number field generated over $\mathbb{Q}$ by the Hecke eigenvalues a_n of f) at a prime $\mathfrak{p} \mid p$ of the ring of its integers O_F. We denote by $\mathcal{O}$ the ring of integers of $\mathcal{K}$. In [Nek92] Nekovar shows that under the condition that $p \nmid 2N\varphi(N)(k-2)!$, where $\varphi(N)$ denotes the Euler function, there is a $G_{\mathbb{Q}}$-stable lattice T in the $(k/2)$-Tate twist $V = W_{\mathfrak{p}}(k/2)$ of this representation, that is analogous to the Tate-module of an elliptic curve: it is self-dual, in the sense that it is endowed with an equivariant $\mathcal{O}$-linear perfect pairing

$$[-,-] \colon T \times T \to \mathcal{O}(1)$$

that induces an isomorphism $T \cong T^*(1)$ as $G_{\mathbb{Q}}$-representations; in the case of elliptic curves this comes from the Weil pairing.

Nekovar then constructs an Euler system for this representation, that is a higher weight analogue of the Heegner point one: he defines a systematic supply of CM cycles Δ_n, usually referred as *Heegner cycles* on the Kuga-Sato variety $\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}$ of level $\Gamma(N)$ and weight k, i.e. the canonical desingularization [see BDP13, Appendix] of the $(k-2)$-fold selfproduct of the universal generalized elliptic curve $\bar{\pi}_{\Gamma(N)} \colon \bar{\mathcal{E}}_{\Gamma(N)} \to X(N)$ over the (closed) modular curve $X(N)$ of level $\Gamma(N)$, and shows that they satisfy properties (as for instance a norm relation) similar to those of the Heegner points. The images $y_n = \Phi_{K[n]}(\Delta_n)$ of these cycles via a suitably defined p-adic étale Abel-Jacobi map

$$\Phi_{K[n]} \colon \mathrm{CH}^{k/2}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}/K[n])_0 \otimes \mathcal{O} \to \mathrm{H}^1_f(K[n], T)$$

define an Euler system, allowing Nekovar to use them as an input of the Kolyvagin method. Here $\mathrm{H}^1_f(K[n], T)$ is the Bloch-Kato Selmer group for T, introduced by Bloch and Kato in [BK90] and $\mathrm{CH}^{k/2}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}/K[n])_0$ is the group of homologically trivial cycles (up to rational equivalence) of codimension $k/2$, defined over $K[n]$, on the *Kuga-Sato variety* $\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}$ of weight k and level $\Gamma(N)$.

In the following statement $y_K = \mathrm{cores}_{K[1]/K}(y_1) \in \mathrm{H}^1_f(K, T)$ is the basic Heegner cycle, $\Lambda_{\mathfrak{p}}(K) \subseteq \mathrm{H}^1_f(K, T)$ is the image of the the Abel-Jacobi map Φ_K and the ($\mathfrak{p}$-primary part of the) Shafarevich-Tate group $\text{Ш}_{\mathfrak{p}^\infty}(f/K)$ is defined to be the cokernel of

$$\Phi_K \otimes \mathcal{K}/\mathcal{O} \colon \mathrm{CH}^{k/2}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}/K)_0 \otimes \mathcal{K}/\mathcal{O} \to \mathrm{H}^1_f(K, A).$$

This definition of the ($\mathfrak{p}$-part of the) Shafarevich-Tate group of f mimics the elliptic curve case, where $\text{Ш}(E/K)[p^\infty]$ sits in the short exact sequence

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\delta} \mathrm{Sel}_{p^\infty}(E/K) \longrightarrow \text{Ш}(E/K)[p^\infty] \longrightarrow 0 \ .$$

In this framework we don't know however if the Abel-Jacobi map is injective, in fact it is a wide open problem whether the Chow group is finitely generated or not, and this led Nekovar to consider the image $\Lambda_{\mathfrak{p}}(K)$ of Φ_K instead of directly using $\mathrm{CH}^{k/2}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}/K)_0$ in order to replace the Mordell-Weil group of an elliptic curve. He obtained therefore the following result:

Theorem ([Nek92, Th. 13.3])**.** *Let $p \nmid 2N\varphi(N)(k-2)!$ and y_K is non-torsion in $\mathrm{H}^1_f(K, T)$, then $\Lambda_{\mathfrak{p}}(K) \otimes \mathcal{K} = \mathcal{K} \cdot y_K$ and $\text{Ш}_{\mathfrak{p}^\infty}(f/K)$ is finite.*

Several authors later improved this result, in particular Besser [Bes97, Th. 1.2] showed that if the prime p is unramified in F and the representation $W_{\mathfrak{p}}$ has "big image", then one can explicitly bound as Kolyvagin did for ellipic curves, the exponent of the Shafarevich-Tate group in terms of the basic Heegner point:

$$p^{2\mathcal{I}_p}\,\text{Ш}_{\mathfrak{p}^\infty}(f/K) = 0,$$

where $\mathcal{I}_p$ is the maximum integer M such that $y_K \in p^M\,\mathrm{H}^1_f(K, T)$. This is finite if y_K is assumed non torsion. As a corollary moreover we get that if $y_K \notin p\,\mathrm{H}^1_f(K, T)$, then $\text{Ш}_{\mathfrak{p}^\infty}(f/K) = 0$. In more recent years [Mas19] gave moreover a structure theorem for $\text{Ш}_{\mathfrak{p}^\infty}(f/K)$, generalizing the analogous result of Kolyvagin for elliptic curves (or better an improvement of it by McCallum [McC91]).

The Heegner cycles of Nekovar are not the unique class of cycles that one can use on order to apply the Kolyvagin method: in [BDP13] Bertolini, Darmon and Prasanna introduced, for reasons involving the study of special values of the p-adic Rankin L-series at critical points that lie outside their range of classical interpolation, another class of cycles Δ_φ indexed over isogenies, that they call *generalized Heegner cycles*, over the product of the Kuga-Sato variety $\tilde{\mathcal{E}}^{k-2}_{\Gamma_1(N)}$ and the $(k-2)$-selfproduct of a fixed CM elliptic curve A defined over the Hilbert class field $K[1]$ of K. We denote this variety by X_{k-2} and we call it *generalized Kuga-Sato variety.* Castella and Hsieh [CH18] showed that a subclass of these cycles can be used in order to construct an Euler system and to apply the Kolyvagin method as modified by Nekovar. If $z_{f,K}$ denotes the basic generalized Heegner cycle, they prove:

Theorem ([CH18, Th. 7.7])**.** *If $z_{f,K}$ is non torsion in $\mathrm{H}^1_f(K,T)$, then $\mathrm{H}^1_f(K,T) = F \cdot z_{f,K}$.*

These cycles are moreover better suited for Iwasawa Theory than the classical Heegner cycles of Nekovar, passing to the Iwasawa theoretical side of the story in fact Longo and Vigni recently proved the following structural result for the Pontryagin dual $\mathcal{X}_\infty$ of the Selmer group $\mathrm{H}^1_f(K_\infty, A)$ of A over the anticyclotomic extension K_∞ of K, building a so called *anticyclotomic Λ-adic Kolyvagin system* starting from them:

Theorem ([LV19, Th. 1.1])**.** *Suppose that $(f, K, \mathfrak{p})$ is an admissible triple in the sense of [LV19, Def. 2.1] (but let us stress that these conditions contains in particular the "big image" property for $W_\mathfrak{p}$, the $\mathfrak{p}$-ordinariety of f and we ask that p is split in K). Then there exists a finitely generated torsion Λ-module M and a pseudo-isomorphism*

$$\mathcal{X}_\infty \sim \Lambda \oplus M \oplus M,$$

where $\Lambda = \mathcal{O}[\![\mathrm{Gal}(K_\infty/K)]\!]$ is the Iwasawa algebra over $\mathcal{O}$ attached to the extension K_∞/K.

Contribution of the Thesis

From the latter theorem of Longo and Vigni we know that in particular, under reasonable assumptions on f and K and p, the Selmer group $\mathrm{H}^1_f(K_\infty, A)$ has Λ-corank 1. The main contribution of this thesis is to find, inspired by the work [MN19] of Nekovar and Matar, the arithmetic conditions under which this group is also cofree.

The following is indeed the main theorem of this thesis:

Theorem (Th. 4.3.6)**.** *Under the assumptions of Section 4.1, suppose moreover that the basic generalized Heegner cycle $z_{f,K}$ is non-torsion and that $z_{f,K} \notin p\,\mathrm{H}^1_f(K,T)$. Then $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K) = 0$ and*

$$\widetilde{\Lambda}_\mathfrak{p}(K) \otimes \mathcal{K}/\mathcal{O} = \mathrm{H}^1_f(K, A) = z_{f,K} \cdot \mathcal{K}/\mathcal{O},$$

moreover $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty) = 0$ and $\mathrm{H}^1_f(K_\infty, A) = \widetilde{\Lambda}_\mathfrak{p}(K_\infty) \otimes \mathcal{K}/\mathcal{O}$, the Pontryagin dual $\mathcal{X}_\infty$ of the latter group beeing free of rank 1 over Λ.

Remark. In Sec. 4.1 we make three technical assumptions. In Assumption 1 we make some assumptions on the prime p, containing in particular the unramifiedness of p in F, the "big image" property for $W_\mathfrak{p}$ and the $\mathfrak{p}$-ordinarity of f: it corresponds to the admissibility assumption of [LV19, Def. 2.1]. Assumption 2 is the triviality of the Tamagawa numbers for the representation A: this implies that the Bloch-Kato Selmer group of A equals the unramified one. Finally Assumption 3 is an assumption on the Hecke eigenvalue a_p: it implies that, if α is the $\mathfrak{p}$-adic unit root of charachteristic polynomial $X^2 - i_p(a_p)X + p^{k-1} = 0$ (which exists since f is $\mathfrak{p}$-ordinary), $\alpha - 1$ is invertible. We use this in order to show that some cohomology groups vanish, establishing equality for the Greenberg and the strict Greenberg Selmer group of A [see Gre91].

The proof of Th. 4.3.6 goes along the same lines of [MN19]: provided that one has a suitable definition of the Shafarevich-Tate group for this purpose, one merges a vanishing result for the Shafarevich-Tate group over K with an abstract Iwasawa theoretical one that extends this vanishing over the anticyclotomic extension. In particular we choose to use a definition that differs a bit from the one of Nekovar since we need to use generalized Heegner cycles, rather then the classical one for the Iwasawa theoretical step. Indeed the generalized ones are cycles that lay in the Chow group $\mathrm{CH}^{k-1}(X_{k-2}/K[n])_0 \otimes \mathbb{Z}_p$ and they become cohomology classes taking their image via an Abel-Jacobi map

$$\Phi'_{K[n]}\colon \mathrm{CH}^{k-1}(X_{k-2}/K[n]) \otimes \mathcal{O} \to \mathrm{H}^1_f(K[n], T),$$

hence, at least in principle, they may not lay into $\Lambda_{\mathfrak{p}}(K[n])$.

We define therefore (Def. 2.2.1) $\widetilde{\Lambda}_{\mathfrak{p}}(K[n])$ to be the image of $\Phi'_{K[n]}$, while the definition of $\widetilde{\Lambda}_{\mathfrak{p}}(K)$ and $\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty)$ is slightly more involved since X_{k-2} is a variety defined not over $\mathbb{Q}$ as it was the case for $\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}$, but just over the Hilbert class field $K[1]$ of K. Thus

$$\Phi'_F\colon \mathrm{CH}^{k-1}(X_{k-2}/F) \otimes \mathcal{O} \to \mathrm{H}^1_f(F, T)$$

is naturally defined only if F is a number field containing $K[1]$, but this is not the case for K and the layers K_n of the anticyclotomic extension. However under our working hypothesis, the restriction morphisms

$$\mathrm{res}\colon \mathrm{H}^1(K, T) \to \mathrm{H}^1(K[1], T), \qquad \mathrm{res}\colon \mathrm{H}^1(K_n, T) \to \mathrm{H}^1(K[p^{n+1}], T)$$

are isomorphisms, hence we put

$$\begin{aligned} \widetilde{\Lambda}_{\mathfrak{p}}(K) &= \mathrm{res}^{-1}\, \widetilde{\Lambda}_{\mathfrak{p}}(K[1])^{\mathrm{Gal}(K[1]/K)} \subseteq \mathrm{H}^1_f(K, T), \\ \widetilde{\Lambda}_{\mathfrak{p}}(K_n) &= \mathrm{res}^{-1}\, \widetilde{\Lambda}_{\mathfrak{p}}(K[p^{n+1}])^{\mathrm{Gal}(K[p^{n+1}]/K_n)} \subseteq \mathrm{H}^1_f(K_n, T) \\ \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) &= \varprojlim_n \widetilde{\Lambda}_{\mathfrak{p}}(K_n) \subseteq \mathrm{H}^1_f(K_\infty, T). \end{aligned}$$

The $\mathfrak{p}$-part of the Shafarevich-Tate group for $F = K, K_n, K_\infty$ is then here defined by the induced short exact sequence

$$0 \longrightarrow \widetilde{\Lambda}_{\mathfrak{p}}(F) \otimes \mathcal{K}/\mathcal{O} \longrightarrow \mathrm{H}^1_f(F, A) \longrightarrow \widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/F) \longrightarrow 0\ .$$

In Chapter 2 we show that with this new definition [Bes97, Th. 1.2] and in particular its vanishing corollary holds again replacing the classical Heegner cycles with the generalized ones, since from the generalized Heegner cycles $z_{f,n}$ one constructs classes $P(n)$ by means of the Kolyvagin derivative operators, as Besser does from the classical ones: we prove that they enjoy the same formal properties and hence the argument of Besser's proof verbatim applies in this case leading to the following result:

Theorem (Th. 2.3.9)**.** *Let p be a non exceptional prime and $z_{f,K}$ be non torsion in $\mathrm{H}^1(K, T)$. Then*

$$p^{2\mathcal{I}_p} \widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K) = 0,$$

where $\mathcal{I}_p$ is the smallest non negative integer such that $z_{f,K}$ is non-zero in $\mathrm{H}^1_f(K, A[p^{\mathcal{I}_p+1}])$. In particular, if $\mathcal{I}_p = 0$, then $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K) = 0$ and $\widetilde{\Lambda}_{\mathfrak{p}}(K) \otimes \mathcal{K}/\mathcal{O} = \mathrm{H}^1_f(K, A) = z_{f,K} \cdot \mathcal{K}/O$.

The abstract Iwasawa theoretical part is treated in Chapter 4, whose main technical step is the followin theorem:

Theorem (Th. 4.3.1)**.** *Under the assumptions of Section 4.1, if the Pontryagin dual* $\mathcal{X}$ *of* $\mathrm{H}^1_f(K, A)$ *is a free* $\mathcal{O}$*-module of rank 1, then the Pontryagin dual* $\mathcal{X}_\infty$ *of* $\mathrm{H}^1_f(K_\infty, A)$ *is a free* Λ*-module of rank* 1*.*

The proof of this result follows that of [MN19, Th. 3.4], proving that the Bloch-Kato Selmer groups of A over the extensions K, K_n, K_∞ coincide with other kind of Selmer groups and with the so called *generalized Selmer groups*, the cohomology objects of the *Selmer complexes* attached to the representations involved. The theory of Selmer complexes, developped by Nekovar in [Nek06] then endows these group of a rich structure: in particular we derive from that an exact control theorem, i.e. an isomorphism

$$\mathrm{H}^1_f(K_n, A) \xrightarrow{\sim} \mathrm{H}^1_f(K_\infty, A)^{\mathrm{Gal}(K_\infty/K_n)}$$

that is the main technical tool that allows us to derive Th. 4.3.1 from [LV19, Th. 1.1]. Th. 4.3.5 follows by abstract nonsense from this abstract version and Th. 2.3.9, provided that $\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) \neq 0$: a nontrivial element of it has been constructed by Longo and Vigni [LV19, Prop. 4.12].

Structure of the thesis

This thesis is subdivided in 4 chapters.

In Chapter 1 we introduce some well known preliminaries: in Section 1.1 we introduce the notion of p-adic representations, their main features and their Selmer groups; in Section 1.2 we introduce the notion of cycles and correspondences and the notion of pure motives; in Section 1.3 we introduce the representation and the motive attached to a modular form and the selfdual lattice of [Nek92]; in Section 1.4 we resume the construction of the anticyclotomic $\mathbb{Z}_p$-extesion K_∞ of K and we discuss the notion of Selmer group over K_∞.

In Chapter 2 we recall from [BDP13] and [CH18] the construction of generalized Heegner cycles and their related Abel-Jacobi map and we use them in order to prove the analogue of [Bes97, Th. 1.2].

In Chapter 3 we give a brief overview of the theory of Selmer complexes that is of interest for us, in Section 3.4 we deduce the statements that one gets from this theory when the Selmer complex comes from a single Galois representation.

Chapter 4 is the core of this thesis: in Section 4.1 we fix a framework for the main result, in Section 4.2 we prove a comparison result between the various Selmer groups of A and the generalized ones, we deduce an exact control theorem for the Bloch-Kato Selmer groups and we prove that the rank 1 cofreeness extends over the anticyclotomic tower, finally in Section 4.3 we combine together the cofreenes extension with the vanishing result Th. 2.3.9 and we prove our main Theorem 4.3.5.

Chapter 1

Selmer Groups and Anticyclotomic Extension

1.1 Selmer Groups

In this section we introduce our basic object of study: p-adic Galois representations and their Selmer groups, following mainly [Rub00] and [MR04]. Fix once and for all a rational prime p and a finite extension $\mathcal{K}$ of $\mathbb{Q}_p$, denote by $\mathcal{O}$ its ring of integers, by $\mathfrak{p}$ its maximal ideal and by κ its residue field. Write $v_{\mathfrak{p}}$ for the non-archimedean valuation on $\mathcal{K}$ and π for a chosen uniformizer. Fix moreover an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, an embedding $i_\infty\colon \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and an algebraic closure $\bar{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ together with an embedding $i_\ell\colon \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ for any rational prime ℓ.

1.1.1 p-adic representations

Let $E \subseteq \bar{\mathbb{Q}}$ a number field and consider a finite set S of primes of E containing all archimedean places and all primes above p. Denote by E_S the maximal extension of E unramified outside S and let $G_{E,S} = \mathrm{Gal}(E_S/E)$. Note that for any finite prime $v \mid \ell$ the embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ fixed above realizes $G_v = \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/E_v)$ as a decomposition group of $G_E = \mathrm{Gal}(\bar{\mathbb{Q}}/E)$.

Definition 1.1.1. An $\mathcal{O}$-adic (resp. $\mathcal{K}$-adic) representation of G_E is a free $\mathcal{O}$-module T (resp. a $\mathcal{K}$-vector space V) of finite rank (resp. dimension) with a continuous $\mathcal{O}$-linear (resp. $\mathcal{K}$-linear) action of G_E with respect to the $\mathfrak{p}$-adic topology on T (resp. V).

Both $\mathcal{O}$-adic and $\mathcal{K}$-adic representations of G_E, for a number field E are usually referred as p-adic Galois representations in the litterature. This is because once we have an $\mathcal{O}$-adic representation T, the vector space $V = T \otimes_{\mathcal{O}} \mathcal{K}$ with the induced action

$$\sigma \cdot (x \otimes r) = (\sigma \cdot x) \otimes r, \quad x \in T, r \in \mathcal{K};$$

is a $\mathcal{K}$-adic representation of dimension equal to the rank of T and conversely any G_E-stable lattice T inside a $\mathcal{K}$-adic representation V is naturally an $\mathcal{O}$-adic representation, with the induced action, of rank equal to the dimension of V.

We may attach to an $\mathcal{O}$-adic representation T also a discrete torsion G_E-module

$$A = V/T = T \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O}$$

and for any $n > 0$ we may consider its π^n-torsion subgroup $A[\pi^n] = \pi^{-n}T/T \cong T/\pi^n T$ (indeed $A[\pi^n]$ is G_E-stable, by the $\mathcal{O}$-linearity of the action). Note that

$$A = \varinjlim_n A[\pi^n] = \bigcup_n A[\pi^n],$$

indeed any $x + T \in A$ is π^n-torsion for a suitable $n > 0$ (let $x = \sum_i a_i t_i$, for t_i generators of T over $\mathcal{O}$ and $a_i \in \mathcal{K}$ and let a_j be the coefficient with minimal $\mathfrak{p}$-valuation: if $n \geq -v_{\mathfrak{p}}(a_j)$, then $\pi^n x \in T$).

Similarly

$$T = \varprojlim_{n,\pi\cdot -} T/\pi^n T \cong \varprojlim_{n,\pi\cdot -} A[\pi^n]$$

indeed if one writes $t = \sum_i a_i t_i$, for t_i generators of T and $a_i \in \mathcal{O}$, one may recover the coefficients a_i (and hence t itself) by their reduction $\bmod \pi^n$.

Remark 1.1.2. All these representations may be equivalently seen as (continuous) group homomorphisms

$$\rho_M : G_E \to \mathrm{GL}(M) \cong \mathrm{GL}_n(B); \quad \rho(\sigma)(x) = \sigma \cdot x; \quad \text{for } \sigma \in G_E, x \in M,$$

where n is the rank of T and $B = \mathcal{O}, \mathcal{K}$ or κ respectively, depending on the fact that $M = T, V$ or $A[\pi]$.

Example 1.1.3. Let $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character, i.e. the map such that $\sigma(\zeta) = \zeta^{\chi_p(\sigma)}$ for any $\sigma \in G_{\mathbb{Q}}$ and $\zeta \in \mu_{p^\infty}(\bar{\mathbb{Q}})$. The action of $G_{\mathbb{Q}}$ on a free $\mathbb{Z}_p$-module of rank one by χ_p gives rise to a $\mathbb{Z}_p$-adic representation. We will use the cyclotomic character moreover in order to twist a p-adic representation: let T be a $\mathcal{O}$-adic representation of G_E, for a number field E, and denote the action of $\sigma \in G_E$ on $x \in T$ by $\sigma \cdot x$, then for any $j \in \mathbb{Z}$ we define $T(j)$ to be the $\mathcal{O}$-module T as a p-adic representation of G_E with the action $\sigma \circ x = \chi_p(\sigma)^j(\sigma \cdot x)$. We will call it the j-th Tate twist of T.

Unramified representations

The most important feature of p-adic representations is unramifiedness. For a finite place $v \mid \ell$, let $I_v = \mathrm{Gal}(\bar{\mathbb{Q}}_p/E_v^{\mathrm{ur}})$ be the inertia subgroup of G_v at v. If v is archimedean (we write $\ell = \infty$) $E_v = \mathbb{R}$ or $\mathbb{C}$ and we define $I_v := G_v$, that is trivial or has order 2.

Definition 1.1.4. Let M a p-adic G_E-representation, we say that M is unramified at a place v of E if I_v acts trivially, or equivalently if $\rho_M(I_v) = \{1\}$.

Note that T is unramified if and only if V or A are so.

Example 1.1.5. Note that the p-adic character χ_p is unramified at any prime $\ell \neq p$. Indeed if $\zeta \in \mu_{p^\infty}(\bar{\mathbb{Q}})$, then $\mathbb{Q}_\ell(\zeta)$ is unramified and hence any $\sigma \in I_\ell = \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell^{\mathrm{ur}})$ fixes ζ. Therefore $\chi_p(I_\ell) = 1$. This is not the case for $\ell = p$, since $\mathbb{Q}_p(\zeta)$ in this case is totally ramified and hence there is a $\sigma \in I_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{ur}})$ that does not fix ζ.

We will be interested in representations unramified outside the places of S. This amounts to consider p-adic representations of $G_{E,S}$, as the following discussion shows.

Denote by G_v^S and I_v^S respectively the decomposition and inertia subgroups of $G_{E,S}$ with respect to v, induced by the embedding i_ℓ, for $v \mid \ell$. Note that for any $v \notin S$, $I_v^S = \{1\}$, since E_S is unramified at v.

Lemma 1.1.6. *$G_{E,S}$ is the quotient of G_E by H, the minimal closed normal subgroup containing all I_v such that $v \notin S$.*

Remark 1.1.7. Note that for a place v its inertia group I_v is defined only up to conjugation, but the lemma does not depend on the particular choice because H is normal and therefore whenever it contains a subgroup, it contains also all its conjugates.

Proof. Note that if π denotes the projection $G_E \twoheadrightarrow G_{E,S}$, by [Neu99, Ch. II, Prop. 9.4] applied to the extensions E_S/E and $\bar{E}/E$, we have a commutative diagram

$$\begin{array}{ccccc} I_v & \hookrightarrow & D_v & \hookrightarrow & G_E \\ \downarrow & & \downarrow & & \downarrow \pi \\ I_v^S & \hookrightarrow & D_v^S & \hookrightarrow & G_{E,S} \end{array} .$$

Hence $I_v \subseteq \ker \pi$ for any $v \notin S$, as π factors trough $I_v^S = \{1\}$. The lemma follows by Galois correspondence and the maximality of E_S. $\square$

Proposition 1.1.8. *A representation ρ of G_E is unramified outside S if and only if it factorizes through $G_{E,S}$.*

Proof. If ρ factorizes as ρ^S through $G_{E,S}$, then $\rho(I_v) = \rho^S \circ \pi(I_v) = \rho^S(I_v^S) = \rho^S(\{1\}) = \{1\}$ for any $v \notin S$. Conversely, let ρ be unramified outside S. By the previous lemma, $H = \ker \pi$ is the minimal normal closed subgroup containing all I_v for $v \in S$, and so $\rho(H) = \{1\}$. In fact, denoting by ρ' the restriction of ρ to H, $\ker \rho'$ is a normal subgroup of H such that $I_v \subseteq \ker \rho'$ for any place $v \notin S$ and hence $H = \ker \rho'$ by minimality. Thus ρ factorizes through $G_E/H \cong G_{E,S}$. $\square$

Duality

We have in our setting two notions of duality. The aim of this paragraph is to define the duality functors and to study the relations among the different dual representations.

Definition 1.1.9. The linear dual of an $\mathcal{O}$-adic (resp. $\mathcal{K}$-adic) representation T (resp. V) is defined to be the free $\mathcal{O}$-module $T^* = \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O})$ (resp. the $\mathcal{K}$-vector space $V^* = \mathrm{Hom}_{\mathcal{K}}(V, \mathcal{K})$) endowed with the $\mathfrak{p}$-adic topology and the continuous G_E-action $\sigma \cdot f(x) = f(\sigma^{-1}x)$ for any $\sigma \in G_E$, $f \in T^*$, $x \in T$ (resp. $f \in V^*$, $x \in V$).

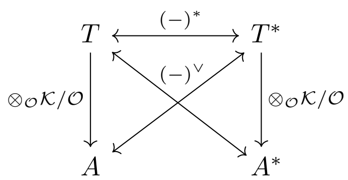
Note that the functor $(-)^*$ is a dualizing functor on the category of finite free $\mathcal{O}$-module (resp. of $\mathcal{K}$-vector spaces), i.e. the canonical map $T \to T^{**}$ is an isomorphism.

For a compact or discrete $\mathcal{O}$-module M we may define moreover its Pontryagin dual.

Definition 1.1.10. Let M be a compact or a discrete $\mathcal{O}$-module, the Pontryagin dual of M is defined to be the $\mathcal{O}$-module $M^\vee = \mathrm{Hom}_{\mathcal{O}}^{\mathrm{cont}}(M, \mathcal{K}/\mathcal{O})$ endowed with the compact-open topology. If moreover M has a continuous G_E-action, it induces a continuous G_E-action on $M^\vee$ defined by $\sigma \cdot f(x) = f(\sigma^{-1}x)$ for any $\sigma \in G_E$, $f \in M^\vee$ and $x \in M$.

It is known (e.g. [NSW00, Ch. I, Th. 1.1.8]) that the $(-)^\vee$ functor defines a duality functor between the categories of compact and discrete $\mathcal{O}$-modules.

If we define moreover $A^* = V^*/T^*$ we may depict the relations among the linear and the Pontryagin dual representations by the following diagram:



This diagram follows from the following proposition applied to $M = T, T^*$ since all morphisms $\varphi\colon M \to \mathcal{K}/\mathcal{O}$ are continuous, as long as M is a finite free $\mathcal{O}$-module. In fact, since φ is $\mathcal{O}$-linear, it is enough to check that φ is continuous at $0 \in M$; that is, as M has the $\mathfrak{p}$-adic topology and $\mathcal{K}/\mathcal{O}$ is discrete, we have to find an $N \geq 0$ such that $\varphi(\mathfrak{p}^N M) = 0 + \mathcal{O}$. Let therefore $m_1, \ldots, m_s$ be a basis of M over $\mathcal{O}$ and $\varphi(m_i) = a_i/\pi^{n_i} + \mathcal{O}$ for $a_i \in \mathcal{O}^\times$, $n_i \geq 0$, let $N = \max_i \{ n_i \}$; then $\varphi(\mathfrak{p}^N M) = 0 + \mathcal{O}$.

Proposition 1.1.11. *If M is a finite free $\mathcal{O}$-module* $\mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O}) \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O} \cong \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{K}/\mathcal{O})$.

Proof. The isomorphism is given by the multiplication map $\varphi \otimes x \mapsto x \cdot \varphi$. Indeed, let $m_1, \ldots, m_s$ be an $\mathcal{O}$-basis of M, and write m_i^* for the $\mathcal{O}$-linear maps in $\mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O})$ such that $m_i^*(m_j) = \delta_{ij}$, where δ_{ij} is the Kronecker symbol. It is straight forward to check that the inverse of the previous map is given by the linear homomorphism $\psi \mapsto \sum_i m_i^* \otimes \psi(m_i)$, as any $\psi \in \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{K}/\mathcal{O})$ is uniquely defined by its image on a basis. ☐

Remark 1.1.12. It is worth observing that in the above definitions we can use $\mathbb{Z}_p$ (resp. $\mathbb{Q}_p$) at any occurrence of $\mathcal{O}$ (resp. $\mathcal{K}$). This follows as $\mathcal{O}$ is free of rank $[\mathcal{K} : \mathbb{Q}_p]$ as $\mathbb{Z}_p$-module [Neu99, Ch. I, Prop. 2.10], say generated by $a_1, \ldots, a_n$. Since T is free over $\mathcal{O}$, say with basis $t_1, \ldots, t_s$, then it is free over $\mathbb{Z}_p$ with basis $a_1 t_1, \ldots, a_1 t_s, \ldots, a_n t_s$ and hence $V = T \otimes_{\mathcal{O}} \mathcal{K} = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ as $\mathbb{Q}_p$-vector spaces. Moreover $A = V/T = T \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O} = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ as discrete $\mathbb{Z}_p$-modules. Indeed the sequences

$$0 \longrightarrow T = T \otimes_{\mathbb{Z}_p} \mathbb{Z}_p \longrightarrow V = T \otimes_{\mathbb{Q}_p} \mathbb{Q}_p \longrightarrow T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

$$0 \longrightarrow T = T \otimes_{\mathcal{O}} \mathcal{O} \longrightarrow V = T \otimes_{\mathcal{O}} \mathcal{K} \longrightarrow T \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O} \longrightarrow 0$$

are both exact, since T is free and hence flat both over $\mathcal{O}$ and $\mathbb{Z}_p$.

However the isomorphisms among the corresponding modules are not always canonical isomorphisms. Now observe that for a compact or discrete $\mathcal{O}$-module M

$$\mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) = \mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(M \otimes_{\mathcal{O}} \mathcal{O}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}}\left(M, \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Q}_p/\mathbb{Z}_p)\right),$$

and

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$$

as $\mathcal{O}$ is finite free over $\mathbb{Z}_p$ (this is Prop. 1.1.11 replacing $\mathcal{O}$ to M and $\mathbb{Z}_p$ to $\mathcal{O}$). Moreover

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Z}_p) \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O}$$

since $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Z}_p)$ is a fractional ideal isomorphic to the inverse different ([Neu99, Ch. III, §2]) and hence free both as $\mathbb{Z}_p$-module (again by [Neu99, Ch. I, Prop. 2.10], for $M = \mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Z}_p)$) and as $\mathcal{O}$-module (as any it is a fractional ideal in a PID is principal). Thus we may use the same arguments we used above for T. In particular $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}, \mathbb{Z}_p)$ has rank one over $\mathcal{O}$ and if we choose a generator we find a non-canonical isomorphism of topological $\mathbb{Z}_p$-modules

$$\mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}}(M, \mathcal{K}/\mathcal{O}).$$

1.1.2 Local conditions and Selmer groups

Local Conditions

In this paragraph T will be an $\mathcal{O}$-adic representation of $G_{E,S}$ and let V and A be the induced representations as in the previous paragraph. We introduce the general formalism of Selmer groups, following [MR04]. In the following all cohomology groups are the *continuous cohomology* groups, introduced by [Tat76]. We refer to [Rub00, App. B.2] or [NSW00, Sec. II.3] for the definition and the properties of these groups.

Definition 1.1.13. A local condition $\mathcal{F} = (\mathcal{F}_v)_{v\in S}$ is the choice, for any place $v \in S$ of a subspace $\mathrm{H}^1_{\mathcal{F}_v}(E_v, V) \subseteq \mathrm{H}^1(E_v, V)$.

Note that the choice induces for any place $v \in S$ the submodules $\mathrm{H}^1_{\mathcal{F}}(E_v, A)$ of $\mathrm{H}^1(E_v, A)$ and $\mathrm{H}^1_{\mathcal{F}}(E_v, T)$ of $\mathrm{H}^1(E_v, T)$ taking respectively the image and the inverse image of $\mathrm{H}^1_{\mathcal{F}_v}(E_v, V)$ under the natural maps. The submodule $\mathrm{H}^1_{\mathcal{F}}(E_v, A[\pi^n])$ of $\mathrm{H}^1(E_v, A[\pi^n])$ can be equally defined [see Rub00, Rk. I.3.9] as the image of $\mathrm{H}^1_{\mathcal{F}_v}(E_v, T)$ under the map induced by

$$T \twoheadrightarrow T/\pi^n T \xrightarrow[\sim]{\cdot \pi^{-n}} \pi^{-n}T/T = A[\pi^n]$$

or as the inverse image of $\mathrm{H}^1_{\mathcal{F}}(E_v, A)$ by the map induced by the inclusion $A[\pi^n] \hookrightarrow A$.

Example 1.1.14. Let $X = T, V, A, A[\pi^n]$ and v a finite place of E. We define the subgroup of unramified cohomology classes as

$$\mathrm{H}^1_{\mathrm{ur}}(E_v, X) = \ker(\mathrm{H}^1(E_v, X) \to \mathrm{H}^1(I_v, X)),$$

where I_v denotes the inertia subgroup of G_v. If $v \nmid p$ we define the *finite* local condition at v to be $\mathrm{H}^1_f(E_v, V) = \mathrm{H}^1_{\mathrm{ur}}(E_v, V)$ and, as in the previous definition, $\mathrm{H}^1_f(E_v, A)$ and $\mathrm{H}^1_f(E_v, T)$ to be respectively the image and the inverse image under the natural morphisms. In particular the commutative diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{H}^1_{\mathrm{ur}}(E_v, T) & \longrightarrow & \mathrm{H}^1(E_v, T) & \longrightarrow & \mathrm{H}^1(I_v, T) \\
 & & & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{H}^1_{\mathrm{ur}}(E_v, V) = \mathrm{H}^1_f(E_v, V) & \longrightarrow & \mathrm{H}^1(E_v, V) & \longrightarrow & \mathrm{H}^1(I_v, V) \\
 & & & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{H}^1_{\mathrm{ur}}(E_v, A) & \longrightarrow & \mathrm{H}^1(E_v, A) & \longrightarrow & \mathrm{H}^1(I_v, A)
\end{array}$$

shows that $\mathrm{H}^1_{\mathrm{ur}}(E_v, T) \subseteq \mathrm{H}^1_f(E_v, T)$ and that $\mathrm{H}^1_f(E_v, A) \subseteq \mathrm{H}^1_{\mathrm{ur}}(E_v, A)$. The index

$$c_v(A) := [\mathrm{H}^1_{\mathrm{ur}}(E_v, A) : \mathrm{H}^1_f(E_v, A)]$$

is finite and it is called the *p-part of the Tamagawa number of A at v*. If V is unramified at v, then $c_v(A) = 1$ [see Rub00, Lemma 3.5.*iv*], i.e. $\mathrm{H}^1_f(E_v, A) = \mathrm{H}^1_{\mathrm{ur}}(E_v, A)$. Moreover by *loc. cit.* if V is unramified at v, then also $\mathrm{H}^1_f(E_v, T) = \mathrm{H}^1_{\mathrm{ur}}(E_v, T)$ and $\mathrm{H}^1_f(E_v, A[\pi^n]) = \mathrm{H}^1_{\mathrm{ur}}(E_v, A[\pi^n])$.

Formalism of Selmer groups

Definition 1.1.15. Let $X = T, V, A, A[p^n]$. The Selmer group of X associated to a local condition $\mathcal{F}$ is defined to be the group

$$\mathrm{H}^1_{\mathcal{F}}(E, X) = \ker\left(\mathrm{H}^1(E_S/E, X) \to \bigoplus_{v\in S} \frac{\mathrm{H}^1(E_v, X)}{\mathrm{H}^1_{\mathcal{F}_v}(E_v, X)}\right).$$

In this thesis we will consider mainly the Block-Kato Selmer groups defined in [BK90], usually denoted by $\mathrm{H}^1_f(E_v, X)$, i.e. the Selmer groups associated with the following local conditions:

$$\mathrm{H}^1_f(E_v, V) = \begin{cases} \mathrm{H}^1_{\mathrm{ur}}(E_v, V) & \text{if } v \in S,\ v \nmid p, \infty, \\ \ker\Big(\mathrm{H}^1(E_v, V) \to \mathrm{H}^1(E_v, V \otimes_{\mathbb{Q}_p} B_{\mathrm{crys}})\Big) & \text{if } v \mid p, \\ \mathrm{H}^1(E_v, V) & \text{if } v \mid \infty. \end{cases}$$

where B_{crys} denote the Fontaine ring of p-adic crystalline periods.

Greenberg Selmer Groups

If the representation V is ordinary at any $v \mid p$, in the sense of [Gre91], we have for any $v \mid p$ a filtration of $\mathcal{K}[G_v]$-submodules $V = F^0_v V \supseteq V^+_v = F^1_v V \supseteq F^2_v V \supseteq \dots$ and we may define for $X = T, V, A$ the Greenberg Selmer group and the strict Greenberg Selmer group. For any $v \mid p$ let $T^+_v = V^+_v \cap T$, $A^+_v = V^+_v / T^+_v$ and $X^-_v = X/X^+_v$; define

$$\mathrm{H}^1_{\mathrm{Gr}}(E, X) = \ker\Bigg(\mathrm{H}^1(E_S/E, X) \to \bigoplus_{v \mid p} \mathrm{H}^1(I_v, X^-_v) \oplus \bigoplus_{\substack{v \in S \\ v \nmid p\infty}} \mathrm{H}^1(I_v, X)\Bigg),$$

$$\mathrm{H}^1_{\mathrm{str}}(E, X) = \ker\Bigg(\mathrm{H}^1(E_S/E, X) \to \bigoplus_{v \mid p} \mathrm{H}^1(G_v, X^-_v) \oplus \bigoplus_{\substack{v \in S \\ v \nmid p\infty}} \mathrm{H}^1(I_v, X)\Bigg).$$

They are related by the exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{str}}(E, X) \to \mathrm{H}^1_{\mathrm{Gr}}(E, X) \to \bigoplus_{v \mid p} \mathrm{H}^1\left(G_v/I_v, \mathrm{H}^0(I_v, X^-_v)\right).$$

Note that the Greenberg Selmer groups of V fit into the general framework described above using the local conditions

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(E_v, V) = \begin{cases} \mathrm{H}^1_{\mathrm{ur}}(E_v, V) & \text{if } v \in S,\ v \nmid p, \infty; \\ \mathrm{H}^1_{\mathrm{ord}}(E_v, V) = \ker\Big(\mathrm{H}^1(E_v, V) \to \mathrm{H}^1(I_v, V^-_v)\Big) & \text{if } v \mid p; \\ \mathrm{H}^1(E_v, V) & \text{if } v \mid \infty \end{cases}$$

and

$$\mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(E_v, V) = \begin{cases} \mathrm{H}^1_{\mathrm{ur}}(E_v, V) & \text{if } v \in S,\ v \nmid p, \infty; \\ \mathrm{H}^1_{\mathrm{str}}(E_v, V) = \ker\Big(\mathrm{H}^1(E_v, V) \to \mathrm{H}^1(G_v, V^-_v)\Big) & \text{if } v \mid p; \\ \mathrm{H}^1(E_v, V) & \text{if } v \mid \infty. \end{cases}$$

It is immediate to observe that $\mathrm{H}^1_{\mathrm{Gr}}(E, V) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(E, V)$ and $\mathrm{H}^1_{\mathrm{str}}(E, V) = \mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(E, X)$, but in general $\mathrm{H}^1_{\mathrm{Gr}}(E, X) \neq \mathrm{H}^1_{\mathcal{F}_{\mathrm{Gr}}}(E, X)$, $\mathrm{H}^1_{\mathrm{str}}(E, X) \neq \mathrm{H}^1_{\mathcal{F}_{\mathrm{str}}}(E, X)$ for $X = T, A$. For instance we have already remarked in Ex. 1.1.14 that $\mathrm{H}^1_{\mathrm{ur}}(E_v, A)$ contains $\mathrm{H}^1_f(E_v, A)$, that is the image of $\mathrm{H}^1_{\mathrm{ur}}(E_v, V)$ via the natural map, but these are not equal in general.

However, defining for any $v \mid p$ and $X = T, V, A$,

$$\mathrm{H}^1_{\mathrm{ord}}(E_v, X) = \ker\Big(\mathrm{H}^1(E_v, X) \to \mathrm{H}^1(I_v, X_v^-)\Big);$$
$$\mathrm{H}^1_{\mathrm{str}}(E_v, X) = \ker\Big(\mathrm{H}^1(E_v, X) \to \mathrm{H}^1(G_v, X_v^-)\Big),$$

we may write the Greenberg and strict Selmer groups in a similar fashion:

$$\mathrm{H}^1_{\mathrm{Gr}}(E, X) = \ker\left(\mathrm{H}^1(E_S/E, X) \to \bigoplus_{v|p} \frac{\mathrm{H}^1(E_v, X)}{\mathrm{H}^1_{\mathrm{ord}}(E_v, X_v)} \oplus \bigoplus_{\substack{v\in S\\ v\nmid p\infty}} \frac{\mathrm{H}^1(E_v, X)}{\mathrm{H}^1_{\mathrm{ur}}(E_v, X)}\right);$$
$$\mathrm{H}^1_{\mathrm{str}}(E, X) = \ker\left(\mathrm{H}^1(E_S/E, X) \to \bigoplus_{v|p} \frac{\mathrm{H}^1(E_v, X)}{\mathrm{H}^1_{\mathrm{str}}(E_v, X_v)} \oplus \bigoplus_{\substack{v\in S\\ v\nmid p\infty}} \frac{\mathrm{H}^1(E_v, X)}{\mathrm{H}^1_{\mathrm{ur}}(E_v, X)}\right).$$

1.2 Cycles and Motives

In this section we review the notion of algebraic cycles and give the definition of Chow (and Grothendieck) motives, We will not need in this work the general theory of motives, but we will see in the next section the construction of the motive attached by Scholl to a modular form in [Sch90].

1.2.1 Algebraic Cycles and Chow group

A good reference for the material of this paragraph is [Ful98]. Given a fixed ground a field K, a variety over K means an integral (reduced and irreducible) scheme X of finite type over $\mathrm{Spec}(K)$ and a subvariety V of X is a closed subscheme of X that is a variety over K. For this kind of schemes we have a well shaped theory of dimension and codimension [see GW10, Ch. 5]. If X is a variety over K, we set $d_X = \dim_K(X)$ and if V is a subvariety of X of generic point η_V, we let $\mathcal{O}_{X,V}$ denote the stalk of $\mathcal{O}_X$ at η_V and we call it the local ring at V; its fraction field $K(V) = \mathrm{Frac}\,\mathcal{O}_{X,V}$ is called the field of rational functions on V.

Definition 1.2.1. Let X be a variety over K. A codimension-r cycle on X is a finite formal sum $\sum_V n_V[V]$ of subvarieties V of X of codimension r. The group of codimension-r cycles is denoted by $Z^r(X)$. Between codimension-r cycles we may define an equivalence $\sim_{\mathrm{rat}}$ called rational equivalence [Ful98, Sec. 1.3] and the subset $\mathrm{Rat}^r(X)$ of cycles rationally equivalent to 0 form a subgroup. The Chow group of codimension-r cycle classes is defined to be the quotient

$$\mathrm{CH}^r(X) = Z^r(X)/\,\mathrm{Rat}^r(X).$$

Definition 1.2.2. Let $f\colon X \to Y$ be a proper morphism of varieties over K. For a subvariety V of X then $W = f(X)$ is a closed subvariety of Y and we have an inclusion of $K(W) \hookrightarrow K(V)$, that is a finite field extension when V and W have the same dimension. Set

$$\deg(V/W) = \begin{cases} [K(V) : K(W)] & \text{if } \dim(W) = \dim(V); \\ 0 & \text{if } \dim(W) < \dim(V) \end{cases}$$

and, for any subvariety V of X, $f_*[V] = \deg\big(V/f(V)\big)[f(V)] \in Z^{d_Y - d_X + r}(Y)$. This extends by linearity to a homomorphism, called (proper) push-forward of cycles,

$$f_*\colon Z^r(X) \longrightarrow Z^{d_Y - d_X + r}(Y).$$

Definition 1.2.3. Let $f\colon X \to Y$ be a flat morphism of varieties of relative dimension n. Then for any subvariety W of Y, all irreducible components of $f^{-1}(W)$ have dimension $\dim(W) + n$ (in particular $n = d_X - d_Y$, using $W = Y$). Set for any subvariety W of Y of codimension r

$$f^*(W) = \sum_{\substack{V \text{ irr. comp.} \\ \text{of } f^{-1}(W)}} m_V[V] \in Z^r(X)$$

where $m_V = \text{lenght}_{\mathcal{O}_{X,V}}(\mathcal{O}_{X,V})$. This extends by linearity to a homomorphism

$$f^*\colon Z^r(Y) \longrightarrow Z^r(X),$$

called (flat) pull back of cycles.

Remark 1.2.4. As we defined cycles in terms of codimension of subvarieties the comparison with the statements in [Ful98], where cycles are defined in terms of their dimension, is not completely straight forward but one has to switch dimension with codimension in order to check that they are really the same.

By [Ful98, Th. 1.4, Th. 1.7] proper push forward and flat pull back are compatible with rational equivalence, hence they induce morphisms at the level of Chow groups:

$$f_*\colon\ \mathrm{CH}^r(X) \longrightarrow \mathrm{CH}^{d_Y - d_X + r}(Y),$$
$$f^*\colon\ \mathrm{CH}^r(Y) \longrightarrow \mathrm{CH}^r(X).$$

Lastly we recall that there is an intersection product, well defined at the level of Chow groups:

$$\cdot\ : \mathrm{CH}^r(X) \times \mathrm{CH}^s(X) \longrightarrow \mathrm{CH}^{r+s}(X)$$

Let now X, Y two smooth projective varieties defined over K.

Definition 1.2.5. A correspondence from a variety X to Y of degree r is an element of

$$\mathrm{Corr}^r(X, Y) := \mathrm{CH}^{r+d_X}(X \times Y).$$

The main example of correspondence is the graph Graph(f) of a morphism $f\colon X \to Y$, that is a subvariety of $X \times Y$. This example shows moreover that, philosophically speaking, a fruitful way to think to correspondences is as a sort of *multivalued maps*.

For any correspondence $\alpha \in \mathrm{Corr}^r(X, Y)$ we define the transposed correspondence ${}^t\alpha$ as

$${}^t\alpha = \sigma_*(\alpha) \in \mathrm{Corr}^{d_Y - d_X + r}(Y, X),$$

where $\sigma\colon X \times Y \to Y \times X$ is the morphism switching the two factors, and pull-back and push-forward on the Chow groups induced by α:

$$\alpha_*\colon\ \mathrm{CH}^j(X) \to \mathrm{CH}^{j+r}(Y), \qquad \beta \mapsto (p_Y)_*(\alpha \cdot p_X^*\beta);$$
$$\alpha_*\colon\ \mathrm{CH}^j(Y) \to \mathrm{CH}^{j+r-d_X-d_Y}(X), \qquad \beta \mapsto (p_X)_*(\alpha \cdot p_Y^*\beta),$$

where $p_X : X \times Y \to X$, $p_Y : X \times Y \to Y$ are the canonical projections.

Two correspondences may also be composed: if we have three smooth projective varieties X, Y, Z over K and two correspondences $\alpha \in \mathrm{Corr}^r(X, Y)$ and $\beta \in \mathrm{Corr}^s(Y, Z)$ we define their composition to be

$$\alpha \circ \beta := (p_{XZ})_*(p_{XY}^*\alpha \cdot p_{YZ}^*\beta) \in \mathrm{Corr}^{r+s}(X, Z),$$

where p_{XZ}, p_{XY}, p_{YZ} are the projections from $X \times Y \times Z$ respectively onto the factors $X \times Z$, $X \times Y$, $Y \times Z$ and the intersection product is the intersection of cycles over $X \times Y \times Z$. This composition law is associative by [Ful98, Prop. 16.1.1(a)] and makes

$$\mathrm{Corr}(X) = \bigoplus_r \mathrm{Corr}^r(X)$$

into an associative ring with as unit the correspondence Δ_X attached to the diagonal embedding $\Delta_X : X \to X \times X$ and an involution (transposition of correspondences) [Ful98, Cor. 16.1.1]. In particular the set of 0-degree correspondences $\mathrm{Corr}^0(X, X)$ form a subring closed under transpositions and containing the graph of endomorphisms of X [see Ful98, Rk. 16.1(i)].

Remark 1.2.6. In the following we will allow coefficients of our cycles in any commutative ring R, it is convenient therefore to define $Z^r(X)_R = Z^r(X) \otimes R$. Similarly as above one defines a notion of rational equivalence thus one get the Chow group $\mathrm{CH}^r(X)_R$ with coefficients in R, it is not obvious, but true that $\mathrm{CH}^r(X)_R = \mathrm{CH}^r(X) \otimes R$; however for other equivalences this fails to be true [see And04, Sec. 3.1.2, 3.2.2]. We extend moreover by R-linearity pull-backs, push-forwards and intersection products to Chow groups with coefficients in R. Thus defining the correspondences with coefficients in R as elements of

$$\mathrm{Corr}^r(X, Y)_R := \mathrm{CH}^{r+d_X}(X \times Y)_R = \mathrm{CH}^{r+d_X}(X \times Y) \otimes R,$$

the formula above defining the composition of two correspondences still make sense over R.

1.2.2 Chow Motives

Euristically, the theory of motive should be a sort of *universal cohomology* that lays above all the others cohomology theories, that have to be thought as *realisations* of it and this would explain the deep relations among them. Developped at first by Grothedieck, the theory of motives is nowadays wide and still highly conjectural. We will however limit ourself to introduce the definition of the categories of Chow and Grothendieck pure motives following [And04], then in Sec. 1.3 we will sketch the construction of the motive attached by Scholl to a modular form of even weight. Here K is a field and R a commutative ring.

Consider at first the category $(\mathrm{Corr}^0_K)_R$ of K-correspondences with coefficients in R, whose objects are the smooth projective varieties defined over K and the morphisms between X and Y are the zero-degree correspondences $\Gamma \in \mathrm{Corr}^0(X, Y)_R$. This is an R-linear category, whose (finite) direct sums are given by the disjoint sum of varieties.

Definition 1.2.7. The category $\mathcal{M}^{\mathrm{eff}}_{\mathrm{rat}}(K)_R$ of pure effective Chow motives over K with coefficients in R is the pseudo-abelian completion of $(\mathrm{Corr}^0_K)_R$; explicitely its objects are of the form (X, e), where

- X is a smooth projective variety defined over K,
- $e = e^2 \in \mathrm{Corr}^0(X, X)_R$ is an idempotent.

If $(X, e), (Y, f) \in \mathrm{Ob}\big(\mathcal{M}_{\mathrm{rat}}(K)^{\mathrm{eff}}_R\big)$,

$$\mathrm{Hom}_{\mathcal{M}^{\mathrm{eff}}_{\mathrm{rat}}(K)_R}\big((X, e), (Y, f)\big) = e \circ \mathrm{Corr}^0(X, Y)_R \circ f$$

where the composition is given by the composition of correspondences. We have moreover a canonical embedding

$$\mathfrak{h}(-) : (\mathrm{Corr}^0_K)_R \to \mathcal{M}^{\mathrm{eff}}_{\mathrm{rat}}(K)_R,$$

given by $X \mapsto (X, \Delta_X)$, where Δ_X is the graph of the diagonal morphism $X \times_K X \to X$ and

$$(X, e) \oplus (Y, f) = (X \amalg Y, e \amalg f)$$

For the definitions of pseudo-abelian categories and of pseudo-abelian completion (called also Karoubian categories and Karoubian completion) and their properties see [SGA4, Exposeé 4, Ex. 7.5] and [Stacks, Tag 09SF]. Let us just remark that in a Karoubian category $\mathscr{C}$, given an idempotent $e\colon X \to X$, it has an image and there exist a direct sum decomposition $X = \operatorname{im} e \oplus X'$, hence it is suggesting to use the alternative notation $e\mathfrak{h}(X)$ for the effective pure motive (X, e), meaning that we would like to interpret an effective pure motive as a direct factor of the (euristic) *universal cohomology* of X, cutted out by the idempotent e. This interpretation reflects on realisations of the motive. For instance later on we will consider the p-adic étale realisation of the Scholl motive that is indeed a direct factor of the étale cohomology of a Kuga-Sato variety.

We would like moreover to take into account in our theory also the Tate Twist of a motive. This is realized by the following definition.

Definition 1.2.8. The category $\mathcal{M}_{\mathrm{rat}}(K)_R$ of pure Chow motives over K with coefficients in R is the category whose objects are of the form (X, e, i), where

- X is a smooth projective variety defined over K,
- $e = e^2 \in \mathrm{Corr}^0(X, X)_R$ is an idempotent,
- $i \in \mathbb{Z}$ is an integer.

If $(X, e, i), (Y, f, j) \in \mathrm{Ob}\big(\mathcal{M}_{\mathrm{rat}}(K)_R\big)$,

$$\mathrm{Hom}_{\mathcal{M}_{\mathrm{rat}}(K)_R}\big((X, e, i), (Y, f, j)\big) = e \circ \mathrm{Corr}^{i-j}(X, Y)_R \circ f$$

where the composition is given by the composition of correspondences. The category of effective motives embeds here by the natural functor $(X, e) \mapsto (X, e, 0)$.

Again it will be euristically convenient to denote the motive (X, e, i) as $e\mathfrak{h}(X)(i)$, when $e = \Delta_X$ or $i = 0$ they will be omitted by the notation.

The category $\mathcal{M}_{\mathrm{rat}}(K)_R$ admits also a $\otimes$-structure, the tensor products being defined as

$$e\mathfrak{h}(X)(i) \otimes f\mathfrak{h}(Y)(j) = (e \times f)\mathfrak{h}(X \times Y)(i + j)$$

and the identity object being $\mathbb{1} = \mathfrak{h}(\mathrm{Spec}(K))$. The Tate twist of $\mathcal{M}$ (by $i \in \mathbb{Z}$) is defined to be $\mathcal{M}(i) := \mathcal{M} \otimes \mathbb{1}(i)$, where $\mathbb{1}(i) := \mathfrak{h}(\mathrm{Spec}(K))(i)$.

Moreover we have a notion of dual motive:

$$\big(e\mathfrak{h}(X)(i)\big)^\vee = {}^t e\mathfrak{h}(X)(d_X - i)$$

and a motive $\mathcal{M}$ is called self-dual if $\mathcal{M}^\vee(1) \cong \mathcal{M}$.

But the most important feature of the category of motives is that for any Weil cohomology there are realisation functors. We refer to [And04, Sec. 3.3, 4.2.5] for the general theory. We simply remark that the étale realisation of the motive $\mathfrak{h}(X)$, where X is a projective variety, is $\mathrm{H}^r_{\text{ét}}(\bar{X}, \mathbb{Q}_p)$, $\bar{X}$ denoting the base change of X to $\bar{K}$, hence the realisation of $e\mathfrak{h}(X)(i)$ is $e\,\mathrm{H}^r_{\text{ét}}\big(\bar{X}, \mathbb{Q}_p(i)\big)$, a direct factor of the i-th Tate twist of $\mathrm{H}^r_{\text{ét}}(\bar{X}, \mathbb{Q}_p)$ cutted by a projector (that we still call e, for its explicit definition see [Kin11, Sec. 1.2]).

1.2.3 Continuous étale cohomology

Our next goal is to introduce a second kind of equivalence on $Z^r(X)$, coarser than the rational one, the so called *homological equivalence*. In order to do that we need first to introduce the continuous étale cohomology.

Let X be a proper and smooth variety of pure dimension d over a field K of characteristic 0. Fix an algebraic closure $\bar{K}$ of K, let $G_K = \mathrm{Gal}(\bar{K}/K)$ and denote $\bar{X} = X \otimes_K \bar{K}$. Classically (see e.g. [Mil80]) one defines the (geometric) étale cohomology with coefficient in $\mathbb{Z}_p(j)$ as

$$\mathrm{H}^r_{\text{ét}}(\bar{X}, \mathbb{Z}_p(j)) := \varprojlim_n \mathrm{H}^r(\bar{X}_{\text{ét}}, \mathbb{Z}/p^n\mathbb{Z}(j)),$$

where the cohomology groups $\mathrm{H}^r(\bar{X}_{\text{ét}}, \mathbb{Z}/p^n\mathbb{Z}(j))$ are the r-th derived functors of the functor of global sections computed on the constant sheaf of abelian groups with stalk $\mathbb{Z}/p^n\mathbb{Z}$ on the variety $\bar{X}$, with respect to the étale topology, twisted by the j-th power of the cyclotomic character.

It is known that an anologous definition of the étale cohomology for X as

$$\varprojlim_n \mathrm{H}^r(X_{\text{ét}}, \mathbb{Z}/p^n\mathbb{Z}(j))$$

does not behave well in general as the groups $\mathrm{H}^r(X_{\text{ét}}, \mathbb{Z}/p^n\mathbb{Z}(j))$ may not be finite (e.g. if K is a number field).

In order to overcome this difficulty Jannsen introduces in [Jan88] a variant of this construction, that he called *continuos étale cohomology*: for an inverse system of étale sheaves $(F_n)_{n\in\mathbb{N}}$, let $\mathrm{H}^r_{\text{ét}}\big(X, (F_n)_n\big)$ be the the right derived functors of the left exact functor

$$\begin{aligned} \{\,\text{inverse systems of étale sheaves}\,\} &\to \{\,\text{abelian groups}\,\} \\ (F_n)_n &\mapsto \varprojlim_n \mathrm{H}^0(X_{\text{ét}}, F_n). \end{aligned}$$

In particular we define the continuous (arithmetic) étale cohomology with values in $\mathbb{Z}_p(j)$ as

$$\mathrm{H}^r_{\text{ét}}(X, \mathbb{Z}_p(j)) := \mathrm{H}^r_{\text{ét}}\big(X, (\mathbb{Z}/p^n\mathbb{Z}(j))_n\big);$$

this notion being related to the inverse limit above by the short exact sequence

$$0 \to \varprojlim_n{}^1 \mathrm{H}^r(X_{\text{ét}}, \mathbb{Z}/p^n\mathbb{Z}(j)) \to \mathrm{H}^r_{\text{ét}}(X, \mathbb{Z}_p(j)) \to \varprojlim_n \mathrm{H}^r(\bar{X}, \mathbb{Z}/p^n\mathbb{Z}(j)) \to 0.$$

For instance in the case when $\mathrm{H}^r(X_{\text{ét}}, \mathbb{Z}/p^n\mathbb{Z}(j))$ are finite (e.g. if K is already algebraically closed) $\varprojlim_n{}^1 = 0$, then

$$\mathrm{H}^r_{\text{ét}}(X, \mathbb{Z}_p(j)) = \varprojlim_n \mathrm{H}^r(\bar{X}, \mathbb{Z}/p^n\mathbb{Z}(j))$$

and hence the continuous geometric étale cohomology coincide with the classical one.

Having a description of derived functor, the continuos étale cohomology enjoys more properties of the naive definition as inverse limit even in the non-gemetrical case. For instance there is a Hochshild-Serre spectral sequence (see [Jan88, Rk. 3.5(b)])

$$E_2^{r,s} = \mathrm{H}^r\big(G_K, \mathrm{H}^s_{\text{ét}}(\bar{X}, \mathbb{Z}_p(j))\big) \Longrightarrow \mathrm{H}^{r+s}_{\text{ét}}(X, \mathbb{Z}_p(j)),$$

degenerating at E_2.

Remark 1.2.9. Recently, in [BS15], Bhatt and Scholze have interpreted these continuous étale cohomology modules of Jannsen as classical cohomology functors of sheaves, not on the étale site $X_{\text{ét}}$ on X, but on the pro-étale site $X_{\text{proét}}$.

1.2.4 Homological equivalence and Gothendieck motives

An other important feature of the continuous étale cohomology for us is that it is endowed by a cycle class map (for any $0 \le r \le d$) [see Jan88, Lemma 6.14 and Th. 3.23]

$$\mathrm{cl}_X = \mathrm{cl}_X^r \colon \mathrm{CH}^r(X) \to \mathrm{H}^{2r}_{\text{ét}}(X, \mathbb{Z}_p(r)).$$

Its kernel, denoted by $\mathrm{CH}^r(X)_0$, is called the subgroup of null-homologous codimension-r cycles. A priori it could depend on the prime p chosen, but since K has charachteristic 0 one can argue as in [Nek00, Sec. 1.3] to show that the definition is independent of it.

Hence we define the so called *homological equivalence* $\sim_{\text{hom}}$ over $Z^r(X)$, by letting $\alpha \sim_{\text{hom}} \beta$ if and only if the class of $\alpha - \beta \in \mathrm{CH}^r(X)_0$. The quotient group $\mathrm{CH}^r_{\text{hom}}(X) = \mathrm{CH}^r(X)/\,\mathrm{CH}^r_0(X)$ is called the group of algebraic cycles modulo homological equivalence.

This would be enough in order to define $\mathcal{M}_{\text{hom}}(K)_{\mathbb{Z}}$, in order to have $\mathcal{M}_{\text{hom}}(K)_R$, for R a $\mathbb{Z}_p$-algebra we need a relative version: we define

$$\mathrm{cl}_{X,R} = \mathrm{cl}_X \otimes R \colon \mathrm{CH}^r(X)_R \cong \mathrm{CH}^r(X) \otimes R \to \mathrm{H}^{2r}_{\text{ét}}(X, \mathbb{Z}_p(r)) \otimes R,$$

and sets $\mathrm{CH}^r(X)_{0,R} = \ker(\mathrm{cl}_{X,R})$ and $\mathrm{CH}^r_{\text{hom}}(X)_R = \mathrm{CH}^r(X)_R/\,\mathrm{CH}^r(X)_{0,R}$.

The category of pure Grothendieck motives $\mathcal{M}_{\text{hom}}(K)_R$ is defined, for $\mathrm{char}(K) = 0$, using homological equivalence instead of the rational one: in the definitions of Sec. 1.2.2 one replaces the group of correspondences as defined in Def. 1.2.5 with the following one.

Definition 1.2.10. A correspondence modulo homological equivalence from a variety X to Y of degree r is an element of

$$\mathrm{Corr}^r_{\text{hom}}(X, Y)_R := \mathrm{CH}^{r+d_X}_{\text{hom}}(X \times Y)_R.$$

Definition 1.2.11. Let K a field of charachteristic 0 and R a $\mathbb{Z}_p$-algebra. The category $\mathcal{M}_{\text{hom}}(K)_R$ of pure Grothendieck motives over K with coefficient in R, is the category whose objects are of the form (X, e, i), where

- X is a smooth projective variety defined over K,
- $e = e^2 \in \mathrm{Corr}^0_{\text{hom}}(X, X)_R$ is an idempotent,
- $i \in \mathbb{Z}$ is an integer;

If $(X, e, i), (Y, f, j) \in \mathrm{Ob}\big(\mathcal{M}_{\text{hom}}(K)_R\big)$,

$$\mathrm{Hom}_{\mathcal{M}_{\text{hom}}(K)_R}\big((X, e, i), (Y, f, j)\big) = e \circ \mathrm{Corr}^{i-j}_{\text{hom}}(X, Y)_R \circ f$$

where the composition is given by the product of correspondences.

Remark 1.2.12. Let us remark that in order to define homological equivalence it would be enough to have any Weil cohomology with coefficents in K, the (continuous) étale cohomology being only one of them. Here we have chosen to follow this definition since we will need continuous étale cohomology and its cycle map speaking about the p-adic Abel-Jacobi map in Sec. 2.2.2. An other more classical choice is to use singular cohomology as in [Ful98, Ch. 19]: more precisely his definition is given in terms Borel-More homology (and this explains the name of *homological* equivalence). For the general theory see [And04, Sec. 3.3.4].

1.3 Modular Forms and their Galois Representations

In this section we recall some properties of Galois representations attached to modular forms. The main references are [NP00], [Rib85] and [Rib77].

Let $f = \sum_{n\geq 1} a_n q^n$ be a cusp form of level $\Gamma_0(N)$ and weight $k \geq 2$. Suppose moreover that f is a normalized newform (thus $a_1 = 1$, $T(\ell)f = a_\ell f$ for any rational prime ℓ). Let F be the finite extension of $\mathbb{Q}$ in $\bar{\mathbb{Q}}$ generated over $\mathbb{Q}$ by all the $i_\infty^{-1}(a_n)$'s, called the *Hecke field* of f, and let $\mathcal{O}_F$ be its ring of integers. For any $\mathfrak{p}$ prime of F over p denote by $\mathcal{K}_\mathfrak{p}$ the completion of F at $\mathfrak{p}$, by $\mathcal{O}_\mathfrak{p}$ its ring of integers and, with a slight abuse of notation, denote by $\mathfrak{p}$ also the maximal ideal of $\mathcal{O}_\mathfrak{p}$. Let

$$\rho_{f,p}\colon G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Z}_p) \subseteq \mathrm{GL}_2(F \otimes_\mathbb{Z} \mathbb{Q}_p)$$

denote the (dual of the) continuous representation of $G_\mathbb{Q}$ attached to f by Deligne in [Del71], that is unramified outside the finte set of rational primes $S = \{\, \ell \text{ prime} : \ell \nmid pN \,\} \cup \{\, \infty \,\}$ and characterized by the conditions

$$\mathrm{Tr}\left(\rho_{f,p}(\mathrm{Frob}_\ell)\right) = i_\infty^{-1}(a_\ell) \otimes 1, \quad \det\left(\rho_{f,p}(\mathrm{Frob}_\ell)\right) = \ell^{k-1} \otimes 1,$$

for any prime $\ell \neq p$ and where Frob_ℓ is an arithmetic Frobenius. The decompositions

$$\mathcal{O}_F \otimes_\mathbb{Z} \mathbb{Z}_p \cong \prod_{\mathfrak{p}|p} \mathcal{O}_\mathfrak{p}, \qquad F \otimes_\mathbb{Z} \mathbb{Q}_p \cong \prod_{\mathfrak{p}|p} \mathcal{K}_\mathfrak{p}$$

given by the map $x \otimes \alpha \mapsto \left(i_p(x)\alpha\right)_{\mathfrak{p}|p}$, induce a decomposition of $\rho_{f,p}$ into the direct sum of the representations

$$\rho_{f,\mathfrak{p}}\colon G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_\mathfrak{p}) \subseteq \mathrm{GL}_2(\mathcal{K}_\mathfrak{p}),$$

for all primes $\mathfrak{p} \mid p$. For any such a prime $\mathfrak{p}$, $\rho_{f,\mathfrak{p}}$ is unramified outside S, irreducible by a result of Ribet [Rib77, Th. 2.3] and characterized by the conditions

$$\mathrm{Tr}\left(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)\right) = i_p \circ i_\infty^{-1}(a_\ell), \quad \det\left(\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)\right) = \ell^{k-1},$$

for any prime $\ell \neq p$. Ribet ([Rib77, Prop.. 2.2]) proves moreover that for any $\sigma \in G_\mathbb{Q}$

$$\det \rho_{f,\mathfrak{p}}(\sigma) = \chi_p^{k-1}(\sigma).$$

1.3.1 $\mathfrak{p}$-ordinary modular forms

From now on let $\mathfrak{p}$ denote the prime of F induced by the chosen embedding $i_p\colon \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, and write $\mathcal{O} = \mathcal{O}_\mathfrak{p}$, $\mathcal{K} = \mathcal{K}_\mathfrak{p}$. We denote the representation space of $\rho_{f,\mathfrak{p}}$ by $V_\mathfrak{p}$. The choice of i_p identifies $G_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ with a decomposition group of $G_\mathbb{Q}$ at p, denote by I_p its inertia subgroup and choose a Frobenius automorphism $\mathrm{Frob}_p \in G_p$. We omit moreover i_∞^{-1} from the notations: for instance we write just $i_p(a_n)$ in place of $i_p \circ i_\infty^{-1}(a_n)$.

Definition 1.3.1. We say that f as above is ordinary at $\mathfrak{p}$ (or $\mathfrak{p}$-ordinary) if $i_p(a_p) \in \mathcal{O}^\times$.

By a result of Wiles ([Wil88, Th. 2.2.2]), in the $\mathfrak{p}$-ordinary case $\rho_{f,\mathfrak{p}|G_p}$ is reducible, as a representation of G_p, and more precisely it is equivalent to a representation of the form

$$\begin{pmatrix} \varepsilon_1 & * \\ 0 & \varepsilon_2 \end{pmatrix},$$

where ε_2 is the unramified character of G_p (i.e. $\varepsilon_2(I_p) = \{\, 1 \,\}$) such that $\varepsilon_2(\mathrm{Frob}_p) = \alpha$, for $\alpha \in \mathcal{O}^\times$ the invertible root of the polynomial $X^2 - i_p(a_p)X + p^{k-1} = 0$ (which exists since f is $\mathfrak{p}$-ordinary).

REMARK 1.3.2. Note that ε_2 is well defined, in fact if ε_2 is unramified and $\varepsilon_2(\mathrm{Frob}_p) = \alpha$, then $\varepsilon_2(\varphi_p) = \alpha$ for any other Frobenius φ_p in G_p (as it differ from Frob_p by some $\sigma \in I_p$).

REMARK 1.3.3. Note that this result endows $V_\mathfrak{p}$ with a $\mathcal{K}[G_p]$-submodule $V_\mathfrak{p}^1$ of dimension 1 over $\mathcal{K}$ such that G_p acts on $V_\mathfrak{p}^1$ as ε_1 and on $V_\mathfrak{p}/V_\mathfrak{p}^1$ as ε_2. In particular it follows that $V_\mathfrak{p}$ is a Galois representation ordinary at p in the sense of [Gre91] with filtration $0 \subsetneq F^1V_\mathfrak{p} = V_\mathfrak{p}^1 \subsetneq F^0V_\mathfrak{p} = V_\mathfrak{p}$, since $V_\mathfrak{p}/V_\mathfrak{p}^1$ is unramified.

1.3.2 Scholl motive

We now review the definition of the motive $\mathcal{M}_f$ attached to a modular form f by Scholl in [Sch90], whose p-adic étale realisation, localized at $\mathfrak{p}$, is the dual of $V_\mathfrak{p}$. All the previous notation are in force and we assume $k > 2$. Let $\Gamma = \Gamma(N), \Gamma_0(N), \Gamma_1(N)$ and let $Y(\Gamma)$ (resp. $X(\Gamma)$) be the open (resp. closed) modular curve with Γ-level structure, considered as a $\mathbb{Q}$-scheme (for N big enough). Denote by $\pi_\Gamma \colon \mathcal{E}_\Gamma \to Y(\Gamma)$ (resp. $\bar{\pi}_\Gamma \colon \bar{\mathcal{E}}_\Gamma \to X(\Gamma)$) the universal elliptic curve (resp. universal generalized elliptic curve) of level structure Γ.

Definition 1.3.4. We call Kuga-Sato variety of level Γ and weight k, denoted by $\tilde{\mathcal{E}}_\Gamma^{k-2}$, the canonical desingularization of the $(k-2)$-fold fibre product

$$\underbrace{\bar{\mathcal{E}}_\Gamma \times_{X(\Gamma)} \cdots \times_{X_1(\Gamma)} \bar{\mathcal{E}}_\Gamma}_{k-2 \text{ times}}$$

over $X(\Gamma)$ of the universal generalized elliptic curve $\bar{\mathcal{E}}_\Gamma$, constructed by Deligne in the case of $\Gamma = \Gamma(N)$. See [BDP13, Appendix] for the general construction.

We define an idempotent $\prod_\varepsilon$ in $\mathrm{Corr}^0(\tilde{\mathcal{E}}_{\Gamma(N)}^{k-2}, \tilde{\mathcal{E}}_{\Gamma(N)}^{k-2})$. Consider the group

$$\Gamma_{k-2} := \left((\mathbb{Z}/N\mathbb{Z})^2 \rtimes \{\pm 1\}\right)^{k-2} \rtimes S_{k-2},$$

where S_{k-2} denotes the symmetric group on $k-2$ letters, Γ_{k-2} acts on $\tilde{\mathcal{E}}_{\Gamma(N)}^{k-2}$ in the following way: $(\mathbb{Z}/n\mathbb{Z})^2$ acts by translation on $\bar{\mathcal{E}}_{\Gamma(N)}$ (where the translation is given by the level-N structure on $\bar{\mathcal{E}}_{\Gamma(N)}$), moreover -1 acts on $\bar{\mathcal{E}}$ by inversion on the fibers and hence we get an action of $\left((\mathbb{Z}/N\mathbb{Z})^2 \rtimes \{\pm 1\}\right)^{k-2}$ on $\bar{\mathcal{E}}_{\Gamma(N)}^{k-2}$. Finally S_{k-2} permutes the factors of $\bar{\mathcal{E}}_{\Gamma(N)}^{k-2}$; we get in this way an action of Γ_{k-2} on $\bar{\mathcal{E}}_{\Gamma(N)}^{k-2}$ and hence, by the properties of the canonical desingularization, also on $\tilde{\mathcal{E}}_{\Gamma(N)}^{k-2}$.

We consider moreover the homomorphism $\varepsilon \colon \Gamma_{k-2} \to \pm 1$ that is trivial on $(\mathbb{Z}/N\mathbb{Z})^{2(k-2)}$, the product map on $(\{\pm 1\})^{k-2}$ and the sign character on S_{k-2}, let $\prod_\varepsilon$ be its attached projector

$$\prod_\varepsilon = \frac{1}{(2N)^{k-2}(k-2)!} \sum_{\gamma \in \Gamma_{k-2}} \varepsilon(\gamma)\gamma \in \mathbb{Z}\left[\frac{1}{2N(k-2)!}\right][\Gamma_{k-2}].$$

Viewing the action of γ as an automorphim of $\tilde{\mathcal{E}}_{\Gamma(N)}^{k-2}$ and taking its graph, then we may see $\prod_\varepsilon$ as a degree 0 correspondence on $\tilde{\mathcal{E}}_{\Gamma(N)}^{k-2}$. Its p-adic étale realisation corresponds to the action of $\prod_\varepsilon$ induced on the étale cohomology by the action of Γ_{k-2} on $\tilde{\mathcal{E}}_{\Gamma(N)}^{k-2}$.

Definition 1.3.5. We call the Chow motive

$$\mathcal{M}_k(N) := \left(\tilde{\mathcal{E}}_{\Gamma(N)}^{k-2}, \prod_\varepsilon\right) \in \mathcal{M}_{\mathrm{rat}}(\mathbb{Q})$$

the motive of modular forms of weight k and level N.

Scholl shows in particular that its p-adic étale realisation is a parabolic cohomology group: let $j\colon Y(N) \hookrightarrow X(N)$ be the canonical embedding of the open into the compact modualr curve, as $\mathbb{Q}$-schemes, and denote by $\pi := \pi_{\Gamma(N)}\colon \mathcal{E}_N := \mathcal{E}_{\Gamma(N)} \to Y(N)$ the universal elliptic curve with level-N structure and $\mathcal{F}_{\mathbb{Q}_p}$ the p-adic sheaf over $Y(N)$ given by

$$\mathcal{F}_n := \mathrm{Sym}^{k-2}\big(R^1\pi_*(\mathbb{Z}/p^n\mathbb{Z})\big), \qquad \mathcal{F} = (\mathcal{F}_n)_n, \qquad \mathcal{F}_{\mathbb{Q}_p} = \mathcal{F} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Theorem 1.3.6 ([Sch90, Th. 1.2.1])**.**

$$\mathrm{H}^1_{\text{ét}}\big(X(N)_{\bar{\mathbb{Q}}}, j_*\mathcal{F}_{\mathbb{Q}_p}\big) = \prod_{\varepsilon} \mathrm{H}^{k-1}_{\text{ét}}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)} \otimes \bar{\mathbb{Q}}, \mathbb{Q}_p).$$

In $\mathcal{M}_{\mathrm{hom}}(\mathbb{Q})_{\mathfrak{h}_k(N)}$ the motive $\mathcal{M}_k(N)$ decomposes and we have a projector Ψ_f assocated with the modular form f. Its kernel is defined to be the motive $\mathcal{M}_f \in \mathcal{M}_{\mathrm{hom}}(\mathbb{Q})_F$ attached to f. In particular Scholl proves [Sch90, Th. 1.2.4] that the p-adic étale realisation of $\mathcal{M}_f$, i.e.

$$M_p \subseteq \mathrm{H}^{k-1}_{\text{ét}}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}, \mathbb{Q}_p),$$

is free of rank 2 over $F \otimes \mathbb{Q}_p$ and its localization $M_{\mathfrak{p}} = M_p \otimes_{F\otimes\mathbb{Q}_p} F_{\mathfrak{p}}$ at $\mathfrak{p}$ is, as $G_{\mathbb{Q}}$-representation, unramified at primes $\ell \nmid Np$ and the characteristic polynomial of the geometric Frobenius Frob_ℓ at ℓ (that is the inverse of the arithmetic Frobenius Frob_ℓ) is

$$\mathrm{char}(\mathrm{Frob}^{\mathrm{geo}}_\ell \,|M_{\mathfrak{p}})(X) = X^2 - i_p(a_\ell)X + \ell^{k-1}.$$

It follows that $M_{\mathfrak{p}}$ is the representation $\rho'_{f,\mathfrak{p}}$ dual to $\rho_{f,\mathfrak{p}}$: the representation space of $\rho'_{f,\mathfrak{p}}$ is by definition $W_{\mathfrak{p}} = \mathrm{Hom}_{\mathbb{Q}_p}(V_{\mathfrak{p}}, \mathbb{Q}_p)$ and it is endowed with the action $\sigma \cdot w(v) = w(\sigma^{-1}v)$ for any $\sigma \in G_{\mathbb{Q}}$, $w \in W_{\mathfrak{p}}$, $v \in V_{\mathfrak{p}}$. Indeed similarly to $V_{\mathfrak{p}}$, also $W_{\mathfrak{p}}$ is unramified outside $S = \{\, \ell \text{ prime} : \ell \nmid pN \,\} \cup \{\, \infty \,\}$, irreducible and characterized by the conditions

$$\mathrm{Tr}\left(\rho'_{f,\mathfrak{p}}(\mathrm{Frob}^{\mathrm{geo}}_\ell)\right) = i_p(a_\ell), \quad \det\left(\rho'_{f,\mathfrak{p}}(\mathrm{Frob}^{\mathrm{geo}}_\ell)\right) = \ell^{k-1},$$

for any prime $\ell \neq pN$ (and hence $M_{\mathfrak{p}}$ coincides with $W_{\mathfrak{p}}$). Moreover one has that for any $\sigma \in G_{\mathbb{Q}}$

$$\det \rho'_{f,\mathfrak{p}}(\sigma) = \chi_p^{1-k}(\sigma).$$

These properties follows as $\rho'_{f,\mathfrak{p}}(\mathrm{Frob}^{\mathrm{geo}}_\ell) = {}^t\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)$ and more generally one proves that $\rho'_{f,\mathfrak{p}}(\sigma) = {}^t\rho_{f,\mathfrak{p}}(\sigma)^{-1}$, where ${}^t*$ denotes the transposed matrix. Indeed for any $w \in W_{\mathfrak{p}}$, $v \in V_{\mathfrak{p}}$,

$$\big(\rho'_{f,\mathfrak{p}}(\sigma)w\big)(v) = (\sigma \cdot w)(v) = w(\sigma^{-1} \cdot v) = w\big(\rho_{f,\mathfrak{p}}(\sigma)^{-1}v\big)$$

hence if $\rho_{f,\mathfrak{p}}(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, then

$$\rho'_{f,\mathfrak{p}}(\sigma)e_1^* = e_1^* \circ \rho_{f,\mathfrak{p}}(\sigma)^{-1} = (1,0) \circ \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}(d,-b),$$
$$\rho'_{f,\mathfrak{p}}(\sigma)e_2^* = e_2^* \circ \rho_{f,\mathfrak{p}}(\sigma)^{-1} = (0,1) \circ \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \frac{1}{ad-bc}(-c,a)$$

and therefore

$$\rho'_{f,\mathfrak{p}}(\sigma) = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = {}^t\rho_{f,\mathfrak{p}}(\sigma)^{-1}.$$

1.3.3 Self-dual twist

Consider, for k even, $V = W_{\mathfrak{p}}(k/2) = M_{\mathfrak{p}}(k/2)$, which we call the *self-dual twist* of $W_{\mathfrak{p}}$ and suppose that $p \nmid 2N\varphi(N)(k-2)!$, where $\varphi(N)$ denotes the Euler's function. In [Nek92] Nekovar defines a lattice T inside V as follows.

Let $B = \Gamma_0(N)/\Gamma(N)$, (that has order $N\varphi(N)$) and $\prod_B$ the idempotent

$$\prod\nolimits_B = \frac{1}{N\varphi(N)} \sum_{b \in B} b \in \mathbb{Z}\left[\frac{1}{N\varphi(N)}\right][B].$$

Note that B is the Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and hence it acts on the parabolic cohomology group $\mathrm{H}^1_{\text{ét}}\big(X(N)_{\bar{\mathbb{Q}}}, j^*\mathcal{F}\big)$, where $\mathcal{F} = (\mathcal{F}_n)$ is the ℓ-adic sheaf given by

$$\mathcal{F}_n := \mathrm{Sym}^{k-2}\big(R^1\pi_*(\mathbb{Z}/p^n\mathbb{Z})\big)$$

as in the previous section. The same proof of 1.3.6 shows that

$$\mathrm{H}^1_{\text{ét}}\big(X(N)_{\bar{\mathbb{Q}}}, j_*\mathcal{F}\big) = \prod\nolimits_{\varepsilon} \mathrm{H}^{k-1}_{\text{ét}}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_p).$$

Let

$$J = \prod\nolimits_B \mathrm{H}^1_{\text{ét}}\big(X(N)_{\bar{\mathbb{Q}}}, j^*\mathcal{F}\big)(k/2)$$

Scholl [Sch90, Sec. 4] also define a geometrical action of the Hecke operators T_ℓ, for $\ell \nmid N$, as linear endomorphisms of $\mathrm{H}^{k-1}_{\text{ét}}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)} \otimes \bar{\mathbb{Q}}, \mathbb{Q}_\ell)$: let $Y(N,\ell)/\mathbb{Q}$ be the modular curve classifying elliptic curves with a level-N structure and a subgroup $C \subseteq E$ of order ℓ. The fibre product $\mathcal{E}_{N,\ell} = \mathcal{E}_N \times_{Y(N)} Y(N,\ell)$ is the universal elliptic curve with a level-N structure and a subgroup $C \subseteq E$ of order ℓ. Let Q be the quotient of $\mathcal{E}_{N,\ell}$ by C. We get a diagram

$$\begin{array}{ccccccc}
\mathcal{E}^{k-2}_N & \xleftarrow{\varphi_1} & \mathcal{E}^{k-2}_{N,\ell} & \xrightarrow{\psi} & Q^{k-2} & \xrightarrow{\varphi_2} & \mathcal{E}^{k-2}_N \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
Y(N) & \longleftarrow & Y(N,\ell) & = & Y(N,\ell) & \longrightarrow & Y(N)
\end{array}$$

and we define the Hecke correspondence on $\mathcal{E}^{k-2}_N$ by $T_\ell = \varphi_{1*}\psi^*\varphi_2^*$. The closure of its graph in $\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)} \times \tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}$, still denoted by T_ℓ, is the Hecke correspondence on $\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}$, inducing endomorphisms on $\mathrm{H}^{k-1}_{\text{ét}}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)} \otimes \bar{\mathbb{Q}}, \mathbb{Q}_\ell)$ and hence on $\mathrm{H}^1_{\text{ét}}\big(X(N)_{\bar{\mathbb{Q}}}, j^*\mathcal{F}\big)$ and on J. Let $\mathbb{T}_N$ be the Hecke algebra generated over $\mathbb{Z}$ by these operators and let

$$\vartheta_f : \mathbb{T}_N \to \mathcal{O}_F$$

defined by $T_\ell \mapsto a_\ell$ and let $I_f = \ker(\vartheta_f)$. Consider the $(\mathcal{O}_F \otimes \mathbb{Z}_p)$-module

$$J_{f,p} = \{\, x \in J : I_f \cdot x = 0 \,\},$$

$T := J_{f,\mathfrak{p}} := J_{f,p} \otimes_{\mathcal{O}_F \otimes \mathbb{Z}_p} \mathcal{O}_{\mathfrak{p}}$ is the lattice T inside V we looked for. From the Poincaré duality for étale cohomology Nekovar [see Nek92, Prop. 3.1(2)] constructs a $G_{\mathbb{Q}}$-equivariant and skew-symmetric pairing

$$[-,-] : : J_{f,p} \times J_{f,p} \to \mathbb{Z}_p(1)$$

over $J_{f,p}$, such that $[\lambda x, y] = [x, \lambda y]$ for any $x, y \in L_{f,\mathfrak{p}}$, $\lambda \in \mathcal{O}_F \otimes \mathbb{Z}_p$. Tensoring it with $\mathcal{O}$ (resp. $\mathcal{K}$), we see that T (resp. V) is equipped with a $G_{\mathbb{Q}}$-equivariant, skew-symmetric, non degenerate $\mathcal{O}$-linerar (resp. $\mathcal{K}$-linear) pairing $T \times T \to \mathcal{O}(1)$ (resp. $V \times V \to \mathbb{Q}_p(1)$). It follows that the map $j\colon V \xrightarrow{\sim} V^*(1)$, given by $v \mapsto (v, -)$, where $V^* = \mathrm{Hom}_{\mathbb{Q}_p}(V, \mathbb{Q}_p)$ is the linear dual of V, is an isomorphism such that $j^*(1) = -j$, where $j^*(1)$ denote the transposed of the linear map j, seen as an equivariant map

$$V \cong \big(V^*(1)\big)^*(1) \xrightarrow{\sim} V^*(1).$$

In fact, if ε_v denote the image of $v \in V$ via the canonical isomorphism $V \cong V^{**}$, for any $v, w \in V$

$$j^*(\varepsilon_v)(w) = \varepsilon_v\big(j(w)\big) = \big(j(w)\big)(v) = (w, v) = -(v, w) = -\big(j(v)\big)(w).$$

Moreover $j(T) \subseteq T^*(1)$, where $T^* = \mathrm{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$ is the $\mathbb{Z}_p$-linear dual of T.

The isomorphism $V \cong V^*(1)$ explains the name for V of *self-dual* twist, the representation $V^*(1)$ being called the *Kummer dual* of V.

REMARK 1.3.7. Let us remark for later reference that by the calculations performed in Sec. 1.3.2 follows that the characteristic polynomial of Frob_ℓ over T for any $\ell \neq p$ is

$$\mathrm{char}(\mathrm{Frob}_\ell\,|T) = X^2 - \frac{i_p(a_\ell)}{\ell^{k/2-1}}X + \ell.$$

Indeed the action of $\sigma \in G_{\mathbb{Q}}$ on T is given by the matrix $\chi_\ell(\sigma)^{k/2} \cdot {}^t\rho_{f,\mathfrak{p}}(\sigma)^{-1}$, hence the action of Frob_ℓ is given by $\ell^{k/2} \cdot {}^t\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell)^{-1}$: its trace is $i_p(a_\ell)/\ell^{k/2-1}$ and its determinant is ℓ.

REMARK 1.3.8. If f is $\mathfrak{p}$-ordinary, then by the results of Sec. 1.3.1 and recalling the relation $\rho'_{f,\mathfrak{p}}(\sigma) = {}^t\rho_{f,\mathfrak{p}}(\sigma)^{-1}$, $\rho'_{f,\mathfrak{p}|G_p}$ is equivalent to a representation of the form

$$\begin{pmatrix} \varepsilon_1^1 & 0 \\ * & \varepsilon_2^{-1} \end{pmatrix},$$

whith $\varepsilon_1, \varepsilon_2$ as above. Conjugating then by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, we see that $\rho'_{f,\mathfrak{p}|G_p}$ is moreover equivalent to a representation of the form

$$\begin{pmatrix} \varepsilon_2^{-1} & * \\ 0 & \varepsilon_1^{-1} \end{pmatrix} = \begin{pmatrix} \delta & * \\ 0 & \delta^{-1}\chi_p^{1-k} \end{pmatrix},$$

denoting ε_2^{-1} by δ, since $\varepsilon_1\varepsilon_2 = \chi_p^{k-1}$. Twisting by the $k/2$-th power of the cyclotomic character $\chi_p\colon G_p \to \mathbb{Z}_p^\times$ it follows that $\rho_{V|G_p}$ is equivalent to a representation of the form

$$\begin{pmatrix} \delta\chi_p^{k/2} & * \\ 0 & \delta^{-1}\chi_p^{1-k/2} \end{pmatrix}.$$

We find therefore an exact sequence of $\mathcal{K}[G_p]$-modules

$$0 \to V^+ \to V \to V^- \to 0,$$

where $V^\pm$ has dimension 1 over $\mathcal{K}$, G_p acts on V^+ as $\delta\chi_p^{k/2}$ and on V^- as $\delta^{-1}\chi_p^{1-k/2}$.

1.4 The Anticyclotomic Extension

The main purpose of this thesis is to describe the generalization of some results of Iwasawa Theory of elliptic curves over the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field. In this section we introduce this extension.

Definition 1.4.1. Let K be an imaginary quadratic field of discriminant d, i.e. $K = \mathbb{Q}[\sqrt{-d}]$, and p an odd prime number. The anticyclotomic $\mathbb{Z}_p$-extension of K is the unique Galois extension K_∞ of K with Galois group $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ pro-dihedral over $\mathbb{Q}$, meaning that

$$\mathrm{Gal}(K_\infty/\mathbb{Q}) \cong \mathrm{Gal}(K_\infty/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}),$$

where the complex conjugation $\tau \in \mathrm{Gal}(K/\mathbb{Q}) = \{1, \tau\}$ acts by inversion, that is $\tau g \tau^{-1} = g^{-1}$ for any $g \in \mathrm{Gal}(K_\infty/K)$.

The existence and uniqueness follow from the following theorem ([Bri07, Lemma 1]).

Theorem 1.4.2. *Let L be the maximal abelian extension unramified outside $p > 2$. We may write*

$$\mathrm{Gal}(L/K) = U \times W \times T \times T',$$

such that $U, W \cong \mathbb{Z}_p$, T finite p-group, T' finite of order prime to p. Moreover τ operates trivially on U and by inversion on W and U. This decomposition is the unique with these properties.

In fact it follows immediately that K_∞ is the fixed field of $W \times T \times T'$ and that the fixed field of $U \times T \times T'$ is the cyclotomic extension. These two extensions are linearly disjoint, i.e. their compositum has Galois group $\mathbb{Z}_p^2$, moreover it contains all the other $\mathbb{Z}_p$-extensions of K.

However there is a more explicit way to construct K_∞ using class field theory. This is the aim of the following discussion.

1.4.1 Construction via ring class fields

First we briefly recall the definition and some properties of orders in quadratic fields and of the ring class fields. The following material is taken from [Cox89, Ch. 2]. Let K denote a quadratic field of discriminant d. Note that we may write its ring of integers as

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d+\sqrt{d}}{2}\right] = \langle 1, w \rangle_{\mathbb{Z}}; \qquad w = \frac{d+\sqrt{d}}{2}.$$

Definition 1.4.3. An order $\mathcal{O}$ in a quadratic field K is a subring of K containing 1 finitely generated as $\mathbb{Z}$-module and containing a $\mathbb{Q}$-basis of K. Equivalently it is a subring containing 1, free of rank 2 as $\mathbb{Z}$-module.

In particular $\mathcal{O}_K$ is an order of K and it is the maximal order, in the sense that it contains any other order $\mathcal{O}$. It follows easily [Cox89, Lemma 7.2] that the index of $\mathcal{O}$ in $\mathcal{O}_K$ is finite, say $f = [\mathcal{O}_K : \mathcal{O}]$, and $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \langle 1, fw \rangle_{\mathbb{Z}}$, and hence $\mathcal{O}$ is uniquely determined by f. We call f the conductor of $\mathcal{O}$ and we denote the unique order of conductor f as $\mathcal{O}_f$.

Note that $\mathcal{O}_1 = \mathcal{O}_K$ and as $\mathcal{O}_K$ an order $\mathcal{O}_f$ is a noetherian ring of dimension 1 (the same proof holds), but it is of course no more integrally closed in K (that is by the definition its field of fractions), unless $f = 1$. Therefore $\mathcal{O}_f$ for $f > 1$ is not a Dedekind domain and we do not have anymore unique factorization of ideals. There is however an interesting class of (fractional) ideals of $\mathcal{O}_f$, called proper ideals, namely those ideals $\mathfrak{a}$ of $\mathcal{O}_f$ such that $\mathcal{O}_f = \{\beta \in K : \beta\mathfrak{a} \subseteq \mathfrak{a}\}$ (for general ideals we have only $\subseteq$). The interesting feature of them is encoded in the following lemma.

Lemma 1.4.4 ([Cox89, Prop. 7.4]). *Let $\mathcal{O}_f$ be a an order in an imaginary quadratic field K and let $\mathfrak{a}$ a fractional ideal of $\mathcal{O}_f$. Then $\mathfrak{a}$ is proper if and only if it is invertible.*

We may therefore define $\mathrm{Pic}(\mathcal{O}_f)$, the class group of the order $\mathcal{O}_f$, to be the group of proper fractional ideals modulo principal fractional ideals. We denote by h_f the order of $\mathrm{Pic}(\mathcal{O}_f)$. Of course $\mathrm{Pic}(\mathcal{O}_1) = \mathrm{Pic}(\mathcal{O}_K)$ is the usual class group of K and $h_1 = h_K$ is the class number of K. The following formula allow us to compute the class number of an order in terms of its conductor f and the class number of K when K is imaginary.

Theorem 1.4.5. *Let $\mathcal{O}_f$ the the order of the conductor f in an imaginary quadratic field K. Then*

$$h_f = \frac{h_K\, f}{[\mathcal{O}_K^\times : \mathcal{O}_f^\times]} \prod_{p|f} \left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right).$$

Above the symbol $\left(\frac{d}{p}\right)$ denotes the classical Legendre symbol for an odd prime p and for $p = 2$ is the Kronecker symbol:

$$\left(\frac{d}{p}\right) = \begin{cases} 0 & \text{if } 2 \mid d, \\ 1 & \text{if } d \equiv 1 \mod 8, \\ -1 & \text{if } d \equiv 5 \mod 8. \end{cases}$$

Note moreover that by the description of units in imaginary quadratic fields $\mathcal{O}_f^\times = \{\pm 1\}$ unless $f = 1$ and hence

$$[\mathcal{O}_K^\times : \mathcal{O}_f^\times] = \begin{cases} u_K := |\mathcal{O}_K^\times|/2 & \text{if } f \neq 1, \\ 1 & \text{if } f = 1. \end{cases}$$

The ring class field $K[f]$ of conductor f is defined to be the (unique) abelian extension that corresponds via class field theory to $\mathrm{Pic}(\mathcal{O}_f)$, i.e. it is characterized by $\mathrm{Gal}(K[f]/K) \cong \mathrm{Pic}(\mathcal{O}_f)$. Note that $K[1]$ is the Hilbert class field, that is the maximal abelian extension of K everywhere unramified; in general $K[f]/K$ is unramified at primes $\mathfrak{p} \nmid f$. Moreover the ring class fields are generalized dihedral over $\mathbb{Q}$, meanig that $\mathrm{Gal}(K[f]/\mathbb{Q}) = \mathrm{Gal}(K[f]/K) \rtimes \{1, \tau\}$, where τ is the complex conjugation and acts on $\mathrm{Gal}(K[f]/K)$ by inversion, i.e. $\tau\sigma\tau^{-1} = \sigma^{-1}$ for any $\sigma \in \mathrm{Gal}(K[f]/K)$.

We pass now to the explicit contruction of the anticyclotomic extension of K.

Lemma 1.4.6 ([Bri07, Lemma 3]). *Let $p \neq 2$ and $n \geq 0$. The group of units of $\mathcal{O}_K/p^{n+1}\mathcal{O}_K$ decomposes as $(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)^\times = U \times V \times S'$, where*

- *the complex conjugation τ operates trivially on U that is cyclic of order p^n;*
- *the complex conjugation τ operates by inversion on V, and*

$$V \cong \begin{cases} \mathbb{Z}/p^n\mathbb{Z} & \text{if } p \nmid d, \\ \mathbb{Z}/p^{n+1}\mathbb{Z} & \text{if } p \mid d, \text{ unless } p = 3 \text{ and } d \equiv 3 \bmod 9, \\ \mathbb{Z}/3^n\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } p = 3 \text{ and } d \equiv 3 \bmod 9. \end{cases}$$

- *S' is the non-p-part of $(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)^\times$ and has order*

$$|S'| = \begin{cases} (p-1)^2 & \text{if } \left(\frac{d}{p}\right) = 1, \\ p^2 - 1 & \text{if } \left(\frac{d}{p}\right) = -1, \\ p - 1 & \text{if } \left(\frac{d}{p}\right) = 0. \end{cases}$$

Moreover there is a subgroup S'' of S' of order $p - 1$ such that $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = U \times S''$ as subgroup of $(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)^\times$.

Consider the tower of field extension, for any prime p,

$$K \hookrightarrow K[1] \hookrightarrow K[p] \hookrightarrow K[p^2] \hookrightarrow \ldots \hookrightarrow K[p^n] \hookrightarrow \ldots \hookrightarrow K[p^\infty] = \bigcup_n K[p^n],$$

it has the following properties

- For any $n \geq 1$, $\mathrm{Gal}(K[p^{n+1}]/K[p^n]) \cong \mathbb{Z}/p\mathbb{Z}$.

  In fact $\mathrm{Gal}(K[p^n]/K) = \frac{\mathrm{Gal}(K[p^{n+1}]/K)}{\mathrm{Gal}(K[p^{n+1}]/K[p^n])}$ and

  $$h_{p^{n+1}}/h_{p^n} = \frac{h_K\, p^{n+1}}{u_K}\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right) \Big/ \frac{h_K\, p^n}{u_K}\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right) = p;$$

- If $p > 3$, then $\mathrm{Gal}(K[p^{n+1}]/K[p])$ is cyclic of order p^n.

  The order of this Galois group is clear:

  $$h_{p^{n+1}}/h_p = \frac{h_K\, p^{n+1}}{u_K}\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right) \Big/ \frac{h_K\, p}{u_K}\left(1 - \left(\frac{d}{p}\right)\frac{1}{p}\right) = p^n.$$

  Let us prove that it is cyclic. Assume for simplicity that $u_K = 1$, in this case by class field theory and Lemma 1.4.6 (as $p \neq 2$)

  $$\mathrm{Gal}(K[p^{n+1}]/K[1]) \cong \frac{(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)^\times}{(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} = V \times (S'/S'').$$

  First consider the case of p ramified in K, hence $|S'| = p - 1$ and $V \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$ and therefore $\mathrm{Gal}(K[p^{n+1}]/K[1]) \cong V \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$. Thus $\mathrm{Gal}(K[p^{n+1}]/K[p])$ is cyclic because it is subgroup of a cyclic group. If instead p does not ramify $|V| = p^n$, $|S''/S'| = p \mp 1$, depending whether $\left(\frac{d}{p}\right) = 1$ or -1, and therefore $\mathrm{Gal}(K[p^{n+1}]/K[p]) = V \cong \mathbb{Z}/p^n\mathbb{Z}$.

  If $u_K > 1$ we have to consider the full exact sequence

  $$1 \to \mathcal{O}_K^\times/\mathbb{Z}^\times \to \frac{(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)^\times}{(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times} \to \mathrm{Gal}(K[p^{n+1}]/K) \to \mathrm{Gal}(K[1]/K) \to 1$$

  hence $\mathrm{Gal}(K[p^{n+1}]/K[1]) \cong \frac{(\mathcal{O}_K/p^{n+1}\mathcal{O}_K)^\times}{(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times}/(\mathcal{O}_K^\times/\mathbb{Z}^\times)$. In particular it follows that

  $$\mathrm{Gal}(K[p^{n+1}]/K[1]) \cong V \times (S''/S')/(\mathcal{O}_K^\times/\mathbb{Z}^\times),$$

  as $p > 3$ and hence $u_K = 2, 3$ prime to $|V|$, that is power of p. The rest is similar as above.

- If $p > 3$, then $\mathrm{Gal}(K[p^\infty]/K[p]) \cong \varprojlim_n \mathrm{Gal}(K[p^{n+1}]/K[p]) \cong \mathbb{Z}_p$.
- $\mathrm{Gal}(K[1]/K)$ has order h_k;
- $\mathrm{Gal}(K[p]/K[1])$ has order $u_K^{-1}\left(p - \left(\frac{d}{p}\right)\right)$.

Remark 1.4.7. Suppose now that $p \nmid h_K$ and that $p > 3$ is not ramified in K (i.e. $\left(\frac{d}{p}\right) \neq 0$), it follows that the abelian extensions $\mathrm{Gal}(K[p^{n+1}]/K)$ admit canonical (and compatible) splittings

$$\mathrm{Gal}(K[p^{n+1}]/K) \cong \mathrm{Gal}(K[p^{n+1}]/K[p]) \times \mathrm{Gal}(K[p]/K) \cong \mathbb{Z}/p^n\mathbb{Z} \times \Delta,$$

where Δ has order prime to p. Therefore

$$\mathrm{Gal}(K[p^\infty]/K) \cong \mathrm{Gal}(K[p^\infty]/K[p]) \times \mathrm{Gal}(K[p]/K) \cong \mathbb{Z}_p \times \Delta.$$

Hence $K_\infty = (K[p^\infty])^\Delta$ is a $\mathbb{Z}_p$-extension of K, dihedral over $\mathbb{Q}$ since any $K[p^n]$ is so. Hence K_∞ is the anticyclotomic extension of K introduced in the previous paragraph.

1.4.2 Selmer groups over K_∞

In the following denote $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ and let K_n, for $n \geq 1$, be the unique subextension of K_∞/K such that $\Gamma_n = \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$. Denote by $\Lambda_n = \mathcal{O}[\Gamma_n]$ the group algebra of Γ_n and let $\Lambda = \varprojlim_n \Lambda_n = \mathcal{O}[\![\Gamma]\!]$ be the completed group algebra of Γ. It is well known that $\Lambda \cong \mathcal{O}[\![X]\!]$ via the map $\gamma \mapsto 1+X$, where γ is a topological generator of Γ ([NSW00, Prop. 5.3.5]). Write $\Gamma^n = \mathrm{Gal}(K_\infty/K_n) \subseteq \Gamma^0 = \Gamma$.

Let T an $\mathcal{O}$-adic representation of $G_{K,S}$, for a finite set S of primes of $\mathcal{K}$ including all archimedean primes and all primes $v \mid p$, and let $A = T \otimes \mathcal{K}/\mathcal{O}$. Note that $\mathrm{H}^1_f(K_n, A)$ and $\mathrm{H}^1_f(K_n, T)$ inherit for any n the $\mathcal{O}$-module structure by A and T (i.e. if $\alpha\colon G_{K_n} \to X$ represent a class $\bar{\alpha} \in \mathrm{H}^1_f(K_n, X)$ for $X = A, T$, then we define $r \cdot \bar{\alpha}$ as the class of the cochain $r \cdot \alpha$ such that $(r \cdot \alpha)(\sigma) = r\alpha(\sigma)$ for any $r \in \mathcal{O}$, $\sigma \in G_{K_n}$). They are moreover endowed with an action of Γ_n, as follows by the following abstract lemma applied to $G = G_K$, $H = G_{K_n}$ and $X = T, A$ as $\Gamma_n = G_K/G_{K_n}$. Thus $\mathrm{H}^1_f(K_n, A), \mathrm{H}^1_f(K_n, T)$ have a natural structure of Λ_n-module.

Lemma 1.4.8. *Let G be a profinite group. If X is a G-module and H a closed normal subgroup of G, then $\mathrm{H}^1(H, X)$ is endowed with a natural action of G/H.*

Proof. Recall that $\mathrm{H}^1(H, X) \cong \frac{Z^1(H,X)}{B^1(H,X)}$, where the elements of

$$Z^1(H, X) = \{\, \alpha\colon H \to X \text{ s.t. } \alpha(gg') = g \cdot \alpha(g') + \alpha(g') \,\}$$

are called (1-)cocycles and those of

$$B^1(H, X) = \{\, \alpha\colon H \to X \text{ s.t } \alpha(g) = g \cdot a - a \text{ for some } a \in X \,\}$$

are called (1-)coboundaries. Note that if a class in $\mathrm{H}^1(H, X)$ is represented by α, the formula

$$(gH \cdot \alpha)(x) = g \cdot \alpha(g^{-1}xg),$$

for any $x \in H$, defines a cocycle whose class in $\mathrm{H}^1(H, X)$ is independent of the choice of the representative g. In fact if $g' = gh$ for $h \in H$ and we denote by δ and δ' the cocycles defined respectively by $\delta(x) = g\alpha(g^{-1}xg)$ and $\delta'(x) = g'\alpha(g'^{-1}xg')$, then, for any $x \in H$,

$$\delta'(x) = gh \cdot \alpha(h^{-1}g^{-1}xgh) = gh \cdot \alpha(h^{-1}) + \delta(x) + xg \cdot \alpha(h)$$

and the cocycle $x \mapsto gh \cdot \alpha(h^{-1}) + xg \cdot \alpha(h)$ is a coboundary. Indeed for any $x \in H$

$$\begin{aligned} gh\alpha(h^{-1}) + xg\alpha(h) &= xg \cdot \alpha(h) - g \cdot \alpha(h) + g \cdot \alpha(h) - gh \cdot \alpha(h) = \\ &= xg \cdot \alpha(h) - g \cdot \alpha(h) - g \cdot \big(h \cdot \alpha(h) + \alpha(h^{-1})\big) = \\ &= xg \cdot \alpha(h) - g \cdot \alpha(h) - g \cdot \alpha(hh') = \\ &= xg \cdot \alpha(h) - g \cdot \alpha(h) - g \cdot \alpha(1) = \\ &= xg \cdot \alpha(h) - g \cdot \alpha(h). \end{aligned}$$

Thus, $\delta = \delta'$ as classes in $\mathrm{H}^1(H, X)$. It is straightforward to check that the above formula defines an action of G/H on $\mathrm{H}^1(H, X)$. □

Remark 1.4.9. Recall the definition of restriction and corestriction ([NSW00, Ch. II, Sec. 5]).

Let G be a profinite group, X a G-module and H a closed normal subgroup of G. The composition of a cochain with the inclusion of H in G gives a morphism of groups

$$\mathrm{res}^G_H\colon\ \mathrm{H}^1(G, X) \to \mathrm{H}^1(H, X)$$

called restriction. There is moreover another morphism

$$\mathrm{cores}_G^H\colon\ \mathrm{H}^1(H,X)\to\mathrm{H}^1(G,X)$$

in the other direction, called corestriction such that (for H open normal subgroup)

$$\mathrm{res}_G^H\circ\mathrm{cores}_G^H=\mathrm{N}_{G/H}:=\sum_{\sigma\in G/H}\sigma,\qquad \mathrm{cores}_G^H\circ\mathrm{res}_G^H=[G:H]$$

defined as follows: fix a class of representative of right cosets in $H\backslash G$ and for a class $y\in H\backslash G$ denote by $\bar{y}$ the representatives of y in the chosen class; the corestriction of a (1-)cocycle α on H is the (1-)cocycle of G such that, for any $x\in G$,

$$\mathrm{cores}_G^H(\alpha)(x)=\sum_{c\in H\backslash G}\bar{c}^{\,-1}\cdot\alpha\big(\bar{c}x(\overline{cx})^{-1}\big).$$

We will use these maps in the rest with $G=G_{K_n}$, $H=G_{K_m}$, for $n<m$ and we will drop them by the notations, as the correct index is always understood.

Define then

$$\mathrm{H}^1_f(K_\infty,A)=\varinjlim_{n,\mathrm{res}}\mathrm{H}^1_f(K_n,A)\quad\text{and}\quad\mathrm{H}^1_f(K_\infty,T)=\varprojlim_{n,\mathrm{cores}}\mathrm{H}^1_f(K_n,T).$$

Both have naturally a Λ-module structure, that we now describe. Take $r=(r_n)_n\in\Lambda$, with $r_n\in\Lambda_n$, and $x\in\mathrm{H}^1_f(K_\infty,A)$. Let m an integer such that x is represented by $x_m\in\mathrm{H}^1_f(K_m,A)$. We define $r\cdot x$ as the element of $\mathrm{H}^1_f(K_\infty,A)$ represented by $r_m\cdot x_m\in\mathrm{H}^1_f(K_m,A)$. The following lemma shows that this definition is independent of the chosen m.

Lemma 1.4.10. *Let $n<m$ non-negative integers, let $\gamma_n\in\Gamma_n$, $\gamma_m\in\Gamma_m$ such that $\gamma_{m|K_n}=\gamma_n$ and let $x_m\in\mathrm{H}^1_f(K_m,A)$ and $x_n\in\mathrm{H}^1_f(K_n,A)$ such that $\mathrm{res}(x_n)=x_m$. Then*

$$\mathrm{res}(\gamma_n\cdot x_n)=\gamma_m\cdot x_m.$$

Proof. Let $g\in G_K$ extending γ_m and hence γ_n: we may use this g in both the definition of the action of Γ_m on $\mathrm{H}^1_f(K_m,A)$ and of Γ_n on $\mathrm{H}^1_f(K_n,A)$. □

The Λ-module structure of $\mathrm{H}^1_f(K_\infty,T)$ is instead defined as follows: if $r=(r_n)_n\in\Lambda$, with $r_n\in\Lambda_n$ and $x=(x_n)_n\in\mathrm{H}^1_f(K_\infty,T)$, with $x_n\in\mathrm{H}^1_f(K_n,T)$ and $x_n=\mathrm{cores}(x_m)$ for $n<m$. Then $r\cdot x=(r_n\cdot x_n)_n$. It is indeed a compatible sequence by the following lemma.

Lemma 1.4.11. *Let $n<m$ non-negative integers, let $\gamma_n\in\Gamma_n$, $\gamma_m\in\Gamma_m$ such that $\gamma_{m|K_n}=\gamma_n$ and let $x_m\in\mathrm{H}^1_f(K_m,T)$ and $x_n\in\mathrm{H}^1_f(K_n,T)$ such that $x_n=\mathrm{cores}(x_m)$. Then*

$$\gamma_n\cdot x_n=\mathrm{cores}(\gamma_m\cdot x_m).$$

Proof. As in the proof of the previous lemma if $g\in G_K$ extends γ_m and γ_n we may use this g in both the definition of the action of Γ_m on $\mathrm{H}^1_f(K_m,T)$ and of Γ_n on $\mathrm{H}^1_f(K_n,T)$. Choose a class of representatives $\{\,t_i\,\}_i$ of $G_{K_m}\backslash G_{K_n}$ and denote, for any coset y, by $\bar{y}$ its representative in $\{\,t_i\,\}_i$. Hence for any $x\in G_{K_n}$

$$\begin{aligned}\mathrm{cores}(\gamma_m\cdot x_m)(x)&=\sum_{c\in G_{K_m}\backslash G_{K_n}}\bar{c}^{\,-1}\cdot(\gamma_m\cdot x_m)\big(\bar{c}x(\overline{cx})^{-1}\big)=\\&=\sum_{c\in G_{K_m}\backslash G_{K_n}}\bar{c}^{\,-1}g\cdot x_m\big(g^{-1}\bar{c}x(\overline{cx})^{-1}g\big).\end{aligned}$$

Note that if for any t_i we let $u_i = g^{-1}t_i g$, then $\{ u_i \}_i$ is another class of representatives of $G_{K_m} \backslash G_{K_n}$ and if we denote, for any class y, by $\tilde{y}$ the representative of y in $\{ u_i \}_i$, then $\tilde{y} = g^{-1}\bar{y}g$ or in other terms $\bar{y} = g\tilde{y}g^{-1}$. Therefore

$$\begin{aligned} \operatorname{cores}(\gamma_m \cdot x_m)(x) &= \sum_{c \in G_{K_m} \backslash G_{K_n}} g\tilde{c}^{\,-1} \cdot x_m\big(\tilde{c}g^{-1}xg(\widetilde{cx})^{-1}\big) = \\ &= g \cdot \operatorname{cores}(x_m)(g^{-1}xg) = (\gamma_n \cdot x_n)(x). \end{aligned}$$

□

If moreover the representation T is ordinary at any prime $v \mid p$ we may define analogously the Greenberg Selmer groups $\mathrm{H}^1_{\mathrm{Gr}}(K_\infty, A)$ and $\mathrm{H}^1_{\mathrm{Gr}}(K_\infty, T)$ and the strict Greenberg Selmer groups $\mathrm{H}^1_{\mathrm{str}}(K_\infty, A)$ and $\mathrm{H}^1_{\mathrm{str}}(K_\infty, T)$ as the inductive and projective limit of the corresponding Selmer groups relative to the finite extensions K_n.

Chapter 2

Generalized Heegner cycles

In this chapter we introduce the so called *generalized Heegner cycles* of Bertolini, Darmon and Prasanna [BDP13]. Their image via the p-adic étale Abel-Jacobi lays into the Block-Kato Selmer group of the selfdual twist T of the representation attached to a modular form f. Castella and Hsieh in [CH18] use them in order to define an anticyclotomic Euler system for T: they get therefore a bound on the size of the Block-Kato Selmer group of the residual representation A, we show that this bound can be improved under some conditions. We will moreover define a notion of ($\mathfrak{p}$-primary) Shafarevich-Tate group for the modular curve f and we find a sufficient condition for its vanishing.

Fix once and for all a prime number p and a positive integer $N \geq 5$, let K be an imaginary quadratic field of discriminant $-d_k$ coprime with pN, with ring of integers $\mathcal{O}_K$, satisfying the so called *Heegner hypothesis* i.e. each prime factor of N splits in K. Fix moreover a cusp-newform of level $\Gamma_0(N)$ and even weight $k > 2$. Assume moreover throughout that $p \nmid 2N\varphi(N)(k-2)!$, where $\varphi(N)$ denote the Euler function, and that $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K.

2.1 Generalized Heegner Cycles

We begin recalling the definition of generalized Heegner cycles, following [BDP13].

2.1.1 Generalized Kuga-Sato variety

Put, in order to simplify the notations, $\bar{\mathcal{E}} = \bar{\mathcal{E}}_{\Gamma_1(N)}$, the universal generalized elliptic curve with $\Gamma_1(N)$-level structure, and $W_{k-2} = \tilde{\mathcal{E}}^{k-2}_{\Gamma_1(N)}$, the Kuga-Sato variety of level $\Gamma_1(N)$ and weight k that we introduced in Sec. 1.3.2, namely the canonical desingularization of the $(k-2)$-fold self-product

$$W^{\sharp}_{k-2} = \underbrace{\bar{\mathcal{E}} \times_{X_1(N)} \cdots \times_{X_1(N)} \bar{\mathcal{E}}}_{k-2 \text{ times}}.$$

Over this variety we define an idempotent ε_W in the ring of the rational correspondences in a fashion similar to what we did in *loc. cit.* First note that the $\Gamma_1(N)$-level structure on $\bar{\mathcal{E}}$ fixes a section of order N on $\bar{\mathcal{E}}$, translations by this section give rise to an action of $\mathbb{Z}/N\mathbb{Z}$ on $\bar{\mathcal{E}}$, thus of $(\mathbb{Z}/N\mathbb{Z})^{k-2}$ on $W^{\sharp}_{k-2}$ and hence on W_{k-2} by the properties of the canonical desingularization.

If σ_a denotes, for any $a = (a_1, \dots a_{k-2}) \in (\mathbb{Z}/N\mathbb{Z})^{k-2}$, the automorphism of W_{k-2} obtained by the action of a, let $\varepsilon_W^{(1)}$ be the idempotent

$$\varepsilon_W^{(1)} = \frac{1}{N^{k-2}} \cdot \sum_{a \in (\mathbb{Z}/N\mathbb{Z})^{k-2}} \sigma_a \in \mathbb{Z}\left[\frac{1}{N}\right]\left[\mathrm{Aut}\big(W_{k-2}/X_1(N)\big)\right].$$

Consider moreover the group $\mu_2^{k-2} \rtimes S_{k-2}$. It acts on W_{k-2}, letting -1 act by inversion on $\bar{\mathcal{E}}$ and $s \in S_{k-2}$ by permuting the factors of $W_{k-2}^{\sharp}$. For any $b \in \mu_2^{k-2} \rtimes S_{k-2}$ denote by σ_b the automorphism obtained by its action on W_{k-2} and let $j\colon \mu_2^{k-2} \rtimes S_{k-2} \to \mu_2$ be the homomorphism which is the identity on μ_2 and the sign charachter on S_{k-2}: we define

$$\varepsilon_W^{(2)} = \frac{1}{2^{k-2}(k-2)!} \cdot \sum_{b \in \mu_2^{k-2} \rtimes S_{k-2}} j(b)\sigma_b \in \mathbb{Z}\left[\frac{1}{2(k-2)!}\right]\left[\mathrm{Aut}\big(W_{k-2}/X_1(N)\big)\right].$$

It is immediate to verify that these are idempotents and commute between each other and hence their composition gives rise to another idempotent.

Definition 2.1.1. Define the idempotent attached to W_{k-2} as

$$\varepsilon_W = \varepsilon_W^{(1)} \circ \varepsilon_W^{(2)} \in \mathbb{Z}\left[\frac{1}{2N(k-2)!}\right]\left[\mathrm{Aut}\big(W_{k-2}/X_1(N)\big)\right].$$

and by a slight abuse of notation we use the same symbol for the correspondence

$$\varepsilon_W \in \mathrm{Corr}^0(W_{k-2}, W_{k-2}) \otimes \mathbb{Z}\left[\frac{1}{2N(k-2)!}\right],$$

obtained taking the graph of the involved automorphisms.

Let us fix once and for all a (complex) elliptic curve A with complex multiplication by $\mathcal{O}_K$. By the theory of complex multiplication (see e.g. [Sil94, Th. II.4.1, Th. II.2.2(b)]) A is defined over the Hilbert class field $K[1]$ of K and there is an isomorphism

$$[\,-\,]\colon \mathcal{O}_K \xrightarrow{\sim} \mathrm{End}_{K[1]}(A),$$

normalized in such a way that $[\alpha]^*\omega = \alpha\omega$ for any $\omega \in \Omega^1_{A/K[1]}$.

Definition 2.1.2. The *generalized Kuga-Sato variety* of level $\Gamma_1(N)$-level and weight k is the $(4k-3)$-dimensional variety defined over $K[1]$

$$X_{k-2} = W_{k-2} \times_{K[1]} A^{k-2}.$$

Like the classical Kuga-Sato variety there is a proper morphism

$$\pi\colon X_{k-2} \to X_0(N)$$

whose fibers over a non cuspidal points are products of elliptic curves of the form $E^{k-2} \times A^{r-2}$, where E varies.

We define moreover an idempotent ε_X in the ring of algebraic correspondences of X_{k-2} into itself: in order to do that first we consider the action of $\mu_2^{k-2} \rtimes S_{k-2}$ on A^{k-2} defined as that on $W_{k-2}^{\sharp}$ replacing $\bar{\mathcal{E}}$ by A and consider the idempotent correspondence

$$\varepsilon_A \in \mathrm{Corr}^0(A^{k-2}, A^{k-2}) \otimes \mathbb{Z}\left[\frac{1}{2(k-2)!}\right].$$

defined precisely as $\varepsilon_W^{(2)}$.

Definition 2.1.3. We define the idempotent correspondence attached to X_{k-2} as

$$\varepsilon_X = (\pi_W \times \pi_W)^* \, \varepsilon_W \circ (\pi_A \times \pi_A)^* \, \varepsilon_A \in \mathrm{Corr}^0(X_{k-2}, X_{k-2}) \otimes \mathbb{Z}\left[\frac{1}{2N(k-2)!}\right],$$

where the multiplication is the composition of correspondences, after pulling them back to X_{k-2} via the canonical projections $\pi_W : X_{k-2} \to W_{k-2}$ and $\pi_A : X_{k-2} \to A^{k-2}$.

2.1.2 Definition

Recall that the Heegner hypothesis ensures that there exists N-cyclic ideal $\mathfrak{N}$ of $\mathcal{O}_K$ (since each prime factors ℓ of N splits in K, $\ell\mathcal{O}_K = \lambda\bar{\lambda}$: take $\mathfrak{N} = \prod_{\ell|N} \lambda$ and let $\overline{\mathfrak{N}} = \prod_{\ell|N} \bar{\lambda}$), let us fix one of them together with a $\mathfrak{N}$-torsion point $t_A \in A[\mathfrak{N}](\mathbb{C})$; by the moduli interpretation $(A(\mathbb{C}), t_A)$ gives rise to a point on $X_1(N)(\mathbb{C})$, since $A[\mathfrak{N}] \subseteq A[N]$. Consider the set

$$\mathrm{Isog}(A) = \{\, (\varphi, A') : A' \text{ elliptic curve and } \varphi\colon A \to A' \text{ is an isogneny defined over } \bar{K} \,\} / \cong,$$

where $(\varphi_1, A_1') \cong (\varphi_2, A_2')$ if there is a $\bar{K}$-isomorphism $\iota\colon A_1' \to A_2'$ such that $\varphi_2 = \iota\varphi_1$.

The generalized Heegner cycles are indexed over the subset $\mathrm{Isog}^{\mathfrak{N}}(A)$ of $\mathrm{Isog}(A)$ consisting of isogenies $\varphi\colon A \to A'$ whose kernel intersect $A[\mathfrak{N}]$ trivially. A couple $(\varphi, A') \in \mathrm{Isog}^{\mathfrak{N}}(A)$ determines a point $P_{A'} = (A', \varphi(t_A))$ on $X_1(N)(\mathbb{C})$ whose fibre with respect to the structural morphism $\pi\colon W_{k-2} \to X_{k-2}$ is $(A')^{k-2}$. Let $\iota_{A'}\colon (A')^{k-2} \hookrightarrow W_{k-2}$ be the embedding of $(A')^{k-2}$ as the fibre of $P_{A'}$.

Consider now the cycle $\Upsilon_\varphi = \mathrm{Graph}(\varphi)^{k-2}$ on the variety

$$(A \times A')^{k-2} \xrightarrow{\sim} (A')^{k-2} \times A^{k-2} \xhookrightarrow{\iota} W_{k-2} \times A^{k-2} = X_{k-2}.$$

Definition 2.1.4. We define the generalized Heegner cycle attached to the isogeny $\varphi \in \mathrm{Isog}^{\mathfrak{N}}(A)$ as the cycle

$$\Delta_\varphi = (\varepsilon_X)_* \Upsilon_\varphi = (\varepsilon_X)^* \Upsilon_\varphi \in CH^{k-1}(X_{k-2}) \otimes \mathbb{Z}\left[\frac{1}{2N(k-2)!}\right]$$

supported (by the construction of Υ_φ and the fact that push-forward and pull back by ε_X respect the fibres) on the fibre $X_P := \pi_W^{-1}(P_{A'}) = (A')^{k-2} \times A^{k-2}$.

Proposition 2.1.5 ([BDP13, Prop. 2.7])**.** *The cycle Δ_φ is homologically trivial*

Proof. A detailed proof of this fact can be found in [BDLP21]. □

In particular this means that Δ_φ lays into the domain of the p-adic Abel-Jacobi map, that we are going to define in the next section.

Remark 2.1.6. As observed in [BDP13] one can deal with rationality questions about the generalized Heegner cycles Δ_φ: they are always defined over some abelian extension of K. The next construction of Castella and Hsieh [see CH18] selects a subclass of these cycles that are rational over the ring class fields $K[n]$ and whose properties are closer to those of the classical CM points, in particular they satisfy a sort of 'Shimura reciprocity law' and some 'norm relations' [see CH18, Lemma 4.3 and Prop. 4.4], these properties are crucial in order to make them into an Euler system and to use them into anticyclotomic Iwasawa Theory: this last observation is the reason why they are better suited for us than the classical Heegner cycles of [Nek92].

First of all, if $k > 2$, we make the extra assumption that $d_K > 3$ is odd or $8|d_K$. Under these assumption there exists a canonical elliptic curve, in the sense of Gross [see Yan04, Th. 0.1]. Let the elliptic curve A fixed above to be such a curve. It is therefore characterized by the following properties:

- it has CM by $\mathcal{O}_K$;
- $A(\mathbb{C}) = \mathbb{C}/\mathcal{O}_K$;
- it is a $\mathbb{Q}$-curve [see Gro80] defined over the real subfield $K[1]^+ = \mathbb{Q}\big(j(\mathcal{O}_K)\big)$ of the Hilbert class field $K[1]$ of K;
- the conductor of A is divisible only by prime factors of d_K.

Let now c be a positive integer and $\mathscr{C}_c = c^{-1}\mathcal{O}_c/\mathcal{O}_K$, where $\mathcal{O}_c$ denotes the order of $\mathcal{O}_K$ with conductor c. Hence $\mathscr{C}_c$ is a cyclic subgroup of order c, the elliptic curve such that $A_c(\mathbb{C}) = A/\mathscr{C}_c$ is an elliptic curve defined over the real subfield $K[c]^+ = \mathbb{Q}\big(j(\mathcal{O}_c)\big)$ of the ring class field of K of conductor c. Let $\varphi_c \colon A \to A_c$ be the isogeny given by the quotient map. Consider now a fractional $\mathcal{O}_c$-ideal $\mathfrak{a}$ prime to $cd_k\mathfrak{p}\mathfrak{N}$ and the elliptic curve $A_\mathfrak{a}$ such that $A_\mathfrak{a}(\mathbb{C}) = \mathbb{C}/\mathfrak{a}^{-1}$. The map $\mathbb{C}/c^{-1}\mathcal{O}_c \to \mathbb{C}/\mathfrak{a}^{-1}$ defined by $z \mapsto cz$ corresponds to an isogeny $\lambda_\mathfrak{a} \colon A_c \to A_\mathfrak{a}$ and we define

$$\varphi_\mathfrak{a} = \lambda_\mathfrak{a} \circ \varphi_c \colon A \to A_\mathfrak{a}.$$

For a suitable choice of t_A (see [CH18, Sec. 2.3], where is called η_c), we have therefore a generalized Heegner cycle

$$\Delta_\mathfrak{a} := \Delta_{\varphi_\mathfrak{a}} \in \mathrm{CH}^{k-1}(X_{k-2}/K[c]) \otimes \mathbb{Z}\left[\frac{1}{2N(k-2)!}\right].$$

In particular we write $\Delta_c := \Delta_{\mathcal{O}_c}$.

2.2 p-adic Abel Jacobi maps

In the following let F be number field containg the Hilbert class field $K[1]$ of K. The aim of this section is to define a p-adic étale Abel-Jacobi map

$$\mathrm{AJ}_F^{\text{ét}} \colon \mathrm{CH}^{k-1}(X_{k-2}/F)_0 \otimes \mathcal{O} \to \mathrm{H}^1_f(F, T)$$

so that if $\Delta_\mathfrak{a}$ is rational over F, its image via $\mathrm{AJ}_F^{\text{ét}}$ gives a cohomology class in the same fashion as the Kummer map attaches a cohomology class to Heegner points in the elliptic curve case. In fact this is more than a simple analogy in the case $k = 2$: the source is the set of 0-divisors on $X_1(N)$ and Δ_φ, that is up to principal equivalence, of the type $[P] - [\infty]$, where P is a CM point on $X_1(N)$.

2.2.1 p-adic cycle map and p-adic Abel-Jacobi map

We now introduce the Abel-Jacobi map for general smooth varieties as in [Jan88, Rk. 6.15(c)]. Recall from Sec. 1.2.3 and 1.2.4 that we have a cycle class map

$$\mathrm{cl}_X = \mathrm{cl}_X^i \colon \mathrm{CH}^i(X/F) \to \mathrm{H}^{2i}_{\text{ét}}(X, \mathbb{Z}_p(i)),$$

with kernel $\mathrm{CH}^i_0(X)$, and the Hochshild-Serre spectral sequence

$$\mathrm{H}^r\big(G_K, \mathrm{H}^s_{\text{ét}}(\bar{X}, \mathbb{Z}_p(j))\big) \Longrightarrow \mathrm{H}^{r+s}_{\text{ét}}(X, \mathbb{Z}_p(j)).$$

The two induce the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{CH}^i(X/F)_0 & \longrightarrow & \mathrm{CH}^i(X/F) & \longrightarrow & \frac{\mathrm{CH}^i(X/F)}{\mathrm{CH}^i(X/F)_0} & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{cl}_X} & & \Big\downarrow{\scriptstyle \mathrm{cl}_X} & \searrow^{\bar{\mathrm{cl}}_X} & \Big\downarrow & & \\
0 & \longrightarrow & \mathrm{F}^1\,\mathrm{H}^{2i}_{\text{ét}}(X,\mathbb{Z}_p(i)) & \hookrightarrow & \mathrm{H}^{2i}_{\text{ét}}(X,\mathbb{Z}_p(i)) & \xrightarrow{\mathrm{res}} & \mathrm{H}^{2i}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))^{G_K} & & \\
 & & \Big\downarrow & & & & & & \\
 & & \mathrm{H}^1\big(G_F,\mathrm{H}^{2i-1}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))\big) & & & & & &
\end{array}.$$

Indeed since the sequence degenerates at E_2,

$$E_2^{p,q} = \mathrm{H}^p\big(G_F,\mathrm{H}^q_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))\big) \cong \frac{\mathrm{F}^p\,\mathrm{H}^{p+q}_{\text{ét}}(X,\mathbb{Z}_p(i))}{\mathrm{F}^{p+1}\,\mathrm{H}^{p+q}_{\text{ét}}(X,\mathbb{Z}_p(i))};$$

applying this isomorphism to the case $p = 1, q = 2i-1$ (resp. $p = 0$, $q = 2i$) we find a canonical quotient map $\mathrm{F}^1\,\mathrm{H}^{2i}_{\text{ét}}(X,\mathbb{Z}_p(i)) \twoheadrightarrow \mathrm{H}^1\big(G_F,\mathrm{H}^{2i-1}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))\big)$ (resp. we find that $\mathrm{F}^1\,\mathrm{H}^{2i}_{\text{ét}}(X,\mathbb{Z}_p(i))$ is the kernel of the restriction map $\mathrm{H}^{2i}_{\text{ét}}(X,\mathbb{Z}_p(i)) \to \mathrm{H}^{2i}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))^{G_F}$).

The exactness of the rows implies that the image of $\mathrm{CH}^i(X/F)_0$ via the cycle map is contained into $\mathrm{F}^1\,\mathrm{H}^{2i}_{\text{ét}}(X,\mathbb{Z}_p(i))$, giving rise to the dotted vertical map. The composition of the two leftmost vertical maps

$$\mathrm{AJ}^{\text{ét}}_X : \mathrm{CH}^i(X/F)_0 \to \mathrm{H}^1\big(G_K,\mathrm{H}^{2i-1}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))\big)$$

is called the (i-th) p-adic Abel-Jacobi map. Via the isomophism

$$\mathrm{H}^1\big(G_F,\mathrm{H}^{2i-1}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))\big) = \mathrm{Ext}^1_{G_F}\big(\mathbb{Z}_p,\mathrm{H}^{2i-1}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i))\big)$$

we can also give an explicit description of this map, sending a cycle Z on X homologous to zero to the extension E obtained by pulling-back the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{H}^{2i-1}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i)) & \longrightarrow & \mathrm{H}^{2i-1}_{\text{ét}}(\bar{U},\mathbb{Z}_p(i)) & \longrightarrow & \mathrm{H}^{2i}_{\text{ét},|\bar{Z}|}(\bar{X},\mathbb{Z}_p(i)) & \longrightarrow & \mathrm{H}^{2i}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i)) \\
 & & \Big\| & & \Big\uparrow & & \Big\uparrow & & \\
0 & \longrightarrow & \mathrm{H}^{2i-1}_{\text{ét}}(\bar{X},\mathbb{Z}_p(i)) & \longrightarrow & E & \longrightarrow & \mathbb{Z}_p\cdot\bar{cl}_X(\bar{Z}) & \longrightarrow & 0
\end{array},$$

where $|\bar{Z}|$ is the support of $\bar{Z}$ and $\bar{U} = \bar{X} \setminus |\bar{Z}|$. For a proof of this fact see [Jan90, Lemma 9.4].

Let now $X = X_{k-2}$, $i = k-1$ and F any finite extension of the Hilbert class field such that Δ_φ is F-rational, after applying ε_X to the previous diagram we get an extension class in

$$\mathrm{Ext}^1_{G_F}\big(\mathbb{Z}_p,\varepsilon_X\,\mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2},\mathbb{Z}_p(k-1))\big) = \mathrm{H}^1\big(G_F,\varepsilon_X\,\mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2},\mathbb{Z}_p(k-1))\big)$$

and hence a map

$$\mathrm{AJ}^{\text{ét}}_F\colon\ \mathrm{CH}^{k-1}(X_{k-2}/F)_0 \otimes \mathbb{Z}_p \to \mathrm{H}^1\big(G_F,\varepsilon_X\,\mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2},\mathbb{Z}_p(k-1))\big)$$

if we use as Z in the diagram the support of a cycle Δ with coefficients in $\mathbb{Z}_p$. Hence we may apply $\mathrm{AJ}^{\text{ét}}_F$ to the the Heegner cycles, since their coefficients have possibly a denominator $2N(k-2)!$, that is invertible in $\mathbb{Z}_p$ (by the assumption $p \nmid 2N(k-2)!$): their image via $\mathrm{AJ}^{\text{ét}}_F$ is therefore given by the extension E_{Δ_φ} given by the following diagram, where $X_P^\flat := X_{k-2} \setminus X_P$, since the cycle Δ_φ is supported in X_P:

$$\begin{array}{ccccccc}
0 \to \varepsilon_X\,\mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2},\mathbb{Z}_p)(k-1) & \longrightarrow & E_{\Delta_\varphi} & \longrightarrow & \mathbb{Z}_p\cdot\bar{cl}_{X_P}(\bar{\Delta}_\varphi) & \longrightarrow & 0 \\
\Big\| & & \Big\downarrow & & \Big\downarrow & & \\
0 \to \varepsilon_X\,\mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2},\mathbb{Z}_p)(k-1) & \to & \varepsilon_X\,\mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_P^\flat,\mathbb{Z}_p)(k-1) & \to & \varepsilon_X\,\mathrm{H}^{2k-4}_{\text{ét}}(\bar{X}_P,\mathbb{Z}_p)(k-2) & \to & 0
\end{array}.$$

2.2.2 Image of the Abel-Jacobi map

In order to get a map lending in $\mathrm{H}^1(F, T)$, as we look for, we need to have a map

$$\varepsilon_X \mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2}, \mathbb{Z}_p(k-1)) \to T,$$

we will obtain it following [CH18, Sec. 4.2]. Let here $\mathcal{K}$ be, as in Sec. 1.3.1, the completion of the Hecke field of f at $\mathfrak{p}$ and $\mathcal{O}$ its ring of integers.

Observe that by the definition of X_{k-2} we have a natural morphism

$$\varepsilon_X \mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2}, \mathbb{Z}_p(k-1)) \to \varepsilon_W \mathrm{H}^{k-1}_{\text{ét}}(\bar{W}_{k-2}, \mathbb{Z}_p)(k/2) \otimes \mathrm{Sym}^{k-2} \mathrm{H}^1_{\text{ét}}(\bar{A}, \mathbb{Z}_p)(k/2-1);$$

now we have a morphism (where the middle terms are defined in Sec. 1.3.3)

$$\varepsilon_W \mathrm{H}^{k-1}_{\text{ét}}(\bar{W}_{k-2}, \mathbb{Z}_p)(k/2) \longrightarrow \textstyle\prod_\varepsilon \mathrm{H}^{k-1}_{\text{ét}}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_p) \longrightarrow J \longrightarrow J_{f,p} \longrightarrow T$$

and moreover we know that $\mathrm{H}^1_{\text{ét}}(\bar{A}, \mathbb{Z}_p)(k/2-1) = T_p(A)(1-k/2)$ and hence we get a morphism

$$\varepsilon_X \mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2}, \mathbb{Z}_p(k-1)) \to T \otimes \mathrm{Sym}^{k-2} T_p(A)(1-k/2).$$

Since A is just defined over the Hilbert class field $K[1]$ of K, we consider its restriction of scalars $B = \mathrm{Res}_{K[1]/K} A$: it is a CM abelian variety of dimension $[K[1] : K]$ and we have a decomposition

$$T_p(B) = \bigoplus_{\rho \in \mathrm{Gal}(K[1]/K)} T_p(A^\rho)$$

therefore we may view $T_p(A) \hookrightarrow T_p(B)$. Castella and Hsieh [CH18, Sec. 4.4] show that for any locally algebraic anticyclotomic character

$$\chi\colon \mathrm{Gal}(K[p^\infty]/K) \to \mathcal{O}_F^\times$$

of infinity type $(j, -j)$ there exists a finite order anticyclotomic charachter χ_t such that χ is realized as direct summand of $\mathrm{Sym}^{k-2} T_p(B)(1-k/2) \otimes \chi_t$ and so we get a G_K-equivariant projection

$$e_\chi\colon \mathrm{Sym}^{k-2} T_p(B)(1-k/2) \otimes \chi_t \to \chi,$$

finally leading to a natural morphism

$$\varepsilon_X \mathrm{H}^{2k-3}_{\text{ét}}(\bar{X}_{k-2}, \mathbb{Z}_p(k-1)) \to T \otimes \chi.$$

for any χ, that for $\chi = \mathbb{1}$ gives exactly the claimed projection. We get therefore in this way

$$\mathrm{AJ}^{\text{ét}}_c\colon \mathrm{CH}^{k-1}(X_{k-2}/K[c])_0 \otimes \mathbb{Z}_p \to \mathrm{H}^1(K[c], T)$$

and tensoring with $\mathcal{O}$ we get a morphism of $\mathcal{O}$-modules:

$$\mathrm{AJ}^{\text{ét}}_{\mathcal{O},c}\colon \mathrm{CH}^{k-1}(X_{k-2}/K[c])_0 \otimes \mathcal{O} \to \mathrm{H}^1(K[c], T).$$

Denote by $z_{f,c} \in \mathrm{H}^1(K[c], T)$ the image of Δ_c via $\mathrm{AJ}^{\text{ét}}_{\mathcal{O},c}$.

2.2.3 The Shafarevich-Tate group

Let $\widetilde{\Lambda}_{\mathfrak{p}}(K[c]) = \mathrm{im}\,\mathrm{AJ}^{\text{ét}}_{\mathcal{O},c}$, that we will take as an analogous in higher weight of the $K[c]$-rational points of an elliptic curve. Note that $\widetilde{\Lambda}_{\mathfrak{p}}(K[c]) \subseteq \mathrm{H}^1_f(K[c], T)$ by [Nek95, Sec. II.1.4] or [Niz97] and hence $\widetilde{\Lambda}_{\mathfrak{p}}(K[c]) \otimes \mathcal{K}/\mathcal{O}$ injects into $\mathrm{H}^1_f(K[c], A)$.

Definition 2.2.1. We define the Shafarevich-Tate group $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K[c])$ of f over $K[c]$ by the exact sequence

$$0 \longrightarrow \widetilde{\Lambda}_{\mathfrak{p}}(K[c]) \otimes \mathcal{K}/\mathcal{O} \longrightarrow \mathrm{H}^1_f(K[c], A) \longrightarrow \widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K[c]) \longrightarrow 0$$

A similar definition could be given for $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K)$, if we had a definition of $\widetilde{\Lambda}_{\mathfrak{p}}(K)$. This in fact cannot be defined as the image of the Abel-Jacobi map as above for $K[c]$, as the Abel-Jacobi map was defined only for a field F cointaining $K[1]$. However we can give an alternative definition of it that suits our purpose. Consider the restriction map

$$\mathrm{res}_{K[1]/K}\colon\ \mathrm{H}^1(K, T) \to \mathrm{H}^1(K[1], T)^{\mathrm{Gal}(K[1]/K)},$$

under some standard assumptions this becomes an isomorphism of $\mathcal{O}$-modules. In particular by standard diagram chasing in the following diagram, where $\mathcal{G}_1 = \mathrm{Gal}(K[1]/K)$,

$$\begin{array}{ccccccc}
0 \longrightarrow & \mathrm{H}^1_f(K,T) & \longrightarrow & \mathrm{H}^1(K,T) & \longrightarrow & \prod_v \frac{\mathrm{H}^1(K_v,T)}{\mathrm{H}^1_f(K_v,T)} \\
 & & & \wr\downarrow \mathrm{res} & & \downarrow \\
0 \longrightarrow & \mathrm{H}^1_f(K[1],T)^{\mathcal{G}_1} & \longrightarrow & \mathrm{H}^1(K[1],T)^{\mathcal{G}_1} & \longrightarrow & \left(\prod_v \frac{\mathrm{H}^1(K[1]_v,T)}{\mathrm{H}^1_f(K[1]_v,T)}\right)^{\mathcal{G}_1}
\end{array}$$

it follows that

$$\mathrm{res}_{K[1]/K}\colon\ \mathrm{H}^1_f(K, T) \xrightarrow{\sim} \mathrm{H}^1_f(K[1], T)^{\mathcal{G}_1}.$$

Definition 2.2.2. Assume that the restriction $\mathrm{res}_{K[1]/K}$ is an isomorphism, in this case define

$$\widetilde{\Lambda}_{\mathfrak{p}}(K) := \mathrm{res}^{-1}_{K[1]/K}\big(\widetilde{\Lambda}_{\mathfrak{p}}(K[1])^{\mathcal{G}_1}\big) \subseteq \mathrm{H}^1_f(K, T).$$

And we define the Shafarevich-Tate group $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K)$ of f over K by the exact sequence

$$0 \longrightarrow \widetilde{\Lambda}_{\mathfrak{p}}(K) \otimes \mathcal{K}/\mathcal{O} \longrightarrow \mathrm{H}^1_f(K, A) \longrightarrow \widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K) \longrightarrow 0$$

The main reason why we give this definition is because, in order to use the Heegner cycles to give informations about $\mathrm{H}^1_f(K, A)$, $\widetilde{\Lambda}_{\mathfrak{p}}(K)$ and $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K)$, we need that $\widetilde{\Lambda}_{\mathfrak{p}}(K)$ contains the *basic generalized Heegner cycle*

$$z_{f,K} = \mathrm{cores}_{K[1]/K}(z_{f,1}).$$

Indeed by Rk. 1.4.9

$$\mathrm{res}_{K[1]/K}(z_{f,K}) = \mathrm{Tr}_{K[1]/K}(z_{f,1}) \in \widetilde{\Lambda}_{\mathfrak{p}}(K[1])^{\mathcal{G}_1}.$$

and hence $z_{f,K} \in \widetilde{\Lambda}_{\mathfrak{p}}(K)$.

REMARK 2.2.3. Several papers [see for instance Nek92; Bes97; LV17; Mas19], use classical Heegner cycles instead of the generalized ones, they consider therefore a different Abel-Jacobi map,

$$\mathrm{AJ}^{\text{ét}}\colon \mathrm{CH}^{k/2}(\tilde{\mathcal{E}}^{k-2}_{\Gamma(N)}/K)_0 \to \mathrm{H}^1_f(K,T)$$

defining $\Lambda_{\mathfrak{p}}(K)$ and the Shafarevich-Tate group $Ш_{\mathfrak{p}^\infty}(f/K)$ respectively as the image and the cokernel of this map. These may, at least in principle, differ by the groups $\widetilde{\Lambda}_{\mathfrak{p}}(K)$ and $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K)$ that we defined here.

2.3 Euler system of generalized Heegner cycles

In [CH18, Sec. 7.3] Castella and Hsieh use the classes $z_{f,c}$ in order to construct an anticyclotomic Euler system as in the following definition. Let here $\mathscr{K}$ denote the set of squarefree products of primes ℓ inert in K such that $\ell \nmid 2pN$ and for any ℓ inert in K denote by Frob_ℓ the Frobenius element at λ in G_K, where λ is the unique prime of K over ℓ. Fix a compatible sequence of primes λ_n of $K[n]$ over λ with $n \in \mathscr{K}$, by $K[n]_\lambda$ we mean the completion of $K[n]$ at λ_n and by κ_n its resudue field. Let loc_ℓ be the localization map

$$\mathrm{loc}_\ell\colon \mathrm{H}^1(K[n],T) \to \mathrm{H}^1(K[n]_\lambda,T).$$

Let $a_\ell(f)$ denote the (ℓ-th) Hecke eigenvalue of f and $w_f \in \{\pm 1\}$ its Atkin-Lehner eigenvalue. Moreover we denote by τ_c the complex conjugation automorphism and by $\sigma_{\overline{\mathfrak{N}}}$ the image by the Artin reciprocity map of $\overline{\mathfrak{N}}$.

Definition 2.3.1. An anticyclotomic Euler system for T is a collection $\{c_n\}_{n\in\mathscr{K}}$ of classes $c_n \in \mathrm{H}^1(K[n],T)$ such that for any $n = m\ell \in \mathscr{K}$:

(E1) $\mathrm{cores}_{K[n]/K[m]}(c_n) = a_\ell(f)\cdot c_m$;

(E2) $\mathrm{loc}_\ell(c_n) = \mathrm{res}_{K[m]_\lambda/K[n]_\lambda}(\mathrm{Frob}_\ell \cdot \mathrm{loc}_\ell(c_m))$;

(E3) $\tau\cdot c_n = w_f(\sigma_{\bar{\mathfrak{N}}}\cdot c_n)$.

The *basic class* of the Euler system is defined to be

$$c_K = \mathrm{cores}_{K[1]/K}(c_1) \in \mathrm{H}^1(K,T).$$

What Castella and Hsieh prove is that the set $\{z_{f,n}\}_{n\in\mathscr{K}}$ form an Euler system and they use it as an input of the Kolyvagin's method, as modified by Nekovar in [Nek92]. They get therefore the following theorem:

Theorem 2.3.2 ([CH18, Th. 7.7])**.** *Let $z_{f,K}$ be non torsion in $\mathrm{H}^1(K,T)$, then*

$$\mathrm{H}^1_f(K,V) = \mathcal{K}\cdot z_{f,K}$$

In fact they prove [see CH18, Th. 7.19] that under the non torsion hypothesis on $z_{f,K}$, there is a constant C such that

$$p^C\left(\frac{\mathrm{H}^1_f(K,A)}{(\mathcal{K}/\mathcal{O})z_{f,K}}\right) = 0,$$

or, if we are in a situation sych that $\mathrm{res}_{K[1]/K}$ is an isomorphism and hence $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K)$ can be defined, that p^C kills $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K)$. In the case of classical Heegner cycles [Bes97] shows that the method of [Nek92] can be refined in some cases, in order to compute this constant C. We will show now that the same holds for generalized Heegner cycles.

We need first to define a set $\Psi(f)$ of *exceptional primes*, that we exclude, depending of f, that we suppose from now on to be a non - CM modular form.

Definition 2.3.3. Let $\Psi(f)$ be the set of rational primes consisting of the following primes:

- the primes $p \mid 6N\varphi(N)(k-2)!$
- the primes that ramify into the Hecke field of f;
- the primes such that the image of $\rho_{f,p}\colon G_{\bar{\mathbb{Q}}} \to \mathrm{GL}_2(\mathcal{O}_F \otimes \mathbb{Z}_p)$ does not contain the set

$$\{\, g \in \mathrm{GL}_2(\mathbb{Z}_p) : \det g \in (\mathbb{Z}_p^\times)^{k-1} \,\}.$$

Remark 2.3.4. The previous definition slightly differs from [Bes97, Def. 6.1] as we need to exclude also $p \mid \varphi(N)(k-2)!$ in order to get the integrality of the Abel Jacobi map and since we want to work with the selfdual lattice T coming from [Nek92]; we exlude also the prime 3 as $SL_2(\mathbb{F}_2) \cong S_3$ is solvable (*cfr.* Lemma 2.3.6) and therefore Lemma 2.3.5 does not hold anymore. However this last condition is not necessary in order to get Th. 2.3.9, but it allows us to state it in terms of $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K)$ and we will assume it in our application in Ch. 4.

The hypothesis on the image of $\rho_{f,\mathfrak{p}}$ is a kind of "big image" property and it is satisfied for all but a finite number of primes by [Rib85, Th. 3.1]. It implies many technical properties on the reduced representations $A[p^k]$ and their cohomology, as the next lemma. From now on we use the notations $\mathcal{G}_n = \mathrm{Gal}(K[n]/K)$ and $G(n) = \mathrm{Gal}(K[n]/K[1])$.

Lemma 2.3.5. *Let p be a non exceptional prime. For any $M \geq 1$ and any n squarefree,* $\mathrm{H}^0(K[n], A[p^M]) = \mathrm{H}^0(K, A[p^M]) = 0$. *In particular the restriction maps*

$$\mathrm{res}_{K[n]/K[1]}\colon \mathrm{H}^1(K[1], A[p^M]) \longrightarrow \mathrm{H}^1(K[n], A[p^M])^{G(n)},$$
$$\mathrm{res}_{K[1]/K}\colon \mathrm{H}^1(K, A[p^M]) \longrightarrow \mathrm{H}^1(K[1], A[p^M])^{\mathcal{G}_1}$$

are isomorphisms.

Proof. By the inflation restriction sequence the second statement follows from the first one; it is moreover enough to show it for $M = 1$. The following argument is taken from [LV17, Lemma 3.9 and 3.10]. By [Bes97, Prop. 6.3(1)] $A[p]$ is an irreducible $\mathbb{F}_p$-representation of $G_{\mathbb{Q}}$. Moreover, if we consider the morphism $\bar{\rho}_{f,\mathfrak{p}}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(A[p])$ attached to the representation $A[p]$, by [Bes97, Lemma 6.2], the image of ρ contains a subgroup isomorphic to $\mathrm{GL}_2(\mathbb{F}_p)$, hence one isomorphic to $\mathrm{SL}_2(\mathbb{F}_p)$. As the latter is not solvable by the following lemma since $p > 3$, then the image of $\bar{\rho}_{f,\mathfrak{p}}$ is not solvable.

Suppose now that $\mathrm{H}^0(K[n], A[p]) \neq 0$. By irreducibility $\mathrm{H}^0(K[n], A[p]) = A[p]^{G_{K[n]}} = A[p]$ and hence $\bar{\rho}_{f,\mathfrak{p}}$ factorizes trough $\mathrm{Gal}(K[n]/\mathbb{Q})$. But $K[n]/\mathbb{Q}$ is solvable, beeing generalized dihedral, and therefore the image of $\bar{\rho}_{f,\mathfrak{p}}$ is solvable, leading to a contraddiction. The same argument works for $\mathrm{H}^0(K, A[p^M])$ and in fact for any solvable extension of $\mathbb{Q}$. □

Lemma 2.3.6. *For $p > 3$ prime number, the group $\mathrm{SL}_2(\mathbb{F}_p)$ is a perfect group, i.e. it equals its derived subgroup. In particular it is not solvable.*

Proof. Note first that the $\mathrm{SL}_2(\mathbb{F}_p)$ is generated by the matrixes of the form $x(\lambda) = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ and $y(\lambda) = \left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)$, varying $\lambda \in \mathbb{F}_p$. Indeed any matrix in $\mathrm{SL}_2(\mathbb{F}_p)$ may be reduced to $\mathbb{1}_2$ via elementary operations (both on row and columns) that correspond to these matrixes.

It is enough to prove therefore that $x(\lambda)$ and $y(\lambda)$ are commutators for any $\lambda \in \mathbb{F}_p$: choose $\alpha \in \mathbb{F}_p^\times$ such that $\alpha^2 \neq 1$ (this is possible as $p > 3$) and define $\beta = \lambda/(\alpha^2 - 1)$. Therefore $x(\lambda) = \left[\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right)\right]$ and $y(\lambda) = \left[\left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ \beta & 1 \end{smallmatrix}\right)\right]$. □

Remark 2.3.7. Lemma 2.3.5 implies in particular that $\widetilde{\Lambda}_{\mathfrak{p}}(K)$ and $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K)$ can be defined. Indeed

$$\mathrm{H}^0(K[1], T) = \varprojlim_m \mathrm{H}^0(K[1], A[p^m]) = 0$$

and therefore $\mathrm{res}_{K[1]/K}$ is an isomorphism by the inflation-restriction sequence.

An other interesting consequence of Lemma 2.3.5 is the following corollary.

Corollary 2.3.8. *If p is not an exeptional prime, then the $\mathcal{O}$-module $\mathrm{H}^1(K,T)$ is torsion free. In particular $\mathrm{H}^1_f(K,T)$ and $\widetilde{\Lambda}_{\mathfrak{p}}(K)$ are free $\mathcal{O}$-modules of finite rank.*

Proof. It is known that $\mathrm{H}^1_f(K,T)$ is finitely generated of finite rank over $\mathcal{O}$, therefore the second statement follows immediately from the first. Since an $\mathcal{O}$-module may have only $\mathfrak{p}$-torsion it is enough to show that $\mathrm{H}^1(K,T)[\mathfrak{p}] = 0$. Under the hypothesis that p is non exeptional, p is a uniformizer of $\mathcal{O}$, (as p is unramified in F) and therefore $\mathrm{H}^1(K,T)[\mathfrak{p}] = \mathrm{H}^1(K,T)[p]$.

Consider now the short exact sequence $0 \longrightarrow T \xrightarrow{\cdot p} T \twoheadrightarrow A[p] \longrightarrow 0$, the induced long exact sequence in cohomology

$$\longrightarrow \mathrm{H}^0(K, A[p]) \longrightarrow \mathrm{H}^1(K,T) \xrightarrow{\cdot p} \mathrm{H}^1(K,T) \longrightarrow \mathrm{H}^1(K, A[p]) \longrightarrow$$

shows that $\mathrm{H}^1(K,T)[p]$ is a quotient of $\mathrm{H}^0(K, A[p])$, the latter beeing trivial by Lemma 2.3.5. □

The following theorem is the analogous of [Bes97, Th. 1.2]

Theorem 2.3.9. *Let p be a non exceptional prime, i.e. $p \notin \Psi(f)$, and $z_{f,K}$ be non torsion in $\mathrm{H}^1(K,T)$. Then*

$$p^{2\mathcal{I}_p}\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K) = 0,$$

where $\mathcal{I}_p$ is the smallest non negative integer such that $z_{f,K}$ is non-zero in $\mathrm{H}^1_f(K, A[p^{\mathcal{I}_p+1}])$. In particular, if $\mathcal{I}_p = 0$, then $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K) = 0$ and $\widetilde{\Lambda}_{\mathfrak{p}}(K) \otimes \mathcal{K}/\mathcal{O} = \mathrm{H}^1_f(K,A) = z_{f,K} \cdot \mathcal{K}/O$.

Remark 2.3.10. The short exact sequence

$$0 \longrightarrow T \xrightarrow{\cdot p^M} T \xrightarrow{\mathrm{red}_{p^M}} \frac{T}{p^M T} \cong A[p^M] \longrightarrow 0$$

induce the long exact sequence

$$\longrightarrow \mathrm{H}^0(K, A[p^M]) \longrightarrow \mathrm{H}^1(K,T) \xrightarrow{\cdot p^M} \mathrm{H}^1(K,T) \xrightarrow{\mathrm{red}_{p^k}} \mathrm{H}^1(K, A[p^M]) \longrightarrow \mathrm{H}^2(K,T) \longrightarrow$$

and hence $z_{f,K} = 0$ in $\mathrm{H}^1(K, A[p^M])$ if and only if it belongs to $p^M\,\mathrm{H}^1(K,T)$, i.e. if and only if it is divisible by p^M in $\mathrm{H}^1(K,T)$. It follows that $\mathcal{I}_p$ can be seen as the order of $z_{f,K}$, i.e. the biggest integer M such that $p^M \mid z_{f,K}$ in $\mathrm{H}^1(K,T)$. In particular $\mathcal{I}_p = 0$ if and only if $z_{f,K}$ is not divisible by p in $\mathrm{H}^1(K,T)$.

The proof of this theorem follows the lines of [Bes97] replacing generalized Heegner cycles to the classical one in the definition of the classes $P(n)$. We summarize their definition for the convenience of the reader and we will show that with the definition in terms of generalized Heegner cycles they enjoy the properties stated in [Bes97, Prop. 3.2]. This is enough: the proof of [Bes97, Th. 1.2] is a formal consequence of these properties and applies vertim to our case, once shown them.

For any $M \geq 1$, we define the set $S(M)$ of *M-admissible primes* as the set of rational primes ℓ such that

- $\ell \nmid Npd_K$;
- ℓ is inert in K;
- $p^M \mid a_\ell(f)$, $\ell + 1$;
- $p^{M+1} \nmid \ell + 1 \pm a_\ell(f)$.

For any n squarefree product of primes $\ell \in S(M)$ recall that we defined $G(n) = \mathrm{Gal}(K[n]/K[1])$ and $\mathcal{G}_n = \mathrm{Gal}(K[n]/K)$. One proves that $G(n) \cong \prod_\ell G(\ell)$ and $G(\ell)$ that is cyclic of order $l+1$, say generated by an element σ_ℓ. For any $\ell \in S(M)$ we define the operator

$$D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i \in \mathbb{Z}[G(\ell)];$$

it satisfies the *telescopic identity*

$$(\sigma_\ell - 1)D_\ell = \ell + 1 - \mathrm{Tr}_\ell,$$

where $\mathrm{Tr}_\ell = \sum_{i=0}^{\ell} \sigma_\ell^i$.

REMARK 2.3.11. Note that the telescopic identity defines uniquely $D_\ell \in G(\ell)$ up to addition of elements of the group $\mathbb{Z}\,\mathrm{Tr}_\ell$, since if $(\sigma_\ell - 1)D = 0$, for $D = \sum_{i=0}^{\ell} a_i\sigma_\ell^i \in \mathbb{Z}[G(\ell)]$, then

$$0 = (\sigma_\ell - 1)D = \sum_{i=0}^{\ell} a_i\sigma_\ell^{i+1} - \sum_{i=0}^{\ell} a_i\sigma_\ell^i = (a_\ell - a_0) + \sum_{i=1}^{\ell}(a_i - a_{i+1})\sigma_\ell^i.$$

Thus $a_0 = a_1 = \cdots = a_\ell =: k \in \mathbb{Z}$ and $D = k\,\mathrm{Tr}_\ell$. In fact several authors, for instance [Gro91], just define D_ℓ as a solution of the telescopic identity. Little would be lost with this definition, however we prefer for simplicity to fix D_ℓ explicitely as above.

We define then the (n-th) Kolyvagin's derivative operator

$$D_n = \prod_{\ell \mid n} D_\ell \in \mathbb{Z}[G(n)],$$

that make sense since D_{ℓ_1} commutes with D_{ℓ_2}, for $\ell_1 \neq \ell_2$. We will see in the following any $D \in \mathbb{Z}[G(n)]$ as an operator on the cohomology groups of T and $A[p^M]$ via the standard Galois action on them (as we did in Sec. 1.4.2). Recall moreover from Rk. 1.4.9 that for any extension of normal number fields L/F, then $\mathrm{res}_{L/F} \circ \mathrm{cores}_{L/F} = \mathrm{Tr}_{L/F}$, where $\mathrm{Tr}_{L/F}$ is seen as an operator on $\mathrm{H}^1(L, *)$ via the standard Galois action of $\mathrm{Gal}(L/K)$.

The starting point of the Kolyvagin method is the following lemma.

Lemma 2.3.12. *The class $D_n\big(\mathrm{red}_{p^M}(z_{f,n})\big) \in \mathrm{H}^1(K[n], A[p^M])$ is fixed by the action of $G(n)$.*

Proof. Let $n = m \cdot \ell$, then

$$\begin{aligned}(\sigma_\ell - 1)D_n(z_{f,n}) &= (\sigma_\ell - 1)D_\ell D_m(z_{f,n}) = \\ &= (l+1)D_m(z_{f,n}) - \mathrm{Tr}_\ell\, D_m(z_{f,n}) = \\ &= (l+1)D_m(z_{f,n}) - D_m\,\mathrm{Tr}_\ell(z_{f,n}) = \\ &= (l+1)D_m(z_{f,n}) - a_\ell(f)\big(\mathrm{res}_{K[n]/K[m]}\, D_m(z_{f,m})\big) \equiv \\ &\equiv 0 \bmod p^M.\end{aligned}$$

Indeed:

- $\mathrm{Tr}_\ell(z_{f,n}) = \mathrm{res}_{K[n]/K[m]} \circ \mathrm{cores}_{K[n]/K[m]}(z_{f,n}) = a_l(f)\,\mathrm{res}_{K[n]/K[m]}(z_{f,m})$ by (E2);
- $\ell+1,\ a_\ell(f) \equiv 0 \mod p^M$ as $\ell \in S(M)$.

Thus, by Rk. 2.3.10, the class $D_n\big(\mathrm{red}_{p^M}(z_{f,n})\big)$ is fixed by the action $G(\ell)$ for any $\ell \mid n$ and hence by the action of $G(n)$. □

Therefore by Lemma 2.3.5 there is a unique class $\mathcal{D}(n) \in \mathrm{H}^1(K[1], A[p^M])$ such that

$$\mathrm{res}_{K[n]/K[1]}\big(\mathcal{D}(n)\big) = D_n\big(\mathrm{red}_{p^M}(z_{f,n})\big),$$

let

$$P(n) = \mathrm{cores}_{K[1]/K}\big(\mathcal{D}(n)\big) \in \mathrm{H}^1(K, A[p^M]).$$

Remark 2.3.13. Note that $D_1 = \mathrm{id}$, hence $P(1) = \mathrm{red}_{p^M}(z_{f,K})$.

We come now to the properties of the classes $P(n)$. For any n squarefreee product of primes of $S(M)$ we define $\varepsilon_n = (-1)^{\omega(n)} w_f$, where $\omega(n)$ is the number of prime factors of n and w_f is the Atkin-Lehner eigenvalue of f.

Proposition 2.3.14. *The class $P(n)$ belongs to the ε_n-eigenspace of the complex conjugation τ_c acting on $\mathrm{H}^1(K, A[p^M])$.*

Proof. As a first step consider the group element $\tau_c D_n \in \mathbb{Z}[\mathrm{Gal}(K[n]/\mathbb{Q})]$, we want to link it to $D_n\tau_c$. Recall that, since the extension $K[n]/K$ is generalized dihedral over $\mathbb{Q}$, $\sigma\tau_c = \tau_c\sigma^{-1}$ for any $\sigma \in \mathcal{G}_n$. In particular for any $\ell \mid n$,

$$\mathrm{Tr}_\ell\,\tau_c = \sum_{i=0}^{\ell} \sigma_\ell^i \tau_c = \tau_c \sum_{i=0}^{\ell} \sigma_\ell^{-i} = \tau_c\,\mathrm{Tr}_\ell$$

hence, applying the telescopic identity,

$$(\sigma_\ell - 1)D_\ell\tau_c = (\ell+1-\mathrm{Tr}_\ell)\tau_c = \tau_c(\ell+1-\mathrm{Tr}_\ell) = \tau_c(\sigma_\ell-1)D_\ell = (\sigma_\ell^{-1}-1)\tau_c D_\ell = -\sigma_\ell^{-1}(\sigma_\ell-1)\tau_c D_\ell$$

and therefore $(\sigma_\ell - 1)(\sigma_\ell D_\ell \tau_c + \tau_c D_\ell) = 0$. It follows by Rk. 2.3.11 that

$$\tau_c D_\ell = -\sigma_\ell D_\ell \tau_c + k\,\tau_c\,\mathrm{Tr}_\ell,$$

since $\sigma_\ell D_\ell \tau_c + \tau_c D_\ell = D\tau_c$, for $D \in \mathbb{Z}[G(\ell)]$ and $(\sigma_\ell - 1)D\tau_c = 0$ if and only if $(\sigma_\ell - 1)D = 0$.

Now consider $D_n z_{f,n} \in \mathrm{H}^1(K[n], T)$ and let $n = \ell_1 \cdots \ell_{\omega(n)}$

$$\begin{aligned}
\tau_c \cdot (D_n z_{f,n}) &= \tau_c \cdot D_{\ell_1} \cdots D_{\ell_{\omega(n)}} \cdot z_{f,n} \equiv \\
&\equiv (-1)^{\omega(n)} \sigma_{\ell_1} D_{\ell_1} \cdots \sigma_{\ell_{\omega(n)}} D_{\ell_{\omega(n)}} \cdot \tau_c \cdot z_{f,n} \equiv \\
&\equiv (-1)^{\omega(n)} w_f \big(\prod_{\ell \mid n} \sigma_\ell\big) D_n \cdot z_{f,n} = \\
&= \varepsilon_n \sigma_{\bar{\mathfrak{N}}} \big(\prod_{\ell \mid n} \sigma_\ell\big)(D_n z_{f,n}) \bmod p^M
\end{aligned}$$

since if $n = \ell \cdot m$, then $\mathrm{Tr}_\ell\, z_{f,n} = a_\ell(f)\,\mathrm{res}_{K[n]/K[m]}(z_{f,m}) \cong 0 \bmod p^M$. Observe that in the previous formula we used the fact that the σ_ℓ's (and hence the D_ℓ's and the Tr_ℓ's) commute with each other and with $\sigma_{\bar{\mathfrak{N}}} \in \mathcal{G}_1$.

Note moreover that $D_n\big(\mathrm{red}_{p^M}(z_{f,n})\big)$ is invariant under the action of the σ_ℓ's by Lemma 2.3.12, therefore

$$\varepsilon_n\sigma_{\bar{\mathfrak{N}}}\big(\prod_{\ell|n}\sigma_\ell\big)D_n\big(\mathrm{red}_{p^M}(z_{f,n})\big) = \varepsilon_n\sigma_{\bar{\mathfrak{N}}}D_n\big(\mathrm{red}_{p^M}(z_{f,n})\big)$$

and in particular, since $\mathrm{res}_{K[n]/K}$ is an isomorphism, $\tau_c\mathcal{D}(n) = \varepsilon_n\sigma_{\bar{\mathfrak{N}}}\mathcal{D}(n)$. Thus

$$\begin{aligned}
\mathrm{res}_{K[1]/K}\big(\tau_c P(n)\big) &= \tau_c\cdot\mathrm{res}_{K[1]/K}\circ\mathrm{cores}_{K[1]/K}\,\mathcal{D}(n) = \tau_c\,\mathrm{Tr}_{K[1]/K}\,\mathcal{D}(n) = \\
&= \mathrm{Tr}_{K[1]/K}\big(\tau_c\mathcal{D}(n)\big) = \mathrm{Tr}_{K[1]/K}\big(\varepsilon_n\sigma_{\bar{\mathfrak{N}}}\mathcal{D}(n)\big) = \\
&= \varepsilon_n(\sigma_{\bar{\mathfrak{N}}}\,\mathrm{Tr}_{K[1]/K})\mathcal{D}(n) = \varepsilon_n\,\mathrm{Tr}_{K[1]/K}\,\mathcal{D}(n) = \varepsilon_n\,\mathrm{res}_{K[1]/K}\,P(n) = \\
&= \mathrm{res}_{K[1]/K}\big(\varepsilon_n P(n)\big),
\end{aligned}$$

where we used the fact that

$$\tau_c\cdot\mathrm{Tr}_{K[1]/K} = \sum_{\sigma\in\mathcal{G}_1}\tau_c\sigma \;=\sum_{\sigma\in\mathcal{G}_1}\sigma^{-1}\tau_c \;= \mathrm{Tr}_{K[1]/K}\cdot\tau_c$$

and that, since $\sigma_{\bar{\mathfrak{N}}}\in\mathcal{G}_1$,

$$\sigma_{\bar{\mathfrak{N}}}\cdot\mathrm{Tr}_{K[1]/K} = \sum_{\sigma\in\mathcal{G}_1}\sigma_{\bar{\mathfrak{N}}}\sigma \;=\sum_{\sigma\in\mathcal{G}_1}\sigma \;= \mathrm{Tr}_{K[1]/K}\,.$$

Being $\mathrm{res}_{K[1]/K}$ is an isomorphism, it follows that $\tau_c P(n) = \varepsilon_n P(n)$. □

We need moreover to study the properties of the localization of the classes $P(n)$.

Proposition 2.3.15. *For any n squarefree products of M-admissible primes,*

$$\mathrm{loc}_v\,P(n)\in\mathrm{H}^1_f(K_v, A[p^M])$$

for any $v\nmid Nn$.

Proof. Note first that we know that $z_{f,n}\in\widetilde{\Lambda}_{\mathfrak{p}}(K,T)\subseteq\mathrm{H}^1_f(K[n],T)$ by Sec. 2.2.2.

Let's consider the case $v\nmid p$, in that case $\mathrm{H}^1_f(K[n],A[p^M]) = \mathrm{H}^1_{\mathrm{ur}}(K[n],A[p^M])$ by Ex. 1.1.14, as the representation attached to a modular form is unramified at $v\nmid Np$. We have to show therefore that $\mathrm{loc}_v\big(\mathrm{red}_{p^M}\,z_{f,n}\big)\in\mathrm{H}^1(K[n]_v, A[p^M])$ goes to 0 under the restriction map

$$\mathrm{H}^1(K[n]_v, A[p^M]) \xrightarrow{\mathrm{res}_{K[n]^{\mathrm{ur}}/K[n]}} \mathrm{H}^1(K[n]_v^{\mathrm{ur}}, A[p^M]),$$

where $K[n]_v$ is the completion of $K[n]$ at a prime $v[n]$ over v. Since $K[n]/K$ is unramified at $v\nmid n$ then $K_v^{\mathrm{ur}} = K[1]_v^{\mathrm{ur}} = K[n]_v^{\mathrm{ur}}$ and hence we get a commutative diagram

$$\begin{array}{ccccc}
\mathrm{H}^1(K,A[p^M]) & \xrightarrow{\mathrm{loc}_v} & \mathrm{H}^1(K_v,A[p^M]) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(K_v^{\mathrm{ur}},A[p^M]) \\
\downarrow{\scriptstyle\mathrm{res}} & & \downarrow{\scriptstyle\mathrm{res}} & & \|{\scriptstyle\mathrm{res}} \\
\mathrm{H}^1(K[1],A[p^M]) & \xrightarrow{\mathrm{loc}_v} & \mathrm{H}^1(K[1]_v,A[p^M]) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(K[1]_v^{\mathrm{ur}},A[p^M]) \\
\downarrow{\scriptstyle\mathrm{res}} & & \downarrow{\scriptstyle\mathrm{res}} & & \|{\scriptstyle\mathrm{res}} \\
\mathrm{H}^1(K[n],A[p^M]) & \xrightarrow{\mathrm{loc}_v} & \mathrm{H}^1(K[n]_v,A[p^M]) & \xrightarrow{\mathrm{res}} & \mathrm{H}^1(K[n]_v^{\mathrm{ur}},A[p^M])
\end{array}$$

and therefore

$$\begin{aligned}\mathrm{res}_{K[1]_v^{\mathrm{ur}}/K[1]_v}\circ \mathrm{loc}_v\,\mathcal{D}(n) &= \mathrm{res}_{K[n]_v^{\mathrm{ur}}/K[n_v]}\circ \mathrm{loc}_v\big(\mathrm{res}_{K[n]/K[1]}\,\mathcal{D}(n)\big) = \\ &= \mathrm{res}_{K[n]_v^{\mathrm{ur}}/K[n_v]}\circ \mathrm{loc}_v\big(D_n\,\mathrm{red}_{p^M}\,z_{f,n}\big) = \\ &= D_n\Big(\mathrm{res}_{K[n]_v^{\mathrm{ur}}/K[n_v]}\circ \mathrm{loc}_v\big(\mathrm{red}_{p^M}\,z_{f,n}\big)\Big) = 0.\end{aligned}$$

Finally $\mathrm{res}_{K_v^{\mathrm{ur}}/K_v}\,\mathrm{loc}_v\,P(n) = 0$ since

$$\begin{aligned}\mathrm{res}_{K_v^{\mathrm{ur}}/K_v}\,\mathrm{loc}_v\,P(n) &= \mathrm{res}_{K[1]_v^{\mathrm{ur}}/K[1]_v}\circ \mathrm{loc}_v\circ(\mathrm{res}_{K[1]/K}\circ \mathrm{cores}_{K[1]/K}\,\mathcal{D}(n)) = \\ &= res_{K[1]_v^{\mathrm{ur}}/K[1]_v}\circ \mathrm{loc}_v\circ\Big(\sum_{\sigma\in\mathcal{G}_1}\sigma\mathcal{D}(n)\Big) = \\ &= \sum_{\sigma\in\mathcal{G}_1} res_{K[1]_v^{\mathrm{ur}}/K[1]_v}\circ \mathrm{loc}_v\circ(\sigma\mathcal{D}(n)) = 0.\end{aligned}$$

Let now $v \mid p$, then

$$\mathrm{loc}_v\big(\mathrm{res}_{K[n]/K[1]}\,\mathcal{D}(n)\big) = \mathrm{loc}_v\big(D_n(\mathrm{red}_{p^M}\,z_{f,n})\big) \in \mathrm{H}^1_f(K[n]_v, A[p^M])$$

and therefore $\mathrm{loc}_v\big(\mathcal{D}(n)\big) \in \mathrm{H}^1_f(K[n]_v, A[p^M])$ since the restriction map

$$\mathrm{res}_{K[n]_v/K[1]_v}: \frac{\mathrm{H}^1(K[1]_v, A[p^M])}{\mathrm{H}^1_f(K[1]_v, A[p^M])} \longrightarrow \frac{\mathrm{H}^1(K[n]_v, A[p^M])}{\mathrm{H}^1_f(K[n]_v, A[p^M])}$$

is injective by [CH18, Lemma 7.5]. Thus $\mathrm{loc}_v\,P(n) \in \mathrm{H}^1_f(K, A[p^M])$. □

Consider now the finite-to-singular isomorphism $\varphi_\ell^{\mathrm{fs}}\colon\ \mathrm{H}^1_f(K_\lambda, A[p^M]) \to \mathrm{H}^1_s(K_\lambda, A[p^M])$ coming from the composition of the two isomorphisms

$$\begin{aligned}\alpha_\ell\colon\ \mathrm{H}^1_f(K_\lambda, A[p^M]) &\cong \mathrm{H}^1(K_\lambda^{\mathrm{ur}}/K_\lambda, A[p^M]) \xrightarrow{\sim} A[p^M] \\ \beta_\ell\colon\ \mathrm{H}^1_s(K_\lambda, A[p^M]) &\cong \mathrm{H}^1(K_\lambda^{\mathrm{ur}}, A[p^M]) \xrightarrow{\sim} A[p^M]\end{aligned}$$

given by evaluation of cocycles respectively at Frob_ℓ and at τ_ℓ, where τ_ℓ is a generator if the pro-p-part of the tame inertia group of K_λ [see Nek92, Sec. 8].

Proposition 2.3.16. *Let $n = m\cdot\ell$. Then there is a p-adic unit $u_{\ell,n}$ such that*

$$\big[\mathrm{loc}_\ell\,P(n)\big]_s = \bar{u}_{\ell,n}\varphi_\ell^{\mathrm{fs}}\big(\mathrm{loc}_\ell\,P(m)\big),$$

where $\bar{u}_{\ell,n}$ is the reduction of $u_{\ell,n}$ to the residue field of $\mathcal{O}_{K,\lambda}$, in particular $\mathrm{loc}_\ell\,P(m) \neq 0$ if and only if $\big[\mathrm{loc}_\ell\,P(n)\big]_s \neq 0$.

Proof. The result follows by the formula of the following Lemma, since ℓ is M-admissible and hence the two coefficients there are p-adic units. □

We obtain the following formula appying the abstract nonsense of [Nek92, Sec. 9].

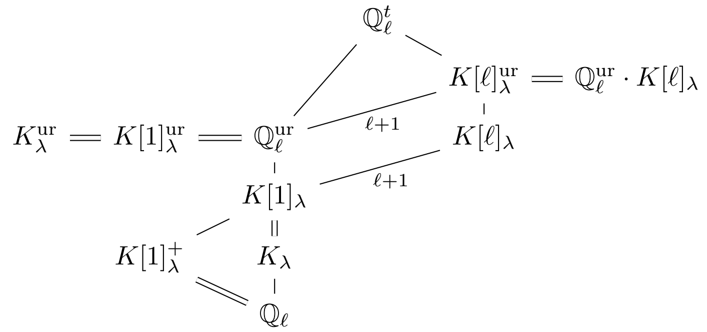
Lemma 2.3.17. *If $n = m\cdot\ell$, then*

$$\left(\frac{(-1)^{k/2-1}\varepsilon_n a_\ell(f)}{p^M} - \frac{\ell+1}{p^M}\right)\big[\mathrm{loc}_\ell\,P(n)\big]_s = \left(-\frac{\ell+1}{p^M}\varepsilon_n - \frac{a_\ell(f)}{p^M}\right)\varphi^\ell_{fs}\big(\mathrm{loc}_\ell\,P(m)\big).$$

Proof. Let us first consider the case where $n = \ell \cdot 1$, i.e. the formula

$$\left(\frac{(-1)^{k/2-1} w_f a_\ell(f)}{p^M} - \frac{\ell+1}{p^M}\right)\left[\mathrm{loc}_\ell P(\ell)\right]_s = \left(\frac{\ell+1}{p^M} w_f - \frac{a_\ell(f)}{p^M}\right)\varphi^\ell_{fs}\left(\mathrm{loc}_\ell P(1)\right).$$

Note that we have the following tower of field extension, where $\mathbb{Q}_\ell^t$ is the maximal tamely ramified extension of $\mathbb{Q}_\ell$ (i.e. the maximal extension which has ramification prime to ℓ) and $K[1]^+_\lambda$ is completion at the prime above ℓ of the maximal totally real subfield $K[1]^+$ of $K[1]$



Indeed

- ℓ is inert (hence unramified) in K and hence $K_\lambda^{\mathrm{ur}} = \mathbb{Q}_\ell^{\mathrm{ur}}$;
- ℓ is totally split in $K[1]/K$, hence $K[1]_\lambda = K_\lambda$;
- λ_1 is totally ramified in $K[\ell]/K[1]$ (that is cyclic of order $\ell+1$), i.e. $\lambda_1 = \lambda_\ell^{\ell+1}$: it follows that $[K[\ell]_\lambda : K[1]_\lambda] = \ell + 1$ and $\mathrm{Gal}(K[\ell]_\lambda/K[1]_\lambda) \cong \mathrm{Gal}(\kappa_\ell/\kappa_1)$, that is cyclic being the Galois group of an extension of finite fields, moreover the ramification of $K[\ell]_\lambda/\mathbb{Q}_\ell$ is prime to ℓ, thus $K[\ell]^{\mathrm{ur}} \subseteq \mathbb{Q}_\ell^t$;
- $K_\lambda \subseteq K[1]_\lambda \subseteq \mathbb{Q}_\ell^{\mathrm{ur}}$, therefore $K_\lambda^{\mathrm{ur}} = K[1]_\lambda^{\mathrm{ur}} = \mathbb{Q}_\ell^{\mathrm{ur}}$;
- $K[\ell]_\lambda^{\mathrm{ur}} = \mathbb{Q}_\ell^{\mathrm{ur}} \cdot K[\ell]_\lambda$;
- $K[\ell]_\lambda^{\mathrm{ur}}/\mathbb{Q}_\ell$ is cyclic of order $\ell+1$, since

$$\mathrm{Gal}\left(\frac{K[\ell]_\lambda^{\mathrm{ur}}}{\mathbb{Q}_\ell}\right) = \mathrm{Gal}\left(\frac{\mathbb{Q}_\ell^{\mathrm{ur}} \cdot K[\ell]_\lambda}{\mathbb{Q}_\ell}\right) \cong \mathrm{Gal}\left(\frac{K[\ell]_\lambda}{\mathbb{Q}_\ell^{\mathrm{ur}} \cap K[\ell]_\lambda}\right) = \mathrm{Gal}\left(\frac{K[\ell]_\lambda}{K[1]_\lambda}\right);$$

- $\mathbb{Q}_\ell \subseteq K[1]^+_\lambda \subseteq K[1]_\lambda = K_\lambda$, but the degree of $K[1]_\lambda/K[1]^+_\lambda$ is at least 2, thus $K[1]^+_\lambda = \mathbb{Q}_\ell$.

Now consider the inclusions

$$\begin{array}{ccccc} \tilde{G} := \mathrm{Gal}(\bar{\mathbb{Q}}/K[1]^+) & \supseteq & G := \mathrm{Gal}(\bar{\mathbb{Q}}/K[1]) & \supseteq & H := \mathrm{Gal}(\bar{\mathbb{Q}}/K[\ell]) \\ \cup\!\!| & & \cup\!\!| & & \cup\!\!| \\ \tilde{G}_0 := \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) & \supseteq & G_0 := \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K[1]_\lambda) & \supseteq & H_0 := \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/K[\ell]_\lambda) \end{array}$$

where the squares are cocartesian, i.e. $G_0 = \tilde{G}_0 \cap G$, $H_0 = \tilde{G}_0 \cap H$, moreover we have that $G/H = \mathrm{Gal}(K[\ell]/K[1]) = \langle \sigma_\ell \rangle$ and $G_0/H_0 = \mathrm{Gal}(K[\ell]_\lambda/K[1]_\lambda) = \langle \sigma_{\ell,0} \rangle$, where $(\sigma_{\ell,0})_{|K[\ell]} = \sigma_\ell$ and $\mathrm{Gal}(K[\ell]_\lambda^{\mathrm{ur}}/K[1]_\lambda^{\mathrm{ur}}) = \langle \sigma_{\ell,0}^{\mathrm{ur}} \rangle$, for $(\sigma_{\ell,0}^{\mathrm{ur}})_{|K[\ell]_\lambda} = \sigma_{\ell,0}$. Write $\sigma = \sigma_\ell$ and $\sigma_0 = \sigma_{\ell,0}$, $\sigma_0^{\mathrm{ur}} = \sigma_{\ell,0}^{\mathrm{ur}}$.

It is well known that we have an explicit description of the Galois group of the maximal tamely ramified extension of $\mathbb{Q}_\ell$:

$$\mathrm{Gal}(\mathbb{Q}_\ell^t/\mathbb{Q}_\ell) = \mathrm{Gal}(\mathbb{Q}_\ell^t/\mathbb{Q}_\ell^{\mathrm{ur}}) \rtimes \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/\mathbb{Q}_\ell) \cong \hat{\mathbb{Z}}'(1) \rtimes \hat{\mathbb{Z}},$$

where $\hat{\mathbb{Z}}'(1) = \prod_{q\neq\ell} \mathbb{Z}_q(1)$: $\hat{\mathbb{Z}}'(1)$ and $\hat{\mathbb{Z}}$ are procyclic and have generators φ and τ respectively such that $\varphi\tau\varphi^{-1} = \tau^\ell$. It follows an analogous description in a compatible way of the subgroups

$$\mathrm{Gal}(\mathbb{Q}_\ell^t/K_\lambda) = \mathrm{Gal}(\mathbb{Q}_\ell^t/\mathbb{Q}_\ell) \rtimes \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/K_\lambda) \cong \langle\tau\rangle \rtimes \langle\varphi^2\rangle = \hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}}$$
$$\mathrm{Gal}(\mathbb{Q}_\ell^t/K[\ell]_\lambda) = \mathrm{Gal}(\mathbb{Q}_\ell^t/K[\ell]_\lambda^{\mathrm{ur}}) \rtimes \mathrm{Gal}(K[\ell]_\lambda^{\mathrm{ur}}/K[\ell]_\lambda) \cong \langle\tau^{\ell+1}\rangle \rtimes \langle\varphi^2\rangle = (\ell+1)\hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}}$$

where $(\varphi')^2$ topologically generates $\mathrm{Gal}(K[l]_\lambda^{\mathrm{ur}}/K[\ell]_\lambda) \cong \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ur}}/K_\lambda) \cong 2\hat{\mathbb{Z}}$. Let us denote by π the natural projection

$$\pi\colon \tilde{G}_0 = \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathrm{Gal}(\mathbb{Q}_\ell^t/\mathbb{Q}_\ell) \cong \mathbb{Z}'(1) \rtimes \hat{\mathbb{Z}}$$

and the induced projections

$$\pi\colon G_0 \to \hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}}, \qquad \pi\colon H_0 \to (\ell+1)\hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}}.$$

Note moreover that

$$G_0/H_0 \cong \mathrm{Gal}(K[\ell]_\lambda^{\mathrm{ur}}/K[1]_\lambda^{\mathrm{ur}}) \cong \hat{\mathbb{Z}}'(1)/(\ell+1)\hat{\mathbb{Z}}'(1),$$

so that we may assume to have choosen σ_ℓ such that $\tau \bmod (\ell+1)\hat{\mathbb{Z}}'(1) = \sigma_{\ell,0}^{\mathrm{ur}}$.

Now before going on with the proof we need the following technical lemma, that is essentially [Nek92, Lemma 4.1].

Lemma 2.3.18. *Let $K/\mathbb{Q}_\ell$ be a finite extension, for $\ell \neq Np$. Then $\mathrm{H}^1(K,T) \cong \mathrm{H}^1(K^{\mathrm{ur}}/K,T)$.*

Proof. Let $P = \mathrm{Gal}(\mathbb{Q}_\ell/K^t)$ the wild inertia group of K, that is a pro-ℓ-group. Consider the inflation-restriction exact sequence

$$0 \to \mathrm{H}^1\big(K^{\mathrm{ur}}/K, \mathrm{H}^0(P,T)\big) \to \mathrm{H}^1(K,T) \to \mathrm{H}^1(K^t,T)^{\mathrm{Gal}(K^t/K)},$$

one has that $\mathrm{H}^1(K^{\mathrm{ur}}/K,T) \cong \mathrm{H}^1(K^t,T)$: indeed P is contained into the inertia group I of G_K, but T is unramified at $\ell \neq Np$ and hence $\mathrm{H}^0(P,T) = T$; moreover (since, as we just observed, P acts trivially on T) $\mathrm{H}^1(K^t,A) = \mathrm{Hom}_{\mathrm{cont}}(P,T) = 0$ as P is a pro-ℓ-group and T a pro-p one.

Now denote by φ the generator of $\mathrm{Gal}(K^{\mathrm{ur}}/K)$ and τ the generator of $\mathrm{Gal}(K^t/K^{\mathrm{ur}})$. We have that $\varphi\tau\varphi^{-1} = \tau^{\ell^d}$, where ℓ^d is the degree of the residue field of K over $\mathbb{F}_\ell$. We apply again the inflation-restriction exact sequence

$$0 \to \mathrm{H}^1(K^{\mathrm{ur}}/K,T) \to \mathrm{H}^1(K^t/K,T) \to \mathrm{H}^1(K^t/K^{\mathrm{ur}},T)^{\mathrm{Gal}(K^{\mathrm{ur}}/K)},$$

the rightmost term is again 0 and therefore

$$\mathrm{H}^1(K^{\mathrm{ur}}/K,T) \cong \mathrm{H}^1(K^t/K,T) \cong \mathrm{H}^1(K^t,T).$$

Indeed $\mathrm{H}^1(K^t/K^{\mathrm{ur}},T) \cong \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}(K^t/K^{\mathrm{ur}}),T\big) \cong T(\ell^d)$, via the evaluation at τ, hence

$$\mathrm{H}^1(K^t/K^{\mathrm{ur}},T)^{\mathrm{Gal}(K^{\mathrm{ur}}/K)} \cong T(\ell^d)^{\mathrm{Gal}(K^{\mathrm{ur}}/K)} = \{\, x \in T : (\varphi - \ell^d)(x) = 0 \,\} = 0,$$

since by the Weil conjectures $\varphi = \mathrm{Frob}_\ell^{\ell^d}$ acts on T in a semisimple way and the absolute value of its eigenvaues α_1, α_2 is $\ell^{d/2}$: if $x = \binom{x_1}{x_2}$, then

$$(\varphi - \ell^d)(x) = \begin{pmatrix} \alpha_1 - \ell^d & 0 \\ 0 & \alpha_2 - \ell^d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} (\alpha_1 - \ell^d)x_1 \\ (\alpha_2 - \ell^d)x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

if and only if $x_1 = x_2 = 0$ as $|\alpha_i| \neq \ell^d$ and hence $\alpha_1 - \ell^d \neq 0$ for $i = 1, 2$. □

Applying this result to K_λ and $K[\ell]_\lambda$ and Lemma [Rub00, B.2.8], then we see that

$$\begin{array}{ccccccc} \mathrm{H}^1(G_0, T) & \xleftarrow{\sim} & \mathrm{H}^1(K_\lambda^t/K_\lambda, T) & \xleftarrow{\sim} & \mathrm{H}^1(K_\lambda^{\mathrm{ur}}/K_\lambda, T) & \xrightarrow{\sim} & T/(\varphi^2 - 1)T \\ & & \downarrow\wr & & \downarrow\wr & \nearrow\sim & \\ & & \mathrm{H}^1(\hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}}) & \xleftarrow{\sim} & \mathrm{H}^1(2\hat{\mathbb{Z}}, T) & & \end{array}$$

where the middle isomorphism is the inflation and the last one is the evaluation at φ^2. Similarly $\mathrm{H}^1(H_0, T) \cong T/(\varphi^2 - 1)T$. This means that for a 1-cocycle $F \in Z^1(\hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}})$,we have

$$F(\tau^u \varphi^{2v}) = (1 + \varphi^2 + \cdots + \varphi^{2(v-1)})a + (\varphi^2 - 1)b,$$

where $a, b \in T$ and $a \cong F(\varphi^2) \bmod (\varphi^2 - 1)T$, i.e. $a \bmod (\varphi^2 - 1)T$ corresponds to the class $[F] \in \mathrm{H}^1(\hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}}, T)$ in the above isomorphism. Indeed, as $F(\tau) = 0$ (since the inflation is an isomorphism) and τ acts trivially on T (that is unramified at $\ell \neq Np$), then

$$F(\tau^v) = F(\tau\tau^{v-1}) = F(\tau) + \tau \cdot F(\tau^{v-1}) = F(\tau^{v-1}) = \cdots = F(\tau) = 0,$$

and therefore

$$\begin{aligned} F(\tau^u \varphi^{2v}) &= F(\tau^u) + \tau^u \cdot F(\varphi^{2v}) = F(\varphi^2 \varphi^{2(v-1)}) = F(\varphi^2) + \varphi^2 \cdot F(\varphi^{2(v-1)}) \equiv \\ &\equiv a + \varphi^2 \cdot (F(\varphi^2) + \varphi^2 \cdot F(\varphi^{2(v-2)})) \equiv a + \varphi^2 \cdot a + \varphi^4 \cdot F(\varphi^{2(v-2)}) = \\ &= \cdots \equiv (1 + \varphi^2 + \cdots + \varphi^{2(v-1)})a \bmod (1 + \varphi^2)T. \end{aligned}$$

Now let $x := z_{f,1} \in \mathrm{H}^1(K[1], T) = \mathrm{H}^1(G, T)$, $y := z_{f,\ell} \in \mathrm{H}^1(K[\ell], T) = \mathrm{H}^1(H, T)$, so that $\mathrm{cores}_H^G(y) = a_\ell x$ and $z := \mathcal{D}(\ell) \in \mathrm{H}^1(G, A[p^M]) = \mathrm{H}^1(K[1], A[p^M])$. In particular we have that $\mathrm{res}_H^G(z) = D_\ell(\mathrm{red}_{p^M}(y)) \in \mathrm{H}^1(H, A[p^M])$. Note that for any $\alpha \in \mathrm{H}^1(H, A[p^M])$,

$$\mathrm{res}_{H_0}^H(D_\ell \alpha) = \sum_{i=1}^{\ell} i\sigma_0^i \cdot \alpha,$$

and for any $t \in T$:

$$\sum_{i=1}^{\ell} i\tilde{\sigma}^i \cdot t = \sum_{i=1}^{\ell} it = \left(\frac{(\ell+1)\ell}{2}\right)t \equiv 0 \bmod p^M T$$

as σ_0 acts as σ_0^{ur}, that corresponds to τ and hence acts trivially on T.

Thus $\mathrm{res}_{H_0}^G(z) = 0 \in \mathrm{H}^1(G, A[p^M]) = \mathrm{H}^1(K[1]_\lambda, A[p^M])$ and hence by the inflation-restriction exact sequence there is

$$z_0 \in \mathrm{H}^1(G_0/H_0, A[p^M]) \cong \mathrm{Hom}_{\mathrm{cont}}(\langle\sigma_0\rangle, A[p^M])$$

such that $\mathrm{infl}^{G_0}_{G_0/H_0}(z_0) = \mathrm{res}^G_{G_0}(z) \in \mathrm{H}^1(G_0, A[p^M])$. Our next goal will be to calculate $z_0(\sigma_0)$. In order to do that we need to perform some computations at the levels of cocycles: let $\tilde{x} \in Z^1(G,T)$, $\tilde{y} \in Z^1(H,T)$ representing respectively x and y.

Since $\mathrm{cores}(y) = a_\ell x$, then $\mathrm{cores}(\tilde{y}) - a_\ell \tilde{x}$ is a coboundary, i.e. there is an element $a \in T$ such that for any $g \in G$,

$$\mathrm{cores}(\tilde{y})(g) - a_\ell \tilde{x} = (g-1)a,$$

moreover the computations of [Nek92, Sec. 7] show that $z(\sigma_0) = -a$. Restricting to $g = g_0 \in G_0$ (fixing a lift $\tilde{\sigma}_0 \in G_0$ of $\sigma_0 \in G_0/H_0$)

$$\sum_{i=0}^{\ell} \tilde{y}(\tilde{\sigma}_0^{-i} g_0 \tilde{\sigma}_0^i) - a_\ell \tilde{x}(g_0) = (g_0 - 1)a.$$

On the other end, if $\pi(g_0) = \varphi^2$, we showed above that

$$\tilde{x}(g_0) = a_x + (\varphi^2 - 1)b_x, \qquad \tilde{y}(g_0) = a_y + (\varphi^2 - 1)b_y,$$

where $a_x, a_y, b_x, b_y \in T$ and $[\mathrm{res}^G_{G_0}(\tilde{x})]$,$[\mathrm{res}^H_{H_0}(\tilde{y})]$ correspond respectively to $a_x, a_y \bmod (\varphi^2-1)T$ and therefore evaluating the formula at $g_0 = \varphi^2$ we get:

$$(\ell+1)a_y - a_\ell a_x = (\varphi^2 - 1)(a + a_\ell b_x - (\ell+1)b_y)$$

and since T is torsion free, but $p^M \mid a_\ell, \ell+1$,

$$\frac{\ell+1}{p^M} a_x - \frac{a_\ell}{p^M} = \frac{(\varphi^2-1)}{p^M}(a + p^M \cdot *),$$

for $* = \frac{a_\ell}{p^M} b_x - \frac{\ell+1}{p^M} b_y \in T$. Now observe that $\mathrm{res}^G_{G_0}(x) = \mathrm{loc}_\ell(z_{f,1})$ and $\mathrm{res}^H_{H_0}(y) = \mathrm{loc}_\ell(z_{f,\ell})$ and φ is the local Frobenius, therefore by (E2) we get that $\varphi(a_x) \cong a_y \bmod (\varphi^2-1)T$: we may safely suppose to have previously choosen $a_y = \varphi(a_x)$. Moreover on T

$$\varphi^2 - \frac{a_\ell}{\ell^{k/2-1}}\varphi + \ell = 0$$

since $\mathrm{char}(\mathrm{Frob}_\ell \,|T) = X^2 - a_\ell/\ell^{k/2-1}\, X + \ell$ by 1.3.7 and therefore the above formula becomes

$$\left(\frac{\ell+1}{p^M}\varphi - \frac{a_\ell}{p^M}\right)a_x = \left(\frac{a_\ell}{p^M}\ell^{1-k/2}\varphi - \frac{(\ell+1)}{p^M}\right)a + p^M \cdot *$$

and hence, reducing to $A[p^M]$:

$$\left(\frac{\ell+1}{p^M}\tau_c - \frac{a_\ell}{p^M}\right)\mathrm{red}_{p^M}(a_x) = \left(\frac{a_\ell}{p^M}(-1)^{1-k/2}\tau_c - \frac{(\ell+1)}{p^M}\right)\mathrm{red}_{p^M}\, a.$$

In fact, since $\tau_c^2 = \mathrm{id}$, then its minimal polynomial over $A[p^M]$ is $X^2 - 1$, therefore it coincides with the minimal polynomial of φ over $A[p^M]$, since $a_\ell \equiv 0 \bmod p^M$ and $\ell \equiv -1 \bmod p^M$. Now we want to express a in terms od $\mathrm{loc}_\ell(z) = \mathrm{infl}^{G_0}_{G_0/H_0}(z_0)$: as σ_0 may be lifted to τ and $a = -z_0(\sigma_0)$, then it is enough to apply the finite singular isomorphism that exchanges cocylces with the same values on τ_ℓ and Frob_ℓ. We then apply the corestriction to trasfer this formula to $P(1)$ and $P(\ell)$: note first that $\tau_c \cdot P(1) = w_f P(1)$ and $\tau_c \cdot P(\ell) = -w_f P(\ell)$, hence we obtain the desired formula.

The general formula is proven in the same way if we put, for $n = m \cdot \ell$, $G = \mathrm{Gal}(K[n]/K[1])$, $H = \mathrm{Gal}(K[n]/K[m])$, $G_0 = \mathrm{Gal}(K[n]_\lambda/K[1]_\lambda)$, $H_0 = \mathrm{Gal}(K[n]_\lambda/K[m]_\lambda)$, $x = \mathcal{D}(m)z_{f,n}$, $y = \mathcal{D}(m)z_{f,m}$ since these groups and classes enjoy all the properties we listed above and that made the proof work. Just observe that in that case $\tau_c \cdot P(n) = \varepsilon_n P(n)$ and $\tau_c \cdot P(m) = \varepsilon_{n-1}P(m) = -\varepsilon_n P(m)$. □

Now we can come back to the proof of Th. 2.3.9

Proof (Th. 2.3.9). We established for the classes $P(n)$, that we defined in terms of generalized Heegner cycles, the properties listed in [Bes97, Th. 3.2]. We don't need to show anything else: indeed the proof of [Bes97, Th. 2.1] is just a formal consequence of these properties and does not depend on their actual definition. It applies *verbatim* therefore to our case, leading to a full proof of 2.3.9. □

Chapter 3

Selmer Complexes

In the first chapter we introduced several notions of Selmer group attached to a p-adic representation, generalizing the notion of Selmer group of an elliptic curve. In this chapter we treat even more general objects: the *Selmer Complexes*, introduced by J. Nekovar in [Nek06]. The importance of Selmer Complexes is that their cohomolgy objects give rise to a notion of *generalized Selmer group*, that in the cases of "bad reduction" beaves better than the usual theory of Selmer groups. However, we will not need the full power of Selmer Complexes, but we use them only as intermediate objects in order to study the structure of more classical Selmer groups. In this chapter we give a brief overview of the theory of Selmer Complexes for the convenience of the reader and we see how the classical (Greenberg) Selmer groups fit into this theory.

Notations

We collect here some notations that we introduce in this chapter:

- $(R\text{-Mod})$: Modules over any commutative ring R;
- $(R\text{-Mod})_{\mathrm{ft}}$: R-modules of finite type (noetherian);
- $(R\text{-Mod})_{\mathrm{coft}}$: R-modules of cofinite type (artinian);
- $\mathrm{C}^*(\mathscr{C})$, for $* = \emptyset, b, +, -$: the category of all (resp. bounded, bounded below, bounded above) complexes in an abelian category $\mathscr{C}$;
- $\mathrm{K}^*(\mathscr{C})$, for $* = \emptyset, b, +, -$: homotopy category (+ bounds) of an abelian category $\mathscr{C}$;
- $\mathrm{D}^*(\mathscr{C})$, for $* = \emptyset, b, +, -$: derived category (+ bounds) of an abelian category $\mathscr{C}$;
- $\mathrm{D}^*_{\mathscr{C}'}(\mathscr{C})$, for $* = \emptyset, b, +, -$: derived category (+ bounds) of an abelian category $\mathscr{C}$ such that the cohomology objects belong (up to iso) to a full subcategory $\mathscr{C}'$ of $\mathscr{C}$.

From Sec. 3.1.2:

- R: a fixed noetherian complete local ring of dimension d, maximal ideal $\mathfrak{m}$ and finite residue field k of characteristic $p > 2$;
- G: a profinite group;
- $(R[G]\text{-Mod})^{\mathrm{ad}}$: Admissible $R[G]$-modules;
- $(R[G]\text{-Mod})^{\text{ind-ad}}$: Ind-admissible $R[G]$-modules;
- $(R[G]\text{-Mod})_{\{\mathfrak{m}\}}$: $R[G]$-modules M supported on $\mathfrak{m}$ (i.e. $M = \bigcup_{n>0} M[\mathfrak{m}^n]$).

3.1 Homological Algebra

In order to introduce Selmer Complexes we first need to recall some constructions that we can make starting from complexes in an abelian category. Let us fix an abelian category $\mathscr{C}$, and consider the corresponding category of complexes $\mathrm{C}(\mathscr{C})$. Given a complex $X \in \mathrm{Ob}\left(\mathrm{C}(\mathscr{C})\right)$ we denote by X^i the object of $\mathscr{C}$ in the i-th position and by $\mathrm{d}_X^i\colon X^i \to X^{i+1}$, the i-th differential of X. Recall that a map of complexes $f \in \mathrm{Hom}_{\mathrm{C}(\mathscr{C})}(X, Y)$ is a collection of morphisms $f^i\colon X_i \to Y_i$ compatible with the differentials. The content of this section can be found in [Nek06, Ch. 1].

3.1.1 Constructions of complexes

Shift and Cone

Definition 3.1.1. For any $n \in \mathbb{Z}$ we define the *translation (or shift) by n* functor

$$[n]\colon \mathrm{C}(\mathscr{C}) \to \mathrm{C}(\mathscr{C});$$

On objects: for any $X \in \mathrm{C}(\mathscr{C})$; $X[n]$ is the complex such that $X[n]^i = X^{n+i}$; $\mathrm{d}^i_{X[n]} = (-1)^n \mathrm{d}_X^{i+n}$. On morphisms: if $X, Y \in \mathrm{C}(\mathscr{C})$ and $f\colon X \to Y$ is a map of complexes, $f[n]\colon X[n] \to Y[n]$ is the map of complexes such that $f[n]^i = f^{i+n}$.

Remark 3.1.2. Note that for us $X[1]$ represent the translation of X by 1 *to the left* and $X[-1]$ the translation by 1 *to the right*, whereas in some references one takes the opposite convention.

Remark 3.1.3. In the following we will see $\mathscr{C}$ embedded in $\mathrm{C}(\mathscr{C})$: $X \in \mathrm{Ob}(\mathscr{C})$ and we see it as the complex, still denoted by X, such that $X^0 = X$, $X^i = 0$ for $i \neq 0$ and everywhere 0-differentials. We say that such a complex is *concentrated in degree* 0. Following the warning of the previous remark: pay attention that $X[k]$ is a complex concentrated in degree $-k$ (and not in degree k, as one could expect).

Definition 3.1.4. Let $X, Y \in \mathrm{C}(\mathscr{C})$ and $f\colon X \to Y$. The *Mapping Cone* of f is the complex $\mathrm{Cone}(f)$ that is $Y \oplus X[1]$ at the level of objects, with differentials

$$\mathrm{d}^i_{\mathrm{Cone}(f)} = \begin{pmatrix} \mathrm{d}_Y & f^{i+1} \\ 0 & -\mathrm{d}_X^{i+1} \end{pmatrix} : Y^i \oplus X^{i+1} \to Y^{i+1} \oplus X^{i+2}.$$

Tensor products and Hom

In this section the capital letters $X, Y, Z, \ldots$ will denote complexes of R-modules, for a commutative ring R.

Definition 3.1.5. We define the complex $X \otimes_R Y$ by

$$(X \otimes_R Y)^n = \bigoplus_{i \in \mathbb{Z}} X^i \otimes Y^{n-i},$$

with differentials defined by the formula

$$\mathrm{d}^n(x \otimes y) = \mathrm{d}_X^i x \otimes y + (-1)^i x \otimes \mathrm{d}_Y^{n-i} y \in (X^{i+1} \otimes Y^{n-i}) \oplus (X^i \oplus Y^{n-i+1}),$$

for $x \otimes y \in X^i \otimes_R Y^{n-i}$.

Definition 3.1.6. We define the complex $\mathrm{Hom}^\bullet_R(X,Y)$ by

$$\mathrm{Hom}^n_R(X,Y) = \prod_{i\in\mathbb{Z}} \mathrm{Hom}_R(X^i, Y^{i+n}),$$

with differentials defined by the formula

$$\mathrm{d}^n f = (\mathrm{d}^{n+i}_Y \circ f_i + (-1)^{n-1} f_{i+1} \circ \mathrm{d}^i_X)_{i\in\mathbb{Z}},$$

for $f = (f_i)_{i\in\mathbb{Z}} \in \mathrm{Hom}^n_R(X,Y)$.

Remark 3.1.7. If Y is a bounded (resp. bounded below) complex of injective R-modules and Y is any (resp. bounded above) complex of R-modules, then the complex $\mathrm{Hom}^\bullet_R(X,Y)$ represents the right derived functor $\mathbb{R}\,\mathrm{Hom}_R(X,Y)$, meaning that its localization into the derived category $\mathrm{D}(R\text{-Mod})$ coincide with $\mathbb{R}\,\mathrm{Hom}_R(X,Y)$. For the reader interested in a complete discussion of this topic see also [KS06, Sec 13.3, 13.4].

Simmetries

We have the following isomorphisms of complexes:

- The associativity isomorphism

$$\begin{array}{ccc} (X\otimes_R Y)\otimes_R Z & \xrightarrow{\sim} & X\otimes_R (Y\otimes_R Z) \\ (x\otimes y)\otimes z & \longmapsto & x\otimes (y\otimes z) \end{array},$$

- The transposition isomorphism s_{12}

$$\begin{array}{rcl} s_{12}\colon X\otimes_R Y & \xrightarrow{\sim} & Y\otimes_R X \\ X^i\otimes_R Y^j \ni x\otimes y & \longmapsto & (-1)^{ij} y\otimes x \end{array},$$

- The transposition isomorphism s_{23}

$$\begin{array}{rcl} s_{23}\colon (X\otimes_R A)\otimes_R (Y\otimes_R B) & \xrightarrow{\sim} & (X\otimes_R Y)\otimes_R (A\otimes_R B) \\ (X^i\otimes_R A^a)\otimes_R (Y^j\otimes_R B^b) \ni (x\otimes a)\otimes (y\otimes b) & \longmapsto & (-1)^{aj}(x\otimes y)\otimes (a\otimes b) \end{array}.$$

And the transposition isomorphisms are compatible, i.e. the following diagram commutes

$$\begin{array}{ccc} (X\otimes_R A)\otimes_R (Y\otimes_R B) & \xrightarrow[s_{23}]{\sim} & (X\otimes_R Y)\otimes_R (A\otimes_R B) \\ {\scriptstyle s_{12}}\downarrow\wr & & \wr\downarrow{\scriptstyle s_{12}\otimes s_{12}} \\ (Y\otimes_R B)\otimes_R (X\otimes_R A) & \xrightarrow[s_{23}]{\sim} & (Y\otimes_R X)\otimes_R (B\otimes_R A) \end{array}.$$

Adjunction

We have an adjunction morphism at the level of complexes

$$\mathrm{adj}\colon \operatorname{Hom}^\bullet_R(X\otimes Y, Z) \longrightarrow \operatorname{Hom}^\bullet_R\big(X, \operatorname{Hom}^\bullet_R(Y,Z)\big)$$

given by the following formula: if $f = \big(f_r\colon (X\otimes Y)^r \to Z^{r+n}\big)_{r\in\mathbb{Z}} \in \operatorname{Hom}^n_R(X\otimes Y, Z)$, then $\mathrm{adj}(f) = \big(\mathrm{adj}(f)_i\colon X^i \to \operatorname{Hom}^{i+n}_R(Y,Z)\big)_{i\in\mathbb{Z}}$, where $\big(\mathrm{adj}(f)_i(x)\big)_j(y) = f_{i+j}(x\otimes y)$, for $x\in X^i$, $y\in Y^j$. It induces an adjunction morphism of R-modules

$$\mathrm{adj}\colon \operatorname{Hom}_{\mathrm{C}(R\text{-Mod})}(X\otimes Y, Z) \longrightarrow \operatorname{Hom}_{\mathrm{C}(R\text{-Mod})}\big(X, \operatorname{Hom}^\bullet_R(Y,Z)\big).$$

Indeed

$$\operatorname{Hom}_{\mathrm{C}(R\text{-Mod})}(A,B) = \{\, f\in \operatorname{Hom}^0_R(A,B) : d_B\circ f = f\circ d_A \,\}$$

so if $f\in \operatorname{Hom}_{\mathrm{C}(R\text{-Mod})}(X\otimes Y, Z)$, then of course $\mathrm{adj}(f)\in \operatorname{Hom}^0_R\big(X, \operatorname{Hom}^\bullet_R(Y,Z)\big)$, but it is easy to check that $\mathrm{adj}(f)$ commutes with the differentials.

Both morphisms are monomorphisms, and isomorphisms if X, Y are bounded above and Z bounded below.

Evaluations

We have two evaluation maps

$$\begin{aligned}\mathrm{ev}_1\colon \operatorname{Hom}^\bullet_R(X,Y)\otimes X &\longrightarrow Y\\ \operatorname{Hom}^i_R(X^r, Y^{r+i})\otimes X^j \ni (f_r : X^r \to Y^{r+i})_{r\in\mathbb{Z}}\otimes x &\longmapsto f_j(x)\in Y_{i+j}\end{aligned}$$

and

$$\begin{aligned}\mathrm{ev}_2\colon X\otimes \operatorname{Hom}^\bullet_R(X,Y) &\longrightarrow Y\\ X^j\otimes \operatorname{Hom}^i_R(X^r, Y^{r+i}) \ni x\otimes (f_r : X^r \to Y^{r+i})_{r\in\mathbb{Z}} &\longmapsto (-1)^{ij} f_j(x)\in Y_{i+j}\end{aligned}$$

and it is easy to check that these are compatible with the transposition morphism, in the sense that the following diagram commutes:

$$\begin{array}{ccc}\operatorname{Hom}^\bullet_R(X,Y)\otimes X & \xrightarrow{\mathrm{ev}_1} & Y\\ {\scriptstyle s_{12}}\big\downarrow & & \big\| \\ X\otimes \operatorname{Hom}^\bullet_R(X,Y) & \xrightarrow{\mathrm{ev}_2} & Y\end{array}.$$

Note moreover that $\mathrm{adj}(\mathrm{ev}_1) = \mathrm{id}$, under the adjunction morphism

$$\mathrm{adj}\colon \operatorname{Hom}_{\mathrm{C}(R\text{-Mod})}(\operatorname{Hom}^\bullet_R(X,Y)\otimes X, Y) \longrightarrow \operatorname{Hom}_{\mathrm{C}(R\text{-Mod})}\big(\operatorname{Hom}^\bullet_R(X,Y), \operatorname{Hom}^\bullet_R(X,Y)\big).$$

Indeed for any $f = (f_r)_{r\in\mathbb{Z}} \in \operatorname{Hom}^i_R(X,Y)$, $x\in X^j$,

$$\big(\mathrm{adj}(\mathrm{ev}_1)_i(f)\big)_j(x) = (\mathrm{ev}_1)_{i+j}(f\otimes x) = f_j(x)\in Y^{i+j}.$$

Dualizing functors

Let I an R-module and consider the functor

$$D_I(\,-\,) = \mathrm{Hom}_R(\,-\,, I)\colon (R\text{-Mod})^{\mathrm{op}} \to (R\text{-Mod}).$$

Definition 3.1.8. We say that D_I is dualizing if the canonical morphims $\varepsilon\colon M \to D\big(D(M)\big)$ are isomorphisms, for any $M \in (R\text{-Mod})_{\mathrm{ft}}$.

If D_I is dualizing, we can construct a duality theory for D, called Maltis Duality. The following proposition resume [BH93, Sec. 3.2].

Proposition 3.1.9. *D_I is dualizing if and only if I is an injective hull of k [BH93, Def. 3.2.3]. Such a module is unique up to a unique isomorphism, therefore we an injective hull I of k and we denote D_I by D_R. The functor D_R is exact and induces an equivalence of categories*

$$(R\text{-Mod})_{\mathrm{ft}}^{\mathrm{op}} \longleftrightarrow (R\text{-Mod})_{\mathrm{coft}}.$$

In particular the map ε is an isomorphism for both $M \in (R\text{-Mod})_{\mathrm{ft}}$ and $M \in (R\text{-Mod})_{\mathrm{coft}}$.

Example 3.1.10. If R is a complete discrete valuation ring with fraction field K, K/R is an injective hull of k. In the case of $R = \mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_p$ then $D_R(M)$ coincide with the Pontryagin dual for R-modules of finite and cofinite type, equipped the finite type modules with the $\mathfrak{m}$-adic topology and the cofinite type ones with the discrete topology. (See [Nek06, Sec 2.9], Def. 1.1.10 and the following discussion).

In the case of $M^\bullet, J^\bullet \in \mathrm{C}(R\text{-Mod})$ the analogous functor is $D_{J^\bullet}(M^\bullet) = \mathrm{Hom}_R^\bullet(M^\bullet, J^\bullet)$. When $J^\bullet = I[n]$, for I an injective hull of k, $n \in \mathbb{Z}$, we denote $D_{I[n]}$, by $D_{R,n}$. The morphism of complexes

$$\varepsilon_n\colon M^\bullet \longrightarrow D_{R,n}\big(D_{R,n}(M^\bullet)\big)$$

is an isomorphism for any $M^\bullet \in \mathrm{D}_*(R\text{-Mod})$, where $* = \mathrm{ft}, \mathrm{coft}$.

3.1.2 Continuous cohomology

Let from now on R be a noetherian complete local ring, with maximal ideal $\mathfrak{m}$, finite residue field k of characteristic $p > 2$. In this section we will extend the notion of continuous cohomology groups to complexes of $R[G]$-modules, for a profinite group G. Recall that an $R[G]$-module is equivalently an R-module endowed with an R-linear action of G, where the action is given by the multiplication by the group-like elements of $R[G]$. For such an M we denote by λ_M the action

$$\lambda_M\colon G \times M \to M; \qquad \lambda_M(g, m) = g(m)$$

and by ρ_M the induced R-linear map

$$\rho_M\colon R[G] \to \mathrm{End}_R(M); \quad \rho_M\big(\sum_i r_i g_i\big)(m) = \sum_i r_i g_i(m).$$

Definition 3.1.11. We say that M is an admissible $R[G]$-module if $\mathrm{Im}(\rho_M)$ is an R-module of finite type and the map $G \to R[G] \to \mathrm{Im}(\rho_M)$ is continuous, when $\mathrm{Im}(\rho_M)$ is equipped with the $\mathfrak{m}$-adic topology.

The admissible $R[G]$-modules form an abelian full subcategory $(R[G]\text{-Mod})^{\mathrm{ad}}$ of $(R[G]\text{-Mod})$ with enough injectives.

We are interested mainly in $R[G]$-modules that are of finite or of cofinite type over R. In this case these modules are admissible if and only if the action of G is continuous, more precisely:

Proposition 3.1.12 ([Nek06, Lemma 3.2.4])**.** *Let T (resp. A) be an $R[G]$-module of finite (resp. cofinite) type over R. If we equip it with the $\mathfrak{m}$-adic topology (resp. discrete) topology, then T (resp. A) is admissible if and only if the action $\lambda_T\colon G\times T\to T$ (resp. $\lambda_A\colon G\times A\to A$) is continuous.*

REMARK 3.1.13. In [Nek06, Def. 3.3.1] Nekovar introduces a more general class of modules for wich the continuous cohomology can be defined, called *ind-admissible*, that are inductive limits of admissible modules. Several of the following definitions and results are stated there in these more general terms. However we will enounce them just in terms of admissible modules by simplicity as for $R[G]$-modules (co)finitely generated over R, namely the class of modules we are interested in, the two notions are equivalent by [Nek06, Prop. 3.3.5.vi]. Therefore when, discussing of Iwasawa Theory, we will meet true ind-admissible modules the reader shouldn't be harmed if we give reference to previous results for admissible ones: they hold also in the ind-admissible case.

For an admissible $R[G]$-module M we may consider the complex of the continuous cochains, introduced by Tate in [Tat76]: we denote

$$\mathrm{C}^i_{\mathrm{cont}}(G,M) := \{\,\text{continuous maps } G^i\to M\,\}\,.$$

and we let $\delta^i_M\colon \mathrm{C}^i_{\mathrm{cont}}(G,M)\to \mathrm{C}^{i+1}_{\mathrm{cont}}(G,M)$ be the standard differential defined by

$$(\delta^i c)(g_1,\dots,g_{i+i}) = g_1c(g_2,\dots,g_{i+1})+\sum_{j=1}^{i}(-1)^j c(g_1,\dots,g_jg_{j+1},\dots,g_{i+1})+(-1)^{i-1}c(g_1,\dots,g_i).$$

Definition 3.1.14. Let $M\in(R[G]\text{-Mod})^{\mathrm{ad}}$. The continuous cohomology $\mathrm{H}^i_{\mathrm{cont}}(G,M)$ of G with values in M is the i-th cohomology object of the complex $(\mathrm{C}^i_{\mathrm{cont}}(G,M),\delta^i)$. It has an R-module structure.

We define a continuous cochains complex $\mathrm{C}^\bullet_{\mathrm{cont}}(G,M^\bullet)$ also for a complex $(M^\bullet,\mathrm{d}_{M^\bullet})$ of $R[G]$-admissible modules: its component of degree n is

$$\mathrm{C}^n_{\mathrm{cont}}(G,M^\bullet) = \bigoplus_{i+j=n}\mathrm{C}^j_{\mathrm{cont}}(G,M^i).$$

and the differential is $\delta^n_{M^\bullet}$ restricts to $\mathrm{C}^j_{\mathrm{cont}}(G_v,\mathrm{d}^i_{M^\bullet})+(-1)^j\delta^j_{M^i}$ on $\mathrm{C}^j_{\mathrm{cont}}(G_v,M^i)$.

Definition 3.1.15. The i-th hypercohomology module $\mathrm{H}^i_{\mathrm{cont}}(G,M^\bullet)$ with values in $M^\bullet$ is defined to be the i-th cohomology of $\mathrm{C}^\bullet_{\mathrm{cont}}(G,M^\bullet)$.

The functor $M^\bullet\mapsto \mathrm{C}^\bullet_{\mathrm{cont}}(G,M^\bullet)$ induces an exact functor on the derived categories

$$\mathbb{R}\Gamma_{\mathrm{cont}}(G,-)\colon\ \mathrm{D}^+(R[G]\text{-Mod})^{\mathrm{ad}}\to\mathrm{D}^+(R\text{-Mod}).$$

REMARK 3.1.16. Note that $\mathrm{C}^\bullet_{\mathrm{cont}}(G,M^\bullet)$ is by definition the total complex of the double complex $\left(\mathrm{C}^j_{\mathrm{cont}}(G,M^i)\right)_{i,j}$ with the differentials of the rows induced by these of $M^\bullet$ and the standard cohomological ones on the columns.

Many features of cohomology groups extend to the case of complexes. Recall for instance the cup products:

Definition 3.1.17. Let $A,B\in(R[G]\text{-Mod})^{\mathrm{ad}}$, the cup products are the R-linear maps

$$\cup_{ij}\colon \mathrm{C}^i_{\mathrm{cont}}(G,A)\otimes_R\mathrm{C}^j_{\mathrm{cont}}(G,B)\to\mathrm{C}^{i+j}_{\mathrm{cont}}(G,A\otimes_R B)$$

defined by the usual formula

$$(\alpha \cup \beta)(g_1, \dots, g_{i+j}) = \alpha(g_1, \dots, g_i) \otimes (g_1 \cdot \dots \cdot g_i)\beta(g_{i+1}, \dots, g_{i+j}).$$

They induce a morphism of complexes

$$\cup \colon \mathrm{C}^\bullet_{\mathrm{cont}}(G, A) \otimes_R \mathrm{C}^\bullet_{\mathrm{cont}}(G, B) \to \mathrm{C}^\bullet_{\mathrm{cont}}(G, A \otimes_R B)$$

since $\delta(\alpha \cup \beta) = \delta\alpha \cup \beta + (-1)^i \alpha \cup \delta\beta$.

This definition can be extended to the cup product of complexes:

Definition 3.1.18. Let $A^\bullet, B^\bullet$ complexes in $(R[G]\text{-Mod})^{\mathrm{ad}}$, the individual cup products

$$\cup^{ab}_{ij} \colon \mathrm{C}^i_{\mathrm{cont}}(G, A^a) \otimes_R \mathrm{C}^j_{\mathrm{cont}}(G, B^b) \to \mathrm{C}^{i+j}_{\mathrm{cont}}(G, A^a \otimes_R B^b)$$

can be combined to the total cup product

$$\cup \colon \mathrm{C}^\bullet_{\mathrm{cont}}(G, A^\bullet) \otimes_R \mathrm{C}^\bullet_{\mathrm{cont}}(G, B^\bullet) \to \mathrm{C}^\bullet_{\mathrm{cont}}(G, A^\bullet \otimes_R B^\bullet)$$

choosing carefully the signs: $\cup$ on $\mathrm{C}^i_{\mathrm{cont}}(G, A^a) \otimes_R \mathrm{C}^j_{\mathrm{cont}}(G, B^b)$ is defined to be $(-1)^{ib}\cup^{ab}_{ij}$.

Remark 3.1.19. If $G = G_v$ is the absolute Galois group of a local field, its cohomological properties show that if A is an R-module with trivial G_v-action and $A(1) = A \otimes \mathbb{Z}_p(1)$ is the first Tate twist of A (see Ex. 1.1.3), then by local class field theory and the since the p-cohomological dimension of G_v is 2 we have that

$$\mathrm{H}^2\big(G_v, A(1)\big) \cong A, \qquad \mathrm{H}^j\big(G_v, A(1)\big) = 0, \text{ for } j > 2.$$

Therefore there is a quasi isomorphism

$$A[-2] \to \tau_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}\big(G_v, A(1)\big),$$

recall indeed that the truncation $\tau_{\geq n}$ of a complex $(M^\bullet, d_M)$ is defined to be the complex

$$\tau_{\geq n}M^\bullet \colon [\dots \to 0 \to 0 \to \operatorname{coker} \mathrm{d}_M^{n-1} \to M^{n+1} \to M^{n+2} \to \dots],$$

and hence by definition

$$\mathrm{H}^i(\tau_{\geq n}M^\bullet) = \begin{cases} \mathrm{H}^i(M^\bullet), & \text{for } i \geq n; \\ 0 & \text{for } i < n. \end{cases}$$

More in general if $A^\bullet$ is a bounded below complex of R-modules, then i_v induce a canonical morphism between the double complexes whose i-th columns are respectively the complexes $A^i[-2]$ and the truncation $\tau_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}\big(G_v, A^i(1)\big)$. Denote the total complex of the latter by $\tau^{II}_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}\big(G_v, A^\bullet(1)\big)$ and observe that the total complex of the former is $A^\bullet[-2]$: there is therefore an induced quasi-isomorphism of complexes

$$i_v \colon A^\bullet[-2] \to \tau^{II}_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}\big(G_v, A^\bullet(1)\big).$$

If $A^\bullet = J$ is a bounded below complex of injective R-modules with trivial G_v action, then i_v has a homotopy inverse (unique up to homotopy)

$$r_v = r_{J,v} \colon \tau^{II}_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}\big(G_v, J(1)\big) \to J[-2].$$

We conclude this section with a definition for later reference.

Definition 3.1.20. An admissible $R[G]$-module is said to be supported on $\mathfrak{m}$ if $M = \varinjlim_n M[\mathfrak{m}^n]$. The full subcategory of such modules will be denoted by $(R[G]\text{-Mod})^{\mathrm{ad}}_{\{\mathfrak{m}\}}$.

3.2 Selmer Complexes

In this section we introduce Selmer Complexes. All the notations and assumptions of the previous sections are in force. Fix moreover a number field K and a finite set S of primes of K containing all the archimedean places and all primes above p. By S_f we denote the finite (non-archimedean) primes of S. In this section the role of G will be played by the Galois groups G_K, $G_{K,S}$ and G_{K_v}. Note that, as in Prop. 1.1.8, an admissible $R[G_{K,S}]$-module is an admissible $R[G_K]$-module unramified at all $v \notin S$. This material can be found in [Nek06, Ch. 6].

3.2.1 General definitions

Definition 3.2.1. Let X a complex in $(R[G_{K,S}]\text{-Mod})^{\mathrm{ad}}$. A local condition for X is a collection $\Delta(X) = (\Delta_v(X))_{v\in S_f}$, where $\Delta_v(X)$ consists of a complex $U_v^+(X)$ of R-modules together with a morphism of complexes

$$i_v^+(X)\colon U_v^+(X) \to \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X).$$

Denote $i_S^+(X) = (i_v^+(X))$.

Definition 3.2.2. The Selmer complex attached to the local condition $\Delta(X)$ on X is the complex

$$\widetilde{\mathbb{R}\Gamma}_f(G_{K,S}, X; \Delta(X)) = \mathrm{Cone}\left(\mathrm{C}^\bullet_{\mathrm{cont}}(G_{K,S}, X) \oplus \bigoplus_{v\in S_f} U_v^+(X) \xrightarrow{\mathrm{res}\, - i_S^+(X)} \bigoplus_{v\in S_f} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X)\right)[-1].$$

We will often see it implicitly as an object of the derived category.

Definition 3.2.3. The i-th generalized Selmer group of X with local conditions $\Delta(X)$ is

$$\widetilde{\mathrm{H}}^i(G_{K,S}, X, \Delta(X)) = \mathrm{H}^i\big(\widetilde{\mathbb{R}\Gamma}_f(G_{K,S}, X; \Delta(X))\big).$$

It has an R-module structure.

Write moreover $U_v^-(X) = \mathrm{Cone}\big(U_v^+(X) \xrightarrow{-i_v^+(X)} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X)\big)$. Explicitely

$$U_v^-(X)^j = \mathrm{C}^j_{\mathrm{cont}}(G_v, X) \oplus U_v^+(X)^{j+1}$$

and the differential is given, for $x \in \mathrm{C}^j_{\mathrm{cont}}(G_v, X)$, $y \in U_v^+(X)^{j+1}$, by

$$\mathrm{d}^j_{U^-}(a, b) = (\delta^j a - i_v^+(X)^j b, -\mathrm{d}^{j+1}_{U^+} b).$$

Orthogonal Local conditions

Fix J a bounded complex of injective R-modules and let X, Y be two complexes of admissible $R[G_{K,S}]$-modules, $\Delta(X), \Delta(Y)$ local conditions for X and Y and a morphism $\pi\colon X \otimes_R Y \to J(1)$ of complexes of $R[G_{K,S}]$-modules. Consider for any place v of K the map

$$\overset{\bullet}{\cup}_\pi\colon \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X) \otimes_R \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Y) \xrightarrow{\cup} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X \otimes Y) \longrightarrow$$

$$\xrightarrow{\pi_*} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, J(1)) \xrightarrow{\tau^{II}_{\geq 2}} \tau^{II}_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, J(1))$$

where π_* denotes the morphism induced by π at level of cochain complexes and $\tau^{II}_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, M)$ is the total complex (second) truncation of $\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, J(1))$ introduced in Rk. 3.1.19. The morphism

$$\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, M) \xrightarrow{\tau^{II}_{\geq 2}} \tau^{II}_{\geq 2}\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, M)$$

is defined on $C^j_{\mathrm{cont}}(G_v, M^i)$ as the identity for $j > 2$, as the projection on $\operatorname{coker} \delta^1_{M^i}$ for $j = 2$ and as the 0-map for $j < 2$.

Definition 3.2.4. For each $v \in S_f$ denote by $\mathrm{prod}_v(X, Y, \pi)$ the morphism of complexes

$$U_v^+(X) \otimes_R U_v^+(Y) \xrightarrow{i_v^+(X)\otimes i_v^+(Y)} C^\bullet_{\mathrm{cont}}(G_v, X) \otimes_R C^\bullet_{\mathrm{cont}}(G_v, Y) \xrightarrow{\overset{\bullet}{\cup}_\pi} \tau^{II}_{\geq 2} C^\bullet_{\mathrm{cont}}(G_v, J(1)).$$

We say that $\Delta_v(X) \perp_{\pi,h_v} \Delta_v(Y)$, or by words that $\Delta_v(X)$ is orthogonal to $\Delta_v(Y)$ with respect to π and h_v, if there is an homotopy (denoted by $\rightsquigarrow$)

$$h_v \colon \mathrm{prod}_v(X, Y, \pi) \rightsquigarrow 0.$$

If $\Delta_v(X) \perp_{\pi,h_v} \Delta_v(Y)$ for any $v \in S_f$ we say that $\Delta(X) \perp_{\pi,h_S} \Delta(Y)$ (here $h_S = (h_v)_{v \in S_f}$), by words we say that $\Delta_v(X)$ is orthogonal to $\Delta_v(Y)$ with respect to π and h_S.

Remark 3.2.5. If the morphism $\mathrm{prod}_v(X, Y, \pi) = 0$, as we will have in our examples, then (trivially) $\Delta_v(X) \perp_{\pi,0} \Delta_v(Y)$.

Local cup product

Fix a place $v \in S_f$ and assume that $\Delta_v(X) \perp_{\pi,h_v} \Delta_v(Y)$. Fix the elements $a_1 \in C^{j-1}_{\mathrm{cont}}(G_v, X)$, $a_2 \in C^{j-1}_{\mathrm{cont}}(G_v, Y)$, $b_1 \in U_v^+(X)^j$, $b_2 \in U_v^+(Y)^j$; the formulas

$$\begin{aligned}(a_1, b_1) \cup_{-,h_v} b_2 &= a_1 \overset{\bullet}{\cup}_\pi i_v(Y)^j(b_2) + h_v(b_1 \otimes b_2);\\ b_1 \cup_{+,h_v} (a_2, b_2) &= (-1)^j\, i_v^+(X)^j(b_1) \overset{\bullet}{\cup}_\pi a_2 + h_v(b_1 \otimes b_2),\end{aligned}$$

composed with the quasi isomorphism $r_{J,v}[-1]$, define morphisms of complexes

$$\begin{aligned}\cup_{-,\pi,h_v} &\colon U_v^-(X)[-1] \otimes_R U_v^+(Y) \longrightarrow \left(\tau^{II}_{\geq 2} C^\bullet_{\mathrm{cont}}(G_v, J(1))\right)[-1] \xrightarrow{r_{J,v}[-1]} J[-3];\\ \cup_{-,\pi,h_v} &\colon U_v^+(X) \otimes_R U_v^-(Y)[-1] \longrightarrow \left(\tau^{II}_{\geq 2} C^\bullet_{\mathrm{cont}}(G_v, J(1))\right)[-1] \xrightarrow{r_{J,v}[-1]} J[-3].\end{aligned}$$

And hence, by adjunction,

$$\begin{aligned}u_{-,\pi,h_v} &= \mathrm{adj}(\cup_{-,\pi,h_v}) \colon U_v^-(X)[-1] \to D_{J[-3]}(U_v^+(Y));\\ u_{+,\pi,h_v} &= \mathrm{adj}(\cup_{+,\pi,h_v}) \colon U_v^+(X) \to D_{J[-3]}(U_v^-(Y)[-1]).\end{aligned}$$

Definition 3.2.6. Fix a place $v \in S_f$ and assume that $\Delta_v(X) \perp_{\pi,h_v} \Delta_v(Y)$, we define the error term at v as

$$\mathrm{Err}_v(\Delta_v(X), \Delta_v(Y), \pi) = \mathrm{Cone}(u_{+,\pi,h_v})$$

and, if $\Delta(X) \perp_{\pi,h_S} \Delta(Y)$, the global error term as

$$\mathrm{Err}_S(\Delta(X), \Delta(Y), \pi) = \bigoplus_{v \in S_f} \mathrm{Err}_v(\Delta_v(X), \Delta_v(Y), \pi).$$

Duality

Definition 3.2.7. Suppose that X, Y are bounded, $J = I[n]$, for some $n \in \mathbb{Z}$ and either the cohomology groups of X are of finite type and those of Y of cofinite type or the converse, then we say that π is a perfect duality if the adjunction morphism $\mathrm{adj}(\pi)\colon X \to D_J(Y)(1)$ (or equivalently $\mathrm{adj}(\pi \circ s_{12})\colon Y \to D_J(X)(1)$) is a quasi isomorphism.

Example 3.2.8. The evaluation morphisms $\mathrm{ev}_1, \mathrm{ev}_2$ are perfect dualities. In fact, as we have already noticed in Sec. 3.1.1, $\mathrm{adj}(\mathrm{ev}_1)\colon D_J(X)(1) \to D_J(X)(1)$ is the identity morphism of $D_J(X)(1)$ and $\mathrm{ev}_2 = \mathrm{ev}_1 \circ s_{12}$.

Definition 3.2.9. Under the assumptions of Def. 3.2.7, suppose that π is a perfect duality and $\Delta_v(X) \perp_{\pi,h_v} \Delta_v(Y)$ for $v \in S_f$. We say that $\Delta_v(X) \perp\!\!\perp_{\pi,h_v} \Delta_v(Y)$, by words that $\Delta_v(X)$ and $\Delta_v(Y)$ are othogonal complements of each other with respect to π and h_v, if the morphism u_{+,π,h_v} (or equivalently u_{-,π,h_v}) is a quasi isomorphism.

Proposition 3.2.10 ([Nek06, Cor. 6.2.8])**.** *Under the assumption of Def. 3.2.9*

$$\Delta_v(X) \perp\!\!\perp_{\pi,h_v} \Delta_v(Y) \Longleftrightarrow \mathrm{Err}_v(\Delta_v(X), \Delta_v(Y), \pi) = 0 \ \textit{ in } \mathrm{D}(R\text{-Mod}).$$

The following theorem is the general form of a whole series of Duality Theorems for Selmer Complexes that we will state in this chapter.

Theorem 3.2.11 ([Nek06, Th. 6.3.4])**.** *Let the assumptions of Def. 3.2.7 hold, π be a perfect duality and $\Delta(X) \perp_{\pi,h_S} \Delta(Y)$. We have than an exact triangle in* $\mathrm{D}(R\text{-Mod})$

$$\widetilde{\mathbb{R}\Gamma}_f(X) \xrightarrow{\gamma_{\pi,h_S}} D_{J[-3]}(\widetilde{\mathbb{R}\Gamma}_f(Y)) \longrightarrow \bigoplus_{v \in S_f} \mathrm{Err}_v(\Delta_v(X), \Delta_v(Y), \pi)$$

and in particular if $\Delta_v(X) \perp\!\!\perp_{\pi,h_v} \Delta_v(Y)$ the map

$$\gamma_{\pi,h_S}\colon \widetilde{\mathbb{R}\Gamma}_f(X) \longrightarrow D_{J[-3]}(\widetilde{\mathbb{R}\Gamma}_f(Y))$$

is an isomorphism in $\mathrm{D}(R\text{-Mod})$.

3.2.2 Local Conditions

In this section we introduce some concrete local conditions for Selmer complexes that will be of interest for us. The reference here is [Nek06, Sec. 6.7, 7.6, 7.8]

Ordinary conditions

The notations and assumptions of the previous paragraph are in force. Fix a prime $v \in S_f$ and X_v^+, Y_v^+ complexes of admissible $R[G_v]$-modules together with morphisms of $R[G_v]$-modules

$$j_v^+(X_v^+)\colon X_v^+ \to X, \quad j_v^+(Y_v^+)\colon Y_v^+ \to Y.$$

This data induce local conditions

$$\Delta_v(X)\colon U_v^+(X) = \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X_v^+) \xrightarrow{j_v^+(X)_*} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X),$$
$$\Delta_v(X)\colon U_v^+(Y) = \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Y_v^+) \xrightarrow{j_v^+(Y)_*} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Y).$$

Put moreover

$$X_v^- = \mathrm{Cone}(X_v^+ \xrightarrow{-j_v^+(X)} X), \quad Y_v^- = \mathrm{Cone}(Y_v^+ \xrightarrow{-j_v^+(Y)} Y),$$

then

$$U_v^-(X) = \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X_v^-) = \mathrm{C}^\bullet_{\mathrm{cont}}\big(G_v, \mathrm{Cone}(X_v^+ \xrightarrow{-j_v^+(X)} X)\big) =$$
$$= \mathrm{Cone}\left(\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X_v^+) \xrightarrow{-j_v^+(X)_*} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X)\right)$$

and similarly $U_v^-(Y) = \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Y_v^-)$.

REMARK 3.2.12. In particular in the case where the complexes X, X_v^+ are concentrated in degree 0 and $j_v(X)$ is injective, the complex

$$X_v^- = [\cdots \to 0 \to X_v^{+,0} \xrightarrow{-j_v(X)} X^0 \to 0 \to \dots]$$

(concentrated in degrees $-1, 0$) is quasi isomorphic to the complex concentrated in 0 with $X_v^0/j_v(X)(X_v^{+,0})$ as 0-term. Therefore in that case $U_v^-(X) = \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X_v^0/j_v^+(X)(X_v^{+,0}))$ in the derived category, since $\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, -)$ respects quasi isomorphisms [Nek06, Prop. 3.5.5].

Definition 3.2.13. We say that $X_v^+ \perp_\pi Y_v^+$ if the morphism

$$X_v^+ \otimes_R Y_v^+ \xrightarrow{j_v^+(X) \otimes j_v^+(Y)} X \otimes_R Y \xrightarrow{\pi} J(1)$$

is zero.

And this definition make sense due to the following lemma:

Lemma 3.2.14 ([Nek06, Prop. 6.7.3])**.** *If $X_v^+ \perp_\pi Y_v^+$, then $\Delta_v(X) \perp_{\pi,0} \Delta_v(Y)$.*

Proof. By the standard functoriality properties of the cup product [see NSW00, Prop. I.1.4.2],

$$\begin{array}{ccc}
\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X_v^+) \otimes \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Y_v^+) & \xrightarrow{\cup} & \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X_v^+ \otimes Y_v^+) \\
\big\downarrow{\scriptstyle j_v^+(X) \otimes j_v^+(Y)} & & \big\downarrow{\scriptstyle j_v^+(X)_* \otimes j_v^+(Y)_*} \\
\mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X) \otimes \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Y) & \xrightarrow{\cup} & \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, X_v^+ \otimes Y_v^+)
\end{array}$$

and hence by definition $\mathrm{prod}_v(X, Y, \pi) = 0$. ☐

Note that the morphism $\pi \circ \big(j_v^+(x) \otimes j_v^+(Y)\big)$ factors through $X \otimes_R Y_v^+$, hence we get by adjunction a morphism

$$\mathrm{adj}\big(\pi \circ \big(\mathrm{id}_X \otimes j_v^+(Y)\big)\big) \colon X \to \mathrm{Hom}^\bullet_R(Y_v^+, J(1)) = D_J(Y_v^+)(1)$$

and if $X_v^+ \perp_\pi Y_v^+$,

$$\mathrm{adj}\big(\pi \circ \big(j_v^+(x) \otimes j_v^+(Y)\big)\big) \colon X_v^+ \to \mathrm{Hom}^\bullet_R(Y_v^+, J(1)) = D_J(Y_v^+)(1)$$

is zero and hence $\mathrm{adj}\big(\pi \circ \big(\mathrm{id}_X \otimes j_v^+(Y)\big)\big)$ induces

$$X_v^- \to \mathrm{Hom}^\bullet_R(Y_v^+, J(1)) = D_J(Y_v^+)(1).$$

Definition 3.2.15. We say that $X_v^+ \perp\!\!\perp_\pi Y_v^+$ if the latter morphism is a quasi isomorphism.

Suppose moreover that X, Y, X_v^+, Y_v^+ are bounded and $J = I[n]$, for some $n \in \mathbb{Z}$ and either the cohomology groups of X, X_v^+ are of finite type and those of Y, Y_v^+ of cofinite type or the converse and that π is a perfect duality. Under these assumptions we have the following lemma.

Lemma 3.2.16 ([Nek06, Prop. 6.7.6])**.** *If $X_v^+ \perp\!\perp_\pi Y_v^+$, then $\Delta_v(X) \perp\!\perp_{\pi,0} \Delta_v(Y)$*

We have also a nice expression of the error term: if we complete the morphism above into an exact triangle

$$W_v \to X_v^- \to D_J(Y_v^+)(1)$$

in $\mathrm{D}^b(R[G_v]\text{-Mod})$ then there is an isomorphism [Nek06, Prop. 6.7.6.iv] in $\mathrm{D}^b(R\text{-Mod})$

$$\mathrm{Err}_v(\Delta_v(X), \Delta_v(Y), \pi) \cong \mathbb{R}\Gamma_{\mathrm{cont}}(G_v, W_v)$$

The Duality Theorem 3.2.11 becomes, using ordinary local conditions for any $v \in S_f$,

Theorem 3.2.17 ([Nek06, Prop. 6.7.7])**.** *Under the previous assumptions on the complexes X, Y, X_v^+, Y_v^+, and on J, suppose that π is a perfect duality and $X_v^+ \perp_\pi Y_v^+$ for all $v \in S_f$. Then we have an exact triangle in $\mathrm{D}_*^b(R\text{-Mod})$ (with $* = \mathrm{ft}, \mathrm{coft}$ depending on the case in wich we are)*

$$\widetilde{\mathbb{R}\Gamma}_f(X) \xrightarrow{\gamma_{\pi,0}} D_{J[-3]}(\widetilde{\mathbb{R}\Gamma}_f(Y)) \longrightarrow \bigoplus_{v \in S_f} \mathbb{R}\Gamma_{\mathrm{cont}}(G_v, W_v)$$

and in particular if $X_v^+ \perp\!\perp_\pi Y_v^+$ the map

$$\gamma_{\pi,0} \colon \widetilde{\mathbb{R}\Gamma}_f(X) \longrightarrow D_{J[-3]}(\widetilde{\mathbb{R}\Gamma}_f(Y))$$

is an isomorphism in $\mathrm{D}_*^b(R\text{-Mod})$.

Unramified local conditions

Another kind of local conditions defining Selmer Complexes are the unramified conditions. These are a generalization of the unramified local condition

$$\mathrm{H}^1_{\mathrm{ur}}(G_v, M) = \ker\big(\mathrm{H}^1(K_v, M) \to \mathrm{H}^1(I_v, M)\big)$$

for the first cohomology groups introduced in Sec. 1.1.2. In this paragraph v is a finite place over a rational prime $l \neq p$.

If $M \in (R[G_v]\text{-Mod})^{\mathrm{ad}}$ it is natural to define the unramified local condition as

$$\Delta_v^{\mathrm{ur}}(M) \colon U_v^+(M) = \mathrm{C}^\bullet_{\mathrm{cont}}(G_v/I_v, M^{I_v}) \xrightarrow{\inf} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, M).$$

In fact the inflation map induce isomorphisms

$$\mathrm{H}^i(G_v/I_v, M^{I_v}) = \begin{cases} M^{G_v} & \text{for } i = 0, \\ \mathrm{H}^1_{\mathrm{ur}}(G_v, M) & \text{for } i = 1, \\ 0 & \text{for } i > 1. \end{cases}$$

The naive generalization to complexes of $R[G_v]$-modules does not work. However, introducing some auxiliary complexes and working with the wild inertia group $I_v^w = \mathrm{Gal}(\bar{K}_v/K_v^t)$, where K_v^t the maximal tamely ramified extension of K_v inside $\bar{K}_v$, one can still define [see Nek06, Sec. 7.2] an unramified local condition for a complex $M^\bullet$ in $\mathrm{C}(R[G_v]\text{-Mod})^{\mathrm{ad}}$

$$\Delta_v^{\mathrm{ur}}(M^\bullet) \colon \mathrm{C}^\bullet_{\mathrm{ur}}(G_v, M) = U^+\big((M^\bullet)^{I_v^w}\big) \to \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, M^\bullet).$$

If J is a bounded complex of injective R-modules, vanishing in all its negative terms and $M^\bullet$ a complex of $R[G_{K,S}]$-modules one has

$$\Delta_v^{\mathrm{ur}}(M^\bullet) \perp_{ev_2,0} \Delta_v^{\mathrm{ur}}\big(D_J(M^\bullet)(1)\big), \qquad \Delta_v^{\mathrm{ur}}\big(D_J(M^\bullet)(1)\big) \perp_{ev_1,0} \Delta_v^{\mathrm{ur}}(M^\bullet)$$

and, if $M^\bullet$ is bounded with cohomology of finite or cofinite type, then

$$\Delta_v^{\mathrm{ur}}(M^\bullet) \perp\!\!\perp_{ev_2,0} \Delta_v^{\mathrm{ur}}\big(D_J(M^\bullet)(1)\big), \qquad \Delta_v^{\mathrm{ur}}\big(D_J(M^\bullet)(1)\big) \perp\!\!\perp_{ev_1,0} \Delta_v^{\mathrm{ur}}(M^\bullet).$$

Greenberg local conditions

Another example of local conditions, that is a combination of the previous ones, are the Greenberg local conditions for a Selmer Complex. These are the ordinary local conditions for the places $v \in \Sigma$, where $\Sigma \subseteq S_f$ contains all $v \mid p$, and the unramified ones for $v \in S_f \smallsetminus \Sigma$. The resulting Selmer Complex is a generalization of the Greenberg Selmer Group of Sec. 1.1.2.

Fix $\Sigma \subseteq S_f$ containing all primes $v \mid p$. Let $J = I$ a complex of injective modules concentrated in degree 0 and $\pi\colon X \otimes_R Y \to J(1)$ a perfect duality. Consider X, Y bounded complexes in $(R[G_{K,S}]\text{-Mod})^{\mathrm{ad}}$ and assume that we are given, for $v \in \Sigma$, X_v^+, Y_v^+ such that either the cohomology groups of X, X_v^+ are of finite type and those of Y, Y_v^+ of cofinite type or vice versa, and morphisms of complexes

$$j_v^+(X)\colon X_v^+ \to X, \quad j_v^+(Y)\colon Y_v^+ \to Y.$$

Assume moreover that $X_v^+ \perp\!\!\perp_\pi Y_v^+$.

The Greenberg local conditions are, for $Z = X, Y$,

$$\Delta_v(Z) = \begin{cases} \Delta_v^+(Z)\colon \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Z_v^+) \to \mathrm{C}^\bullet_{\mathrm{cont}}(G, Z) & \text{if } v \in \Sigma, \\ \Delta_v^{\mathrm{ur}}(Z)\colon C^\bullet_{\mathrm{ur}}(G_v, Z) \to \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Z) & \text{if } v \in S_f \smallsetminus \Sigma. \end{cases}$$

In this case Th. 3.2.11 becomes

Theorem 3.2.18 ([Nek06, Sec. 7.8.4.2])**.** *There is an isomorphism in* $\mathrm{D}^b(R\text{-Mod})$

$$\gamma_{\pi,0}\colon \widetilde{\mathbb{R}\Gamma}_f(X) \longrightarrow D_{I[-3]}\big(\widetilde{\mathbb{R}\Gamma}_f(Y)\big)$$

Proof. We have that $\Delta_v(X) \perp\!\!\perp_{\pi,0} \Delta_v(Y)$ for any $v \in \Sigma$ by Lemma 3.2.16 since for such primes the local conditions are the ordinary ones and we assumed that $X_v^+ \perp\!\!\perp_\pi Y_v^+$. Furthermore, since π is perfect in the sence of definition 3.2.7, we have a commutative diagram with quasi isomorphism vertical arrows

$$\begin{array}{ccc} X \otimes_R Y & \xrightarrow{\ \pi\ } & J(1) \\ \downarrow{\scriptstyle \mathrm{id}\otimes \mathrm{adj}(\pi\circ s_{12})} & & \downarrow \\ X \otimes_R D_J(X)(1) & \xrightarrow{\ \mathrm{ev}_2\ } & J(1) \end{array}$$

and hence, since (as we observed in the previous paragraph)

$$\Delta_v^{\mathrm{ur}}(X) \perp\!\!\perp_{ev_2,0} \Delta_v^{\mathrm{ur}}\big(D_J(X)(1)\big),$$

it follows that $\Delta_v(X) \perp\!\!\perp_{\pi,0} \Delta_v(Y)$ for any $v \in S_f \smallsetminus \Sigma$ as for such primes the local conditions are the unramified ones. $\square$

3.3 Iwasawa Theory and Selmer Complexes

In this section we treat Selmer Complexes over a $\mathbb{Z}_p^r$-extension K_∞/K following [Nek06, Ch. 8].

3.3.1 Abstract theory

Let $U \subseteq G$ be an open normal subgroup of a profinite group G and X be a discrete U-module. The induced module

$$\mathrm{Ind}_U^G(X) = \{\, f\colon G \to X : \text{s.t. } f \text{ locally constant, } f(ug) = uf(g) \text{ for any } u \in U, g \in G \,\}$$

is a discrete G-module with the left G-action given by $g \cdot f(g') = f(gg')$. We have the classic:

Lemma 3.3.1 (Shapiro)**.** *There is a quasi isomorphism* $\mathrm{sh}\colon \mathrm{C}^\bullet_{\mathrm{cont}}(G, \mathrm{Ind}_U^G(X)) \to \mathrm{C}^\bullet_{\mathrm{cont}}(U, X)$.

If moreover X is a discrete G-module and we denote, with a slight abuse of notations, again by X its restriction as U-module, then $\mathrm{Ind}_U^G(X)$ is isomorphic to the following discrete G-modules:

$$\begin{aligned} X_U &= \mathbb{Z}[G/U] \otimes_{\mathbb{Z}} X, & g\cdot(\beta\otimes x) &= g\beta \otimes g\cdot x, && \text{for } \beta \in G/U,\ x \in X; \\ {}_U X &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], X), & (g\cdot a)(\beta) &= g\cdot a(g^{-1}\beta), && \text{for } a\colon G/U \to X,\ \beta \in G/U. \end{aligned}$$

The isomorphisms being given by

$$\begin{aligned} \mathrm{Ind}_U^G(X) &\xrightarrow{\sim} {}_U X, & f &\mapsto \big[gU \mapsto g\big(f(g^{-1})\big)\big]; \\ \mathrm{Ind}_U^G(X) &\xrightarrow{\sim} X_U, & &\sum_{gU \in G/U} gU \otimes g\big(f(g^{-1})\big). \end{aligned}$$

Denoting moreover by δ_β the Kroneker delta function of $\beta \in G/U$, i.e. for any $\beta' \in G/U$

$$\delta_\beta(\beta') = \begin{cases} 1 & \text{if } \beta' = \beta \\ 0 & \text{if } \beta' \neq \beta \end{cases},$$

the composed G-equivariant isomorphism $X_U \xrightarrow{\sim} {}_U X$ is given

$$\sum_{\beta \in G/U} \beta \otimes x_\beta \mapsto \sum_{\beta \in G/U} x_\beta \delta_\beta.$$

Therefore for general $M \in (R[G]\text{-Mod})^{\mathrm{ad}}$ we take as analogous of the induced module

$$\begin{aligned} M_U &= \mathbb{Z}[G/U] \otimes_{\mathbb{Z}} M, & g\cdot(\beta\otimes m) &= g\beta \otimes g\cdot m, && \text{for } \beta \in G/U,\ x \in M; \\ {}_U M &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/U], M), & (g\cdot a)(\beta) &= g\cdot a(g^{-1}\beta), && \text{for } a\colon G/U \to M,\ \beta \in G/U. \end{aligned}$$

Note that the G-actions above make them into $R[G]$-modules and, as in the discrete case, the formula $\sum \beta \otimes x_\beta \mapsto \sum x_\beta \delta_\beta$ give an isomorphism $M_U \xrightarrow{\sim} {}_U M$ and we have the Shapiro-type quasi isomorphisms

$$\mathrm{C}^\bullet_{\mathrm{cont}}(G, M_U) \longrightarrow \mathrm{C}^\bullet_{\mathrm{cont}}(U, M) \longleftarrow \mathrm{C}^\bullet_{\mathrm{cont}}(G, {}_U M).$$

All the definitions above extend verbatim to complexes $M^\bullet$ in $(R[G]\text{-Mod})^{\mathrm{ad}}$. If moreover $M^\bullet$ is bounded below or $\mathrm{cd}_p(G)$ is finite, then we have Shapiro-type quasi-isomorphisms

$$\mathrm{C}^\bullet_{\mathrm{cont}}(G, M_U^\bullet) \longrightarrow \mathrm{C}^\bullet_{\mathrm{cont}}(U, M^\bullet) \longleftarrow \mathrm{C}^\bullet_{\mathrm{cont}}(G, {}_U M^\bullet).$$

Note moreover that for an admissible R-module M both M_U and ${}_U M$ have a structure of $R[G/U][G]$-modules, the (left) action of G/U being given by the Ad-actions (that in the discrete case they correspond to the classical Ad-action on the induced module)

$$\begin{aligned} (gU)\cdot(hU\otimes x) &= (hg^{-1}U)\otimes x \quad \text{for } g,h\in G,\ x\in M_U;\\ (gU)\cdot a\colon g'U &\mapsto a(g'gU) \quad \text{for } g,g'\in G,\ a\in {}_U M. \end{aligned}$$

Define $\iota\colon R[G/U]\to R[G/U]$ as the R-linear involution induced by $g\mapsto g^{-1}$. If G/U is abelian the action of $\beta\in R[G/U]$ on M_U (resp. on ${}_U M$) is given by $\mathrm{id}\otimes\iota(\beta)$ (resp. by $\mathrm{Hom}(\beta,\mathrm{id})$). We have moreover the following results

Proposition 3.3.2 ([Nek06, Lemma 8.2.5])**.** *Assume that G/U is abelian. Then:*

1. *if M is an admissible $R[G]$-module, then M_U and ${}_U M$ are admissible $R[G/U][G]$-modules;*
2. *if M is of finte (resp. co-finite) type over R, then M_U and ${}_U M$ are of finite (resp. cofinite) type over $R[G/U]$.*

Therefore we may see the functors $M\mapsto M_U$ and $M\mapsto {}_U M$ as functors

$$(R[G]\text{-Mod})^{\mathrm{ad}}_{R-*}\longrightarrow (R[G/U][G]\text{-Mod})^{\mathrm{ad}}_{R[G/U]-*},$$

where $*=\mathrm{ft},\mathrm{coft}$.

Infinite Extensions

Now let H be a closed normal subgroup of G and put $\Gamma=G/H$. Denote by $\mathscr{U}$ the family of all U open subgroups of G containing H and let

$$\bar R = R[\![\Gamma]\!] = \varprojlim_{U\in\mathscr{U}} R[G/U].$$

For any $M\in(R[G]\text{-Mod})^{\mathrm{ad}}$ the collection of modules $\{\,M_U\,\}_{U\in\mathscr{U}}$ (resp. $\{\,{}_U M\,\}_{U\in\mathscr{U}}$) form a projective (resp. injective) system with respect to the projection maps $R[G/U]\to R[G/V]$, for $V\subset U$, $U,V\in\mathscr{U}$. Hence we may define their limits

$$\mathscr{F}_\Gamma(M)=\varprojlim_{U\in\mathscr{U}} M_U;\quad F_\Gamma(M)=\varinjlim_{U\in\mathscr{U}} {}_U M,$$

that are both (left) $\bar R$-modules. Similarly we define $\mathscr{F}_\Gamma(M^\bullet)$ and $F_\Gamma(M^\bullet)$ for a complex $M^\bullet$ of admissible $R[G]$-modules. Note that in general $\mathscr{F}_\Gamma(M)$ is only an ind-admissible $\bar R[G]$-module, as direct limit of admissible $R[G]$-modules. However this is not a problem by Rk. 3.1.13. Moreover if $M^\bullet$ is supported on $\mathfrak{m}$, then so is $F_\Gamma(M^\bullet)$.

Lemma 3.3.3 ([Nek06, Prop. 8.3.2])**.** *If $M^\bullet$ is a complex of admissible $R[G]$-module, then $F_\Gamma(M^\bullet)$ is a complex of ind-admissible $\bar R[G]$-modules and the canonical map*

$$\varinjlim_{U\in\mathscr{U}} \mathrm{C}^\bullet_{\mathrm{cont}}(G,{}_U M^\bullet)\longrightarrow \mathrm{C}^\bullet_{\mathrm{cont}}\big(G,F_\Gamma(M^\bullet)\big)$$

is an isomorphism of complexes.

We may perform moreover the projective limit

$$\varprojlim_{U\in\mathscr{U}} \mathrm{C}^\bullet_{\mathrm{cont}}(G,M^\bullet_U),$$

but the analogous lemma does not hold: we denote by

$$\mathbb{R}\Gamma_{\mathrm{Iw}}(G,H;M^\bullet)\in \mathrm{D}(\bar R\text{-Mod})$$

the corresponding object in the derived category and by $\mathrm{H}^i_{\mathrm{Iw}}(G,H;M^\bullet)$ its cohomology groups.

$\mathbb{Z}_p^r$-extensions

Now suppose that $\Gamma \cong \mathbb{Z}_p^r$, for some $r > 0$. In this case, chosen a set $\{\gamma_i\}_{i=1,\dots,r}$ of topological generators of Γ,

$$\bar{R} \xrightarrow{\sim} R[\![X_1, \dots, X_r]\!]; \qquad \gamma_i \mapsto 1 + X_i.$$

In particular $\bar{R}$ is a complete local Noetherian ring, of dimension $d+r$. Let $\bar{\mathfrak{m}} \cong \mathfrak{m}\bar{R} + (X_1, \dots, X_r)$ be the maximal ideal of $\bar{R}$ and note that the residue field of $\bar{R}$ is $\bar{R}/\bar{\mathfrak{m}} = k$.

Definition 3.3.4. Let $\chi_\Gamma \colon G \twoheadrightarrow \Gamma = G/H \hookrightarrow R[\Gamma]^*$. For any $n \in \mathbb{Z}$ and M an $R[\Gamma][G]$-module, define a new $R[\Gamma][G]$-module $M\langle n\rangle$ as M itself as $R[\Gamma]$-module, the G-action being given by

$$g \cdot_n x = \chi_\Gamma(g)^n g \cdot x; \qquad g \in G, x \in M.$$

Definition 3.3.5. Recall the involution $\iota \colon R[\Gamma] \to R[\Gamma]$ induced by the inversion on group-like elements. Let M be a $R[\Gamma][G]$-module and define the $R[\Gamma][G]$-module M^ι as M itself as $R[G]$-module, with the action of Γ given by

$$x \cdot_\iota y = \iota(x) \cdot y; \qquad x \in R[\Gamma], y \in M.$$

We may relate these two constructions: $M\langle n\rangle^\iota \xrightarrow{\sim} M^\iota\langle -n\rangle$. We may moreover use them in order to give a characterization of $F_\Gamma(M)$ and $\mathscr{F}_\Gamma(M)$:

Lemma 3.3.6 ([Nek06, Prop. 8.4.4.1])**.** *If M is an admissible $R[G]$-module of finite type, then we have canonical isomorphisms of $\bar{R}[G]$-modules*

$$\mathscr{F}_\Gamma(M) \xrightarrow{\sim} (M \otimes_R \bar{R})\langle -1\rangle; \qquad \mathscr{F}_\Gamma(M)^\iota \xrightarrow{\sim} (M \otimes_R \bar{R})\langle 1\rangle.$$

The two functors $\mathscr{F}_\Gamma, F_\Gamma$ derive to exact functors

$$F_\Gamma \colon \mathrm{D}^*(R[G]\text{-Mod})^{\mathrm{ad}}_{R-\mathrm{coft}} \longrightarrow \mathrm{D}^*(\bar{R}[G]\text{-Mod})^{\mathrm{ad}}_{\bar{R}-\mathrm{coft}};$$
$$\mathscr{F}_\Gamma \colon \mathrm{D}^*(R[G]\text{-Mod})^{\mathrm{ad}}_{R-\mathrm{ft}} \longrightarrow \mathrm{D}^*(\bar{R}[G]\text{-Mod})^{\mathrm{ad}}_{\bar{R}-\mathrm{ft}},$$

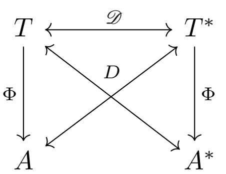
where $* = \emptyset, +, -, b$.

Looking for a relation between the two functors we have to consider the dualizing functors $D = D_R$ and $\bar{D} = D_{\bar{R}}$. Note that if I is an injective hull of k over R, and therefore $D = D_I$, then $\bar{D} = D_{\bar{I}}$, for $\bar{I} = F_\Gamma(I)$, as one can show that $\bar{I}$ is an injective hull of k over $\bar{R}$.

Proposition 3.3.7 ([Nek06, Lemma 8.4.5.1])**.** *For any admissible $R[G]$-module M there are canonical isomorphisms*

$$F_\Gamma(M) \xrightarrow{\sim} \bar{D}\big(\mathscr{F}_\Gamma(D(M))^\iota\big); \qquad \bar{D}(F_\Gamma(M)) \xrightarrow{\sim} \mathscr{F}_\Gamma(D(M))^\iota$$

And one may show that if $T, T^* \in \mathrm{D}^b_{R-\mathrm{ft}}(R[G]\text{-Mod})^{\mathrm{ad}}$ and $A, A^* \in D^b_{R-\mathrm{coft}}(R[G]\text{-Mod})^{\mathrm{ad}}$ are related by the duality diagram



(that is the analogous of the diagram for representations of Sec. 1.1.1), then one has that $\mathscr{F}_\Gamma(T), \mathscr{F}_\Gamma(T^*) \in \mathrm{D}^b_{\bar{R}-\mathrm{ft}}(\bar{R}[G]\text{-Mod})^{\mathrm{ad}}$ and $F_\Gamma(A), F_\Gamma(A^*) \in \mathrm{D}^b_{\bar{R}-\mathrm{coft}}(\bar{R}[G]\text{-Mod})^{\mathrm{ad}}$ and there is a duality diagram

$$\begin{array}{ccc} \mathscr{F}_\Gamma(T) & \overset{\bar{\mathscr{D}}}{\longleftrightarrow} & \mathscr{F}_\Gamma(T^*) \\ {\scriptstyle \bar{\Phi}}\downarrow & \overset{\bar{D}}{\times} & \downarrow{\scriptstyle \bar{\Phi}} \\ F_\Gamma(A) & & F_\Gamma(A^*) \end{array}$$

3.3.2 Greenberg's conditions in Iwasawa Theory

Consider now a $\mathbb{Z}_p^r$-extension K_∞/K contained in K_S, for $r > 0$, and let $G = \mathrm{Gal}(K_S/K)$, $H = \mathrm{Gal}(K_S/K_\infty)$, hence $\Gamma = \mathrm{Gal}(K_\infty/K)$. Assume moreover that all the finite places $v \notin \Sigma$ are unramified in K_∞/K. We apply the results of Sec. 3.3.1. The notations of Sec. 3.2.2 are in force, too.

Let T, M complexes respectively in $(R[G_{K,S}]\text{-Mod})^{\mathrm{ad}}_{R-\mathrm{ft}}$ and in $(R[G_{K,S}]\text{-Mod})^{\mathrm{ad}}_{R-\mathrm{coft},\{\mathfrak{m}\}}$, both bounded below. Assume moreover that we are given for any $v \in \Sigma$ a couple of bounded below complexes T_v^+, M_v^+ respectively in $(R[G_v]\text{-Mod})^{\mathrm{ad}}_{R-\mathrm{ft}}$ and in $(R[G_v]\text{-Mod})^{\mathrm{ad}}_{R-\mathrm{coft},\{\mathfrak{m}\}}$ and morphisms of complexes $T_v^+ \to T$, $M_v^+ \to M$.

These data define Greenberg local conditions $\Delta_v(Z)$ for $Z = T, M, T_U, M_U, \mathscr{F}_\Gamma(T), F_\Gamma(M)$ (where U is an open subgroup of G_K), as in Sec. 3.2.2. Fix moreover an embedding $\bar{K} \hookrightarrow \bar{K}_v$ for any $v \in S_f$. Write

$$\widetilde{\mathbb{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K, T) = \widetilde{\mathbb{R}\Gamma}_f\left(G_{K,S}, \mathscr{F}_\Gamma(T), \Delta\big(\mathscr{F}_\Gamma(T)\big)\right);$$
$$\widetilde{\mathbb{R}\Gamma}_f(K_S/K_\infty, M) = \widetilde{\mathbb{R}\Gamma}_f\left(G_{K,S}, F_\Gamma(M), \Delta\big(F_\Gamma(M)\big)\right).$$

and denote by $\widetilde{\mathrm{H}}^i_{f,\mathrm{Iw}}(K_\infty/K, T)$, $\widetilde{\mathrm{H}}^i_f(K_S/K_\infty, M)$ their cohomology.

For any K'/K finte subextension of K_∞/K if v' is the prime of K' induced by the previous embedding the same data define Greenberg local conditions $\Delta_{v'}(Z)$, for $Z = T, M$ over $G_{K',S}$, defining the Selmer complexes

$$\widetilde{\mathbb{R}\Gamma}_f(K'/K, T) := \widetilde{\mathbb{R}\Gamma}_f(G_{K',S'}, T, \Delta'(T)); \qquad \widetilde{\mathbb{R}\Gamma}_f(K_S/K', M) := \widetilde{\mathbb{R}\Gamma}_f(G_{K',S'}, M, \Delta'(M)).$$

Denote their cohomology respectively by $\widetilde{\mathrm{H}}^i_f(K'/K, T)$ and $\widetilde{\mathrm{H}}^i_f(K_S/K', M)$.

The following proposition says that these notations are compatible.

Proposition 3.3.8 ([Nek06, Prop. 8.8.6]). *1. We have an isomorphism of $\bar{R}$-modules*

$$\widetilde{\mathrm{H}}^i_f(K_S/K_\infty, M) \xrightarrow{\sim} \varinjlim_{\mathrm{res}, K'} \widetilde{\mathrm{H}}^i_f(K_S/K', M);$$

2. We have a canonical isomorphism of complexes

$$\widetilde{\mathbb{R}\Gamma}_{f,\mathrm{Iw}}(K_\infty/K, T) \xrightarrow{\sim} \varprojlim_U \widetilde{\mathbb{R}\Gamma}_f\left(G_{K,S}, T_U, \Delta(T_U)\right),$$

inducing on cohomology an isomorphism of $\bar{R}$-modules

$$\widetilde{\mathrm{H}}^i_{f,\mathrm{Iw}}(K_\infty/K, T) \xrightarrow{\sim} \varinjlim_{\mathrm{cores}, K'} \widetilde{\mathrm{H}}^i_f(K'/K, T).$$

Duality

Let now $T, T^*(1)$ be two bounded complexes in $(R[G_{K,S}]\text{-Mod})^{\text{ad}}_{R-\text{ft}}$ and $T_v^+, T^*(1)_v^+$ two bounded complexes in $(R[G_v]\text{-Mod})^{\text{ad}}_{R-\text{ft}}$, for any $v \in \Sigma$, together with morphisms of complexes $T_v^+ \to T$, $T^*(1)_v^+ \to T^*(1)$ that induce local conditions on T and $T(1)^*$. Recall that $T_v^- = \text{Cone}(T_v^+ \to T)$, $T^*(1)_v^- = \text{Cone}(T^*(1)_v^+ \to T^*(1))$. Define moreover the bounded complexes

$$A = D(T^*(1))(1), \quad A^*(1) = D(T)(1), \quad A_v^+ = D(T^*(1)_v^-)(1), \quad A^*(1)_v^+ = D(T_v^-)(1).$$

Note that $A, A^*(1)$ are complexes in $(R[G_{K,S}]\text{-Mod})^{\text{ad}}_{R-\text{coft}}$, $A_v^+, A_v^*(1)$ in $(R[G_v]\text{-Mod})^{\text{ad}}_{R-\text{coft}}$ and applying D to the canonical morphisms $T^*(1) \to T^*(1)_v^-$, $T \to T_v^-$ we get the morphisms $A_v^+ \to A$, $A^*(1)_v^+ \to A^*(1)$ inducing Greenberg's local conditions on $A, A^*(1)$.

By these definitions follows immediately that the pairings

$$\text{ev}_2 \colon T \otimes_R A^*(1) \longrightarrow I(1), \qquad \text{ev}_1 \colon A \otimes_R T^*(1) \longrightarrow I(1)$$

are perfect and

$$T_v^+ \perp\!\!\perp_{\text{ev}_2} A^*(1)_v^+, \qquad A_v^+ \perp\!\!\perp_{\text{ev}_1} T^*(1)^+.$$

As explained in the previous paragraph these data induce corresponding Greenberg data on $\mathscr{F}_\Gamma(T), \mathscr{F}_\Gamma(T^*(1))$, and $F_\Gamma(A), F_\Gamma(A^*(1))$. By Prop. 3.3.7 we have two perfect morphisms

$$\text{ev}_2 \colon \mathscr{F}_\Gamma(T) \otimes_R F_\Gamma(A^*(1))^\iota \to \bar{I}(1), \qquad \text{ev}_1 \colon \mathscr{F}_\Gamma(A) \otimes_R \mathscr{F}_\Gamma(A^*(1))^\iota \to \bar{I}(1)$$

and

$$\mathscr{F}_\Gamma(T)_v^+ \perp\!\!\perp_{\text{ev}_2} (F_\Gamma(A^*(1))^\iota)_v^+; \qquad F_\Gamma(A)_v^+ \perp\!\!\perp_{\text{ev}_1} (\mathscr{F}_\Gamma(T^*(1))^\iota)_v^+.$$

Therefore applying Theorem 3.2.18 to the couples $\mathscr{F}_\Gamma(T), F_\Gamma(A^*(1))^\iota$ and $F_\Gamma(A), \mathscr{F}_\Gamma(A^*(1))^\iota$:

Theorem 3.3.9 ([Nek06, Sec. 8.9.6.1]). *We have isomorphisms*

$$\widetilde{\mathbb{R}\Gamma}_{f,\text{Iw}}(K_\infty/K, T) \xrightarrow{\sim} D_{\bar{I}[-3]}\left(\widetilde{\mathbb{R}\Gamma}_f(K_S/K_\infty, A^*(1))^\iota\right),$$
$$\widetilde{\mathbb{R}\Gamma}_f(K_S/K_\infty, A) \xrightarrow{\sim} D_{\bar{I}[-3]}\left(\widetilde{\mathbb{R}\Gamma}_{f,\text{Iw}}(K_\infty/K, T^*(1))^\iota\right)$$

respectively in $\mathrm{D}^b_{\text{ft}}(\bar{R}\text{-Mod})$ *and* $\mathrm{D}^b_{\text{coft}}(\bar{R}\text{-Mod})$.

Control theorem

A classic tool in Iwasawa Theory for elliptic curves is Mazur's Control Theorem: it studies the relations between the Selmer groups over K and K_∞. In our context it generalizes to the following Exact Control Theorem.

Theorem 3.3.10 ([Nek06, Prop. 8.10.1]). *There is a canonical isomorphism*

$$\widetilde{\mathbb{R}\Gamma}_{f,\text{Iw}}(K_\infty/K, T) \overset{\mathbb{L}}{\otimes}_{\bar{R}} R \xrightarrow{\sim} \widetilde{\mathbb{R}\Gamma}_f(K, T)$$

in $\mathrm{D}^b(R\text{-Mod})$ *inducing a homological spectral sequence*

$$E^2_{i,j} = \mathrm{H}_{i,\text{cont}}\left(\Gamma, \widetilde{\mathrm{H}}^{-j}_{f,\text{Iw}}(K_S/K_\infty, T)\right) \Longrightarrow \widetilde{\mathrm{H}}_f^{-i-j}(K, T).$$

In particular dualizing it we get also a cohomological spectral sequence

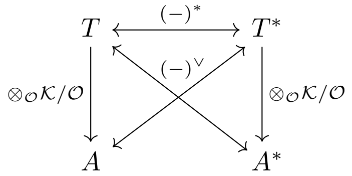
$$E_2^{i,j} = \mathrm{H}^i_{\text{cont}}\left(\Gamma, \widetilde{\mathrm{H}}^j_f(K_\infty/K, A)\right) \Longrightarrow \widetilde{\mathrm{H}}_f^{i+j}(K, A).$$

3.4 Comparison with classical Selmer groups

Consider now a special case of the theory described so far: let $R = \mathcal{O}$ the ring of integers of a finite extension $\mathcal{K}$ of $\mathbb{Q}_p$ and take T a free $\mathcal{O}$-module, equipped with a continuous $\mathcal{O}$-linear action of $G_{K,S}$. Define as in Sec. 1.1.1 the auxiliary (continuous) representations

$$\begin{aligned} V &= T \otimes \mathcal{O}, & A &= V/T = T \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O}, \\ T^* &= \mathrm{Hom}_{\mathcal{O}}(T, \mathcal{O}), & A^* &= \mathrm{Hom}_{\mathcal{O}}(T^*, \mathcal{O}) = T^* \otimes \mathcal{K}/\mathcal{O}. \end{aligned}$$

Related by a diagram



where $(\,-\,)^* = \mathrm{Hom}_{\mathcal{O}}(\,-\,,\mathcal{O})$ denotes the linear dual, while

$$(-)^\vee = \mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}}(\,-\,,\mathcal{K}/\mathcal{O}) = \mathrm{Hom}_{\mathcal{O}}(\,-\,,\mathcal{K}/\mathcal{O}) = D(\,-\,)$$

is the Pontryagin one. Being finite free over $\mathcal{O}$, T is a finite type $\mathcal{O}$-module and hence by Prop. 3.1.12 it is an admissible $\mathcal{O}[G_{K,S}]$-module. The same applies to A, T^*, A^*: indeed T, T^* are finite free over $\mathcal{O}$ and hence both $A = D(T^*)$ and $A^* = D(T)$ are of cofinite type. By similar arguments all the modules labeled with a T (resp. A) in the following are admissible $\mathcal{O}[G_{K,S}]$-module of finite (resp. cofinite) type over $\mathcal{O}$.

Assume we are given a (continuous) $\mathcal{K}[G_v]$-submodule V_v for each $v \mid p$. Let

$$T_v^+ = T \cap V_v^+, \quad A_v^+ = V_v^+/T_v^+ \subseteq V/T = A, \quad X_v^- = X/X_v^+ \text{ for } X = T, V, A$$

and

$$V^*(1)_v^\pm = \mathrm{Hom}_{\mathcal{K}}(V_v^\mp, \mathcal{K})(1), \;\; T^*(1)_v^\pm = \mathrm{Hom}_{\mathcal{O}}(T_v^\mp, \mathcal{O})(1), \;\; A^*(1)^\pm = V^*(1)_v^\pm / T^*(1)_v^\pm.$$

These data define Greenberg's local conditions for $Z = T, V, A, T^*(1), V^*(1), A^*(1)$ in the sense of Sec. 3.2.2, letting $Z^\bullet$ and $Z_v^{\bullet,+}$ be the complexes concentrated in degree 0 with respectively Z and Z_v^+ as 0-term, for $v \mid p$ and letting $Z_v^{\bullet,+} \to Z^\bullet$ to be the inclusion in the 0-term, the zero map otherwise. Note, as we observed in Rk. 3.2.12, $Z_v^{-,\bullet}$ is quasi isomorphic to the complex concentrated in degree 0, with Z_v^- as its zero term. Explicitly the local conditions are the inclusions of

$$U_v^+(Z) = \begin{cases} \mathrm{C}^\bullet_{\mathrm{cont}}(G_v, Z_v^+) & \text{for } v \mid p, \\ \mathrm{C}^\bullet_{\mathrm{cont}}(G_v/I_v, Z^{I_v}) & \text{for } v \in S_f, v \nmid p. \end{cases}$$

into $\mathrm{C}^\bullet_{\mathrm{cont}}(G_{K,S}, Z)$. Denote the resulting Selmer complexes by $\widetilde{\mathbb{R}\Gamma}_f(K, Z)$ and the generalized Selmer groups by $\widetilde{\mathrm{H}}^i_f(K, Z)$. In particular $\widetilde{\mathrm{H}}^i_f(K, Z) = 0$ for $i < 0$, as $\widetilde{\mathbb{R}\Gamma}_f(Z)^i = 0$ when $i < 0$ (by the very definition of Selmer complex). The first generalized Selmer group $\widetilde{\mathrm{H}}^1_f(K, Z)$ of Z often coincide with some more classical Selmer Groups as those defined in Sec. 1.1.2; in general it is related to the strict Greenberg Selmer group in the following way:

Proposition 3.4.1 ([Nek06, Lemma 9.6.3])**.** *For each $Z = T, V, A$, there is an exact sequence*

$$0 \to \widetilde{\mathrm{H}}^0_f(K, Z) \to \mathrm{H}^0(K, Z) \to \bigoplus_{v|p} \mathrm{H}^0(G_v, Z) \to \widetilde{\mathrm{H}}^1_f(K, Z) \to \mathrm{H}^1_{\mathrm{str}}(K, Z) \to 0.$$

If we consider moreover K_∞ a $\mathbb{Z}_p$-extension of K we define $\widetilde{\mathrm{H}}^1_f(K_S/K_\infty, A)$, $\widetilde{\mathrm{H}}^1_f(K_\infty/K, T)$ as in Sec. 3.3.2. Consider the generalized Selmer groups $\widetilde{\mathrm{H}}^1_f(K'/K, T)$ and $\widetilde{\mathrm{H}}^1_f(K_S/K', A)$ for any finite subextension $K \subseteq K' \subseteq K_\infty$, by Prop. 3.3.8

$$\widetilde{\mathrm{H}}^1_f(K_S/K_\infty, A) \cong \varinjlim_{\mathrm{res}, K'} \widetilde{\mathrm{H}}^1_f(K_S/K', A); \qquad \widetilde{\mathrm{H}}^1_{f,\mathrm{Iw}}(K_\infty/K, T) \cong \varinjlim_{\mathrm{cores}, K'} \widetilde{\mathrm{H}}^1_f(K'/K, T).$$

In the rest, when the base field K will be clear from the context, we will drop the notations K'/K and K_S/K' (resp. K_∞/K and K_S/K_∞) and we will label the generalized Selmer groups by K' (resp. K_∞). The Iw will be dropped by the notations, too.

Duality

In this special case Th. 3.2.18 has the following form:

Theorem 3.4.2. *There are isomorphisms*

$$\widetilde{\mathrm{H}}^i_f(K, T) \xrightarrow{\sim} D\big(\widetilde{\mathrm{H}}^{3-i}_f(K, A^*(1))\big);$$
$$\widetilde{\mathrm{H}}^i_f(K, A) \xrightarrow{\sim} D\big(\widetilde{\mathrm{H}}^{3-i}_f(K, T^*(1))\big).$$

Proof. Observe that $I = \mathcal{K}/\mathcal{O}$ is an injective hull of k (as we saw in Ex. 3.1.10) and let $J = I[0]$. By Th. 3.2.18

$$\widetilde{\mathrm{H}}^i_f(\mathcal{K}, T) = \mathrm{H}^i\left(\widetilde{\mathbb{R}\Gamma}_f(K, T)\right) \cong \mathrm{H}^i\left(D_{I[-3]}\left(\widetilde{\mathbb{R}\Gamma}_f\left(K, A^*(1)\right)\right)\right)$$

But

$$D_{I[-3]}\left(\widetilde{\mathbb{R}\Gamma}_f\left(K, A^*(1)\right)\right)^i = \prod_{j\in\mathbb{Z}} \mathrm{Hom}_{\mathcal{O}}\left(\widetilde{\mathbb{R}\Gamma}_f\left(K, A^*(1)\right)^j, J^{i+j-3}\right) =$$
$$= \mathrm{Hom}_{\mathcal{O}}\left(\widetilde{\mathbb{R}\Gamma}_f\left(K, A^*(1)\right)^{3-i}, \mathcal{K}/\mathcal{O}\right) = D\left(\widetilde{\mathbb{R}\Gamma}_f\left(K, A^*(1)\right)^{3-i}\right)$$

as

$$J^{i+j-3} = \begin{cases} \mathcal{K}/\mathcal{O} & \text{if } j = 3-i, \\ 0 & \text{else.} \end{cases}$$

Therefore, since $\mathcal{K}/\mathcal{O}$ is injective and therefore $D = \mathrm{Hom}_{\mathcal{O}}(-, \mathcal{K}/\mathcal{O})$ is exact and commutes with taking the i-th cohomology of complexes

$$\widetilde{\mathrm{H}}^i(K, T) \cong \mathrm{H}^i\left(D_{I[-3]}\left(\widetilde{\mathbb{R}\Gamma}_f\left(K, A^*(1)\right)\right)\right) \cong D\left(\widetilde{\mathrm{H}}^{3-i}_f\left(K, A^*(1)\right)\right). \qquad \square$$

The formulation of Th. 3.3.9 simplifies too. The proof is analogous to the previous one, using $\bar{D}, \bar{I}$ in place of D, I. But note that, since $\Lambda = \mathcal{O}[\![\Gamma]\!]$ has k as residue field, $\bar{I} = \mathcal{K}/\mathcal{O}$. Therefore $\bar{D}(M)$ coincides as $\mathcal{O}$-modules with the Pontryagin dual $M^\vee$ of M. However one has to be careful: the natural Γ-action on $M^\vee$ is $\gamma \cdot f(m) = f(\gamma^{-1} \cdot m)$. We will write $D(M)$ for the Λ-module $M^\vee$ with the induced Λ-scalar multiplication: this Λ-module structure is not the same of $\bar{D}(M)$. The latter is in fact given by $\lambda \cdot f(m) = f(\lambda m)$, i.e. $\bar{D}(M) = D(M)^\iota$.

Theorem 3.4.3. *There are isomorphisms*

$$\widetilde{\mathrm{H}}^i_f(K_S/K_\infty, T) \xrightarrow{\sim} D\big(\widetilde{\mathrm{H}}^{3-i}_f(K_\infty/K, A^*(1))\big);$$
$$\widetilde{\mathrm{H}}^i_f(K_\infty/K, A) \xrightarrow{\sim} D\big(\widetilde{\mathrm{H}}^{3-i}_f(K_S/K_\infty, T^*(1))\big),$$

where $D(M)$ is the Pontryagin dual $M^\vee$ of M seen as a Λ-module with the action of Γ defined by $\gamma \cdot f(m) = f(\gamma^{-1} \cdot m)$ for any $\gamma \in \Gamma$, $m \in M$.

Exact Control Theorem

We begin this section recalling a classical definition in Iwasawa Theory: for any Λ-module M the $\mathcal{O}$-module of coinvariants is the module $M_\Gamma = M/I_\Gamma M$, where I_Γ is the augmentation ideal, i.e. the ideal generated by $\gamma - 1$, being γ a topological generator of Γ. This is an important notion in the theory of Iwasawa modules, mainly because of the following version of Nakayama's lemma.

Lemma 3.4.4 (Nakayama)**.** *If M is a finitely generated Λ-module and $M_\Gamma = 0$, then $M = 0$*

We have moreover the following lemma, that explains the name "coinvariants".

Lemma 3.4.5. *For any Λ-module M we have an isomorphism of Λ-modules $\bar{D}(M)_\Gamma \cong \bar{D}(M^\Gamma)$.*

Proof. If $\Phi \colon M \to M$ is the multiplication by $(\gamma - 1)$ map, then $\ker(\Phi) = M^\Gamma$, we have therefore an exact sequence

$$0 \longrightarrow M^\Gamma \xrightarrow{\ j\ } M \xrightarrow{\ \Phi\ } M$$

and dualizing it

$$\bar{D}(M) \xrightarrow{\bar{D}(\Phi)} \bar{D}(M) \xrightarrow{\bar{D}(j)} \bar{D}(M^\Gamma) \longrightarrow 0$$

But $\bar{D}(\Phi)$ is again the multiplication by $\gamma - 1$ as for any $\varphi \in \bar{D}(M)$, $m \in M$

$$\bar{D}(\Phi)(\varphi)(m) = (\varphi \circ \Phi)(m) = \varphi\big((\gamma - 1)m\big) = \big((\gamma - 1) \cdot \varphi\big)(m).$$

Thus $\operatorname{im} \bar{D}(\Phi) = (\gamma - 1)\bar{D}(M) = I_\Gamma \bar{D}(M)$ and hence

$$\bar{D}(M^\Gamma) = \operatorname{coker} \bar{D}(\Phi) = \bar{D}(M)/\operatorname{im} \bar{D}(\Phi) = \bar{D}(M)/I_\Gamma \bar{D}(M) = \bar{D}(M)_\Gamma. \qquad \square$$

Remark 3.4.6. The previous lemma can be stated also in terms of the natural action of Γ on $M^\vee$: applying ι on both sides we get indeed $D(M)_\Gamma \cong D(M^\Gamma)$.

This property will be used into the proof of the next theorem, that is the version of the Exact Control Theorem 3.3.10 that holds in this particular case. It moreover explains why the theorem was called in that way.

Theorem 3.4.7. *Suppose that $\widetilde{\mathrm{H}}^0(K, A) = 0$. It follows that the canonical map*

$$\widetilde{\mathrm{H}}^1_f(K, A) \xrightarrow{\sim} \widetilde{\mathrm{H}}^1_f(K_\infty/K, A)^\Gamma$$

is an isomorphism of $\mathcal{O}$-modules.

Proof. Consider the first quadrant spectral sequence

$$E_2^{i,j} = \mathrm{H}^i\left(\Gamma, \widetilde{\mathrm{H}}_f^j(K_\infty/K, A)\right) \Longrightarrow \widetilde{\mathrm{H}}_f^{i+j}(K, A)$$

given by Th. 3.3.10. Note that, since the spectral sequence sits in the first quadrant, then

$$E_\infty^{0,0} \cong E_2^{0,0} = \widetilde{\mathrm{H}}_f^0(K_\infty/K, A)^\Gamma \cong \frac{F^0\,\widetilde{\mathrm{H}}_f^0(K, A)}{F^1\,\widetilde{\mathrm{H}}_f^0(K, A)} = \widetilde{\mathrm{H}}_f^0(K, A) = 0$$

But then by the Duality Theorem 3.4.3

$$0 = D\big(\widetilde{\mathrm{H}}_f^0(K_\infty/K, A)^\Gamma\big) \cong \widetilde{\mathrm{H}}_f^3(K_S/K_\infty, T)_\Gamma$$

and hence $\widetilde{\mathrm{H}}_f^3(K_S/K_\infty, T) = 0$ by Nakayama's lemma (it in fact a fintite type Λ-module). It follows that, being its Pontryagin dual, also $\widetilde{\mathrm{H}}_f^0(K_\infty/K, A) = 0$.

Therefore we obtain that $E_2^{i,j} = 0$ if $j \neq 1, 2$ (i.e. the E_2-sheet of this spectral sequence has nonzero terms only in the horizontal half-lines $j = 1, 2$, $i \geq 0$); in fact $\widetilde{\mathrm{H}}^j(K_\infty/K, A) = 0$ for any $j < 0$ by construction, for $j = 0$ since we just showed that $\widetilde{\mathrm{H}}_f^j(K_\infty/K, A) = 0$ and for $j > 3$ since

$$\widetilde{\mathrm{H}}^j(K_\infty/K, A) \cong D\big(\widetilde{\mathrm{H}}_f^{3-j}(K_S/K_\infty, T)\big) = 0.$$

In particular the five term exact sequence

$$0 \to E_2^{1,0} \to E^1 \to E_2^{0,1} \to E_2^{2,0} \to E^2$$

becomes

$$0 \to 0 \to \widetilde{\mathrm{H}}_f^1(K, A) \to \widetilde{\mathrm{H}}_f^1(K_\infty/K, A)^\Gamma \to 0 \to \widetilde{\mathrm{H}}_f^2(K, A)$$

and hence the edge morphism $\widetilde{\mathrm{H}}_f^1(K, A) \to \widetilde{\mathrm{H}}_f^1(K_\infty/K, A)^\Gamma$ is an isomorphism. □

Chapter 4

Vanishing of $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K)$ and its consequences for Anticyclotomic Iwasawa Theory

In this chapter, based on the results of the previous ones, we prove our main result Th. 4.3.6 following [MN19], showing under some conditions on the basic generalized Heegner cycle, that the Shafarevich-Tate group $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty)$ of a modular form f over the anticyclotomic extension K_∞ of an imaginary quadratic field K (that will be defined in Def. 4.3.3) vanishes.

4.1 Setup

Notations of Sec. 1.3 are in force. Note in particular we fix a rational prime p and everything depends on the choice of embeddings $i_\infty\colon \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $i_p\colon \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ and that $\mathfrak{p}$ is the prime induced by i_p on the Hecke field $F = \mathbb{Q}[a_i]_{i>0}$ of a cusp-newform $f = \sum_{n=1}^\infty a_n q^n$ of level $\Gamma_0(N)$ of even weight $k > 2$. Assume that f is ordinary at $\mathfrak{p}$ and that is not a CM-form in the sense of [Rib77]. Let $\mathcal{K}$ denote the completion $F_\mathfrak{p}$ of the Hecke field F at $\mathfrak{p}$ and let $\mathcal{O}$ be its ring of integers. Let $V = W_\mathfrak{p}(k/2)$ be the selfdual Galois representation attached to f, T the selfdual lattice as introduced in Sec. 1.3.3 and let $A = V/T$. In the rest fix moreover a natural number N not divisible by p and a quadratic imaginary field K of discriminant d_K coprime to Np satisfying the *Heegner hypotesis*, i.e. in which all primes dividing N split.

Assumption 1. Take the following hypothesis on the prime p.

(*i*) $p \nmid 6N\varphi(N)(k-2)!$, where φ is the Euler function;

(*ii*) the image of $\rho_{f,p}\colon G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_F \otimes \mathbb{Z}_p)$ contains the set

$$\{\, g \in \mathrm{GL}_2(\mathcal{O}_F \otimes \mathbb{Z}_p) : \det g \in (\mathbb{Z}_p^\times)^{k-1} \,\};$$

(*iii*) p does not ramify in F;

(*iv*) p splits in K;

(*v*) $p \nmid h_K$, where h_K is the class number of K;

(*vi*) $p \nmid c_f = \left[\mathcal{O}_F : \mathcal{O}_f\right]$, where $\mathcal{O}_f = \mathbb{Z}[a_i]_{i>0}$.

REMARK 4.1.1. Note that the first three hypothesis say that p is an admissible prime as in Def. 2.3.3. For a discussion of the significance of these hypothesis see Rk. 2.3.4. The assumption *iv.* is a technical hypotesis in the construction of the generalized Heegner cycles. We already discussed the role of *v.* in Rk. 1.4.7. Finally the hypothesis *vi.* is a technical hypothesis coming from [LV19]: assuming it $\mathcal{O}_f \otimes \mathbb{Z}_p = \mathcal{O}_F \otimes \mathbb{Z}_p$. As observed in [LV19, Rk. 2.2] once f and K are given the restrictions of Assumption 1 are satisfied by an infinite set of primes.

Let then K_∞ denote the anticyclotomic $\mathbb{Z}_p$-extension of K, and write $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, denote by K_n the subextension of $K \subseteq K_\infty$ with Galois group $\Gamma_n \cong \mathbb{Z}/p^n\mathbb{Z}$. Let $\Lambda_n = \mathcal{O}[\Gamma_n]$, $\Lambda = \mathcal{O}[\![\Gamma]\!] = \varprojlim_n \Lambda_n$.

For any $n \geq 0$ define $\mathcal{X}_n = \mathrm{H}^1_f(K_n, A)^\vee$, that is naturally a Λ_n-module (see Sec. 1.4.2), in particular we will write $\mathcal{X} = \mathcal{X}_0 = \mathrm{H}^1_f(K, A)^\vee$ (that is a module over $\mathcal{O} = \Lambda_0$). Their projective limit

$$\mathcal{X}_\infty = \varprojlim_n \mathcal{X}_n = \mathrm{H}^1_f(K_\infty, A)^\vee,$$

has a structure of Λ-module, as we saw in Sec. 1.4.2. In the framework of Assumption 1, Longo and Vigni constructed in [LV19] the Λ-adic anticyclotomic Kolyvagin system of generalized Heegner cycles and they use it in order to describe the structure of $\mathcal{X}_\infty$ as a Λ-module.

Theorem 4.1.2 ([LV19, Th. 1.1]). *There is a finitely generated torsion Λ-module M such that $\mathcal{X}_\infty$ is pseudoisomorphic to $\Lambda \oplus M \oplus M$, i.e. there exists a morphism $\eta\colon \mathcal{X}_\infty \to \Lambda \oplus M \oplus M$ of Λ-modules with finite kernel and cokernel.*

Our goal is to refine this result, showing that if the basic generalized Heegner cycle $z_{f,K}$ is non-torsion and not divisible by p in $\mathrm{H}^1_f(K, T)$, then $\mathcal{X}_\infty$ is in fact free of rank one over Λ: this is the content Th. 4.3.6. We will obtain it following the method of [MN19], i.e. putting together the Euler system argument of Sec. 2.3 with an abstract Iwasawa theoretical one.

We need moreover some other technical assumptions. In Ex. 1.1.14 we defined, for an extension E/K and a finite place $v \nmid p$, $c_v(A)$ to be the p-part of the Tamagawa number of A. Recall that if the representation V is unramified at v, then $c_v(A) = 1$. Therefore in our case $c_v(A) = 1$ for any finite place $v \nmid Np$.

ASSUMPTION 2. Assume that $c_v(A) = 1$ for any place v of K such that $v \mid N$.

We take the following assumption on the q-expansion of f.

ASSUMPTION 3. $i_p(a_p) \not\equiv 1 \mod \mathfrak{p}$.

4.2 Comparison of Selmer groups, Exact Control Theorem

We now make a comparison of the Selmer groups introduced in Sec. 1.1.2 and the generalized ones introduced in Sec. 3.4. In Sec. 1.3.8 we saw that V is (the $k/2$-twist of the dual of) a $\mathfrak{p}$-ordinary representation, more precisely we have an exact sequence

$$0 \to V^+ \to V \to V^- \to 0$$

of $\mathcal{K}[G_p]$-modules such that $V^\pm$ has dimension 1 and G_p acts on V^+ by $\delta\chi_p^{k/2}$ and on V^- by $\delta^{-1}\chi_p^{1-k/2}$, for δ an unramified character and χ_p the p-adic cyclotomic character.

Let E a number field and $v \mid p$ a place and see the previous exact sequence as an exact sequence of $\mathcal{K}[G_{E_v}]$-modules. We have

Lemma 4.2.1. $\mathrm{H}^0(E_v, V^-) = 0$

Proof. By [NP00, (3.1.5)], in the case $p \nmid N$. It can be done also directly observing that $\sigma \in I_p$ acts as $\chi_p(\sigma)^{1-k/2}$ and there is a σ such that this $\chi_p(\sigma)^{1-k/2} \neq 1$, as $k > 2$. But by loc. cit. this holds even for $k = 2$ if $p \nmid N$. □

Proposition 4.2.2. $\widetilde{\mathrm{H}}^1_f(E,V) = \mathrm{H}^1_f(E,V) = \mathrm{H}^1_{\mathrm{str}}(E,V) = \mathrm{H}^1_{\mathrm{Gr}}(E,V)$.

Proof. The first equality follows from the exact sequence [Nek06, Prop. 12.5.9.2(*iii*)] for the representation attached to an ordinary modular form

$$0 \to \bigoplus_{v|p} \mathrm{H}^0(E_v, V^-) \to \widetilde{\mathrm{H}}^1_f(E,V) \to \mathrm{H}^1_f(E,V) \to 0.$$

and the previous lemma. The second equality follows from the exact sequence

$$0 \to \widetilde{\mathrm{H}}^0_f(E,V) \to \mathrm{H}^0(E,V) \to \bigoplus_{v|p} \mathrm{H}^0(E_v, V^-) \to \widetilde{\mathrm{H}}^1_f(E,V) \to \mathrm{H}^1_{\mathrm{str}}(E,V) \to 0$$

of Prop. 3.4.1 plus Lemma 4.2.1. For the equality $\mathrm{H}^1_f(E,V) = \mathrm{H}^1_{\mathrm{Gr}}(E,V)$ it is enough to prove that $\mathrm{H}^1_f(E_v,V) = \ker\left(\mathrm{H}^1(E_v,V) \to \mathrm{H}^1(I_v,V^-)\right)$ for any place $v \mid p$ of E. This is shown in [LV21, Sec. 3.3.3]. □

If we restrict to $E = K$ or $E = K_n$, the n-th layer of the anticyclotomic extension K_∞ of K, we may compare also the Selmer groups of A. First let us make a technical remark.

Remark 4.2.3. The aim of this remark is to fix a Frobenius automorphism φ_p in G_p such that $\chi_p(\varphi_p) = 1$. Recall that the maximal unramified extension of $\mathbb{Q}_p$ is $\mathbb{Q}_p^{\mathrm{ur}} = \mathbb{Q}_p(\mu_{p^\infty - 1})$ and consider the short exact sequence

$$1 \to I_p = \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{ur}}) \to G_p \to \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \to 1.$$

A Frobenius automorphism is any lift to G_p of the the p-power map $x \mapsto x^p$ of $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$; in particular its restriction to $\mathbb{Q}_p^{\mathrm{ur}}$ is uniquely determined by this property, as

$$G_p/I_p = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \cong \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$$

via the reduction map. It follows that for any Frobenius automorphism Frob_p, its restriction to $\mathbb{Q}_p^{\mathrm{ur}}$ is the unique $\mathbb{Q}_p$-automorphism of $\mathbb{Q}_p^{\mathrm{ur}}$ such that $\zeta \mapsto \zeta^p$ for any $\zeta \in \mu_{p^\infty-1}$. Conversely we may freely choose its extension from $\mathbb{Q}_p^{\mathrm{ur}}$ to $\bar{\mathbb{Q}}_p$, let φ_p be the Frobenius of G_p extended by the identity.

We want to compute the value of $\chi_p(\varphi_p)$. It is enough to observe that $\mu_{p^\infty} \cap \mathbb{Q}_p^{\mathrm{ur}} = 1$ being the extension $\mathbb{Q}_p(\mu_{p^n})/\mathbb{Q}_p$ totally ramified for any $n > 0$. It follows that φ_p fixes μ_{p^∞} and so $\chi_p(\varphi_p) = 1$ as $\zeta^{\chi_p(\varphi_p)} = \varphi_p(\zeta) = \zeta$, for any $\zeta \in \mu_{p^\infty}$. Note that if we choose another Frobenius Frob_p the value of $\chi_p(\mathrm{Frob}_p)$ could be different, in fact it differs from φ_p by some $\sigma \in I_p$, but χ_p is a ramified character and hence possibly $\chi_p(\sigma) \neq 1$.

Consider now K_∞. Recall how the ramification in a $\mathbb{Z}_p$-extension K_∞ of a number field K [see Was97, Prop. 13.2, 13.3] works: it is concentrated at places above p and one of them must ramify. Furthermore if $v \mid p$ ramifies in K_∞/K, it may in general be unramified in K_n/K up to some layer n, but after that it is totally ramified in K_∞/K_n. In fact in our case since $K_\infty/\mathbb{Q}$ and p slits in K, both places $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ of K over p have the same beaviour in K_∞/K, namely they are totally ramified as $K_\infty \cap K[1] = K$ (since $p \nmid h_K$ and K_∞ is a p-extension) and therefore they cannot be unramified in any layer K_n for $n \geq 1$. It follows, again since p splits in K, that p is totally ramified in $K_\infty/\mathbb{Q}$.

Choose a compatible sequence of places v_n of K_n over p and let $K_{n,v}$ be the completion of K_n at v_n. By the previous discussion the inertia degree of $K_{v,n}/\mathbb{Q}_p$ is 1 and hence the residue field of $K_{v,n}$ is $\mathbb{F}_p$. Hence φ_p is a Frobenius of the absolute Galois group $G_{n,v}$ of $K_{n,v}$. Let $I_{n,v} = I_p \cap G_{n,v}$ be the inertia subgroup of $G_{n,v}$, note that $G_{n,v}/I_{n,v}$ is cyclic generated by $\varphi_p \bmod I_{n,v}$.

Lemma 4.2.4. *For any place $v_n \mid p$, $\mathrm{H}^1\left(G_{n,v}/I_{n,v}, \mathrm{H}^0(I_{n,v}, A^-)\right) = 0$.*

Proof. Since $\mathrm{H}^0(I_{n,v}, A^-)$ is a subgroup of $A^- \cong \mathcal{K}/\mathcal{O}$, and so torsion and discrete, we may apply [Rub00, B.2.8]. Therefore,

$$\mathrm{H}^1\left(G_{n,v}/I_{n,v}, \mathrm{H}^0(I_{n,v}, A^-)\right) \cong \frac{\mathrm{H}^0(I_{n,v}, A^-)}{(\varphi_p - 1)\,\mathrm{H}^0(I_{n,v}, A^-)}.$$

Let α be the $\mathfrak{p}$-adic unit root of the polynomial $X^2 - i_p(a_p)X + p^{k-1}$, as defined in Rk. 1.3.8 and let β be the non unit root. Recall that we may see A^- as $\mathcal{K}/\mathcal{O}$ together with the action given by $\delta^{-1}\chi_p^{1-k/2}$, where δ is the unramified character of G_p such that $\delta(\mathrm{Frob}_p) = \alpha^{-1}$, for any arithmetic Frobenius Frob_p. Then

$$\varphi_p \cdot x = \delta(\varphi_p)^{-1}\chi_p(\varphi_p)^{(1-k/2)}x = \alpha x$$

for any $x \in \mathrm{H}^0(I_{n,v}, A^-)$ (seen as a subgroup of $\mathcal{K}/\mathcal{O}$), as $\chi_p(\varphi_p) = 1$. It follows that

$$\mathrm{H}^1\left(G_{n,v}/I_{n,v}, \mathrm{H}^0(I_{n,v}, A^-)\right) \cong \frac{\mathrm{H}^0(I_{n,v}, A^-)}{(\alpha - 1)\,\mathrm{H}^0(I_{n,v}, A^-)}.$$

Note that $\alpha + \beta = i_p(a_p)$ and hence (as $\beta \equiv 0 \bmod \mathfrak{p}$)

$$\alpha \equiv i_p(a_p) \bmod \mathfrak{p}.$$

By Assumption 3, $\alpha \not\equiv 1 \bmod \mathfrak{p}$. Hence $\alpha - 1$ is a $\mathfrak{p}$-adic unit and so

$$(\alpha - 1)\,\mathrm{H}^0(I_{n,v}, A^-) = \mathrm{H}^0(I_{n,v}, A^-),$$

as the inclusion ($\subseteq$) is trivial, while for ($\supseteq$) it is enough to observe that if $x + \mathcal{O} \in \mathrm{H}^0(I_{n,v}, A^-)$, then $x + \mathcal{O} = (\alpha - 1)y + \mathcal{O}$, for $y + \mathcal{O} = (\alpha - 1)^{-1}x + \mathcal{O} \in \mathrm{H}^0(I_{n,v}, A^-)$. Thus,

$$\mathrm{H}^1\left(G_{n,v}/I_{n,v}, \mathrm{H}^0(I_{n,v}, A^-)\right) = 0$$

□

Lemma 4.2.5. *For any place $v_n \mid p$, $\mathrm{H}^0(K_{n,v}, A^-) = 0$.*

Proof. In the isomorphism $A^- \cong \mathcal{K}/\mathcal{O}$, $\varphi_p \in G_{n,v}$ acts as α and $(\alpha - 1) \in \mathcal{O}^\times$, as we saw in the previous lemma. Therefore for any $x + \mathcal{O} \in \mathcal{K}/\mathcal{O}$, with $v_\mathfrak{p}(x) < 0$,

$$\varphi_p \cdot (x + \mathcal{O}) = \alpha x + \mathcal{O} \neq x + \mathcal{O}.$$

because $v_\mathfrak{p}(\alpha x - x) = v_\mathfrak{p}\big((\alpha - 1)x\big) = v_\mathfrak{p}(x) < 0$. This means that there exists for any nonzero element of A^- an automorphism of $G_{n,v}$ that does not fix it and so $\mathrm{H}^0(K_{n,v}, A^-) = 0$. □

We may now compare the various selmer groups of A that we know. We first deal with the comparison of finite and unramified local conditions at primes v of bad reduction, i.e. $v \mid N$.

Lemma 4.2.6. *For any place v_n of K_n such that $v_n \mid N$, we have $c_{v_n}(A) = 1$.*

Proof. For any p-adic field L write $\mathcal{A}_L = \mathrm{H}^0(I_L, A)/\,\mathrm{H}^0(I_L, A)_{\mathrm{div}}$. By [Rub00, Lemma I.3.2(*iii.*)]

$$\frac{\mathrm{H}^1_{\mathrm{ur}}(L, A)}{\mathrm{H}^1_f(L, A)} \xrightarrow{\sim} \frac{\mathcal{A}_L}{(\mathrm{Frob}_L - 1)\mathcal{A}_L}.$$

Since by Assumption 2, $c_v(A) = 1$ for any $v \mid N$, then $\mathrm{H}^1_{\mathrm{ur}}(K_v, A) = \mathrm{H}^1_f(K_v, A)$ and hence $\mathcal{A}_{K_v}/(\mathrm{Frob}_{K_v} - 1)\mathcal{A}_{K_v} = 0$. But since $v \nmid p$, K_n/K is unramified at v, hence $I_{n,v} = I_v$ and therefore $\mathcal{A}_{K_{n,v}} = \mathcal{A}_{K_v}$. Thus $\mathrm{H}^1_{\mathrm{ur}}(K_{n,v}, A) = \mathrm{H}^1_f(K_{n,v}, A)$, too. □

Proposition 4.2.7. $\widetilde{\mathrm{H}}^1_f(K_n, A) = \mathrm{H}^1_f(K_n, A) = \mathrm{H}^1_{\mathrm{str}}(K_n, A) = \mathrm{H}^1_{\mathrm{Gr}}(K_n, A)$ *for any* $n \geq 0$.

Proof. Observe that $\widetilde{\mathrm{H}}^1_f(K_n, A) = \mathrm{H}^1_{\mathrm{str}}(K_n, A)$, by the exact sequence of Prop. 3.4.1

$$0 \to \widetilde{\mathrm{H}}^0_f(K_n, A) \to \mathrm{H}^0(K_n, A) \to \bigoplus_{v_n \mid p} \mathrm{H}^0(K_{n,v}, A^-) \to \widetilde{\mathrm{H}}^1_f(E_n, A) \to \mathrm{H}^1_{\mathrm{str}}(K_n, A) \to 0,$$

as $\mathrm{H}^0(K_{n,v}, A^-) = 0$ by Lemma 4.2.5. Moreover by Lemma 4.2.4 the exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{str}}(K_n, A) \to \mathrm{H}^1_{\mathrm{Gr}}(K_n, A) \to \bigoplus_{v_n \mid p} \mathrm{H}^1\left(G_{n,v}/I_{n,v}, \mathrm{H}^0(I_{n,v}, A^-)\right) = 0$$

shows that $\mathrm{H}^1_{\mathrm{str}}(K_n, A) = \mathrm{H}^1_{\mathrm{Gr}}(K_n, A)$. Finally $\mathrm{H}^1_{\mathrm{Gr}}(K_n, A) = \mathrm{H}^1_f(K_n, A)$ by comparing each local condition: in fact for any $v_n \nmid p$, $\mathrm{H}^1_f(E_{n,v}, A) = \mathrm{H}^1_{\mathrm{ur}}(K_{n,v}, A)$ as $c_{v_n}(A) = 1$ and for $v_n \mid p$ the proof of [LV21, Lemma 5.4] shows (it is the injectivity of the first map considered there) that

$$\mathrm{H}^1_f(K_{n,v}, A) = \ker\left(\mathrm{H}^1(K_{n,v}, A) \to \mathrm{H}^1(I_{n,v}, A^-)\right) = \mathrm{H}^1_{\mathrm{ord}}(K_{n,v}, A).$$ □

Remark 4.2.8. Lemma 4.2.4 and 4.2.5 would work even if p were inert in K, if we asked

$$i_p(a_p) \not\equiv \pm 1 \bmod \mathfrak{p}.$$

In fact in that case the inertia degree of $K_{n,v}/\mathbb{Q}_p$ would have been 2 and hence $G_{n,v}/I_{n,v}$ would have been generated by φ_p^2 mod $I_{n,v}$ and the lemmas would follow once $\alpha^2 - 1$ is a unit.

We may state a more precise theorem about generalized Selmer groups, we need first some technical lemmas about the vanishig of the H^0 of A over the anticyclotomic tower.

Proposition 4.2.9. $\mathrm{H}^0(K_n, A[p]) = 0$ *for any* $n \geq 0$

Proof. The proof is anologous to the proof of Lemma 2.3.5 replacing K_n to $K[n]$. In fact $K_n/\mathbb{Q}$ is solvable as $K/\mathbb{Q}$ is abelian and K_n/K is a cyclic extension. □

Proposition 4.2.10.

1. $\mathrm{H}^0(K_n, A[p^m]) = 0$ *for any* $n \geq 0$*,* $m > 0$*;*
2. $\mathrm{H}^0(K_n, A) = 0$ *for any* $n \geq 0$*;*
3. $\mathrm{H}^0(K_\infty, A) = \mathrm{H}^0(K_\infty, A[p^m]) = 0$ *for any* $m > 0$*;*
4. $\mathrm{H}^0(K_n, V) = 0$, $\mathrm{H}^0(K_n, T) = 0$ *for any* $n \geq 0$*;*
5. $\mathrm{H}^0(K_n, V^*(1)) = 0$, $\mathrm{H}^0(K_n, T^*(1)) = 0$ *for any* $n \geq 0$.

Proof. (1) follows by induction: Prop. 4.2.9 is the base case. As H^0 and taking torsion commute, for $m > 1$ and $x \in \mathrm{H}^0(K_n, A[p^m])$ then $px \in \mathrm{H}^0(K_n, A[p^{m-1}])$. Therefore $x \in \mathrm{H}^0(K_n, A[p])$, since $\mathrm{H}^0(K_n, A[p^{m-1}]) = 0$ by inductive hypothesis, and so $x = 0$ again by Prop. 4.2.9.

(2) follows from (1) taking inductive limit over m as $A \cong \varinjlim_m A[p^m]$ and the fact that H^0 commutes with $\varinjlim$. (3) then follows from (2) and (1) taking inductive limit over n. (4) follows from (2): Suppose that there is an element $0 \neq x \in V$ fixed by any $\sigma \in G_{K_n}$, then its image $\bar{x} \in A$ is still fixed. We may moreover assume $x \notin T$, up to multiplication by a suitable power of p (the action of σ is linear), i.e. $\bar{x} \neq 0$. This proves the claim for V. The claim for T follows because $T \subseteq V$, so $\mathrm{H}^0(K_n, T) \subseteq \mathrm{H}^0(K_n, V)$. At last by (4) and the isomorphism $V \cong V^*(1)$ follows that $\mathrm{H}^0(K_n, T^*(1)) \subseteq \mathrm{H}^0(K_n, V^*(1)) = 0$ and hence (5) is proved. □

Proposition 4.2.11. *For V the selfdual Galois representation attached to a $\mathfrak{p}$-ordinary newform*

$$\widetilde{\mathrm{H}}^i_f(K_n, A) = \begin{cases} \mathrm{H}^1_f(K_n, A) & \text{for } i = 1; \\ D\Big(\widetilde{\mathrm{H}}^1_f\left(K_n, T^*(1)\right)\Big) & \text{for } i = 2; \\ 0 & \text{for } i \neq 1, 2. \end{cases}$$

Proof. We have $\widetilde{\mathrm{H}}^i_f(K_n, A) = \mathrm{H}^1_f(K_n, A)$ by Prop. 4.2.7. By Prop. 3.4.2, there is an isomorphism $\widetilde{\mathrm{H}}^i_f(K_n, A) \cong D\big(\widetilde{\mathrm{H}}^{3-i}_f(K_n, T^*(1))\big)$. It follows that $\widetilde{\mathrm{H}}^i_f(K_n, A) \cong D\big(\widetilde{\mathrm{H}}^{3-i}_f(K_n, T^*(1))\big)$ for any $i \in \mathbb{Z}$. Therefore, as $\widetilde{\mathrm{H}}^j_f(K_n, A) = 0$ if $j < 0$ by definition, it follows that $\widetilde{\mathrm{H}}^i_f(K_n, A) = 0$ for $i \neq 0, 1, 2, 3$. Furthermore $\widetilde{\mathrm{H}}^3_f(K_n, A) = 0$, as it is the dual of $\widetilde{\mathrm{H}}^0_f(K_n, T^*(1))$, that is a submodule of $\mathrm{H}^0(K_n, T^*(1))$ and the latter vanishes by Prop. 4.2.10(5). Similarly $\widetilde{\mathrm{H}}^0_f(K_n, A) = 0$ as it is a submodule of $\mathrm{H}^0(K_n, A)$, that vanishes by Prop. 4.2.10(2). □

Taking the direct limit over n we have:

Proposition 4.2.12. *For V the selfdual Galois representation attached to a $\mathfrak{p}$-ordinary newform*

$$\widetilde{\mathrm{H}}^i_f(K_\infty, A) = \begin{cases} \mathrm{H}^1_f(K_\infty, A), & \text{for } i = 1; \\ D\Big(\widetilde{\mathrm{H}}^1_f\left(K_\infty, T^*(1)\right)\Big), & \text{for } i = 2; \\ 0 & \text{for } i \neq 1, 2. \end{cases}$$

Therefore Th. 3.4 becomes:

Theorem 4.2.13 (Exact Control Theorem)**.** *The canonical map*

$$\mathrm{H}^1_f(K_n, A) \xrightarrow{\sim} \mathrm{H}^1_f(K_\infty, A)^{\mathrm{Gal}(K_\infty/K_n)}$$

is an isomorphism.

Proof. Apply Th. 3.4 to K_∞/K_n and combine with Prop. 4.2.11 and 4.2.12. □

Remark 4.2.14. Recall that for any Λ-module M the $\mathcal{O}$-module of co-invariants is defined to be $M_\Gamma = M/IM$, where I is the ideal of Λ generated by $\gamma - 1$, for a topological generator γ of Γ. In terms of coinvariants the exact control theorem is equivalent to an isomorphism of Λ-modules

$$(\mathcal{X}_\infty)_\Gamma \xrightarrow{\sim} \mathcal{X},$$

as $D(M^\Gamma) \cong D(M)_\Gamma$ by Rk. 3.4.6.

4.3 Vanishing of $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty)$

In this section we obtain our main theorem. As a first step we show that we may extend the corank one of the Bloch-Kato Selmer group over the anticyclotomic extension K_∞/K.

Theorem 4.3.1. *Let $\mathcal{X}$ be a free $\mathcal{O}$-module of rank 1, then $\mathcal{X}_\infty$ is a free Λ-module of rank 1.*

Proof. By Th. 4.2.13 and Rk. 4.2.14 $(\mathcal{X}_\infty)_\Gamma \cong \mathcal{X} \cong \mathcal{O}$, i.e. there is an $x \in \mathcal{X}_\infty$ whose image in $\mathcal{X}_\infty$ generates it as an $\mathcal{O}$-module. It follows that $(\mathcal{X}_\infty/x\Lambda)_\Gamma = 0$ and therefore by Nakayama's lemma $\mathcal{X}_\infty = x\Lambda$, i.e. $\mathcal{X}_\infty$ is a cyclic Λ-module. In fact, if we consider the short exact sequence

$$0 \to x\Lambda \to \mathcal{X}_\infty \to \mathcal{X}_\infty/x\Lambda \to 0$$

and hence, taking coinvariants, the sequence

$$(x\Lambda)_\Gamma \to (\mathcal{X}_\infty)_\Gamma \to (\mathcal{X}_\infty/x\Lambda)_\Gamma \to 0$$

is exact. Therefore $(\mathcal{X}_\infty/x\Lambda)_\Gamma = 0$, since the map $(x\Lambda)_\Gamma \to (\mathcal{X}_\infty)_\Gamma$ is an isomorphism.

It is left to show that $\mathcal{X}_\infty$ it is not Λ-torsion. Suppose by contraddiction that this is the case. Consider the map $\eta\colon \mathcal{X}_\infty \to \Lambda \oplus M \oplus M$ of Th. 4.1.2. The Λ-module $\mathcal{X}_\infty$ is cyclic and torsion and so Im $\eta = \alpha\Lambda$, with α a torsion element, i.e. $\alpha \in M \oplus M$. Therefore

$$\operatorname{coker}\eta = \frac{\Lambda \oplus M \oplus M}{\alpha\Lambda} = \Lambda \oplus \frac{M \oplus M}{\alpha\Lambda}$$

is infinite, contradicting Th. 4.1.2. □

The previous theorem can be rephrased, using the notions introduced in Ch. 2, in terms of the ($\mathfrak{p}$-primary) Shafarevich-Tate group of f. In order to do that we need to define $\widetilde{\Lambda}_\mathfrak{p}$, the analogous of the Mordell-Weil group of an elliptic curve, over the anticyclotomic extension K_∞ of K and its layers K_n. As for the definition of $\widetilde{\Lambda}_\mathfrak{p}(K)$, in order to define it we assume that the restriction map

$$\operatorname{res}_{K[p^{n+1}]/K_n}\colon \mathrm{H}^1(K_n, T) \to \mathrm{H}^1(K[p^{n+1}], T)^{\mathrm{Gal}(K[p^{n+1}]/K_n)}$$

is an isomorhism for $n > 0$.

Definition 4.3.2. We define for any $n > 0$,

$$\widetilde{\Lambda}_\mathfrak{p}(K_n) := \operatorname{res}^{-1}_{K[p^{n+1}]/K_n}\big(\widetilde{\Lambda}_\mathfrak{p}(K[p^{n+1}])^{\mathrm{Gal}(K[p^{n+1}]/K_n)}\big).$$

and $\widetilde{\Lambda}_\mathfrak{p}(K_\infty) = \varprojlim_{n,\mathrm{cores}} \widetilde{\Lambda}_\mathfrak{p}(K_n) \subseteq \mathrm{H}^1_f(K_\infty, T)$.

Definition 4.3.3. The $\mathfrak{p}$-divisible Tate-Shafarevich group $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_n)$ of f over K_n is defined, for any $n = 0, \dots, \infty$, by the exact sequence

$$0 \longrightarrow \widetilde{\Lambda}_\mathfrak{p}(K_n) \otimes \mathcal{K}/\mathcal{O} \longrightarrow \mathrm{H}^1_f(K_n, A) \longrightarrow \widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_n) \longrightarrow 0$$

Remark 4.3.4. Note that under our assumptions the restriction is indeed an isomorphism: it follows by Lemma 2.3.5 with the same argument of Rk. 2.3.7 and therefore $\widetilde{\Lambda}_\mathfrak{p}(K_n)$ and $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_n)$ are well defined. In particular, since $\mathrm{H}^0(K_n, A[p]) = 0$ by Prop. 4.2.9, the same argument of Lemma 2.3.5 shows that $\widetilde{\Lambda}_\mathfrak{p}(K_n)$ is a free $\mathcal{O}$-module of finite rank. Moreover each $\widetilde{\Lambda}_\mathfrak{p}(K_n)$ is endowed of an action of $\mathrm{Gal}(K_n/K)$ and hence $\widetilde{\Lambda}_\mathfrak{p}(K_\infty)$ has a structure of Λ-module, compatible with the inclusion into $\mathrm{H}^1_f(K_\infty, T)$.

Using this language we may enhance Th. 4.3.1.

Theorem 4.3.5. *Suppose that $\widetilde{\Lambda}_{\mathfrak{p}}(K) \otimes \mathcal{K}/\mathcal{O}$ and $\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty)$ are nontrivial. If $\mathcal{X}$ is free of rank* 1 *over $\mathcal{O}$, then*

$$\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K) = \widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty) = 0; \quad \mathrm{H}^1_f(K_\infty, A) = \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) \otimes \mathcal{K}/\mathcal{O},$$

the Pontryagin dual $\mathcal{X}_\infty$ of the latter group being free of rank 1 *over* Λ.

Proof. If $\mathcal{X} \cong \mathcal{O}$, then $\mathrm{H}^1_f(K, A) \cong \mathcal{K}/\mathcal{O}$. Now by Cor. 2.3.8 $\widetilde{\Lambda}_{\mathfrak{p}}(K) = \mathcal{O}^j$ for some $j > 0$

$$0 \neq \widetilde{\Lambda}_{\mathfrak{p}}(K) \otimes \mathcal{K}/\mathcal{O} \cong (\mathcal{K}/\mathcal{O})^j \subseteq \mathrm{H}^1_f(K, A) \cong \mathcal{K}/\mathcal{O},$$

therefore $j = 1$ and the inclusion must be an equality and hence $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K) = 0$.

Let us now pass to K_∞. By Th. 4.3.1 we already know that $\mathcal{X}_\infty$ has rank 1 over Λ, let us show that $\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty) = 0$. Let

$$\mathcal{Z}_\infty = D\big(\widetilde{Ш}_{\mathfrak{p}^\infty}(f/K_\infty)\big), \qquad \mathcal{Y}_\infty = D\big(\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) \otimes \mathcal{K}/\mathcal{O}\big),$$

we have by duality a short exact sequence

$$0 \longrightarrow \mathcal{Z}_\infty \longrightarrow \mathcal{X}_\infty \longrightarrow \mathcal{Y}_\infty \longrightarrow 0$$

and hence our vanishing claim is equivalent to show that $\mathcal{X}_\infty/\mathcal{Z}_\infty = \mathcal{Y}_\infty$ is not Λ-torsion: indeed being $\mathcal{Y}_\infty$ a quotient of $\mathcal{X}_\infty \cong \Lambda$, it is Λ-torsion if and only if $\mathcal{Z}_\infty \neq 0$. Observe that

$$\begin{aligned} \mathcal{Y}_\infty &= \mathrm{Hom}_{\mathcal{O}}\big(\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) \otimes \mathcal{K}/\mathcal{O}, \mathcal{K}/\mathcal{O}\big) = \\ &= \mathrm{Hom}_{\mathcal{O}}\big(\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty), \mathrm{Hom}_{\mathcal{O}}(\mathcal{K}/\mathcal{O}, \mathcal{K}/\mathcal{O})\big) = \\ &= \mathrm{Hom}_{\mathcal{O}}\big(\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty), \mathcal{O}\big) = \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty)^* \end{aligned}$$

and that in particular $\mathcal{Y}_\infty[p] = \mathrm{Hom}_{\mathcal{O}}\big(\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty), \mathcal{O}[p]\big) = 0$, since $\mathcal{O}[p] = 0$.

It follows that if $\mathcal{Y}_\infty$ were Λ-torsion, then it would be a free $\mathcal{O}$-module of finite type. Indeed there would be a nonzero ideal J of $\mathcal{O}[\![T]\!]$ such that $\mathcal{Y}_\infty \cong \mathcal{O}[\![T]\!]/J$, moreover since $\mathcal{Y}_\infty[p] = 0$ all power series $f = \sum_{j=0}^\infty a_j T^j \in J$ are such that $a_j \notin \mathfrak{p}$ for some j (otherwise the power series $f' = \sum_{j=0}^\infty (a_j/p) T^j \in \mathcal{O}[\![T]\!]$ would be p-torsion mod$J$): fix such a series and let s be the smallest index j such that $a_j \notin \mathfrak{p}$. By the division lemma [NSW00, Lemma 5.3.1], for any $g \in \mathcal{O}[\![T]\!]$, $f = gq + r$ for $q \in \mathcal{O}[\![T]\!]$ and $r \in \mathcal{O}[T]^{\leq s-1}$ and in particular the powers $T, \ldots, T^{s-1}$ would be a set of generators of $\mathcal{O}[\![T]\!]/(f)$, and hence of its quotient $\mathcal{O}[\![T]\!]/J$, as an $\mathcal{O}$-module. Thus $\mathcal{Y}_\infty$ would be of finite type over $\mathcal{O}$ and free since $\mathcal{Y}_\infty[p] = 0$, following the same argument of the proof of Cor. 2.3.8.

But since $\mathcal{Y}_\infty = \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty)^*$, then also $\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty)$ would be a free $\mathcal{O}$-module of finite rank; in particular there would be an m such that $\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) = \mathrm{res}_{K_\infty/K_m}\Big(\widetilde{\Lambda}_{\mathfrak{p}}(K_m)\Big)$, then

$$\begin{aligned} \mathrm{cores}_{K_{n+k}/K_n}\big(\widetilde{\Lambda}_{\mathfrak{p}}(K_{n+k})\big) &= \mathrm{cores}_{K_{n+k}/K_n} \circ \mathrm{res}_{K_{n+k}/K_n}\Big(\widetilde{\Lambda}_{\mathfrak{p}}(K_n)\Big) = \\ &= [K_{n+k} : K_n]\widetilde{\Lambda}_{\mathfrak{p}}(K_n) = p^k \widetilde{\Lambda}_{\mathfrak{p}}(K_n) \end{aligned}$$

for any $k > 0, n \geq m$. But then $\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) = 0$, contraddicting our hypothesis. Let indeed $(\varepsilon_n)_n \in \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty)$, for any $n \geq m$ this fact implies that $\varepsilon_n = \mathrm{cores}_{K_{n+k}/K_n}(\varepsilon_{n+k})$ is divisible by p^k for any $k > 0$, but then $\varepsilon_n = 0$ since $\widetilde{\Lambda}_{\mathfrak{p}}(K_n)$ is finite free over $\mathcal{O}$ and therefore it does not have infinitely divisible nonzero elements. Hence $\varepsilon_n = 0$ for any n. □

Let us now consider the generalized Heegner cycles $z_{f,c}$ of Sec. 2.2.2. We saw in Sec. 2.3 that they may be used in order to bound the size of $\mathrm{H}^1_f(K,A)$. We may moreover use them in order to endow the $\widetilde{\Lambda}_{\mathfrak{p}}(K_n)$'s with a sistematic supply of classes

$$\alpha_n = \mathrm{cores}_{K[p^{n+1}]/K_n}(z_{f,p^{n+1}}) \in \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty);$$

Longo and Vigni in [LV19, T. 4.12] proved that starting from them we may construct a nontrivial element $\tilde{\kappa}_1 \in \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty)$. Therefore, in particular, the condition $\widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) \neq 0$ is always satisfied under our assumptions.

Finally we may gather everything together and state our main theorem.

Theorem 4.3.6. *Suppose that the basic generalized Heegner cycle $z_{f,K}$ is non-torsion and that $z_{f,K} \notin p\,\mathrm{H}^1_f(K,T)$. Then $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K) = 0$ and*

$$\widetilde{\Lambda}_{\mathfrak{p}}(K) \otimes \mathcal{K}/\mathcal{O} = \mathrm{H}^1_f(K,A) = z_{f,K} \cdot \mathcal{K}/\mathcal{O},$$

moreover $\widetilde{\text{Ш}}_{\mathfrak{p}^\infty}(f/K_\infty) = 0$ and $\mathrm{H}^1_f(K_\infty,A) = \widetilde{\Lambda}_{\mathfrak{p}}(K_\infty) \otimes \mathcal{K}/\mathcal{O}$, the Pontryagin dual $\mathcal{X}_\infty$ of the latter group beeing free of rank 1 over Λ.

Proof. This is the combination of Th. 2.3.9 and Th. 4.3.5. In order to glue them together observe that $z_{f,K}$, beeing non torsion in $\widetilde{\Lambda}_{\mathfrak{p}}(K)$, is nontrivial in $\widetilde{\Lambda}_{\mathfrak{p}}(K) \otimes \mathcal{K}/\mathcal{O}$ and that

$$z_{f,K} \cdot \mathcal{K}/\mathcal{O}$$

has corank 1 over $\mathcal{O}$. □

Bibliography

[And04] Yves André, *Une introduction aux motifs (motifs purs, motifs mixtes, périodes)*, vol. 17, Panoramas et Synthèses [Panoramas and Syntheses], Société Mathématique de France, Paris, 2004, ISBN: 2-85629-164-3, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=2115000`.

[BDLP21] Massimo Bertolini, Henri Darmon, David Lilienfeldt and Kartik Prasanna, "Generalised Heegner cycles and the complex Abel-Jacobi map", in: *Math. Z.* 298.1-2 (2021), pp. 385–418, ISSN: 0025-5874, DOI: `10.1007/s00209-020-02603-8`, URL: `https://doi.org/10.1007/s00209-020-02603-8`.

[BDP13] Massimo Bertolini, Henri Darmon and Kartik Prasanna, "Generalized Heegner cycles and p-adic Rankin L-series", in: *Duke Math. J.* 162.6 (2013), With an appendix by Brian Conrad, pp. 1033–1148, ISSN: 0012-7094, DOI: `10.1215/00127094-2142056`, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=3053566`.

[Bes97] Amnon Besser, "On the finiteness of Ш for motives associated to modular forms", in: *Doc. Math.* 2 (1997), pp. 31–46, ISSN: 1431-0635, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=1443065`.

[BH93] Winfried Bruns and Jürgen Herzog, *Cohen-Macaulay rings*, vol. 39, Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1993, ISBN: 0-521-41068-1, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=1251956`.

[BK90] Spencer Bloch and Kazuya Kato, "L-functions and Tamagawa numbers of motives", in: *The Grothendieck Festschrift, Vol. I*, vol. 86, Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 333–400, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=1086888`.

[Bri07] David Brink, "Prime decomposition in the anti-cyclotomic extension", in: *Math. Comp.* 76.260 (2007), pp. 2127–2138, ISSN: 0025-5718, DOI: `10.1090/S0025-5718-07-01964-3`, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=2336287`.

[BS15] Bhargav Bhatt and Peter Scholze, "The pro-étale topology for schemes", in: *Astérisque* 369 (2015), pp. 99–201, ISSN: 0303-1179, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=3379634`.

[CH18] Francesc Castella and Ming-Lun Hsieh, "Heegner cycles and p-adic L-functions", in: *Math. Ann.* 370.1-2 (2018), pp. 567–628, ISSN: 0025-5831, DOI: `10.1007/s00208-017-1517-3`, URL: `https://mathscinet.ams.org/mathscinet-getitem?mr=3747496`.

[Cox89] David A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, Fermat, class field theory and complex multiplication, John Wiley & Sons, Inc., New York, 1989, ISBN: 0-471-50654-0; 0-471-19079-9, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1028322.

[Del71] Pierre Deligne, "Formes modulaires et représentations l-adiques", in: *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, vol. 175, Lecture Notes in Math. Springer, Berlin, 1971, Exp. No. 355, 139–172, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=3077124.

[Ful98] William Fulton, *Intersection theory*, Second, vol. 2, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], Springer-Verlag, Berlin, 1998, ISBN: 3-540-62046-X; 0-387-98549-2, DOI: 10.1007/978-1-4612-1700-8, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1644323.

[Gre91] Ralph Greenberg, "Iwasawa theory for motives", in: *L-functions and arithmetic (Durham, 1989)*, vol. 153, London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1991, pp. 211–233, DOI: 10.1017/CBO9780511526053.008, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1110394.

[Gro80] Benedict H. Gross, *Arithmetic on elliptic curves with complex multiplication*, vol. 776, Lecture Notes in Mathematics, With an appendix by B. Mazur, Springer, Berlin, 1980, pp. iii+95, ISBN: 3-540-09743-0, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=563921.

[Gro91] Benedict H. Gross, "Kolyvagin's work on modular elliptic curves", in: *L-functions and arithmetic (Durham, 1989)*, vol. 153, London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1991, pp. 235–256, DOI: 10.1017/CBO9780511526053.009, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1110395.

[GW10] Ulrich Görtz and Torsten Wedhorn, *Algebraic geometry I*, Advanced Lectures in Mathematics, Schemes with examples and exercises, Vieweg + Teubner, Wiesbaden, 2010, ISBN: 978-3-8348-0676-5, DOI: 10.1007/978-3-8348-9722-0, URL: https://doi.org/10.1007/978-3-8348-9722-0.

[Jan88] Uwe Jannsen, "Continuous étale cohomology", in: *Math. Ann.* 280.2 (1988), pp. 207–245, ISSN: 0025-5831, DOI: 10.1007/BF01456052, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=929536.

[Jan90] Uwe Jannsen, *Mixed motives and algebraic K-theory*, vol. 1400, Lecture Notes in Mathematics, With appendices by S. Bloch and C. Schoen, Springer-Verlag, Berlin, 1990, ISBN: 3-540-52260-3, DOI: 10.1007/BFb0085080, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1043451.

[Kin11] Guido Kings, "The equivariant Tamagawa number conjecture and the Birch-Swinnerton-Dyer conjecture", in: *Arithmetic of L-functions*, vol. 18, IAS/Park City Math. Ser. Amer. Math. Soc., Providence, RI, 2011, pp. 315–349, DOI: 10.1090/pcms/018/12, URL: https://doi.org/10.1090/pcms/018/12.

[KL89] V. A. Kolyvagin and D. Yu. Logachëv, "Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties", in: *Algebra i Analiz* 1.5 (1989), pp. 171–196, ISSN: 0234-0852, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1036843.

[Kol90] V. A. Kolyvagin, “Euler systems”, in: *The Grothendieck Festschrift, Vol. II*, vol. 87, Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 435–483, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1106906.

[Kol91] V. A. Kolyvagin, “On the structure of Shafarevich-Tate groups”, in: *Algebraic geometry (Chicago, IL, 1989)*, vol. 1479, Lecture Notes in Math. Springer, Berlin, 1991, pp. 94–121, DOI: 10.1007/BFb0086267, URL: https://doi.org/10.1007/BFb0086267.

[KS06] Masaki Kashiwara and Pierre Schapira, *Categories and sheaves*, vol. 332, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 2006, ISBN: 978-3-540-27949-5; 3-540-27949-0, DOI: 10.1007/3-540-27950-4, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=2182076.

[LV17] Matteo Longo and Stefano Vigni, “A refined Beilinson-Bloch conjecture for motives of modular forms”, in: *Trans. Amer. Math. Soc.* 369.10 (2017), pp. 7301–7342, ISSN: 0002-9947, DOI: 10.1090/tran/6947, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=3683110.

[LV19] Matteo Longo and Stefano Vigni, “Kolyvagin systems and Iwasawa theory of generalized Heegner cycles”, in: *Kyoto J. Math.* 59.3 (2019), pp. 717–746, ISSN: 2156-2261, DOI: 10.1215/21562261-2019-0005, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=3990184.

[LV21] Matteo Longo and Stefano Vigni, “On Bloch-Kato Selmer groups and Iwasawa theory of p-adic Galois representations”, in: *New York J. Math.* 27 (2021), pp. 437–467, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=4226154.

[Mas19] Daniele Masoero, “On the structure of Selmer and Shafarevich-Tate groups of even weight modular forms”, in: *Trans. Amer. Math. Soc.* 371.12 (2019), pp. 8381–8404, ISSN: 0002-9947, DOI: 10.1090/tran/7407, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=3955550.

[McC91] William G. McCallum, “Kolyvagin’s work on Shafarevich-Tate groups”, in: *L-functions and arithmetic (Durham, 1989)*, vol. 153, London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1991, pp. 295–316, DOI: 10.1017/CBO9780511526053.012, URL: https://doi.org/10.1017/CBO9780511526053.012.

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, No. 33, Princeton University Press, Princeton, N.J., 1980, ISBN: 0-691-08238-3, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=559531.

[MN19] Ahmed Matar and Jan Nekovář, “Kolyvagin’s result on the vanishing of $Ш(E/K)[p^\infty]$ and its consequences for anticyclotomic Iwasawa theory”, in: *J. Théor. Nombres Bordeaux* 31.2 (2019), pp. 455–501, ISSN: 1246-7405, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=4030918.

[MR04] Barry Mazur and Karl Rubin, “Kolyvagin systems”, in: *Mem. Amer. Math. Soc.* 168.799 (2004), ISSN: 0065-9266, DOI: 10.1090/memo/0799, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=2031496.

[Nek00] Jan Nekovář, “p-adic Abel-Jacobi maps and p-adic heights”, in: *The arithmetic and geometry of algebraic cycles (Banff, AB, 1998)*, vol. 24, CRM Proc. Lecture Notes, Amer. Math. Soc., Providence, RI, 2000, pp. 367–379, DOI: 10.1090/crmp/024/18, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1738867.

[Nek06] Jan Nekovář, “Selmer complexes”, in: *Astérisque* 310 (2006), ISSN: 0303-1179, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=2333680.

[Nek92] Jan Nekovář, “Kolyvagin’s method for Chow groups of Kuga-Sato varieties”, in: *Invent. Math.* 107.1 (1992), pp. 99–125, ISSN: 0020-9910, DOI: 10.1007/BF01231883, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1135466.

[Nek95] Jan Nekovář, “On the p-adic height of Heegner cycles”, in: *Math. Ann.* 302.4 (1995), pp. 609–686, ISSN: 0025-5831, DOI: 10.1007/BF01444511, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1343644.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, vol. 322, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder, Springer-Verlag, Berlin, 1999, ISBN: 3-540-65399-6, DOI: 10.1007/978-3-662-03983-0, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1697859.

[Niz97] Wieslawa Niziol, “On the image of p-adic regulators”, in: *Invent. Math.* 127.2 (1997), pp. 375–400, ISSN: 0020-9910, DOI: 10.1007/s002220050125, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1427624.

[NP00] Jan Nekovář and Andrew Plater, “On the parity of ranks of Selmer groups”, in: *Asian J. Math.* 4.2 (2000), pp. 437–497, ISSN: 1093-6106, DOI: 10.4310/AJM.2000.v4.n2.a11, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1797592.

[NSW00] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg, *Cohomology of number fields*, vol. 323, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 2000, ISBN: 3-540-66671-0, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1737196.

[Rib77] Kenneth A. Ribet, “Galois representations attached to eigenforms with Nebentypus”, in: *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, 1977, 17–51. Lecture Notes in Math., Vol. 601, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=0453647.

[Rib85] Kenneth A. Ribet, “On l-adic representations attached to modular forms. II”, in: *Glasgow Math. J.* 27 (1985), pp. 185–194, ISSN: 0017-0895, DOI: 10.1017/S0017089500006170, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=819838.

[Rub00] Karl Rubin, *Euler systems*, vol. 147, Annals of Mathematics Studies, Hermann Weyl Lectures. The Institute for Advanced Study, Princeton University Press, Princeton, NJ, 2000, ISBN: 0-691-05075-9; 0-691-05076-7, DOI: 10.1515/9781400865208, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1749177.

[Sch90] A. J. Scholl, “Motives for modular forms”, in: *Invent. Math.* 100.2 (1990), pp. 419–430, ISSN: 0020-9910, DOI: 10.1007/BF01231194, URL: https://doi.org/10.1007/BF01231194.

[SGA4] Michael Artin, Alexander Grothendieck and Jean-Louis Verdier, eds., *Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*, Lecture Notes in Mathematics, Vol. 269, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck, et J. L. Verdier. Avec la collaboration de N. Bourbaki, P. Deligne et B. Saint-Donat, Springer-Verlag, Berlin-New York, 1972, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=0354652.

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, vol. 151, Graduate Texts in Mathematics, Springer-Verlag, New York, 1994, ISBN: 0-387-94328-5, DOI: 10.1007/978-1-4612-0851-8, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=1312368.

[Stacks] The Stacks Project Authors, *Stacks Project*, https://stacks.math.columbia.edu, 2018.

[Tat76] John Tate, "Relations between K_2 and Galois cohomology", in: *Invent. Math.* 36 (1976), pp. 257–274, ISSN: 0020-9910, DOI: 10.1007/BF01390012, URL: https://doi.org/10.1007/BF01390012.

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, Second, vol. 83, Graduate Texts in Mathematics, Springer-Verlag, New York, 1997, ISBN: 0-387-94762-0, DOI: 10.1007/978-1-4612-1934-7, URL: https://doi.org/10.1007/978-1-4612-1934-7.

[Wil88] A. Wiles, "On ordinary λ-adic representations associated to modular forms", in: *Invent. Math.* 94.3 (1988), pp. 529–573, ISSN: 0020-9910, DOI: 10.1007/BF01394275, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=969243.

[Yan04] Tonghai Yang, "On CM abelian varieties over imaginary quadratic fields", in: *Math. Ann.* 329.1 (2004), pp. 87–117, ISSN: 0025-5831, DOI: 10.1007/s00208-004-0511-8, URL: https://mathscinet.ams.org/mathscinet-getitem?mr=2052870.

Acknowledgements

I would like to thank all those who made this thesis possible and who supported me during these three years.

Firstly, my deepest gratitude goes to my supervisor prof. Matteo Longo, who proposed to me the topic of this thesis and guided me into the vast world of Number Theory. I have to thank him in particular for having been always available to answer my annoying questions.

Thanks to all my PhD fellows, over all to Daniele who shared all the steps and efforts of my PhD. You have become to me more than a friend and a collegue. Also all the other 35th cycle PhDs of the "Ufficio 712" deserve my sincere gratitude for the warm atmosphere they created in the office, that made working an enjoyable experience.

Many thanks should also go to the whole PhDs and postdocs Number Theory group in Padova, with whom we have been running several seminars: my apologies for having caused to you sometimes some extra-work, I hope you enjoyed it.

Last but not least, I would like to thank my family for everything they have meant to me.