The Euler system of generalized Heegner cycles.

Yara Elias

Doctor of Philosophy

Department of Mathematics and Statistics

McGill University

Montreal,Quebec

May 2015

A thesis submitted to McGill University in partial fulfilment of the requirements of the degree of Doctor of Philosophy

DEDICATION

To Gorka, Greta, Jean and Rayane

ACKNOWLEDGEMENTS

I am grateful to my advisor Henri Darmon for suggesting this beautiful problem, for his guidance and patience, and for his exceptional teaching. It was a privilege to be his student. I sincerely thank him for numerous discussions of the subject of this thesis and for his valuable feedback on its development.

I am also thankful to Eyal Goren, Adrian Iovita and Matilde Lalín whose teaching was instrumental to my understanding of the subject. I am grateful to the members of the thesis defence committee Olivier Fouquet, Eyal Goren and Matilde Lalín for accepting to examine my thesis and for providing many useful corrections and suggestions.

I am grateful to Francesc Castella, Daniel Disegni and Ari Shnidman for many useful discussions of the subject of this thesis. I would also like to thank my friends and colleagues at McGill University for the time we shared together.

I would like to express my gratitude to my parents Greta and Jean and my sister Rayane whose constant support and encouragements are precious to me. I thank my partner Gorka for his unwavering faith in me and for always standing by me.

I gratefully acknowledge the financial support I received from the Fonds Québécois de la Nature et des Technologies through a doctoral scholarship and from the department of Mathematics and Statistics at McGill University.

ABSTRACT

In this thesis, we study the Selmer group of the p-adic étale realization of certain motives using Kolyvagin's method of Euler systems [34].

In Chapter 3, we use an Euler system of Heegner cycles to bound the Selmer group associated to a modular form of higher even weight twisted by a ring class character. This is an extension of Nekovář's result [39] that uses Bertolini and Darmon's refinement of Kolyvagin's ideas, as described in [3].

In Chapter 4, we construct an Euler system of generalized Heegner cycles to bound the Selmer group associated to a modular form twisted by an algebraic self -dual character of higher infinity type. The main argument is based on Kolyvagin's machinery explained by Gross [27] while the key object of the Euler system, the generalized Heegner cycles, were first considered by Bertolini, Darmon and Prasanna in [5].

RÉSUMÉ

Cette thèse est consacrée à l'étude du groupe de Selmer de la réalisation étale p-adique de certains motifs suivant la méthode de Kolyvagin basée sur les systèmes d'Euler [34].

Dans la première partie de cette thèse, nous exploitons le système d'Euler des cycles de Heegner afin de borner le groupe de Selmer associé à une forme modulaire de poids pair différent de 2 tordue par certains caractères d'un corps de classe. Il s'agit d'une extension du travail de Nekovář [39] basée sur l'article de Bertolini et Darmon [3].

Dans la deuxième partie de cette thèse, nous édifions un système d'Euler à partir de cycles de Heegner généralisés et nous l'utilisons pour borner le groupe de Selmer associé à une forme modulaire et un caractère algébrique de Hecke. L'argument principal est basé sur l'approche de Kolyvagin telle que décrite par Gross [27] tandis que l'objet principal du système d'Euler, les cycles de Heegner généralisés, ont été étudiés en premier par Bertolini, Darmon et Prasanna [5].

TABLE OF CONTENTS

CHAPTER 1
Introduction

One of the most beautiful results in algebraic number theory is the class number formula which relates local arithmetic of number fields with global arithmetic. This local-global principle is a manifestation of a general phenomenon in arithmetic. Indeed, special values of L-functions of algebraic varieties over number fields appear to be related to the global geometry of these varieties. This observation gave rise to the Birch and Swinnerton-Dyer conjecture, and more generally to the Beilinson-Bloch conjectures.

An important tool in establishing results in this area is the construction of appropriate algebraic cycles such as Heegner cycles. They are used to construct cohomology classes with convenient norm compatibilities satisfying the properties of Euler systems, crucial to the study of the geometric aspect of the algebraic varieties. Kolyvagin developed the case where the algebraic variety is an elliptic curve over $\mathbb{Q}$ and introduced a beautiful theory of Euler systems. Nekovář extended the argument to p-adic étale realizations of motives attached to classical modular forms. In my thesis, I consider first the case of a modular form twisted by a ring class character and then the case of a modular form twisted by an algebraic self-dual character of higher infinity type.

1.1 Introduction

Given an elliptic curve E and a number field K, the Mordell-Weil theorem implies that

$$E(K) \simeq \mathbb{Z}^r + E(K)_{tor},$$

where r is the algebraic rank of E and $E(K)_{tors}$ is the finite torsion subgroup of $E(K)$. This gives rise to the following questions:

- When is $E(K)$ finite, that is, when is $r = 0$?
- How do we compute r?
- Could we produce a set of generators for $E(K)/E(K)_{tors}$?

The main insight in the field is one of the seven Millennium Prize Problems listed by the Clay Mathematics Institute, Birch and Swinnerton-Dyer's conjecture that the algebraic rank of E is equal to its analytic rank, that is, the order of vanishing at $s = 1$ of the Hasse-Weil L-function $L(E/K,s)$ associated to E over K. Let

$$L^*(E/K,s) = ((2\pi)^{-s}\Gamma(s))^d N^{s/2} L(E/K,s),$$

where $d = [K : \mathbb{Q}]$, $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$ is the Γ-function and N is the conductor of E be the completed L-function associated to E/K. The Hasse-Weil conjecture stipulates that $L(E/K,s)$ has analytic continuation to the whole complex plane $\mathbb{C}$ and $L^*(E/K,s)$ satisfies a functional equation of the form

$$L^*(E/K,2-s) = w(E/K)\, L^*(E/K,s),$$

where

$$w(E/K) = \pm 1$$

is the global root number of E/K. Together with Birch and Swinnerton-Dyer's conjecture, it would imply the parity conjecture

$$(-1)^r = w(E/K).$$

The short exact sequence in Galois cohomology

$$0 \longrightarrow E(K)/pE(K) \longrightarrow \mathrm{Sel}_p(E/K) \longrightarrow Ш(E/K)_p \longrightarrow 0$$

relates the rank of $E(K)$ to the size of the so-called Selmer group $\mathrm{Sel}_p(E/K)$. The Shafarevich-Tate conjecture on the finiteness of $Ш(E/K)$, the Shafarevich group of E over K, implies that $\mathrm{Sel}_p(E/K)$ and $E(K)/pE(K)$ have the same size for all but finitely many primes p. This is the reason why the study of Selmer groups is a crucial step towards the understanding of the equality conjectured by Birch and Swinnerton-Dyer.

We describe next some of the most interesting advances in this area. Coates and Wiles [14] proved that if E has complex multiplication by the ring of integers of an imaginary quadratic field K of class number 1 and if it is defined over $F = K$ or $F = \mathbb{Q}$, then

$$r(E/F) \geq 1 \implies r_{an}(E/F) \geq 1.$$

Kolyvagin [34, 27] uses an Euler system to bound the size of the Selmer group of certain elliptic curves over imaginary quadratic fields assuming the non-vanishing of a suitable Heegner point. This implies that they have algebraic rank 1, and that their associated Tate-Shafarevich group is finite. Combined with results of Gross and Zagier [28], this proves the Birch and Swinnerton-Dyer conjecture for analytic rank 1. Using results of Kumar and Ram Murty [38], it can be shown that the Birch and Swinnerton-Dyer conjecture holds for analytic rank less than or equal to 1. Bertolini and Darmon adapt Kolyvagin's descent to Mordell-Weil groups over ring class fields [3]. We denote by r_p the corank of the Selmer group

$$r_p = \mathrm{rank}(\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K), \mathbb{Q}/\mathbb{Z})).$$

In [41], Nekovář proves that if E is an elliptic curve over $\mathbb{Q}$ with good ordinary reduction at p, then

$$w(E/\mathbb{Q}) = (-1)^{r_p(E/\mathbb{Q})}.$$

Tim and Vladimir Dokchister [20] show that if E/K has a rational isogeny of prime degree $p \geq 3$, and E is semistable at all primes over p, then

$$w(E/K) = (-1)^{r_p(E/K)}.$$

Skinner and Urban [51] prove that for a large class of elliptic curves,

$$r_p = 0 \Rightarrow \mathrm{ord}_{s=1} L(E,s) = 0.$$

Skinner [50] shows that if E is a semistable elliptic curve over $\mathbb{Q}$ that has non-split multiplicative reduction at at least one odd prime or split multiplicative reduction at at least two odd primes then

$$\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 1 \text{ and } |\text{Ш}(E)| \text{ is finite } \Rightarrow \ \mathrm{ord}_{s=1} L(E,s) = 1.$$

He also proves the corresponding result for the abelian variety associated with a weight two newform of trivial character. Wei Zhang [56] proves that for a large class of elliptic curves over $\mathbb{Q}$,

$$r_p = 1 \Rightarrow \mathrm{ord}_{s=1} L(E,s) = 1.$$

No assumptions are made about the primes for which E has additive reduction. However, the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ representation of $E[p]$, the p-torsion points of E, is required to ramify for certain primes of multiplicative reduction. Bhargava and Shankar [6] show that the average size of the 5-Selmer group of elliptic curves over $\mathbb{Q}$ is equal to 6. Combining this with a new lower bound on the equidistribution of root numbers of elliptic curves, they deduce that the average rank of elliptic curves over $\mathbb{Q}$ when ordered by height is less than 1 and at least four fifths of all elliptic curves over $\mathbb{Q}$ have rank either 0 or 1. Furthermore, at least one fifth of all elliptic curves in fact have rank 0. Bhargava, Skinner and Wei Zhang prove in [7] that

$$\lim_{x\to\infty} \frac{|\{E/\mathbb{Q} \mid r(E) = \mathrm{ord}_{s=1}L(E,s),\ \text{Ш}(E) \text{ finite },\ H(E) < X\}|}{|\{E/\mathbb{Q} \mid H(E) < X\}|} > 66.48\%,$$

where $H(E)$ is the height of the elliptic curve E. In other words, a majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch-Swinnerton-Dyer conjecture and have finite Shafarevich group over $\mathbb{Q}$.

More generally, one can associate to a modular form f of even weight $2r$ and level $\Gamma_0(N)$ a p-adic Galois representation A [32, 46]. For a given number field K, there is a p-adic Abel-Jacobi map

$$\Phi : \mathrm{CH}^r(X/K)_0 \longrightarrow H^1(K,A),$$

where

- X represents the Kuga-Sato varieties of dimension $2r-1$, that is, a compact desingularization of the $2r-2$-fold fibre product of the universal generalized elliptic curve over the modular curve $X_1(N)$,
- $\mathrm{CH}^r(X/K)_0$ is the r-th Chow group of X over K, that is the group of homologically trivial cycles on X of codimension r modulo rational equivalence,
- $H^1(K,A)$ stands for the first Galois cohomology group of $\mathrm{Gal}(\overline{K}/K)$ acting on A.

The Beilinson-Bloch conjecture, which generalizes Birch and Swinnerton-Dyer's, predicts that

$$\dim_{\mathbb{Q}_p}(\mathrm{Im}(\Phi)\otimes\mathbb{Q}_p) = \mathrm{ord}_{s=r}L(f\otimes K,s). \tag{1.1}$$

This motivates the study of the Selmer group $\mathrm{Sel}_p(A/K)$ of A over K as $\mathrm{Im}(\Phi)$ closely relates to it.

In [39], Nekovář shows that

$$\dim_{\mathbb{Q}_p}(\mathrm{Im}(\Phi)\otimes\mathbb{Q}_p) = 1 \tag{1.2}$$

assuming that a suitable cycle of $H^1(K,A)$ is non-torsion. Combined with results of Gross-Zagier and Brylinski [11, 28] and results of Bump, Friedberg and Hoffstein [12], this provides further grounds to believe the Beilinson-Bloch conjecture for analytic rank less than or equal to 1.

We extend Nekovář's work described in 1.2 to more general settings. Firstly, we adapt ideas and techniques from [3] and [39] to provide a bound on the size of the Selmer group associated to a modular form of even weight strictly larger than 2 *twisted by a ring class character.* Secondly, we exploit the construction of so-called *generalized Heegner cycles* by Bertolini, Darmon and Prasanna [5] to construct an Euler system attached to a modular form *twisted by an algebraic self-dual character of higher infinity type.* Following Nekovář [39], we subsequently use the tools introduced by Kolyvagin to bound the size of the associated Selmer group.

1.2 First contribution

Let f be a normalized newform of level $\Gamma_0(N)$ where $N \geq 5$, of trivial nebentype and even weight $2r > 2$ and let

$$K = \mathbb{Q}(\sqrt{-D})$$

be an imaginary quadratic field satisfying the *Heegner hypothesis* relative to N, that is, rational primes dividing N split in K. For simplicity, we assume that $|\mathscr{O}_K^\times| = 2$. We fix a prime p not dividing $ND\phi(N)$. Let H be the ring class field of K of conductor c with $(c, NDp) = 1$ and let e be the exponent of $\mathrm{Gal}(H/K)$. Let

$$F = \mathbb{Q}(a_1, a_2, \cdots, \mu_e)$$

be the field generated over $\mathbb{Q}$ by the coefficients of f and the e-th roots of unity μ_e and let $\mathscr{O}_F$ be its ring of integers. We denote by A the p-adic étale realization of the motive associated to f by Scholl [46] and Deligne [18] twisted by r. It will be viewed (by extending scalars appropriately) as a free $\mathscr{O}_F \otimes \mathbb{Z}_p$ module of rank 2, equipped with a continuous $\mathscr{O}_F$-linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $A_\wp$ be the localization of A at a prime $\wp$ of $\mathscr{O}_F$ dividing p. Then $A_\wp$ is a free module of rank 2 over $\mathscr{O}_\wp$, the completion of $\mathscr{O}_F$ at $\wp$. For a p-torsion $\mathrm{Gal}(\overline{H}/H)$ module M, the Selmer group

$$S \subseteq H^1(H, M)$$

consists of the cohomology classes c whose localizations c_v at a prime v of H lie in

$$\begin{cases} H^1(H_v^{ur}/H_v, M) \text{ for } v \text{ not dividing } Np \\ H^1_f(H_v, M) \text{ for } v \text{ dividing } p \end{cases}$$

where $H^1_f(H_v,M)$ is the *finite part* of $H^1(H_v,M)$ as in [9]. In our setting, since $A_\wp$ has good reduction at p, $H^1_f(H_v,M) = H^1_{cris}(H_v,M)$. Note that the assumptions we make will ensure that $H^1(H_v^{ur}/H_v, A_\wp/p) = 0$ for v dividing N. The Galois group

$$G = \mathrm{Gal}(H/K)$$

acts on $H^1(H,M)$ hence it acts on S. Assume that p does not divide $|G|$. We denote by $\hat{G} = \mathrm{Hom}(G,\mu_e)$ the group of characters of G and by

$$e_\chi = \frac{1}{|G|}\sum_{g\in G}\chi^{-1}(g)g$$

the projector onto the χ-eigenspace given a character χ of $\hat{G}$. By the Heegner hypothesis, there is an ideal $\mathscr{N}$ of $\mathscr{O}_c$, the order of K of conductor c, such that

$$\mathscr{O}_c/\mathscr{N} = \mathbb{Z}/N\mathbb{Z}.$$

Therefore, $\mathbb{C}/\mathscr{O}_c$ and $\mathbb{C}/\mathscr{N}^{-1}$ define elliptic curves related by an N-isogeny. As points of $X_0(N)$ correspond to elliptic curves related by N-isogenies, this provides a *Heegner point* x_1 of $X_0(N)$. By the theory of complex multiplication, x_1 is defined over H. Let E be the corresponding elliptic curve. Then E has complex multiplication by $\mathscr{O}_c$. The Heegner cycle of conductor c is defined as

$$e_r(\mathrm{graph}(\sqrt{-D}))^{r-1}$$

for some appropriate projector e_r, (see Section 3.2 for more details). Let y_1 be its image by the p-adic étale Abel-Jacobi map in $H^1(H,A_\wp/p)$. We denote by $Fr(v)$ the arithmetic

Frobenius element generating $\mathrm{Gal}(H_v^{ur}/H_v)$, and by $I_v = \mathrm{Gal}(\overline{H_v}/H_v^{ur})$. In Chapter 3 which is submitted for publication, we prove the following statement.

Theorem 1.2.1. *Assume that p is such that*

$$\mathrm{Gal}\left(\mathbb{Q}(A_{\wp}/p)/\mathbb{Q}\right) \simeq \mathrm{GL}_2(\mathscr{O}_{\wp}/p), \quad (p, ND\phi(N)) = 1, \text{ and } p \nmid |G|.$$

Suppose further that the eigenvalues of $Fr(v)$ acting on $A_{\wp}^{I_v}$ are not equal to 1 modulo p for v dividing N. Let $\chi \in \hat{G}$ be such that

$$e_{\overline{\chi}} y_1 \neq 0.$$

Then the χ-eigenspace S^{χ} of the Selmer group S has rank 1 over $\mathscr{O}_{\wp}/p$.

1.3 Second contribution

Kolyvagin and Nekovář respectively use Heegner points and Heegner cycles to define a pertinent Euler system which is subsequently exploited to obtain a bound on the size of an associated Selmer group. Bertolini, Darmon and Prasanna constructed generalized Heegner cycles in the product of a Kuga-Sato variety with a power of a CM elliptic curve [5]. In Chapter 4, we adapt Nekovář's work to the setting where Heegner cycles are replaced by generalized Heegner cycles. This determines the left-hand side of the equality (1.1) conjectured by Beilinson and Bloch for the étale realization of a motive attached to a modular form twisted by an algebraic self -dual character of higher infinity type, when the relevant generalized Heegner cycle has non-trivial image by the p-adic Abel-Jacobi map.

Let f be a normalized newform of level $\Gamma_0(N)$ and trivial nebentype where $N \geq 5$ and of even weight $r+2 > 2$. Denote by $K = \mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field with odd discriminant satisfying the Heegner hypothesis, that is primes dividing N split in K. For simplicity, we assume that $|\mathscr{O}_K^\times| = 2$. Let

$$\psi : \mathbb{A}_K^\times \longrightarrow \mathbb{C}^\times$$

be an unramified algebraic Hecke character of K of infinity type $(r, 0)$. Then there is an elliptic curve A defined over the Hilbert class field K_1 of K with complex multiplication by $\mathscr{O}_K$ such that ψ is the Hecke character associated to A [25, Theorem 9.1.3]. Furthermore, A is a $\mathbb{Q}$-curve by the assumption on the parity of D, that is A is K_1- isogenous to its conjugates in $\mathrm{Aut}(K_1)$. (See [25, Section 11]). Consider a prime p not dividing $ND\phi(N)N_A$, where N_A is the conductor of A. We denote by V_f the f-isotypic part of the p-adic étale realization of the motive associated to f by Scholl [46] and Deligne [18] twisted by $\frac{r+2}{2}$ and by V_ψ the p-adic étale realization of the motive associated to ψ twisted by $\frac{r}{2}$. More precisely, V_ψ is the ψ-isotypic component of

$$\mathrm{res}_{K_1/\mathbb{Q}}(A) = \prod_{\sigma \in \mathrm{Gal}(K_1/\mathbb{Q})} A^\sigma$$

where A^σ is the σ-conjugate of A, (see Section 4.2 for more details). Let $\mathscr{O}_F$ be the ring of integers of

$$F = \mathbb{Q}(a_1, a_2, \cdots, b_1, b_2, \cdots),$$

where the a_i's are the coefficients of f and the b_i's are the coefficients of the theta series

$$\theta_\psi = \sum_{a \subset \mathscr{O}_K} \psi(a) q^{N(a)}$$

associated to ψ. Then V_f and V_ψ will be viewed (by extending scalars appropriately) as free $\mathscr{O}_F \otimes \mathbb{Z}_p$-modules of rank 2. We denote by

$$V = V_f \otimes_{\mathscr{O}_F \otimes \mathbb{Z}_p} V_\psi$$

the p-adic étale realization of the twisted motive associated to f and ψ and let $V_\wp$ be its localization at a prime $\wp$ in F dividing p. Then $V_\wp$ is a four dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in

$$\mathrm{End}(A/\mathbb{Q}) = \oplus_{\sigma \in \mathrm{Gal}(H/\mathbb{Q})} \mathrm{Hom}(A, A^\sigma).$$

We also denote by $\mathscr{O}_{F,\wp}$ the localization of $\mathscr{O}_F$ at $\wp$. By the Heegner hypothesis, there is an ideal $\mathscr{N}$ of $\mathscr{O}_K$ satisfying

$$\mathscr{O}_K/\mathscr{N} = \mathbb{Z}/N\mathbb{Z}.$$

We can therefore fix level $\Gamma_1(N)$ structure on A, that is a point of exact order N defined over the ray class field L_1 of K of conductor $\mathscr{N}$. Consider a pair (φ_1, A_1) where A_1 is an elliptic curve defined over K_1 with level $\Gamma_1(N)$ structure and

$$\varphi_1 : A \longrightarrow A_1$$

is an isogeny over $\overline{K}$. We associate to it a codimension $r+1$ cycle on V

$$\Upsilon_{\varphi_1} = Graph(\varphi_1)^r \subset (A \times A_1)^r \simeq (A_1)^r \times A^r \subset W_r \times A^r$$

and define a *generalized Heegner cycle* of conductor 1

$$\Delta_{\varphi_1} = e_r \Upsilon_{\varphi_1},$$

where e_r is an appropriate projector (4.1). Then Δ_{φ_1} is defined over L_1. The Selmer group

$$S \subseteq H^1(K, V_\wp/p)$$

consists of the cohomology classes which localizations at a prime v of L_1 lie in

$$\begin{cases} H^1(K_v^{ur}/K_v, V_\wp/p) \text{ for } v \text{ not dividing } NN_Ap \\ H^1_f(K_v, V_\wp/p) \text{ for } v \text{ dividing } p \end{cases}$$

where K_v is the completion of K at v, and

$$H^1_f(K_v, V_\wp/p) = H^1_{cris}(K_v, V_\wp/p)$$

is the *finite part* of $H^1(K_v, V_\wp/p)$ [9]. Note that the assumptions we make will ensure that $H^1(K_v^{ur}/K_v, V_\wp/p) = 0$ for v dividing NN_A. We denote by $Fr(v)$ the arithmetic Frobenius element generating $\mathrm{Gal}(K_v^{ur}/K_v)$, and by $I_v = \mathrm{Gal}(\overline{K_v}/K_v^{ur})$. In Chapter 4 which is submitted for publication, we prove the following statement.

Theorem 1.3.1. *Let p be such that*

$$\mathrm{Gal}\left(K(V_\wp/p)/K\right) \simeq \mathrm{Aut}_K(V_\wp/p), \ \ \textit{and} \ \ (p, ND\phi(N)N_A) = 1.$$

Suppose that $V_\wp/p$ is a simple $\mathrm{Aut}(V_\wp/p)$-module. Suppose further that the eigenvalues of $Fr(v)$ acting on $V_\wp^{I_v}$ are not equal to 1 modulo p for v dividing NN_A. Assume the corestriction $\mathrm{cor}_{L_1,K}\Phi(\Delta_{\varphi_1}) \neq 0$ where

$$\Phi(\Delta_{\varphi_1}) \in H^1(K, V_\wp/p)$$

is the image by the p-adic Abel-Jacobi map of the generalized Heegner cycle Δ_{φ_1}. Then the Selmer group S has rank 1 over $\mathscr{O}_{F,\wp}/p$.

One could consider other flavours of Selmer groups. Instead of studying the Selmer group with coefficients in $V_{\wp}/p$, one could look at the Selmer group with coefficients in the p-torsion submodule $V[p]$ of V. The duality between these two types of Selmer groups allows us to deduce information about the latter from the study of the former.

CHAPTER 2
Preliminaries

In this chapter, we explain some of the key concepts used in Kolyvagin's method of Euler systems adapted to modular forms of higher even weight. We invite the reader to consult these sections as they are referenced in Chapters 3 and 4.

2.1 Abel-Jacobi map

The Kolyvagin cohomology classes we construct are derived from the image by the p-adic Abel-Jacobi map of (possibly generalized) Heegner cycles. We follow [1] and [5] in the description of the Abel-Jacobi map. Consider a smooth projective variety X of dimension d over a field K of characteristic 0. An irreducible cycle Z of codimension c is a closed irreducible subvariety of codimension c. We denote by $Z^c(X)$ the abelian group generated by codimension c cycles. Two cycles α, β are *rationally equivalent* if there is $U \subseteq \mathbb{P}^1$ and γ in $Z^c(X \times U)$ such that for all $u \in U$, we have

$$\gamma_u = \gamma \cap Z^c(X \times u) \text{ and there is } u_0 \neq u_1 \in U \text{ with } \gamma_{u_0} = \alpha \text{ and } \gamma_{u_1} = \beta.$$

The cycle class map

$$cl : Z^c(X/K) \longrightarrow H^{2c}_{et}(X \otimes \overline{K}, \mathbb{Z}_p(c))$$

factors through rational equivalence. Therefore, it induces a map

$$cl : CH^c(X/K) \longrightarrow H^{2c}_{et}(X \otimes \overline{K}, \mathbb{Z}_p(c))$$

on the c-th Chow group $CH^c(X)$ consisting of $Z^c(X)$ modulo rational equivalence. Two cycles α, β are *homologically equivalent* if $cl(\alpha) = cl(\beta)$. We denote by $CH^c(X)_0$ the group of homologically trivial cycles. Let $i : Z \hookrightarrow X$ be a closed immersion and $j : U \hookrightarrow X$ an open immersion such that X is the disjoint union of $i(Z)$ and $j(U)$. Let $\mathscr{F}$ be an étale sheaf on the étale site of X and let $i^!$ be the right adjoint of i_*. The group of sections of $\mathscr{F}$ with support on Z is

$$\Gamma(X, i_* i^! \mathscr{F}) = \Gamma(Z, i^! \mathscr{F}) = \ker(\mathscr{F}(X) \longrightarrow \mathscr{F}(U)).$$

The étale cohomology groups of $\mathscr{F}$ with support on Z are

$$H^k_{|Z|}(X, \mathscr{F}) : \mathscr{F} \longrightarrow R^k\Gamma(Z, i^! \mathscr{F}).$$

Assume that Z is smooth over K. For $0 \leq k \leq 2c-2$, we have

$$H^k_{et}(X, \mathscr{F}) \simeq H^k_{et}(U, \mathscr{F}).$$

The long exact excision sequence in étale cohomology gives rise to an exact sequence

$$\begin{aligned} 0 \to H^{2c-1}_{et}(X, \mathscr{F}) \to H^{2c-1}_{et}(U, \mathscr{F}) \to H^{2c}_{|Z|}(X, \mathscr{F}) \xrightarrow{i^*} H^{2c}_{et}(X, \mathscr{F}) \cdots \\ \to H^{2d}_{|Z|}(X, \mathscr{F}) \to H^{2d}_{et}(X, \mathscr{F}) \to H^{2d}_{et}(U, \mathscr{F}) \to 0, \end{aligned}$$

where

$$H^k_{|Z|}(X, \mathscr{F}) \simeq H^{k-2c}_{et}(Z, i^* \mathscr{F}(-c)).$$

Taking $\mathscr{F} = \mathbb{Z}_p(c)$, the Gysin map i^* induces by restriction to rational cycles the cycle class map

$$cl : \ CH^c(X) \longrightarrow H^{2c}_{et}(\overline{X}, \mathbb{Z}_p(c))^{G_K}$$

where $\overline{X} = X \otimes \overline{K}$. For $Z \in CH^c(X)_0$, consider the diagram

$$\begin{array}{ccccccccc}
0 \longrightarrow & H^{2c-1}_{et}(\overline{X}, \mathbb{Z}_p(c)) & \longrightarrow & H^{2c-1}_{et}(\overline{X} - \overline{Z}, \mathbb{Z}_p(c)) & \longrightarrow & H^{2c}_{|Z|}(\overline{X}, \mathbb{Z}_p(c))_0 & \longrightarrow 0 \\
& \downarrow & & \uparrow & & \uparrow & \\
0 \longrightarrow & H^{2c-1}_{et}(\overline{X}, \mathbb{Z}_p(c)) & \longrightarrow & E_Z & \longrightarrow & \mathbb{Z}_p & \longrightarrow 0
\end{array}$$

where

$$H^{2c}_{|Z|}(\overline{X}, \mathbb{Z}_p(c))_0 \; = \; \ker(\; H^{2c}_{|Z|}(\overline{X}, \mathbb{Z}_p(c)) \; \longrightarrow \; H^{2c}_{et}(\overline{X}, \mathbb{Z}_p(c)) \;)$$

is the kernel of the Gysin map and

$$\mathbb{Z}_p \longrightarrow H^{2c}_{|Z|}(\overline{X}, \mathbb{Z}_p(c))_0 : 1 \mapsto \overline{Z}.$$

Here, E_Z is identified with a subquotient of

$$\{e \in H^{2c-1}_{et}(\overline{X} - \overline{Z}, \mathbb{Z}_p(c)) \;\mid\; \mathrm{Im}(e) \in H^{2c}_{|Z|}(\overline{X}, \mathbb{Z}_p(c))_0 \cap \mathrm{Im}(\mathbb{Z}_p)\}.$$

The p-adic Abel-Jacobi map is the map

$$AJ^{et}_p : CH^c_0(X) \longrightarrow \; Ext^1(\mathbb{Z}_p, H^{2c-1}_{et}(\overline{X}, \mathbb{Z}_p(c))) = H^1(K, H^{2c-1}_{et}(\overline{X}, \mathbb{Z}_p(c)))$$

which associates to $Z \in CH^c(X)_0$ the isomorphism class of E_Z in the group of extensions of $\mathbb{Z}_p$ by $H^{2c-1}_{et}(\overline{X}, \mathbb{Z}_p(c))$ in the category of p-adic representations of $\mathrm{Gal}(\overline{K}/K)$.

2.2 Frobenius substitution

The choice of the primes determining the Kolyvagin cohomology classes which are central to the proof relies on the theory of *Frobenius substitution* which we summarize in this section. Let L be a finite Galois extension of F. Consider a prime q of L lying above an unramified prime p of F. There is an element

$$\sigma = (q, L/F) \in \mathrm{Gal}(L/F)$$

uniquely determined by the condition that

$$\sigma(\alpha) \equiv \alpha^{N(p)} \mod q \text{ for all } \alpha \in \mathscr{O}_L,$$

where $N(p) = |\mathscr{O}_F/p|$. If q_i is another prime of L lying above p then $(q_i, L/F)$ is conjugate to $(q, L/F)$. In particular, if L/F is an abelian extension then the set $\{(q, L/F),\ q \mid p\}$ consists of a single element

$$\mathrm{Frob}_p(L/F) = (p, L/F) = (q_i, L/F),$$

the Frobenius substitution of p. When p is a real infinite place, $(p, L/F)$ is the complex conjugation τ. When p is a complex infinite place, $(p, L/F)$ is the identity. *Cebotarev's density theorem* which plays a crucial role in the proof of Theorem 1.2.1 and Theorem 1.3.1 is a statement about the occurence of a conjugacy class $[\sigma]$ of an element $\sigma \in \mathrm{Gal}(L/F)$ as a Frobenius substitution. Cebotarev proved that the set of unramified prime ideals p of F such that $(p, L/F) \in [\sigma]$ has Dirichlet density

$$\frac{|\,[\sigma]\,|}{[L:F]} = \frac{|\,[\sigma]\,|}{|\mathrm{Gal}(L/F)|}. \tag{2.1}$$

and is hence infinite. In particular, if L/F is abelian, then the set of unramified primes such that $\mathrm{Frob}_p(L/F)$ belongs to $[\sigma]$ has density $1/[L:F]$.

We discuss the *transfer* of an element from a group to a subgroup following Serre's development [48]. This will be applied to move the Frobenius substitution of an unramified prime from a Galois group to a Galois subgroup. Let G be a group, H a subgroup of finite index and $X = G/H$ the set of left cosets of X. For $x \in X$, we denote by $\bar{x}$ a representative of x in G. Assume $s \in G$ and $x \in X$, then $s\bar{x} \in G$ has image sx in X. Therefore, if $\overline{sx}$ is a representative of sx in X, then there exists $h_{s,x} \in H$ such that

$$s\bar{x} = \overline{sx}\, h_{s,x}.$$

Consider the map

$$\text{Ver} \;:\; G \longrightarrow H^{ab} \;:\; s \mapsto \prod_{x \in X} h_{s,x} \mod [H,H],$$

where the product is computed in $H^{ab} = H/[H,H]$. This is a group homomorphism that does not depend on the choice of representatives $\{\bar{x}\}_{x \in X}$. Let C be the cyclic subgroup of G generated by s. We denote by $\mathscr{O}_\alpha$ the orbits of X under the action of C and by f_α the cardinality of $\mathscr{O}_\alpha$. If x_α belongs to $\mathscr{O}_\alpha$, then $s^{f_\alpha} x_\alpha = x_\alpha$. This implies that given a representative g_α of x_α in G, there exists h_α in H such that

$$s^{f_\alpha} g_\alpha = g_\alpha h_\alpha.$$

Therefore, it is enough to show that

$$Ver(s) = \prod_\alpha h_\alpha = \prod_\alpha g_\alpha^{-1}\, s^{f_\alpha}\, g_\alpha \mod [H,H]$$

to conclude that the homomorphism $G^{ab} \longrightarrow H^{ab} \longrightarrow G^{ab}$ maps s to s^n. Indeed,

$$g_\alpha^{-1} s^{f_\alpha} g_\alpha = s^{f_\alpha} \mod [G,G], \quad \text{and} \quad s^{\sum_\alpha f_\alpha} = s^n.$$

In particular, if G is abelian, we obtain a homomorphism

$$Ver\ :\ G \longrightarrow H\ :\ s \mapsto s^n.$$

2.3 Local class field theory

In this section, we develop certain aspects of local class field theory that are relevant to the definition and understanding of (generalized) Heegner cycles following Cox [16] and Gala [23]. A modulus m in a number field F is a formal product

$$m = \prod_p p^{m_p}$$

running over the places p of F where

$$\begin{cases} m_p \geq 0 \text{ is non-zero for finitely many places } p \\ m_p = 0 \text{ or } 1 \text{ for infinite real places} \\ m_p = 0 \text{ for infinite complex places} \end{cases}$$

Writing m as $m = m_0 m_\infty$, the product over finite and infinite places of F respectively, we denote

$$P_{F,1}(m) = \{a \in F^* \mid v_p(a-1) \geq m_p \text{ for all } p \mid m_0 \text{ and } p(a) > 0 \text{ for all } p \mid m_\infty\}.$$

Let $I_F(m)$ be the set of fractional ideals of F generated by the prime ideals which do not divide m. The *ray class group* of F modulo m is

$$C_m = I_F(m)/P_{F,1}(m).$$

Assume E/F is a finite abelian extension and m is a modulus of F divisible by the primes of F that ramify in E. Then the *Artin map* is the surjective homomorphism

$$\psi :\ I_F(m) \longrightarrow \mathrm{Gal}(E/F)\ :\ \prod_{p_i} p_i^{m_i} \mapsto \prod_{p_i} (p_i, E/F)^{m_i}.$$

A prime ideal of F splits completely in E if and only if it is in the kernel of the Artin map. Consider the norm map

$$N_{E/F} :\ I_E \longrightarrow I_F\ :\ \ q \mapsto p^{f(q/p)},$$

where p is the prime of F lying below the prime q of E and $f(q/p) = [F_q : F_p]$ is the residue degree. We have

$$N_{E/F}(I_E) \subseteq ker(\psi).$$

Indeed, it is enough to see that

$$\psi(p^{f(q/p)}) = (p, E/F)^{f(q/p)} = 1.$$

Artin's reciprocity law further states that there is a modulus m of F which satisfies the following properties:

1. m is divisible by the primes of F that ramify in E
2. $P_{F,1}(m) \subseteq \ker(\psi)$
3. $\ker(\psi) = P_{F,1}(m)\, N_{E/F}(I_E(m'))$, where m' is divisible by the primes of E lying above primes of m

The minimal such modulus m is called the *conductor* of the extension. A subgroup H of $I_F(m)$ is called a *congruence subgroup modulo* m if

$$P_{F,1}(m) \subset H \subset I_F(m).$$

There is a unique abelian extension E of F such that the primes of F ramified in E divide m and such that

$$H = P_{F,1}(m)\, N_{E/F}(I_E(m')),$$

where m' is divisible by the primes of E lying above primes of m. The Artin map induces an isomorphism

$$\psi:\ I_F(m)/H \longrightarrow \mathrm{Gal}(E/F).$$

In the case where m is the trivial modulus 1, the congruence subgroup $H = P_{F,1}(1)$ gives rise to the *Hilbert class field* F_1 of F, the maximal abelian unramified extension of F. In the case where m is a product of finite places, we consider the order

$$\mathscr{O}_m = \mathbb{Z} + m\mathscr{O}_K$$

of conductor m in an imaginary quadratic field $F = K$ with $\mathscr{O}_K^\times = \{\pm 1\}$. Let $\mathrm{Pic}(\mathscr{O}_m)$ be the Picard group of $\mathscr{O}_m$. Then

$$\mathrm{Pic}(\mathscr{O}_m) \simeq Cl(\mathscr{O}_m) \simeq I_K(m\mathscr{O}_K)/P_{K,\mathbb{Z}}(m\mathscr{O}_K),$$

where

$$P_{K,\mathbb{Z}}(m\mathscr{O}_K) = \{\alpha \in \mathscr{O}_K \mid \alpha \equiv a \mod m\mathscr{O}_K,\ a \in \mathbb{Z},\ (a,m) = 1\}.$$

Since $P_{K,\mathbb{Z}}(m)$ is a congruence subgroup modulo m, there is an extension K_m of K, the *ring class field* of K of conductor m, such that

$$\mathrm{Pic}(\mathscr{O}_m) \simeq \mathrm{Gal}(K_m/K).$$

The Galois group $\mathrm{Gal}(K_m/K_1)$ is the subgroup of $\mathrm{Gal}(K_m/K)$ acting trivially on K_1. Therefore, we have

$$\mathrm{Gal}(K_m/K_1) \simeq \frac{I_K(m\mathscr{O}_K) \cap P_K(\mathscr{O}_K)}{P_{K,\mathbb{Z}}(m\mathscr{O}_K)} \simeq \frac{(\mathscr{O}_K/m)^*}{(\mathbb{Z}/m)^*}.$$

This provides a formula for the ratio of the class numbers of a ring and a suborder. The complex conjugation τ which generates $\mathrm{Gal}(K/\mathbb{Q})$ acts on an element σ of $\mathrm{Gal}(K_m/K)$ by $\tau\sigma\tau^{-1} = \sigma^{-1}$ and we have

$$\mathrm{Gal}(K_m/\mathbb{Q}) \simeq \mathrm{Gal}(K_m/K) \rtimes \mathrm{Gal}(K/\mathbb{Q}).$$

2.4 Brauer group and local reciprocity

The local reciprocity law is the principal tool used to transform global information about the elements of the Selmer group into local information. We describe this law and the Brauer group with Serre's book [47] as a reference. The *Brauer group* of a field k is the direct limit

$$B_k = \varinjlim_{K} H^2(K/k, K^*)$$

as K runs through the set of finite Galois extensions of k. For an algebraic number field k, let k_v be the completion of k with respect to the place v of k. Then

$$\begin{cases} B_{k_v} = \mathbb{Q}/\mathbb{Z} \text{ for finite primes } v \text{ of } k, \\ B_{k_v} = \{0, 1/2\} \ \text{ if } \ k_v = \mathbb{R}, \\ B_{k_v} = 0 \ \text{ if } \ k_v = \mathbb{C}. \end{cases}$$

The embedding $k \hookrightarrow k_v$ induces a map

$$B_k \longrightarrow \prod_v B_{k_v}$$

that is injective by the Hasse principle. In fact B_k embeds into $\oplus_v B_{k_v}$. Combining [47, Theorem XII.3.2] and the corollary of [47, Proposition XIII.1.1], we obtain an exact sequence

$$0 \to B_k \to \oplus_v B_{k_v} \xrightarrow{\sigma} \mathbb{Q}/\mathbb{Z} \longrightarrow 0,$$

where $\sigma(\oplus_v x_v) = \sum_v x_v$. If k_v is a field complete under a discrete valuation with finite residue field then we have an isomorphism

$$inv_{k_v} : \ B_{k_v} \simeq \mathbb{Q}/\mathbb{Z}.$$

(See [47, Proposition XIII.3.6]).

Let L be a finite extension of K of degree n for a field K that is complete with respect to a discrete valuation v with quasi-finite residue field $\overline{K}$ (see [47, Paragraph XIII.2] for the definition of a quasi-finite field). Let

$$\mathrm{res}_{K,L} : B_K \longrightarrow B_L$$

be the canonical homomorphism of B_K into B_L. Then

$$inv_L \circ \mathrm{res}_{K,L} = n \cdot inv_K.$$

Suppose L/K is Galois with Galois group G. Then the isomorphism inv_K maps the subgroup $H^2(L/K, L^*)$ of B_K onto the subgroup $\mathbb{Z}/n\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$ by [47, Corollary XIII.3.2]. Assume K contains the group μ_n of n-th roots of unity. We choose a primitive n-th root of unity ω identifying μ_n with the group $\mathbb{Z}/n\mathbb{Z}$. The exact sequence

$$0 \to \mu_n \to \overline{K}^* \xrightarrow{v} \overline{K}^* \longrightarrow 0,$$

where $v(x) = x^n$ induces the exact sequence

$$0 \to H^2(G, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{i} B_K \to B_K$$

since $H^1(G, K^*) = 0$. Given elements a, b of K^* we can associate elements ϕ_a, ϕ_b of $H^1(G, \mathbb{Z}/n\mathbb{Z})$. The cup product then yields an element $\phi_a\phi_b$ of $H^2(G, \mathbb{Z}/n\mathbb{Z})$. We let

$$(a, b) = i(\phi_a\phi_b).$$

We define

$$(a, b)_v = \omega^{n \cdot inv_K(a,b)},$$

an n-th root of unity which does not depend on the choice of ω by the corollary to [47, Proposition XIV.2.6]. Assume $L = K\left(a^{\frac{1}{n}}\right)$, and $b \in K^*$. Artin's reciprocity law implies that $\psi(b) = 1$, (see Section 2.3). One can then deduce that

$$\prod_v (a, b)_v = 1$$

by relating the elements $(a,b)_v$ to the Frobenius substitution at the primes dividing b by the formula

$$(a,b)_v = (b,*/K)(a^{\frac{1}{n}})/a^{\frac{1}{n}}$$

where $(b,*/K)$ is an appropriate limit of $(b,F/K)$ over increasing extensions F of K, (see [47, Proposition XI.3] for the precise definition).

2.5 Local Tate duality

Local Tate duality is one of the main ingredients of the proof of Theorems 1.2.1 and 1.3.1. We succinctly explain the main ideas following Nekovář [39] and Tate [53]. Let K_λ be a local field with residue field F_q and let A be a finite group with an unramified action of $\mathrm{Gal}(\overline{K_\lambda}/K_\lambda)$ killed by a prime p. Assume p divides $q-1$ so that $\mu_p \subset K_\lambda$ and let $A' = \mathrm{Hom}(A,\mu_p)$. We denote by K_λ^{ur}, the maximal unramified extension of K_λ, by K_λ^t, the maximal tamely ramified extension of K_λ, and by $H^1_{ur}(K_\lambda,*)$, the group $H^1(K_\lambda^{ur}/K_\lambda,*)$. The natural pairing $A \times A' \longrightarrow \mu_p$ yields the cup product pairing

$$H^1(K_\lambda,A) \times H^1(K_\lambda,A') \longrightarrow H^2(K_\lambda,\mu_p) = \mathbb{Z}/p\mathbb{Z}$$

which induces a perfect local Tate pairing

$$H^1(K_\lambda^{ur}/K_\lambda,A) \times H^1(K_\lambda,A')/H^1(K_\lambda^{ur}/K_\lambda,A) \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Let

$$\alpha : H^1(K_\lambda^{ur}/K_\lambda,A) \xrightarrow{\sim} A/(\phi-1)A$$

be the evaluation map at the Frobenius element ϕ where

$$Gal(K_\lambda^{ur}/K_\lambda) = <\phi> .$$

Then α is an isomorphism. The exact sequence of Galois groups

$$0 \longrightarrow \mathrm{Gal}(\overline{K_\lambda}/K_\lambda^t) \longrightarrow \mathrm{Gal}(\overline{K_\lambda}/K_\lambda^{ur}) \longrightarrow \mathrm{Gal}(K_\lambda^t/K_\lambda^{ur}) \longrightarrow 0$$

induces the exact sequence

$$H^1(K_\lambda^t/K_\lambda^{ur},A') \longrightarrow H^1(K_\lambda^{ur},A') \longrightarrow H^1(K_\lambda^t,A') \longrightarrow 0,$$

where $H^1(K_\lambda^t,A') = 0$ since $\mathrm{Gal}(\overline{K_\lambda}/K_\lambda^t)$ is a pro-q group. Therefore,

$$H^1(K_\lambda^{ur},A') \simeq H^1(K_\lambda^t/K_\lambda^{ur},A') \simeq \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}(1),A') \simeq \mathrm{Hom}(\mu_p,A').$$

Hence we have an isomorphism

$$H^1(K_\lambda^{ur},A') \xrightarrow{\sim} \mathrm{Hom}(\mu_p,A').$$

The exact sequence of Galois cohomology groups

$$0 \longrightarrow H^1(K_\lambda^{ur}/K,A') \longrightarrow H^1(K_\lambda,A') \longrightarrow H^1(K_\lambda^{ur},A')^\phi \longrightarrow 0$$

allows us to identify $H^1(K_\lambda,A')/H^1(K_\lambda^{ur}/K_\lambda,A')$ with

$$H^1(K_\lambda^{ur},A')^\phi \simeq \mathrm{Hom}(\mu_p,A')^\phi.$$

Hence, we obtain a perfect local pairing

$$\langle\,\cdot\,,\,\cdot\,\rangle_p \;:\; H^1(K_\lambda^{ur}/K_\lambda,A) \times H^1(K_\lambda^{ur},A')^\phi \longrightarrow \mathbb{Z}/p\mathbb{Z}.$$

Alternatively, the local Tate pairing can be viewed as a duality between invariants

$$(A')^{\phi=N(\lambda)} = H^1(K_\lambda^{ur},A')^\phi$$

of the dual of A under the action of ϕ and Frobenius co-invariants

$$A/(\phi-1)A = H^1(K_\lambda^{ur}/K, A)$$

of A.

We will be interested in the particular situation where $A = A'$, K is an imaginary quadratic field and K_ℓ is its ring class field of conductor ℓ. Since the extension $K_{\lambda_\ell}/K_\lambda$ is totally ramified, the generator σ_ℓ of $Gal(K_{\lambda_\ell}/K_\lambda)$ can be lifted to a generator

$$\tau_\ell \in Gal(K_\lambda^t/K_\lambda^{ur}) \simeq \hat{\mathbb{Z}}'(1) = \prod_{q\neq\ell} \mathbb{Z}_q(1).$$

Let $\zeta_{\lambda,p}$ be the image of τ_ℓ by the projection

$$\hat{\mathbb{Z}} \longrightarrow \mu_p.$$

We obtain the map β

$$\beta \ : \ H^1(K_\lambda^{ur}, A)^\phi \xrightarrow{\sim} A^{\phi=N(\lambda)}$$

as the composition of the isomorphism $H^1(K_\lambda^{ur}, A)^\phi \simeq \mathrm{Hom}(\mu_p, A)^\phi$ with the evaluation map

$$\mathrm{Hom}(\mu_p(K_\lambda), A)^\phi \xrightarrow{\sim} A^{\phi=N(\lambda)}$$

at $\zeta_{\lambda,p}$. This induces an isomorphism

$$\gamma = \beta^{-1} \circ \alpha \ : \ H^1_{ur}(K_\lambda, A) \simeq H^1(K_\lambda^{ur}, A)^\phi \tag{2.2}$$

where elements of $A/(\phi-1)A$ are viewed as the corresponding dual elements of $A^{\phi=N(\lambda)}$. The map γ switches cocycles with same values on ϕ and τ_ℓ modulo p.

2.6 Weil conjectures

We recall the *Weil conjectures* which play an important role in the study of the localization of Kolyvagin cohomology classes. We follow Mazur's notes [36]. Consider an abelian variety V over a field k of cardinality q and denote by k_n the subfield of $\overline{k}$ of cardinality q^n. We can associate to V a zeta function

$$Z(V/k,t) = \exp\left(\sum_n N_n(V/k)\,\frac{t^n}{n}\right),$$

where $N_n(V/k)$ is the cardinality of $V(k_n)$. This zeta function can be expressed as

$$Z(V/k,t) = \frac{\prod_{\mathrm{odd}\,j} \det(1-t\phi \mid H^j(\overline{V}))}{\prod_{\mathrm{even}\,j} \det(1-t\phi \mid H^j(\overline{V}))},$$

where ϕ is the Frobenius endomorphism acting on the étale cohomology H^j of $\overline{V}$. (See [36, Discussion 1.4,1.5]). The Weil conjectures predict the following

1. *Rationality:* $Z(V/k,t)$ is a rational function of t with coefficients in $\mathbb{Q}$ whose poles and zeros are algebraic integers.

2. *Functional equation:* If V/k is connected, proper and smooth of dimension d then the map $\alpha \mapsto q^d/\alpha$ is a permutation of the zeros of $Z(V/k,t)$ and of its poles.

3. *Riemann hypothesis:* If α is an eigenvalue of the geometric Frobenius acting on $H^j(\overline{V})$ for an étale cohomology H^j and $|\cdot|$ is any archimedean absolute value then $|\alpha| = q^{\frac{j}{2}}$.

CHAPTER 3

Kolyvagin's method for Chow groups of Kuga-Sato varieties over ring class fields

3.1 Introduction

Let f be a normalized newform of level $\Gamma_0(N)$ and trivial nebentype where $N \geq 5$ and of even weight $2r > 2$ and let

$$K = \mathbb{Q}(\sqrt{-D})$$

be an imaginary quadratic field satisfying the *Heegner hypothesis* relative to N, that is, rational primes dividing N split in K. For simplicity, we assume that $|\mathscr{O}_K^\times| = 2$. We fix a prime p not dividing $ND\phi(N)$. Let H be the ring class field of K of conductor c with $(c, NDp) = 1$, (see Chapter 2, Section 2.3 for more details) and let e be the exponent of $\mathrm{Gal}(H/K)$. Let $F = \mathbb{Q}(a_1, a_2, \cdots, \mu_e)$ be the field generated over $\mathbb{Q}$ by the coefficients of f and the e-th roots of unity μ_e. We denote by A the p-adic étale realization of the motive associated to f by Scholl [46] and Deligne [18] twisted by r. It will be viewed (by extending scalars appropriately) as a free $\mathscr{O}_F \otimes \mathbb{Z}_p$ module of rank 2, equipped with a continuous $\mathscr{O}_F$-linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $A_\wp$ be the localization of A at a prime $\wp$ of $\mathscr{O}_F$ dividing p. Then $A_\wp$ is a free module of rank 2 over $\mathscr{O}_\wp$, the completion of $\mathscr{O}_F$ at $\wp$. The Selmer group

$$S \subseteq H^1(H, A_\wp/p)$$

consists of the cohomology classes c whose localizations c_v at a prime v of H lie in

$$\begin{cases} H^1(H_v^{ur}/H_v, A_\wp/p) \text{ for } v \text{ not dividing } Np \\ H_f^1(H_v, A_\wp/p) \text{ for } v \text{ dividing } p \end{cases}$$

where $H_f^1(H_v, A_\wp/p)$ is the *finite part* of $H^1(H_v, A_\wp/p)$ as in [9]. In our setting, since $A_\wp$ has good reduction at p, $H_f^1(H_v, M) = H_{cris}^1(H_v, M)$. Note that the assumptions we make will ensure that $H^1(H_v^{ur}/H_v, A_\wp/p) = 0$ for v dividing N. The Galois group

$$G = \mathrm{Gal}(H/K)$$

acts on $H^1(H, A_\wp/p)$ and preserves the unramified and cristalline classes, hence it acts on S. Assume that p does not divide $|G|$. We denote by $\hat{G} = \mathrm{Hom}(G, \mu_e)$ the group of characters of G and by

$$e_\chi = \frac{1}{|G|} \sum_{g \in G} \chi^{-1}(g) g$$

the projector onto the χ-eigenspace given a character χ of $\hat{G}$.

By the Heegner hypothesis, there is an ideal $\mathscr{N}$ of $\mathscr{O}_c$, the order of K of conductor c, such that

$$\mathscr{O}_c / \mathscr{N} = \mathbb{Z}/N\mathbb{Z}.$$

Therefore, $\mathbb{C}/\mathscr{O}_c$ and $\mathbb{C}/\mathscr{N}^{-1}$ define elliptic curves related by an N-isogeny. As points of $X_0(N)$ correspond to elliptic curves related by N-isogenies, this provides a *Heegner point* x_1 of $X_0(N)$. By the theory of complex multiplication, x_1 is defined over H. Let E be the corresponding elliptic curve. Then E has complex multiplication by $\mathscr{O}_c$. The Heegner cycle of conductor c is defined as

$$e_r(\mathrm{graph}(\sqrt{-D}))^{r-1}$$

for some appropriate projector e_r, (see Section 3.2 for more details). Let δ be the image by the p-adic étale Abel-Jacobi map of the Heegner cycle of conductor c viewed as an element of $H^1(H, A_\wp/p)$. We denote by $Fr(v)$ the arithmetic Frobenius element generating $\mathrm{Gal}(H_v^{ur}/H_v)$, and by $I_v = \mathrm{Gal}(\overline{H_v}/H_v^{ur})$. This chapter is dedicated to the proof of the following statement:

Theorem 1.2.1. Assume that p is such that

$$\mathrm{Gal}\left(\mathbb{Q}(A_\wp/p)/\mathbb{Q}\right) \simeq \mathrm{GL}_2(\mathscr{O}_\wp/p), \quad (p, ND\phi(N)) = 1, \text{ and } p \nmid |G|.$$

Suppose further that the eigenvalues of $Fr(v)$ acting on $A_\wp^{I_v}$ are not equal to 1 modulo p for v dividing N. Let $\chi \in \hat{G}$ be such that $e_{\overline{\chi}}\delta$ is not divisible by p. Then the χ-eigenspace S^χ of the Selmer group S has rank 1 over $\mathscr{O}_\wp/p$.

To prove Theorem 1.2.1, we first view the p-adic étale realization A of the twisted motive associated to f in the middle étale cohomology of the associated Kuga-Sato varieties. The main two ingredients of the proof are the refinement of an Euler system of so-called Heegner cycles first considered by Nekovář and Kolyvagin's descent machinery adapted by Nekovář [39] to the setting of modular forms. In order to bound the rank of the χ-eigenspace of the Selmer group S^χ, we use Local Tate duality and the local reciprocity law to obtain information on the local elements of the Selmer group. Using a global pairing of the Selmer group and Cebotarev's density theorem, we translate this local information about the elements of S^χ into global information.

The main novelty is the adaptation of the techniques by Bertolini and Darmon in [3] to the setting of modular forms that allow us to get around the action of complex conjugation. Indeed, unlike the case where χ is trivial, the complex conjugation τ does not act on S^{χ} as it maps it to $S^{\overline{\chi}}$.

3.2 Motive associated to a modular form

In this section, we describe the p-adic étale realization A of the motive associated to f by Scholl [46] and Deligne [18] twisted by r. Consider the congruence subgroup $\Gamma_0(N)$ for $N \geq 5$ of the modular group $\mathrm{SL}_2(\mathbb{Z})$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ \middle|\ c \equiv 0 \mod N \right\}.$$

We denote by $Y_0(N)$ the smooth irreducible affine curve that is the moduli space classifying elliptic curves with $\Gamma_0(N)$ level structure, that is elliptic curves with cyclic subgroups of order N. Equivalently, $Y_0(N)$ classifies pairs of elliptic curves related by an N-isogeny. Over $\mathbb{C}$, we have

$$\mathbb{H}/\Gamma_0(N) \ \simeq \ Y_0(N)_{\mathbb{C}} \ : \ \tau \ \mapsto \ \left(\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)\ ,\ \langle \frac{1}{N} \rangle\right).$$

We denote by $X_0(N)$ the compactification of $Y_0(N)$ viewed as a Riemann surface and we let j be the inclusion map

$$j : Y_0(N) \hookrightarrow X_0(N).$$

The assumption $N \geq 5$ allows for the definition of the universal elliptic curve

$$\pi : \mathscr{E} \longrightarrow X_0(N).$$

Let

$$\mathbb{Z}^2 \setminus (\mathbb{C} \times \mathbb{H})$$

be the universal generalized elliptic curve over the Poincaré upper half plane where (m,n) in $\mathbb{Z}^2$ acts on $\mathbb{C} \times \mathbb{H}$ by

$$(z,\tau) \ \mapsto \ (z+m\tau+n,\tau).$$

We denote by $\mathscr{E}$ the compact universal generalized elliptic curve of level $\Gamma_0(N)$. Let W_r be the *Kuga-Sato variety* of dimension $r+1$, that is a compact desingularization of the r-fold fibre product

$$\mathscr{E} \times_{X_0(N)} \cdots \times_{X_0(N)} \mathscr{E},$$

(see [18] and the appendix by Conrad in [5] for more details).

Fix a prime p with $(p, N\phi(N)) = 1$. Consider the sheaf

$$\mathscr{F} = Sym^{2r-2}(R^1\pi_*\mathbb{Z}/p).$$

Let

$$\Gamma_{2r-2} = (\mathbb{Z}/N \rtimes \mu_2)^{2r-2} \rtimes \Sigma_{r-2}$$

where $\mu_2 = \{\pm 1\}$ and Σ_{2r-2} is the symmetric group on $2r-2$ elements. Then Γ_{2r-2} acts on W_{2r-2}, (see [46, Sections 1.1.0,1.1.1] for more details.) The projector

$$e_r \in \mathbb{Z}\left[\frac{1}{2N(r-2)!}\right][\Gamma_{2r-2}]$$

associated to Γ_{2r-2}, called Scholl's projector, belongs to the group of zero correspondences $\mathrm{Corr}^0(W_{2r-2}, W_{2r-2})_{\mathbb{Q}}$ from W_{2r-2} to itself over $\mathbb{Q}$, (see [4, Section 2.1] for more details.).

Remark 3.2.1. The hypothesis $((2r-2)!,p)=1$ is not necessary by a combination of the work of Tsuji [54] on p-adic comparison theorems and Saito [43] on the Weight-Monodromy conjecture for Kuga-Sato varieties.

Proposition 3.2.2.

$$H^1_{et}(X_0(N)\otimes\overline{\mathbb{Q}}, j_*\mathscr{F}) \simeq e_r \oplus_{i=0}^{r+1} H^i_{et}(W_r\otimes\overline{H}, \mathbb{Z}/p).$$

Proof. The proof is a combination of [46, theorem 1.2.1] and [5, proposition 2.4]. Note that the proof in [46, theorem 1.2.1] involves $\mathbb{Q}_p$ coefficients but it is still valid in our setting, (see the Remark following [39, Proposition 2.1]). $\square$

Define

$$J = H^1_{et}(X_0(N)\otimes\overline{\mathbb{Q}}, j_*\mathscr{F}).$$

For primes ℓ prime to N, the Hecke operators T_ℓ act on $X_0(N)$, which induces an endomorphism of $H^1_{et}(X_0(N)\otimes\overline{\mathbb{Q}}, j_*\mathscr{F})$. Let A be its f-isotypic component with respect to the action of the Hecke operators. Let

$$I = Ker\{\mathbb{T} \longrightarrow \mathscr{O}_F : T_\ell \longrightarrow a_\ell, \forall \ell \nmid N\}.$$

Then $A = \{x\in J \mid Ix = 0\}$ is isomorphic to J/IJ. A is a free $\mathscr{O}_F\otimes\mathbb{Z}_p$ module of rank 2, equipped with a continuous $\mathscr{O}_F$-linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Hence, there is a map $e_A : J \longrightarrow A$ that is equivariant under the action of Hecke operators and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Consider the étale p-adic Abel-Jacobi map

$$\Phi : CH^r(W_{2r-2}/H)_0 \longrightarrow H^1(H, H^{2r-1}_{et}(W_{2r-2}\otimes\overline{H}, \mathbb{Z}_p(r)))$$

where $CH^r(W_{2r-2}/H)_0$ is the group of homologically trivial cycles of codimension $2r-2$ on W_{2r-2} defined over H, modulo rational equivalence. Composing the Abel-Jacobi map with the projector e_r, we obtain a map

$$\Phi : CH^r(W_{2r-2}/H)_0 \longrightarrow H^1(H,J).$$

The Abel-Jacobi map commutes with automorphisms of W_{2r-2}, so Φ factors through

$$e_r(CH^r(W_{2r-2}/H)_0 \otimes \mathbb{Z}_p).$$

Proposition 3.2.2 implies that $e_r H^{r+1}(W_{2r-2} \otimes \overline{H}, \mathbb{Z}_p) = 0$. Since

$$CH^r(W_{2r-2}/H)_0 = Ker(CH^r(W_{2r-2}/H) \longrightarrow H^{r+1}(W_{2r-2} \otimes \overline{H}, \mathbb{Z}_p)),$$

we have $e_r(CH^r(W_{2r-2}/H)_0 \otimes \mathbb{Z}_p) = e_r(CH^r(W_{2r-2}/H) \otimes \mathbb{Z}_p)$. Composing the former map with the map $e_A : J \longrightarrow A$, we get

$$\Phi : e_r CH^r(W_{2r-2}/H)_0 \longrightarrow H^1(H,A).$$

3.3 Heegner cycles

Consider an integer m such that $(m, cNDp) = 1$. Recall that $H = K_c$ is the ring class field of K of conductor c. We denote by

$$H_m = K_{cm}$$

the ring class field of K of conductor cm for $m > 1$. We describe Nekovář's construction of Heegner cycles as in [39, Section 5].

By the Heegner hypothesis, there is an ideal $\mathscr{N}$ of $\mathscr{O}_{cm}$, the order of K of conductor cm, such that

$$\mathscr{O}_{cm}/\mathscr{N} = \mathbb{Z}/N\mathbb{Z}.$$

Therefore, $\mathbb{C}/\mathscr{O}_{cm}$ and $\mathbb{C}/\mathscr{N}^{-1}$ define elliptic curves over $\mathbb{C}$ related by an N-isogeny. As points of $X_0(N)$ correspond to elliptic curves over $\mathbb{C}$ related by N-isogenies, this provides a *Heegner point* x_m of $X_0(N)$. By the theory of complex multiplication, x_m is defined over the ring class field H_m of K of conductor cm, (see [26] for more details). Let E be the elliptic curve corresponding to x_m. Then E has complex multiplication by $\mathscr{O}_{cm}$. Letting $graph(\sqrt{-D})$ be the graph of the multiplication by $\sqrt{-D}$ on E, we denote by Z_E the image of the divisor

$$(graph(\sqrt{-D}) - E \times 0 - D(0 \times E))$$

in the Néron-Severi group $NS(E \times E)$ of $E \times E$, that is, the group of divisors of $E \times E$ modulo algebraic equivalence. Consider the inclusion

$$i : E^{2r-2} \longrightarrow W_{2r-2}.$$

Then $i_*(Z_E^{r-1})$ belongs to the Chow group $\mathrm{CH}^r(W_{2r-2}/H_m)_0$. Denote by y_m the image of $i_*(Z_E^{r-1})$ by the p-adic étale Abel-Jacobi map

$$\Phi : \mathrm{CH}^r(W_{2r-2}/H_m)_0 \longrightarrow H^1(H_m, A)$$

as described in [31] and briefly explained in Chapter 2, Section 2.1. We consider two crucial properties of the Galois cohomology classes thus obtained from Heegner cycles.

Proposition 3.3.1. *Consider cocycles y_n and y_m with $n = \ell m$, where ℓ is a prime inert in K. Then*

$$T_\ell y_m = \mathrm{cor}_{H_n/H_m} y_n = a_\ell y_m.$$

Proof. Let E_m be the elliptic curve corresponding to x_m. Then, we have

$$T_\ell(i_*(Z^{r-1}_{E_m})) = \sum_y i_*(Z^{r-1}_{E_y}),$$

where the elements $y \in Y_0(N)$ correspond to ℓ-isogenies $E_y \to E_m$ compatible with level $\Gamma_0(N)$ structure. The set $\{y\}$ consists of the orbit of x_n in

$$\mathrm{Gal}(H_n/H_m) \simeq \mathrm{Gal}(K_n/K_m) \simeq \mathrm{Gal}(K_\ell/K_1).$$

Let E_n be the elliptic curve corresponding to x_n. We have

$$\sum_y i_*(Z^{r-1}_{E_y}) = \sum_{g \in \mathrm{Gal}(H_n/H_m)} g \cdot i_*(Z^{r-1}_{E_n}) = \mathrm{cor}_{H_n/H_m} i_*(Z^{r-1}_{E_n}).$$

Since the action of the Hecke operators commutes with the Abel-Jacobi map, we obtain

$$T_\ell y_m = \mathrm{cor}_{H_n/H_m} y_n.$$

The equality

$$T_\ell y_m = a_\ell y_m$$

follows from the definition of A on which Hecke operators T_ℓ act by a_ℓ. $\square$

We denote by $(y_n)_v$ the image of an element $y_n \in H^1(H_n, A)$ in $H^1(H_{n,v}, A)$.

Proposition 3.3.2. *Consider cocycles y_n and y_m with $n = \ell m$, where ℓ is a prime inert in K. Let λ_m be a prime above ℓ in K_m and λ_n the prime above λ_m in K_n. Then*

$$(y_n)_{\lambda_n} = Fr(\ell)(\mathrm{res}_{K_{\lambda_m},K_{\lambda_n}}(y_m)_{\lambda_m}) \text{ in } H^1(K_{\lambda_n}, A).$$

Proof. The proof can be found in [39, proposition 6.1(2)]. □

3.4 The Euler system

Let $n = \ell_1 \cdots \ell_k$ be a squarefree product of primes ℓ_i inert in K satisfying

$$(\ell_i, DNpc) = 1 \text{ for } i = 1, \cdots, k.$$

The Galois group $G_n = \mathrm{Gal}(H_n/H)$ is isomorphic to the product over the primes ℓ dividing n of the cyclic groups $\mathrm{Gal}(H_\ell/H)$ of order $\ell + 1$. Let σ_ℓ be a generator of G_ℓ. We denote by $\mathscr{O}_\wp$, the completion of $\mathscr{O}_F$ at a prime $\wp$ dividing p. Then $\mathscr{O}_F \otimes \mathbb{Z}_p = \oplus_{\wp|p} \mathscr{O}_\wp$. Let $A_\wp = A \otimes_{\mathscr{O}_F \otimes \mathbb{Z}_p} \mathscr{O}_\wp$ be the localization of A at $\wp$. Denote by

$$y_{n,\wp} \in H^1(H_n, A_\wp)$$

the $\wp$-component of $y_n \in H^1(H_n, A)$. In this section, we use Operators (3.2) considered by Kolyvagin to define Kolyvagin cohomology classes $P(n) \in H^1(H, A_\wp/p)$ using the cohomology classes $y_n \in H^1(H_n, A)$ for appropriate n. Let

$$L = H(A_\wp/p)$$

be the smallest Galois extension of H such that $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ acts trivially on $A_\wp/p$. We will denote by $\mathrm{Frob}_{F_1/F_2}(\alpha)$, the conjugacy class of the Frobenius substitution of the prime α of F_2 in $\mathrm{Gal}(F_1/F_2)$.

A prime ℓ will be referred to as a *Kolyvagin prime* if it is such that

$$(\ell, DNpc) = 1 \text{ and } \mathrm{Frob}_\ell(L/\mathbb{Q}) = \mathrm{Frob}_\infty(L/\mathbb{Q}),$$

where $\mathrm{Frob}_\infty(L/\mathbb{Q})$ refers to the conjugacy class of complex conjugation. Given a Kolyvagin prime ℓ, the Frobenius condition implies that it is inert in K. Denote by λ the unique prime in K above ℓ. Since λ is unramified in H and has the same image as $\mathrm{Frob}_\infty(L/K) = \tau^2 = Id$ by the Artin map, it splits completely in H. Let λ' be a prime of H lying above λ, then λ' splits completely in L as it lies in the kernel of the Artin map:

$$\mathrm{Frob}_{\lambda'}(L/H) = \tau^2 = Id.$$

The Frobenius condition also implies that

$$a_\ell \equiv \ell + 1 \equiv 0 \mod p. \tag{3.1}$$

Indeed, the characteristic polynomial of the complex conjugation acting on $A_\wp/p$ is $x^2 - 1$ while the characteristic polynomial of $\mathrm{Frob}(\ell)$ is

$$x^2 - a_\ell/\ell^r x + 1/\ell.$$

The latter corresponds to the polynomial $x^2 - a_\ell x + \ell^{2r-1}$ where we make the change of variable $x \to \ell^r x$ dictated by the Tate twist r of Y_p. As a consequence, we obtain the polynomial

$$x^2\ell^{2r} - a_\ell \ell^r x + \ell^{2r-1} = \ell^{2r}(x^2 - a_\ell/\ell^r x + 1/\ell).$$

Let

$$\mathrm{Tr}_\ell = \sum_{i=0}^{\ell} \sigma_\ell^i, \qquad D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i. \tag{3.2}$$

These operators are related by

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

We define $D_n = \prod_{\ell|n} D_\ell$ in $\mathbb{Z}[G_n]$. And we denote by $\mathrm{red}(x)$ the image of an element x of $H^1(H_n, A_\wp)$ in $H^1(H_n, A_\wp/p)$ obtained by composing x with the projection

$$A_\wp \longrightarrow A_\wp/p.$$

Proposition 3.4.1. *We have*

$$D_n\mathrm{red}(y_{n,\wp}) \textit{ belongs to } H^1(H_n, A_\wp/p)^{G_n}.$$

Proof. It is enough to show that for all ℓ dividing n,

$$(\sigma_\ell - 1)D_n\mathrm{red}(y_{n,\wp}) = 0$$

in $H^1(H_n, A_\wp/p)$. We have

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

Since $\mathrm{res}_{H_m,H_n} \circ \mathrm{cor}_{H_n/H_m} = \mathrm{Tr}_\ell$, Proposition 3.3.1 implies

$$(\ell + 1 - \mathrm{Tr}_\ell)D_m\mathrm{red}(y_{n,\wp}) = (\ell+1)D_m\mathrm{red}(y_{n,\wp}) - a_\ell\mathrm{res}_{H_m,H_n}(D_m\mathrm{red}(y_{m,\wp})).$$

The latter is congruent to 0 modulo p by Equation (3.1). $\square$

Proposition 3.4.2. *For n such that* $(n, cpND) = 1$*, we have*

$$H^0(H_n, A_\wp/p) = H^0(\mathbb{Q}, A_\wp/p) = 0,$$

and $\mathrm{Gal}(H_n(A_\wp/p)/H_n) \simeq \mathrm{Gal}(H(A_\wp/p)/H) \simeq \mathrm{Gal}(K(A_\wp/p)/K) \simeq \mathrm{Gal}(\mathbb{Q}(A_\wp/p)/\mathbb{Q})$.

Proof. Indeed, $H_n/\mathbb{Q}$ and $\mathbb{Q}(A_\wp/p)/\mathbb{Q}$ are unramified outside primes dividing cnD and Np respectively, so $H_n \cap \mathbb{Q}(A_\wp/p)$ is unramified over $\mathbb{Q}$. Since $\mathbb{Q}$ has no unramified extensions, we obtain that $H_q \cap \mathbb{Q}(A_\wp/p) = \mathbb{Q}$, and therefore $H^0(H_q, A_\wp/p) = H^0(\mathbb{Q}, Y_p)$. The hypothesis $\mathrm{Gal}(\mathbb{Q}(A_\wp/p)/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathscr{O}_\wp/p)$ further implies that $H^0(\mathbb{Q}, A_\wp/p) = 0$. The result follows. □

Proposition 3.4.3. *The restriction map*

$$\mathrm{res}_{H,H_n} : H^1(H, A_\wp/p) \longrightarrow H^1(H_n, A_\wp/p)^{G_n}$$

is an isomorphism for $(n, cpND) = 1$.

Proof. This follows from the inflation-restriction sequence:

$$0 \to H^1(H_n/H, A_\wp/p) \xrightarrow{inf} H^1(H, A_\wp/p) \xrightarrow{\mathrm{res}} H^1(H_n, A_\wp/p)^{G_n} \to H^2(H_n/H, A_\wp/p)$$

using the fact that $H^0(H_n, A_\wp/p) = 0$ by Proposition 3.4.2. □

As a consequence, the cohomology classes $D_n \mathrm{red}(y_{n,\wp})$ can be lifted to cohomology classes $P(n)$ in $H^1(H, A_\wp/p)$ such that

$$\mathrm{res}_{H,H_n} P(n) = D_n \mathrm{red}(y_{n,\wp}).$$

Proposition 3.4.4. *Let v be a prime of H. If $v|N$, then $P(n)_v$ is trivial. If $v \nmid Nnp$, then $P(n)_v$ lies in $H^1(H_v^{ur}/H_v, A_\wp/p)$.*

Proof. If v divides N, we follow the proof in [39, lemma 10.1]. We denote by

$$(A_\wp/p)^{dual} = \mathrm{Hom}(A_\wp/p, \mathbb{Z}/p\mathbb{Z}(1))$$

the local Tate dual of $A_\wp/p$. The local Euler characteristic formula [37, Section 1.2] yields

$$|H^1(H_v, A_\wp/p)| = |H^0(H_v, A_\wp/p)| \times |H^2(H_v, A_\wp/p)|.$$

Local Tate duality then implies

$$|H^1(H_v, A_\wp/p)| = |H^0(H_v, A_\wp/p)|^2.$$

The Weil conjectures and the assumption on $Fr(v)$ imply that $((A_\wp/p)^{I_v})^{Fr(v)} = 0$ where

$$< Fr(v) > = \mathrm{Gal}(H_v^{ur}/H_v)$$

and $I_v = \mathrm{Gal}(\overline{H_v}/H_v^{ur})$ is the inertia group. (See Section 2.6 for more details). Therefore, $((A_\wp/p)^{I_v})^{G(H_v^{ur}/H_v)} = (A_\wp/p)^{G(\overline{H_v}/H_v)} = H^0(H_v, A_\wp/p) = 0$.

To prove the second assertion, if v does not divide Nnp, we observe that

$$\mathrm{res}_{H,H_n} P(n)_v = D_n red(y_{n,\wp})_{v'}$$

belongs to $H^1(H_{n,v'}^{ur}/H_{n,v'}, A_\wp/p)$ and $H_{n,v'}/H_v$ is unramified for v' in H_n above v. $\square$

3.5 Localization of Kolyvagin classes

Nekovář [39] studied the relation between the localization of Kolyvagin cohomology classes $P(m\ell)$ and $P(m)$, for appropriate m and ℓ by explicitly computing cocycles using the Euler system properties. We briefly explain his development in this section.

Set up. We denote by

$$G_1 = \mathrm{Gal}(\overline{\mathbb{Q}}/H_1), \;\; G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}/H_\ell), \;\; \tilde{G}_1 = \mathrm{Gal}(\overline{\mathbb{Q}}/H_1^+),$$
$$\text{and } G_{\lambda_1} = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/H_{1,\lambda_1}), \;\; G_{\lambda_\ell} = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/H_{\ell,\lambda_\ell}), \;\; \tilde{G_{\lambda_1}} = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell),$$

where H_1^+ is the maximal real subfield of H_1. Then

$$G_1/G_\ell =< \sigma >, \;\; \tilde{G}_1/G_1 =< \tau >, \;\; \tilde{G}_1/G_\ell = \mathrm{Gal}(H_\ell/H^+) =< \sigma > \rtimes < \tau >$$

for some σ and τ of order $\ell+1$ and 2 respectively. There is a surjective homomorphism

$$\pi : \tilde{G_{\lambda_1}} \xrightarrow{res} \mathrm{Gal}(\mathbb{Q}_\ell^t/\mathbb{Q}_\ell) = \hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}},$$

where

$$\mathrm{Gal}(\mathbb{Q}_\ell^t/\mathbb{Q}_\ell^{ur}) \simeq \hat{\mathbb{Z}}'(1) = \prod_{q\neq\ell} \mathbb{Z}_\ell$$

is generated by an element τ_ℓ and

$$\mathrm{Gal}(\mathbb{Q}_\ell^{ur}/\mathbb{Q}_\ell) \simeq \hat{\mathbb{Z}}$$

is generated by the Frobenius element ϕ at ℓ and $\phi\tau_\ell\phi^{-1} = (\tau_\ell)^\ell$. One can show that

$$H^1(G_{\lambda_1}, A_\wp/p) = H^1(G_{\lambda_\ell}, A_\wp/p) \simeq H^1(2\hat{Z}, A_\wp/p) \simeq (A_\wp/p)/((\phi^2-1)A_\wp/p)$$

and a cocycle F in $Z^1(\,\hat{\mathbb{Z}}'(1) \rtimes 2\hat{\mathbb{Z}},\, A_{\wp}/p)$ acts by

$$F(\tau_\ell^u \phi^{2v}) = (1+\phi^2+\cdots+\phi^{2(v-1)})a + (\phi^2-1)b,$$

where $[F] = a \mod (\phi^2-1)A_{\wp}/p$.

Proposition 3.5.1. *We have*

$$\left(\frac{\ell+1}{p}\varepsilon - \frac{a_\ell}{p}\right)\gamma(P(m)_{\lambda_1}) = \frac{a_\ell\varepsilon/\ell^r - 1/\ell - 1}{p} P(\ell m)_{\lambda_1} \tag{3.3}$$

where γ is the map defined by (2.2)*, λ_1 is a prime of H_1 dividing ℓ, and $\varepsilon = \pm 1$. Furthermore, $P(\ell m)_{\lambda_1}$ is unramified at ℓ.*

Proof. We denote by

$$x = D_m y_m \in H^1(G_1, A_{\wp}/p), \text{ and } y = D_m y_{\ell m} \in H^1(G_\ell, A_{\wp}/p).$$

Let $z = P(\ell m)$ in $H^1(G_1, A_{\wp}/p)$. Then

$$\mathrm{res}_{G_1,G_\ell}(z) = D_\ell red(y) \in H^1(G_\ell, A_{\wp}/p).$$

For a in $A_{\wp}/p$, we have

$$D_\ell a = \sum_{i=1}^{\ell} i\sigma^i(a) = \sum_{i=1}^{\ell} i = \frac{\ell(\ell+1)}{2} \equiv 0 \mod p.$$

Therefore, $\mathrm{res}_{G_1,G_{\lambda_\ell}}(z) = 0$, which implies that $P(\ell m)_{\lambda_1}$ is ramified at a place λ_1 of H_1 above ℓ. Hence, using the inflation-restriction sequence

$$0 \longrightarrow H^1(G_{\lambda_1}/G_{\lambda_\ell}, A_{\wp}/p) \longrightarrow H^1(G_{\lambda_1}, A_{\wp}/p) \longrightarrow H^1(G_{\lambda_\ell}, A_{\wp}/p) \longrightarrow 0,$$

we obtain

$$P(\ell m)_{\lambda_1} = \mathrm{res}_{G_1, G_{\lambda_1}}(z) = \mathrm{inf}_{G_{\lambda_1}/G_{\lambda_\ell}, G_{\lambda_1}}(z_1)$$

for some

$$z_1 \in H^1(G_{\lambda_1}/G_{\lambda_\ell}, A_\wp/p) = \mathrm{Hom}(<\sigma>, A_\wp/p).$$

Since $cor_{G_\ell, G_1}(y) = a_\ell x$, there is an element a in $A_\wp/p$ such that

$$\mathrm{cor}_{G_\ell, G_1}(y)(g_1) - a_\ell\, x(g_1) = (g_1 - 1)a \tag{3.4}$$

for g_1 in G_1. It is shown in [39, section 7] that

$$a = z_1(\sigma).$$

We let

$$a_x = \mathrm{res}_{G, G_{\lambda_1}}(x), \text{ and } a_y = \mathrm{res}_{H, G_{\lambda_\ell}}(y).$$

Restricting g_1 to $g_{\lambda_1} \in G_{\lambda_1}$ in equation (3.4) where $\pi(g_{\lambda_1}) = \sigma^u \phi^{2v}$, we obtain

$$\sum_{i=0}^{\ell} a_y(\tilde{\sigma}^{-i} g_{\lambda_1} \tilde{\sigma}^i) - a_\ell a_x(g_{\lambda_1}) = (\ell+1)a_y(g_{\lambda_1}) - a_\ell a_x(g_{\lambda_1}) = (\phi^2 - 1)a,$$

where $\tilde{\sigma}$ is a lift of σ in G_1/G_ℓ to G_1. We have

$$x(g_{\lambda_1}) = (1 + \phi^2 + \cdots + \phi^{2(v-1)})a_x + (\phi^2 - 1)b_x,$$
$$\& \;\; y(g_{\lambda_1}) = (1 + \phi^2 + \cdots + \phi^{2(v-1)})a_y + (\phi^2 - 1)b_y.$$

For $u = 0, v = 1$, we obtain from the last three equations

$$(\ell+1)y(g_{\lambda_1}) - a_\ell x(g_{\lambda_1}) = (\phi^2 - 1)a + (\phi^2 - 1)(-a_\ell b_x + (\ell+1)b_y), \tag{3.5}$$

where

$$(\phi^2 - 1)(-a_\ell b_x + (\ell+1) b_y) = 0 \mod p$$

as $a_\ell \equiv \ell + 1 \equiv 0 \mod p$. The second property of the Euler system

$$a_y = \phi(a_x) \mod (\phi^2 - 1)\, A_\wp/p$$

implies that

$$\frac{\ell+1}{p} y(g_{\lambda_1}) - \frac{a_\ell}{p} x(g_{\lambda_1}) = \left(\frac{\ell+1}{p}\varepsilon - \frac{a_\ell}{p}\right) x(g_{\lambda_1})$$

where ε is such that $\phi \equiv \tau$ acts by ε on a_x. Therefore, by Equation (3.5),

$$\left(\frac{\ell+1}{p}\varepsilon - \frac{a_\ell}{p}\right) x(g_{\lambda_1}) = \frac{\phi^2 - 1}{p} a \mod p.$$

The characteristic polynomial of ϕ implies that

$$\phi^2 - a_\ell \phi/\ell^r + 1/\ell = 0 \text{ on } A_\wp/p.$$

Therefore,

$$\left(\frac{\ell+1}{p}\varepsilon - \frac{a_\ell}{p}\right) x(g_{\lambda_1}) = \frac{a_\ell \phi/\ell^r - 1/\ell - 1}{p} a \equiv \frac{a_\ell \varepsilon/\ell^r - 1/\ell - 1}{p} a.$$

We seek to express $a = z_1(\sigma)$ in terms of $P(\ell m)_{\lambda_1} = \inf_{G_{\lambda_1}/G_{\lambda_\ell}, G_{\lambda_1}}(z_1)$ where the generator σ of $G_{\lambda_1}/G_{\lambda_\ell}$ can be lifted to the generator τ_ℓ of $G_{\lambda_1} = \mathrm{Gal}(H^t_{\lambda_1}/H^{ur}_{\lambda_1})$. It is therefore enough to apply the map γ defined by (2.2) to a to obtain $P(\ell m)_{\lambda_1}$ where γ switches cocycles with same values on $\mathrm{Frob}(\ell)$ and τ_ℓ. The result follows. $\square$

3.6 Statement

Recall that the Galois group $G = \mathrm{Gal}(H/K)$ where H is the ring class field of K of conductor c acts on $H^1(H, A_\wp/p)$. We denoted by

$$\hat{G} = \mathrm{Hom}(G, \mu_e)$$

the group of characters of G and by

$$e_\chi = \frac{1}{|G|}\sum_{g\in G}\chi^{-1}(g)g$$

the projector onto the χ-eigenspace given a character χ of $\hat{G}$. We let

$$\delta = \mathrm{red}(y_1) \text{ in } H^1(H, A_\wp/p).$$

Then $e_{\overline{\chi}}\delta$ belongs to the $\overline{\chi}$-eigenspace of $H^1(H, A_\wp/p)$. We recall the statement of the theorem we prove.

Theorem 1.2.1. Assume that p is such that

$$\mathrm{Gal}\left(\mathbb{Q}(A_\wp/p)/\mathbb{Q}\right) \simeq \mathrm{GL}_2(\mathscr{O}_\wp/p), \quad (p, ND\phi(N)) = 1, \text{ and } p \nmid |G|. \tag{3.6}$$

Suppose further that the eigenvalues of $Fr(v)$ acting on $A_\wp^{I_v}$ are not equal to 1 modulo p for v dividing N. Assume $\chi \in \hat{G}$ is such that $e_{\overline{\chi}}\delta$ is non-zero. Then the χ-eigenspace S^χ of the Selmer group S has rank 1 over $\mathscr{O}_\wp/p$.

Set up of the proof. Consider the prime λ of K lying above a prime ℓ inert in $\mathbb{Q}$ and let λ' be a prime of H above λ. The self-duality of $A_\wp/p$ given by

$$A_\wp/p \simeq \mathrm{Hom}(A_\wp/p, \mathbb{Z}/p\mathbb{Z}(1)),$$

where $\mathrm{Hom}(A_\wp/p, \mathbb{Z}/p\mathbb{Z}(1))$ is the Tate dual of $A_\wp/p$ and local Tate duality as explained in Section 2.5 gives a perfect pairing

$$\langle .,. \rangle_{\lambda'} : H^1(H^{ur}_{\lambda'}/H_{\lambda'}, (A_\wp/p)^{I_{\lambda'}}) \times H^1(H^{ur}_{\lambda'}, A_\wp/p) \longrightarrow \mathbb{Z}/p\mathbb{Z},$$

where $I_{\lambda'} = \mathrm{Gal}(\overline{H_{\lambda'}}/H^{ur}_{\lambda'})$ and $\mathscr{O}_\wp$-linear isomorphisms

$$\{H^1(H^{ur}_{\lambda'}, A_\wp/p)\}^{dual} \simeq H^1(H^{ur}_{\lambda'}/H_{\lambda'}, (A_\wp/p)^{I_{\lambda'}}) \simeq (A_\wp/p)^{I_{\lambda'}}/(\phi - 1). \tag{3.7}$$

where ϕ is the arithmetic Frobenius element generating $\mathrm{Gal}(H^{ur}_{\lambda'}/H_{\lambda'})$. Recall that the Selmer group $S \subseteq H^1(H, A_\wp/p)$ consists of the cohomology classes whose localizations lie in $H^1(H^{ur}_v/H_v, A_\wp/p)$ for v not dividing Np and in $H^1_f(H_v, A_\wp/p)$ for v dividing p. Here, $H^1_f(H_v, A_\wp/p)$ is the *finite part* of $H^1(H_v, A_\wp/p)$ as in [9]. We denote by

$$\mathrm{res}_\lambda : H^1(H, A_\wp/p) \longrightarrow \oplus_{\lambda'|\lambda} H^1(H_{\lambda'}, A_\wp/p)$$

the direct sum of the restriction maps from $H^1(H, A_\wp/p)$ to $H^1(H_{\lambda'}, A_\wp/p)$ for λ' dividing λ in H. Restricting res_λ to the Selmer group, we obtain the following map

$$\mathrm{res}_\lambda : S \longrightarrow \oplus_{\lambda'|\lambda} H^1(H^{ur}_{\lambda'}/H_{\lambda'}, (A_\wp/p)^{I_{\lambda'}}).$$

Taking the $(\mathbb{Z}/p)$-linear dual of the previous map and using isomorphism (3.7), we obtain a homorphism

$$\psi_\ell : \oplus_{\lambda'|\lambda} H^1(H^{ur}_{\lambda'}, A_\wp/p) \longrightarrow S^{dual}.$$

Let

$$X_\ell = \mathrm{Im}(\psi_\ell)$$

be the image of ψ_ℓ in S^{dual}. We aim to bound S^{dual} from above by using the Kolyvagin classes $P(n)$ introduced in Section 3.4 to produce explicit elements in the kernel of ψ_ℓ.

3.7 Generating the dual of the Selmer group

Lemma 3.7.1. *We have*

$$H^1(Aut(A_\wp/p), A_\wp/p) = 0.$$

Proof. Sah's lemma [35, 8.8.1] states that if G is a group, M a G-representation, and g an element of Center(G), then the map $x \longrightarrow (g-1)\,x$ is the zero map on $H^1(G,M)$. In our context, since

$$g = 2I \in \mathrm{Aut}(A_\wp/p)$$

belongs to Center$(\mathrm{Aut}(A_\wp/p))$, we have that $g - I = I$ is the zero map on the group $H^1(Aut(A_\wp/p), A_\wp/p)$ and the result follows. □

Proposition 3.7.2. *There exists a prime q such that q is a Kolyvagin prime, and such that*

$$\mathrm{res}_{\beta'} e_{\overline{\chi}} \delta \neq 0,$$

where β' is a prime dividing q in H.

Proof. For the purpose of this proof, we denote the cocycle $e_{\overline{\chi}}\delta$ by c_1 and the Galois group $G(L/H)$ by G. By Proposition 3.4.4, c_1 belongs to $S^{\overline{\chi}}$. The restriction map

$$r : H^1(H, A_\wp/p) \longrightarrow H^1(L, A_\wp/p)^G = \mathrm{Hom}_G(L, A_\wp/p)$$

is injective. Indeed, Proposition 3.4.2 and Proposition 3.7.1 imply that

$$\mathrm{Ker}(r) = H^1(H(A_\wp/p)/H, A_\wp/p) = 0.$$

Consider the evaluation pairing

$$r(S^{\overline{\chi}}) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow A_{\wp}/p$$

and let $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ be the annihilator of $r(S^{\overline{\chi}})$. Let L^S be the extension of L fixed by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ and denote by G_S the Galois group $\mathrm{Gal}(L^S/L)$. We obtain an injective homomorphism of $\mathrm{Gal}(H/\mathbb{Q})$-modules

$$r(S^{\overline{\chi}}) \hookrightarrow \mathrm{Hom}_G(G_S, A_{\wp}/p).$$

We denote by s the image of $r(c_1)$ in $\mathrm{Hom}_G(G_S, A_{\wp}/p)$.

If $s(G_S^+) = 0$, then as s belongs to $S^{\pm}$, we have

$$s : G_S^- \longrightarrow A_{\wp}/p^{\pm},$$

where $A_{\wp}/p^{\pm}$ are the $\pm$ eigenspaces of $A_{\wp}/p$ with respect to the action of τ. On the one hand, the eigenspace $A_{\wp}/p^{\pm}$ is of rank one over $\mathscr{O}_{\wp}/p$. On the other hand, by Proposition 3.4.2 and Assumption (3.6),

$$G = G(L/H) \simeq \mathrm{GL}_2(\mathscr{O}_{\wp}/p).$$

Hence, $A_{\wp}/p^{\pm}$ has no non-trivial G-submodules and $s(G_S^-) = 0$, that is $s = 0$. This is a contradiction because $c_1 \neq 0$ in $S^{\overline{\chi}}$ as c_1 is not divisible by p in $S^{\overline{\chi}}$. As a consequence, we have that $s(G_S^+) \neq 0$, where

$$G_S^+ = G_S^{\tau+1} = \{h^{\tau}h \mid h \text{ in } G_S\} = \{(\tau h)^2 \mid h \text{ in } G_S\}.$$

Therefore, there exists h in G_S such that $c_1((\tau h)^2) \neq 0$. Consider the element τh in $\mathrm{Gal}(L^S/\mathbb{Q})$. Cebotarev's density theorem, (see Chapter 2, Theorem 2.1 for more details) implies the existence of q in $\mathbb{Q}$ such that

$$\mathrm{Frob}_q(L^S/\mathbb{Q}) = \tau h$$

and such that $(q, cpND) = 1$. In particular, q is a Kolyvagin prime since $\mathrm{res}|_L(\tau h) = \tau$. For β in L above q, we have that

$$\mathrm{Frob}_\beta(L^S/L) = (\tau h)^2$$

generates the local extension L^S/L at β. This implies that $\mathrm{res}_{\beta'} c_1$ does not vanish for $\beta' = \beta \cap H$. □

We consider the restriction d of an element c of $H^1(H, A_\wp/p)$ to $H^1(F, A_\wp/p)$. Then d factors through some finite extension $\tilde{F}$ of F. We denote by

$$F(c) = \tilde{F}^{\ker(d)}$$

the subextension of $\tilde{F}$ fixed by $\ker(d)$. Note that $F(c)$ is an extension of F.

Consider the following extensions

$$\begin{tikzcd}
 & I_{01} = I_0 I_1 & \\
I_0 = F(\mathrm{red}(y_{1,\wp}))^{\mathrm{Gal}} \arrow[ur] & & I_1 = F(D_q \mathrm{red}(y_{q,\wp}))^{\mathrm{Gal}} \arrow[ul] \\
 & F = H_q(A_\wp/p) \arrow[ul, "V_0"] \arrow[ur, "V_1"'] \arrow[uu, dashed, "V"] &
\end{tikzcd}$$

where the abbreviation Gal indicates taking Galois closure over $\mathbb{Q}$. We define

$$V_0 = \mathrm{Gal}(I_0/F),\ V_1 = \mathrm{Gal}(I_1/F), \text{ and } V = \mathrm{Gal}(I_0 I_1/F).$$

We have an isomorphism of $\mathrm{Aut}(A_\wp/p)$-modules $V_0 \simeq V_1 \simeq A_\wp/p$. Let

$$I_0^{\overline{\chi}} = F(e_{\overline{\chi}}\mathrm{red}(y_{1,\wp}))^{\mathrm{Gal}} \text{ and } I_1^{\overline{\chi}} = F(e_{\overline{\chi}}D_q red(y_{q,\wp}))^{\mathrm{Gal}}.$$

We denote by $V_0^{\overline{\chi}}$ and $V_1^{\overline{\chi}}$ their respective Galois groups over F. We will show that

$$V^{\overline{\chi}} = \mathrm{Gal}(I_0^{\overline{\chi}} I_1^{\overline{\chi}}/F) \simeq V_0^{\overline{\chi}} \times V_1^{\overline{\chi}}.$$

Proposition 3.7.3. *The extensions $I_0^{\overline{\chi}}$ and $I_1^{\overline{\chi}}$ are linearly disjoint over F.*

Proof. Linearly independent cocycles c_1, c_2 of $H^1(H_q, A_\wp/p)$ over $\mathscr{O}_\wp/p$ can be viewed as linearly independent homomorphisms h_1, h_2 in $\mathrm{Hom}_{\mathrm{Gal}(F/H_q)}(V, A_\wp/p)$ over $\mathscr{O}_\wp/p$. The restriction map

$$H^1(H_q, A_\wp/p)^{\mathrm{Gal}(F/H_q)} \xrightarrow{(r)} H^1(F, A_\wp/p)^{\mathrm{Gal}(F/H_q)}$$

is injective. Indeed, combining Proposition 3.4.2 with Proposition 3.7.1 that implies that

$$H^1(K(A_\wp/p)/K, A_\wp/p) = 0,$$

we obtain that

$$\mathrm{Ker}(r) = H^1(F/H_q, A_\wp/p) = 0.$$

Furthermore, cocycles of $H^1(F, A_\wp/p)^{\mathrm{Gal}(F/H_q)}$ factor through

$$H^1(I_{01}/F, A_\wp/p)^{\mathrm{Gal}(F/H_q)} = \mathrm{Hom}_{\mathrm{Gal}(F/H_q)}(I_{01}/F, A_\wp/p).$$

Consider the extension $I_0^{\overline{\chi}} \cap I_1^{\overline{\chi}}$ of F. It is a $\mathrm{Gal}(F/H_q)$-submodule of $A_{\wp}/p$. The hypothesis $\mathrm{res}_{\beta'} e_{\overline{\chi}} \mathrm{red}(y_{1,\wp}) \neq 0$ implies that

$$\mathrm{res}_{\beta'} e_{\overline{\chi}} \mathrm{red}(D_q y_{q,\wp}) \neq 0$$

by (3.3.2). On the one hand, since $\mathrm{res}_{\beta'} e_{\overline{\chi}} \mathrm{red}(D_q y_{q,\wp})$ is ramified, $e_{\overline{\chi}} D_q \mathrm{red}(y_{q,\wp})$ does not belong to $S^{\overline{\chi}}$. On the other hand, $e_{\overline{\chi}} \mathrm{red}(y_{1,\wp}) \neq 0$ belongs to $S^{\overline{\chi}}$ by Proposition 3.4.4. Therefore $I_0^{\overline{\chi}} \cap I_1^{\overline{\chi}} = 0$ since $A_{\wp}/p$ is a simple $\mathrm{Gal}(F/H_q)$-module. Note that the cocycles c_1 and c_2 cannot be linearly dependent either since one of them belongs to $S^{\overline{\chi}}$ while the other one does not. $\square$

For a subset $U \subseteq V$, we denote by

$$L(U) = \{\ell \text{ rational prime } | \mathrm{Frob}_\ell(I_{01}/\mathbb{Q}) = [\tau u], u \in U\}.$$

Note that a rational prime ℓ in $L(U)$ is a Kolyvagin prime as

$$\mathrm{Frob}_\ell(H(A_{\wp}/p)/\mathbb{Q}) = \mathrm{res}|_{H(A_{\wp}/p)} \mathrm{Frob}_\ell(I_{01}/\mathbb{Q}) = \tau$$

since $u \in U$. In fact, it satisfies

$$\mathrm{Frob}_\ell(H_q(A_{\wp}/p)/\mathbb{Q}) = \mathrm{res}|_{H_q(A_{\wp}/p)} \mathrm{Frob}_\ell(I_{01}/\mathbb{Q}) = \tau.$$

Hence, a prime above ℓ in H splits completely in H_q. Indeed, it lies in the kernel of the Artin map because of the Frobenius condition

$$\mathrm{Frob}_\ell(H_q/H) = \tau^{|D(H/\mathbb{Q})|} = \tau^2 = Id,$$

where $|D(H/\mathbb{Q})|$ is the order of the decomposition group $D(H/\mathbb{Q})$, also the order of the residue extension. Similarly, a prime above ℓ in H_q splits completely in $H_q(A_\wp/p)$; it lies in the kernel of the Artin map because of the Frobenius condition

$$\mathrm{Frob}_\ell(H_q(A_\wp/p)/H_q) = \tau^{|D(H_q/\mathbb{Q})|} = \tau^2 = Id.$$

Proposition 3.7.4. *Assume U^+ generates V^+. Then $\{X_\ell\}_{\ell\in L(U)}$ generates S^{dual}.*

Proof. The proof consists of the following steps:

1. An element s of S can be identified with an element h of $\mathrm{Hom}_G(F, A_\wp/p)$.

2. To show the statement of the theorem, it is enough to show that $\mathrm{res}_\lambda(s) = 0$ for all $\ell \in L(U)$ implies $s = 0$.

3. The assumption $\mathrm{res}_\lambda(s) = 0$ for all $\ell \in L(U)$ implies that h vanishes on U^+.

4. The assumption U^+ generates V^+ implies $h = s = 0$.

1. Let s be an element of S. For the purpose of this proof, we denote

$$G = \mathrm{Gal}(H(A_\wp/p)/H) \simeq \mathrm{GL}_2(\mathscr{O}_\wp/p).$$

We denote by h the image of s by restriction in

$$H^1(F, A_\wp/p)^G \subset \mathrm{Hom}_G(\mathrm{Gal}(\overline{F}/F), A_\wp/p).$$

Here, restriction can be viewed as the composition of the following two restriction maps

$$H^1(H, A_\wp/p) \xrightarrow{(r_1)} H^1(H(A_\wp/p), A_\wp/p)^G \xrightarrow{(r_2)} H^1(F, A_\wp/p)^G.$$

Combining Proposition 3.4.2 and 3.7.1 we obtain that

$$\mathrm{Ker}(r_1) = H^1(H(A_\wp/p)/H, A_\wp/p) = 0.$$

By Proposition 3.4.2, we have

$$\mathrm{Gal}(H_q(A_\wp/p)/H(A_\wp/p)) \simeq \mathrm{Gal}(H_q/H) \simeq \mathbb{Z}/(q+1)\mathbb{Z}.$$

On the one hand, the group G acts trivially on $\mathrm{Gal}(H_q(A_\wp/p)/H(A_\wp/p))$. On the other hand, $A_\wp/p$ is simple as a G-module. Hence,

$$\mathrm{Ker}(r_2) = \mathrm{Hom}_G(\mathrm{Gal}(F/H(A_\wp/p)), A_\wp/p) \simeq \mathrm{Hom}_G(H_q/H, A_\wp/p) = 0$$

since such a G-homomorphism maps an element of $\mathrm{Gal}(H_q/H)$ to a G-invariant element of $A_\wp/p$, that is, to 0.

2. By Isomorphism (3.7), local Tate duality identifies $\oplus_{\lambda'|\lambda} H^1(H_{\lambda'}^{ur}, A_\wp/p)$ with

$$\oplus_{\lambda'|\lambda} H^1(H_{\lambda'}^{ur}/H_{\lambda'}, (A_\wp/p)^{I_{\lambda'}}).$$

So if we show that

$$\{\mathrm{res}_\lambda\}_{\ell\in L(U)} : S \longrightarrow \{\oplus_{\lambda'|\lambda} H^1(H_{\lambda'}^{ur}/H_{\lambda'}, (A_\wp/p)^{I_{\lambda'}})\}_{\ell\in L(U)}$$

is injective, then the induced map between the duals

$$\{\oplus_{\lambda'|\lambda} H^1(H_{\lambda'}^{ur}, A_\wp/p)\}_{\ell\in L(U)} \longrightarrow S^{dual}$$

would be surjective. Hence, it is enough to show that $\mathrm{res}_\lambda(s) = 0$ for all $\ell \in L(U)$ implies $s = 0$.

3. Consider $\tilde{I_{01}}$, the minimal Galois extension of $\mathbb{Q}$ containing I_{01} such that h factors through $\mathrm{Gal}(\tilde{I_{01}}/F)$. Let x be an element of $\mathrm{Gal}(\tilde{I_{01}}/F)$ such that $x|_{I_{01}}$ belongs to U. By Cebotarev's density theorem, there exists ℓ in $L(U)$ such that $\mathrm{Frob}_\ell(\tilde{I_{01}}/\mathbb{Q}) = [\tau x]$. The hypothesis $\mathrm{res}_\lambda(s) = 0$ implies that $h(\mathrm{Frob}_{\lambda''}(\tilde{I_{01}}/F)) = 0$ for λ'' above ℓ in F since $\mathrm{Frob}_{\lambda''}(\tilde{I_{01}}/F)$ is a generator of the local extension of $\mathrm{Gal}(\tilde{I_{01}}/F)$ at λ''. In fact,

$$\mathrm{Frob}_{\lambda''}(\tilde{I_{01}}/F) = (\tau x)^{|D(F/\mathbb{Q})|} = (\tau x)^2 = x^\tau x = 2x^+,$$

where $|D(F/\mathbb{Q})|$ is the order of the decomposition group $D(F/\mathbb{Q})$, and is also the order of the residue extension and $x^+ = \frac{1}{2}x^\tau x$. Therefore, $h(x^+) = 0$ for all $x \in \mathrm{Gal}(\tilde{I_{01}}/F)$ such that $x|_{I_{01}}$ belongs to U.

4. The hypothesis U^+ generates V^+ then implies that h vanishes on $\mathrm{Gal}(\tilde{I_{01}}/F)^+$. Hence, $\mathrm{Im}(h)$ lies in $A_\wp/p^-$, the minus eigenspace of $A_\wp/p$ for the action of τ which is a free $\mathcal{O}_\wp/p$-module of rank 1. In particular, it cannot be a proper non-trivial G-submodule of $A_\wp/p$. Therefore, $h = 0$ which implies $s = 0$.

$\square$

Next, we study the action of complex conjugation on the χ-component of the cocycles $y_{q,\wp}$.

Proposition 3.7.5. *There is an element σ_0 in $\mathrm{Gal}(H_q/K)$ such that*

$$\tau e_\chi y_{q,\wp} = \varepsilon\overline{\chi}(\sigma_0) e_{\overline{\chi}} y_{q,\wp},$$

where $-\varepsilon$ is the sign of the functional equation of $L(f,s)$.

Proof. [39, proposition 6.2] that uses a result in [26] states that

$$\tau y_{q,\wp} = \varepsilon \sigma_0 y_{q,\wp} \tag{3.8}$$

for some σ_0 in $\mathrm{Gal}(H_q/K)$. Since τ acts on an element g of G by

$$\tau g \tau^{-1} = g^{-1},$$

we have

$$\tau e_\chi = \frac{1}{|G|}\sum_{g\in G} \tau \chi^{-1}(g) g = \frac{1}{|G|}\sum_{g\in G} \chi(g^{-1}) g^{-1}\tau = \frac{1}{|G|}\sum_{g\in G} \overline{\chi}^{-1}(g^{-1}) g^{-1}\tau = e_{\overline{\chi}}\tau.$$

Also,

$$e_{\overline{\chi}}\sigma_0 = \frac{1}{|G|}\sum_{g\in G} \overline{\chi}^{-1}(g)\sigma_0 g = \frac{1}{|G|}\sum_{g\in G} \overline{\chi}(\sigma_0)\overline{\chi}^{-1}(\sigma_0 g)\sigma_0 g = \overline{\chi}(\sigma_0) e_{\overline{\chi}}.$$

Therefore, applying $e_{\overline{\chi}}$ to Equation (3.8) yields

$$\tau e_\chi y_{q,\wp} = \varepsilon \overline{\chi}(\sigma_0) e_{\overline{\chi}} y_{q,\wp}.$$

□

Let us look at the action of complex conjugation on $V^{\overline{\chi}} = V_0^{\overline{\chi}} V_1^{\overline{\chi}}$. For (v_0, v_1) in $V_0 V_1$, we use the identity $\tau D_q = -D_q \tau \mod p$ to obtain

$$\tau v_0 \tau(e_{\overline{\chi}} y_{1,\wp}) = \varepsilon \chi(\sigma_0) \tau v_0 (e_\chi y_{1,\wp}).$$

$$\tau v_1 \tau(e_{\overline{\chi}} D_q y_{q,\wp}) = -\tau v_1 D_q \tau(e_{\overline{\chi}} y_{q,\wp}) = -\varepsilon \chi(\sigma_0) \tau v_1 (e_\chi D_q y_{q,\wp}).$$

When $\chi = \overline{\chi}$, for (x,y) in $V_0^{\overline{\chi}} V_1^{\overline{\chi}}$,

$$\tau(x,y)\tau = (\varepsilon\chi(\sigma_0)\tau x, -\varepsilon\chi(\sigma_0)\tau y).$$

In this case, we define

$$U = \{(x,y) \text{ in } V_0 \times V_1 | \varepsilon\overline{\chi}(\sigma_0)\tau x + x, -\varepsilon\overline{\chi}(\sigma_0)\tau y + y \text{ generate } A_{\wp}/p\}.$$

When $\chi \neq \overline{\chi}$, for (x,y,z,w) in $V_0^{\chi} V_0^{\overline{\chi}} V_1^{\chi} V_1^{\overline{\chi}} = V$,

$$\tau(x,y,z,w)\tau = (\varepsilon\overline{\chi}(\sigma_0)\tau y, \varepsilon\chi(\sigma_0)\tau x, -\varepsilon\overline{\chi}(\sigma_0)\tau w, -\varepsilon\chi(\sigma_0)\tau z).$$

In this case, we define

$$U = \{(x,y,z,w) \text{ in } V_0^{\chi} V_0^{\overline{\chi}} V_1^{\chi} V_1^{\overline{\chi}} | \varepsilon\chi(\sigma_0)\tau x + y, -\varepsilon\overline{\chi}(\sigma_0)\tau z + w \text{ generate } A_{\wp}/p\}.$$

In both cases, Proposition 3.7.3 and Congruence (3.1) imply that U^+ generates

$$V^+ \simeq V_0^+ \times V_1^+ \simeq \mathscr{O}_{\wp}/p \times \mathscr{O}_{\wp}/p \simeq A_{\wp}/p.$$

Let ℓ be a prime in $L(U)$, and let λ be the prime of K lying above it.

Proposition 3.7.6. *The elements*

$$\mathrm{res}_{\lambda} e_{\overline{\chi}} P(\ell) \textit{ and } \mathrm{res}_{\lambda} e_{\overline{\chi}} P(\ell q)$$

generate $\oplus_{\lambda'|\lambda} H^1(H_{\lambda'}^{ur}, A_{\wp}/p)^{\overline{\chi}}$.

Proof. We have

$$\oplus_{\lambda'|\lambda} H^1(H_{\lambda'}^{ur}, A_{\wp}/p)^{\overline{\chi}} \simeq \oplus_{\lambda'|\lambda} \left((A_{\wp}/p)^{I_{\lambda'}}/(\phi - 1)\right)^{\overline{\chi}}$$

since the former is isomorphic to its dual by Isomorphism (3.7). The module

$$\oplus_{\lambda'|\lambda}\left((A_{\wp}/p)^{I_{\lambda'}}/(\phi-1)\right)^{\overline{\chi}}$$

is of rank at most 2 over $\mathscr{O}_{\wp}/p$, hence, so is $\oplus_{\lambda'|\lambda}H^1(H^{ur}_{\lambda'},A_{\wp}/p)^{\overline{\chi}}$. The Frobenius condition on ℓ implies that

$$\mathrm{res}_\lambda e_{\overline{\chi}}\mathrm{red}(y_{1,\wp}) \text{ and } \mathrm{res}_\lambda e_{\overline{\chi}}D_q\mathrm{red}(y_{q,\wp})$$

are linearly independent over $\oplus_{\lambda'|\lambda}A_{\wp}/p$. Indeed, if they were linearly dependent then, in the case $\chi=\overline{\chi}$,

$$(\mathrm{res}_\lambda e_{\overline{\chi}}\mathrm{red}(y_{1,\wp}))^{(\tau x)^2}-\mathrm{res}_\lambda e_{\overline{\chi}}\mathrm{red}(y_{1,\wp})$$
$$\text{and } (\mathrm{res}_\lambda e_{\overline{\chi}}D_q red(y_{q,\wp}))^{(\tau y)^2}-\mathrm{res}_\lambda e_{\overline{\chi}}D_q\mathrm{red}(y_{q,\wp})$$

where $\mathrm{Frob}_\ell(I_{01}/\mathbb{Q})=\tau u=(\tau x,\tau y)$ would also be linearly dependent. The Frobenius condition implies that

$$\mathrm{Frob}_\ell(I_0^{\overline{\chi}}/F)=x^\tau x=(\tau x)^2 \text{ and } \mathrm{Frob}_\ell(I_1^{\overline{\chi}}/F)=y^\tau y=(\tau y)^2$$

generate $A_{\wp}/p$, which yields a contradiction as $(\tau x)^2$ acts on the element $\mathrm{res}_\lambda e_{\overline{\chi}}\mathrm{red}(y_{1,\wp})$ generating the local extension of $I_0^{\overline{\chi}}$ over F by

$$(\mathrm{res}_\lambda e_{\overline{\chi}}\mathrm{red}(y_{1,\wp}))^{(\tau x)^2}-\mathrm{res}_\lambda e_{\overline{\chi}}\mathrm{red}(y_{1,\wp})$$

and $(\tau y)^2$ acts on the element $\mathrm{res}_\lambda e_{\overline{\chi}}D_q red(y_{q,\wp})$ generating the local extension of $I_1^{\overline{\chi}}$ over F by

$$\mathrm{res}_\lambda e_{\overline{\chi}}D_q red(y_{q,\wp}))^{(\tau y)^2}-\mathrm{res}_\lambda e_{\overline{\chi}}D_q\mathrm{red}(y_{q,\wp}).$$

Similarly, in the case $\chi \neq \overline{\chi}$,

$$(\mathrm{res}_\lambda e_{\overline{\chi}} \mathrm{red}(y_{1,\wp}))^{x^\tau y} - \mathrm{res}_\lambda e_{\overline{\chi}} \mathrm{red}(y_{1,\wp})$$
$$\text{and } (\mathrm{res}_\lambda e_{\overline{\chi}} D_q \mathrm{red}(y_{q,\wp}))^{z^\tau w} - \mathrm{res}_\lambda e_{\overline{\chi}} D_q \mathrm{red}(y_{q,\wp})$$

where $\mathrm{Frob}_\ell(I_{01}/\mathbb{Q}) = \tau u = (\tau x, \tau y, \tau z, \tau w)$ would also be linearly dependent. The Frobenius condition implies that

$$\mathrm{Frob}_\ell(I_0^{\overline{\chi}}/F) = x^\tau y = (\tau x)(\tau y) \text{ and } \mathrm{Frob}_\ell(I_1^{\overline{\chi}}/F) = z^\tau w = (\tau z)(\tau w)$$

generate $A_\wp/p$, which yields a contradiction.

Equation (3.3) implies that if $\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell q)$ and $\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell)$ were linearly dependent then

$$\mathrm{res}_\lambda e_{\overline{\chi}} P(q) = \mathrm{res}_\lambda e_{\overline{\chi}} D_q \mathrm{red} y_{q,\wp} \text{ and } \mathrm{res}_\lambda e_{\overline{\chi}} P(1) = \mathrm{res}_\lambda e_{\overline{\chi}} \mathrm{red} y_{1,\wp}$$

would be linearly dependent as well. □

3.8 Bounding the size of the dual of the Selmer group

In what follows, we study the modules $X_\ell^{\overline{\chi}}$ for ℓ in $L(U)$.

Proposition 3.8.1. *We have*

$$\sum_{\lambda' | \ell | n} \langle s_{\lambda'}, \mathrm{res}_{\lambda'} P(n) \rangle_{\lambda'} = 0.$$

Proof. The proof follows [39, proposition 11.2(2)] where both the reciprocity law, (see Chapter 2, Section 2.4 for more details) and the local ramification properties of $P(n)$ in Proposition 3.4.4 are used. □

Proposition 3.8.2. *The element $\psi_\ell(\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell q))$ generates $X_\ell^{\overline{\chi}}$ over $O_\wp/p$ for ℓ in $L(U)$.*

Proof. The image of $\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell)$ by the map

$$\psi_\ell : \oplus_{\lambda'|\lambda} H^1(H^{ur}_{\lambda'}, A_\wp/p)^{\overline{\chi}} \longrightarrow X_\ell^{\overline{\chi}}$$

is the homomorphism from $S^{\overline{\chi}}$ to $\mathbb{Z}/p$ given by:

$$e_{\overline{\chi}} s \mapsto \sum_{\lambda'|\lambda} \langle e_{\overline{\chi}} s_{\lambda'}, e_{\overline{\chi}} P(\ell)_{\lambda'} \rangle_{\lambda'}.$$

Proposition 3.8.1 implies that

$$\sum_{\lambda'|\lambda} \langle e_{\overline{\chi}} s_{\lambda'}, e_{\overline{\chi}} P(\ell)_{\lambda'} \rangle_{\lambda'} = 0.$$

Hence, the image by ψ_ℓ of $\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell)$, one of the two generators of

$$\oplus_{\lambda'|\lambda} H^1(H^{ur}_{\lambda'}, A_\wp/p)^{\overline{\chi}}$$

by Proposition 3.7.6, is trivial. $\square$

Proposition 3.8.3. *The modules $X_\ell^{\overline{\chi}}$ that are non-zero are all equal for $\ell \in L(U)$.*

Proof. Proposition 3.8.1 implies that

$$\sum_{\lambda'|\lambda} \langle e_{\overline{\chi}} s_{\lambda'}, e_{\overline{\chi}} P(\ell q)_{\lambda'} \rangle + \sum_{\beta'|\beta} \langle e_{\overline{\chi}} s_{\beta'}, e_{\overline{\chi}} P(\ell q)_{\beta'} \rangle = 0.$$

Hence,

$$\psi_\ell(\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell q)) + \psi_q(\mathrm{res}_\beta e_{\overline{\chi}} P(\ell q)) = 0.$$

If $\psi_\ell(\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell q)) = 0$, then by Proposition 3.8.2, $X_\ell^{\overline{\chi}} = 0$. Otherwise, since

$$\psi_\ell(\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell q))$$

generates $X_\ell^{\overline{\chi}}$ over $\mathscr{O}_\wp/p$, we have that

$$-\psi_\ell(\mathrm{res}_\lambda e_{\overline{\chi}} P(\ell q)) = \psi_q(\mathrm{res}_\beta e_{\overline{\chi}} P(\ell q)) \in X_q^{\overline{\chi}}$$

is non-zero. Therefore, the non-trivial element $\psi_q(\mathrm{res}_\beta e_{\overline{\chi}} P(\ell q))$ generates a rank 1 module $X_q^{\overline{\chi}}$ over $\mathscr{O}_\wp/p$ and $X_\ell^{\overline{\chi}} = X_q^{\overline{\chi}}$. □

In what follows, we prove theorem 1.2.1.

Proof. By Proposition 3.7.4, the set $\{X_\ell^{\overline{\chi}}\}$ generates $S^{dual,\overline{\chi}}$ as ℓ ranges over $L(U)$. Hence, the set $\{X_\ell^{\overline{\chi}}\}$ generates $S^{dual,\overline{\chi}}$ as ℓ ranges over $L(U)$, where, by Proposition 3.8.2, the modules $X_\ell^{\overline{\chi}}$ that are non-zero are of rank 1 over $\mathscr{O}_\wp/p$ and are all equal. Hence, $\mathrm{rank}(S^\chi) \leq 1$. Also, $e_\chi \mathrm{red}(y_{1,\wp})$ belongs to S^χ by Proposition 3.4.4 and is not divisible by p in S^χ. Indeed, this follows from the hypothesis on $e_{\overline{\chi}}\mathrm{red}(y_{1,\wp})$ and Proposition 3.7.5 where $\overline{\chi}(\sigma_0)$ is a root of unity since $\mathrm{Gal}(H/K)$ is a finite group. This implies that $\mathrm{rank}(S^\chi) \geq 1$. Therefore,

$$\mathrm{rank}(S^\chi) = \mathrm{rank}(S^{dual,\overline{\chi}}) = 1.$$

□

Remark 3.8.4. Because the p-adic Abel-Jacobi map factors through the Selmer group, (see [39, Proposition 11.2.1] for a proof)

$$\Phi^\chi : \mathrm{CH}^r(W_{2r-2}/H)_0^\chi \otimes \mathscr{O}_\wp/p\mathscr{O}_\wp \longrightarrow S^\chi,$$

Theorem 1.2.1 implies that $\mathrm{rank}_{\mathscr{O}_\wp/p}(\mathrm{Im}(\Phi^\chi)) = 1$.

Remark 3.8.5. In Kolyvagin's argument for elliptic curves E over $\mathbb{Q}$ and certain imaginary quadratic fields K, the non- triviality of the Heegner point y_K in $E(K)/pE(K)$ for suitable primes p immediately implied the non-triviality of y_K in $\mathrm{Sel}_p(E/K)$. In our situation, even though the p-adic Abel-Jacobi map is conjectured to be injective, it is non-trivial to check whether a non-trivial Heegner cycle in the Chow group has non-trivial image in $H^1(H, A_{\wp}/p)$.

CHAPTER 4
On the Selmer group attached to a modular form and an algebraic Hecke character

4.1 Introduction

Kolyvagin [34, 27] constructs an Euler system based on Heegner points and uses it to bound the size of the Selmer group of certain (modular) elliptic curves E over imaginary quadratic fields K assuming the non-vanishing of a suitable Heegner point. In particular, this implies that

$$\mathrm{rank}(E(K)) = 1,$$

and the Tate-Shafarevich group $Ш(E/K)$ is finite. Bertolini and Darmon adapt Kolyvagin's descent to Mordell-Weil groups over ring class fields [3]. More precisely, they show that for a given character χ of $\mathrm{Gal}(K_c/K)$ where K_c is the ring class field of K of conductor c,

$$\mathrm{rank}(E(K_c)^{\chi}) = 1$$

assuming that the projection of a suitable Heegner point is non-zero. Nekovář [39] adapts the method of Euler systems to modular forms of higher even weight to describe the image by the Abel-Jacobi map Φ of Heegner cycles on the associated Kuga-Sato varieties, hence showing that

$$\dim_{\mathbb{Q}_p}(\mathrm{Im}(\Phi) \otimes \mathbb{Q}_p) = 1$$

assuming the non-vanishing of a suitable Heegner cycle. In Chapter 3, we combined these two approaches to study modular forms of higher even weight twisted by ring class characters of imaginary quadratic fields and showed that

$$\dim_{\mathbb{Q}_p}(\mathrm{Im}(\Phi)\otimes\mathbb{Q}_p)=1$$

assuming the non-vanishing of a suitable generalized Heegner cycle. In this chapter, we study the Selmer group associated to a modular form of even weight $r+2$ and an unramified algebraic Hecke character ψ of infinity type $(r,0)$. The case of a Hecke character of infinity type $(0,0)$ corresponds to the setting of Nekovář's work [39] and its generalization in Chapter 3. Our setting involves the *generalized Heegner cycles* introduced by Bertolini, Darmon and Prasanna in [5].

Our motivation stems from the Beilinson-Bloch conjecture that predicts that

$$\dim_{\mathbb{Q}}(\mathrm{Im}(\Phi)\otimes\mathbb{Q})=ord_{s=r+1}L(f\otimes\theta_\psi,s),$$

where θ_ψ is the theta series associated to ψ [44, 32].

Let f be a normalized newform of level $\Gamma_0(N)$ where $N\geq 5$ and even weight $r+2>2$. Denote by $K=\mathbb{Q}(\sqrt{-D})$ an imaginary quadratic field with odd discriminant satisfying the Heegner hypothesis, that is primes dividing N split in K. For simplicity, we assume that $|\mathscr{O}_K^\times|=2$. Let

$$\psi:\mathbb{A}_K^\times\longrightarrow\mathbb{C}^\times$$

be an unramified algebraic Hecke character of K of infinity type $(r,0)$. Then there is an elliptic curve A defined over the Hilbert class field K_1 of K with complex multiplication by $\mathscr{O}_K$ such that ψ is the Hecke character associated to A by [25, Theorem 9.1.3]. Furthermore, A is a $\mathbb{Q}$-curve by the assumption on the parity of D, that is A is K_1- isogenous to its conjugates in $\mathrm{Aut}(K_1)$. (See [25, Section 11]). Consider a prime p not dividing

$ND\phi(N)N_A$, where N_A is the conductor of A. We denote by V_f the f-isotypic part of the p-adic étale realization of the motive associated to f by Scholl [46] and Deligne [18] twisted by $\frac{r+2}{2}$ and by V_ψ the p-adic étale realization of the motive associated to ψ twisted by $\frac{r}{2}$. More precisely, V_ψ is the ψ-isotypic component of

$$\mathrm{res}_{K_1/\mathbb{Q}}(A) = \prod_{\sigma \in \mathrm{Gal}(K_1/\mathbb{Q})} A^\sigma$$

where A^σ is the σ-conjugate of A, (see Section 4.2 for more details). Let $\mathscr{O}_F$ be the ring of integers of

$$F = \mathbb{Q}(a_1, a_2, \cdots, b_1, b_2, \cdots),$$

where the a_i's are the coefficients of f and the b_i's are the coefficients of the theta series

$$\theta_\psi = \sum_{a \subset \mathscr{O}_K} \psi(a) q^{N(a)}$$

associated to ψ. Then V_f and V_ψ will be viewed (by extending scalars appropriately) as free $\mathscr{O}_F \otimes \mathbb{Z}_p$-modules of rank 2. We denote by

$$V = V_f \otimes_{\mathscr{O}_F \otimes \mathbb{Z}_p} V_\psi$$

the p-adic étale realization of the tensor product of V_f and V_ψ and let $V_\wp$ be its localization at a prime $\wp$ in F dividing p. Then $V_\wp$ is a four dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in

$$\mathrm{End}(A/\mathbb{Q}) = \oplus_{\sigma \in \mathrm{Gal}(H/\mathbb{Q})} \mathrm{Hom}(A, A^\sigma),$$

(see Section 4.2). We also denote by $\mathscr{O}_{F,\wp}$ the localization of $\mathscr{O}_F$ at $\wp$.

By the Heegner hypothesis, there is an ideal $\mathscr{N}$ of $\mathscr{O}_K$ satisfying

$$\mathscr{O}_K/\mathscr{N} = \mathbb{Z}/N\mathbb{Z}.$$

We can therefore fix $\Gamma_1(N)$ level structure on A, that is a point of exact order N defined over the ray class field L_1 of K of conductor $\mathscr{N}$. Consider a pair (φ_1, A_1) where A_1 is an elliptic curve defined over K_1 with level N structure and

$$\varphi_1 : A \longrightarrow A_1$$

is an isogeny over $\overline{K}$. We associate to it a codimension $r+1$ cycle on V

$$\Upsilon_{\varphi_1} = Graph(\varphi_1)^r \subset (A \times A_1)^r \simeq (A_1)^r \times A^r$$

and define a *generalized Heegner cycle* of conductor 1

$$\Delta_{\varphi_1} = e_r \Upsilon_{\varphi_1},$$

where e_r is an appropriate projector (4.1). Then Δ_{φ_1} is defined over L_1. We consider the corestriction

$$P(1) = cor_{L_1,K}\Phi(\Delta_{\varphi_1}) \in H^1(K, V_\wp/p)$$

where Φ is the p-adic étale Abel-Jacobi map. The Selmer group

$$S \subseteq H^1(K, V_\wp/p)$$

consists of the cohomology classes which localizations at a prime v of K lie in

$$\begin{cases} H^1(K_v^{ur}/K_v, V_{\wp}/p) \text{ for } v \text{ not dividing } NN_A p \\ H^1_f(K_v, V_{\wp}/p) \text{ for } v \text{ dividing } p \end{cases}$$

where K_v is the completion of K at v, and

$$H^1_f(K_v, V_{\wp}/p) = H^1_{cris}(K_v, V_{\wp}/p)$$

is the *finite part* of $H^1(K_v, V_{\wp}/p)$ [9]. Note that the assumptions we make will ensure that $H^1(K_v^{ur}/K_v, V_{\wp}/p) = 0$ for v dividing NN_A. We denote by $Fr(v)$ the arithmetic Frobenius element generating $\mathrm{Gal}(K_v^{ur}/K_v)$, and by $I_v = \mathrm{Gal}(\overline{K_v}/K_v^{ur})$.

Theorem 1.3.1. Let p be such that

$$\mathrm{Gal}\left(K(V_{\wp}/p)/K\right) \simeq \mathrm{Aut}_K(V_{\wp}/p), \text{ and } (p, ND\phi(N)N_A) = 1.$$

Suppose that $V_{\wp}/p$ is a simple $\mathrm{Aut}_K(V_{\wp}/p)$-module. Suppose further that the eigenvalues of $Fr(v)$ acting on $V_{\wp}^{I_v}$ are not equal to 1 modulo p for v dividing NN_A. Assume $P(1) \neq 0$ in $H^1(K, V_{\wp}/p)$. Then the Selmer group S has rank 1 over $\mathscr{O}_{F,\wp}/p$.

To prove Theorem 1.3.1, we first consider the p-adic étale realization of the twisted motive V associated to f and ψ in the middle étale cohomology of the associated Kuga-Sato varieties. This provides us with a p-adic Abel-Jacobi map that lands in the Selmer group S. Next, we construct an Euler system of generalized Heegner cycles which where first considered by Bertolini, Darmon and Prasanna in[5]. These algebraic cycles lie in the domain of the p-adic Abel Jacobi map. In order to bound the rank of the Selmer group S, we apply Kolyvagin's descent using local Tate duality, the local reciprocity law, an appropriate global pairing of S and Cebotarev's density theorem.

Our development is an adaptation of Nekovář's techniques [39] and Gross' exposition of Kolyvagin's method of Euler systems [27]. The main novelty is that the algebraic Hecke character ψ is of infinite type. In particular, the Galois representation associated to V is four-dimensional.

4.2 Motive associated to a modular form and a Hecke character

In this section, we describe the construction of the four dimensional $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation

$$V_{\wp} = (V_f \otimes_{\mathscr{O}_F \otimes \mathbb{Z}_p} V_{\psi})_{\wp},$$

where $\wp$ is a prime of F dividing p.

Denote by $Y_1(N)$ the affine modular curve over $\mathbb{Q}$ parametrising elliptic curves with level $\Gamma_1(N)$. Let $j : Y_1(N) \hookrightarrow X_1(N)$ be its proper compact desingularization classifying generalized elliptic curves of level $\Gamma_1(N)$.. The assumption $N \geq 5$ allows for the definition of the generalized universal elliptic curve $\pi : \mathscr{E} \longrightarrow X_1(N)$. Denote by W_r the Kuga-Sato variety of dimension $r+1$, that is a compact desingularization of the r-fold fiber product of $\mathscr{E}$ over $X_1(N)$. We let W be the $2r+1$-dimensional variety defined by

$$W = W_r \times A^r.$$

We denote by $[\alpha]$ the element of $\mathrm{End}_{K_1}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ corresponding to an element α of K. Consider the projectors

$$e_A^{(1)} = \left(\frac{\sqrt{-D}+[\sqrt{-D}]}{2\sqrt{-D}}\right)^{\otimes r} + \left(\frac{\sqrt{-D}-[\sqrt{-D}]}{2\sqrt{-D}}\right)^{\otimes r}, \; e_A^{(2)} = \left(\frac{1-[-1]}{2}\right)^{\otimes r}$$

and

$$e_A = e_A^{(1)} \circ e_A^{(2)}$$

in $\mathbb{Q}[\mathrm{End}(A)]^r$. These projectors $e_A^{(1)}$, $e_A^{(2)}$ and e_A belong to the group of correspondences $\mathrm{Corr}^0(A,A)_{\mathbb{Q}}$ from A to itself, (see [4, Section 2] for more details). Let

$$\Gamma_r = (\mathbb{Z}/N \rtimes \mu_2)^r \rtimes \Sigma_r$$

where $\mu_2 = \{\pm 1\}$ and Σ_r is the symmetric group on r elements. Then Γ_r acts on W_r, (see [46, Sections 1.1.0,1.1.1] for more details.) The projector e_W in $\mathbb{Z}\left[\frac{1}{2Nr!}\right][\Gamma_r]$ associated to Γ_r, called Scholl's projector, belongs to the group of zero correspondences $\mathrm{Corr}^0(W_r,W_r)_{\mathbb{Q}}$ from W_r to itself over $\mathbb{Q}$, (see [4, Section 2.1]). Recall that the hypothesis $(r!,p)=1$ is not necessary by a combination of the work of Tsuji [54] on p-adic comparison theorems and Saito [43] on the Weight-Monodromy conjecture for Kuga-Sato varieties. Let

$$e_r = e_W e_A, \tag{4.1}$$

be the projector in the group of zero correspondences $\mathrm{Corr}^0(W,W))_{\mathbb{Q}}$ from W to itself over $\mathbb{Q}$. We consider the sheafs

$$\mathscr{F} = j_* Sym^r(R^1\pi_*\mathbb{Z}_p) \text{ and } \mathscr{F}_A = j_* Sym^r(R^1\pi_*\mathbb{Z}_p) \otimes e_A H^r_{et}(\overline{A^r},\mathbb{Z}_p).$$

Proposition 4.2.1. *The étale cohomology group*

$$H^1_{et}(X_1(N)\otimes\overline{\mathbb{Q}},\mathscr{F}_A)$$

is isomorphic to

$$e_r H^{2r+1}_{et}(\overline{W}\otimes\overline{\mathbb{Q}},\mathbb{Z}_p) = e_r \oplus_{i=0}^{r+1} H^i_{et}(\overline{W}\otimes\overline{\mathbb{Q}},\mathbb{Z}_p)$$

and

$$H^1_{et}(X_1(N)\otimes\overline{\mathbb{Q}},\mathscr{F})\otimes e_A H^r_{et}(\overline{A^r},\mathbb{Z}_p).$$

Proof. The proof is a combination of [46, theorem 1.2.1] and [5, proposition 2.4]. Note that the proof in [46, theorem 1.2.1] involves $\mathbb{Q}_p$ coefficients but it is still valid in our setting, (see the Remark following [39, Proposition 2.1]). $\square$

Let $B=\Gamma_0(N)/\Gamma_1(N)$. We define

$$\widetilde{V}=e_B H^1_{et}(X_1(N)\otimes\overline{\mathbb{Q}},\mathscr{F})(r+1)$$

where $e_B=\frac{1}{|B|}\sum_{b\in B}b$. Given a rational prime ℓ coprime to N, the Hecke operator T_ℓ acts on $X_1(N)$ [46], inducing an endomorphism of $\widetilde{V}$. Letting

$$I=\mathrm{Ker}\{\mathbb{T}\longrightarrow\mathscr{O}_F : T_\ell\mapsto a_\ell b_\ell,\ \forall\ell\nmid NN_A\},$$

we can define the (f,ψ)-isotypic component of $\widetilde{V}$ by

$$V=\{x\in\widetilde{V}\mid Ix=0\}.$$

Hence, there is a map $m:\widetilde{V}\longrightarrow V$ that is equivariant under the action of Hecke operators T_ℓ, for ℓ not dividing NN_A and under the action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The f-isotypic component of $e_B H^1_{et}(X_1(N)\otimes\overline{\mathbb{Q}},\mathscr{F})(\frac{r}{2}+1)$ gives rise (by extending scalars appropriately) to V_f and $e_A H^r_{et}(\overline{A^r},\mathbb{Z}_p)(\frac{r}{2})$ gives rise to V_ψ. They are free $\mathscr{O}_F\otimes\mathbb{Z}_p$-modules of rank 2. Hence, $V_\wp=(V_f\otimes_{\mathscr{O}_F\otimes\mathbb{Z}_p}V_\psi)_\wp$ is a four dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in

$$\mathrm{End}(A/\mathbb{Q})=\oplus_{\sigma\in\mathrm{Gal}(H/\mathbb{Q})}\mathrm{Hom}(A,A^\sigma).$$

4.3 p-adic Abel-Jacobi map

We use Proposition 4.2.1 to view the p-adic étale realization of the twisted motive V associated to f and ψ in the middle étale cohomology of the associated Kuga-Sato varieties.

Consider the p-adic étale Abel-Jacobi map

$$\Phi : \mathrm{CH}^{r+1}(W/L_n)_0 \longrightarrow H^1\left(L_n, H_{et}^{2r+1}\left(W \otimes \overline{\mathbb{Q}}, \mathbb{Z}_p(r+1)\right)\right),$$

where $\mathrm{CH}^{r+1}(W/L_n)_0$ is the group of homologically trivial cycles of codimension $r+1$ on W defined over the compositum L_n of the ring class field K_n of K of conductor n and L_1, modulo rational equivalence. (See Chapter 2, Section 2.1 for more details on the Abel-Jacobi map). Composing the Abel-Jacobi map with the projectors e_r and e_B, we obtain a map

$$\Phi : \mathrm{CH}^{r+1}(W/L_n)_0 \longrightarrow H^1(L_n, \widetilde{V}).$$

In fact, Φ factors through $e_r(\mathrm{CH}^{r+1}(W/L_n)_0 \otimes \mathbb{Z}_p)$ as the Abel-Jacobi map commutes with correspondences on W. Combining Proposition 4.2.1 which implies that

$$e_r H^{2r+2}(W \otimes \overline{\mathbb{Q}}, \mathbb{Z}_p) = 0,$$

with the definition of

$$\mathrm{CH}^{r+1}(W/L_n)_0 = \mathrm{Ker}(\mathrm{CH}^{r+1}(W/L_n) \longrightarrow H^{2r+2}(W \otimes \overline{\mathbb{Q}}, \mathbb{Z}_p(r+1))),$$

we deduce that

$$e_r(\mathrm{CH}^{r+1}(W/L_n)_0 \otimes \mathbb{Z}_p) = e_r(\mathrm{CH}^{r+1}(W/L_n) \otimes \mathbb{Z}_p).$$

Hence, composing Φ with $m : \widetilde{V} \longrightarrow V$, we obtain

$$\Phi : e_r(\mathrm{CH}^{r+1}(W/L_n)_0 \otimes \mathbb{Z}_p) \longrightarrow H^1(L_n, V),$$

which is $\mathbb{T}[\mathrm{Gal}(L_n/\mathbb{Q})]$-equivariant.

Beilinson and Bloch's conjectures. Beilinson and Bloch formulated conjectures about values of L-functions that arise from algebraic varieties, that is, motivic L-functions at integers. Bloch [8] defined a regulator map

$$r : K_2(X) \longrightarrow H^1(X(\mathbb{C}), \mathbb{C}^*)$$

for any curve X over $\mathbb{C}$, where $K_2(X)$ is the K_2 group of X and $H^1(X(\mathbb{C}), \mathbb{C}^*)$ is the de Rham cohomology group of $X(\mathbb{C})$. More generally, Beilinson defined a regulator map

$$r : H^1_M(X, \mathbb{Q}(n)) \longrightarrow H^{i+1}_D(X \otimes \mathbb{R}, \mathbb{R}(n))$$

from the motivic cohomology of X, that is, a suitable piece of the K-theory of X, to the Deligne cohomology of X. The L-function $L(h^i(X), s)$ associated to the i-th cohomology $h^i(X)$ of the Chow motive $h(X)$ associated to X is expected to satisfy a functional equation relating its values at s and $i+1-s$. Beilinson's conjectures [2] relate the order of vanishing of $L(h^i(X), s)$ at $i+1-n$ with the dimension of $H^{i+1}_D(X \otimes \mathbb{R}, \mathbb{R}(n))$.

In our setting, as explained in [33] [44, section 6] and [32], Beilinson and Bloch conjecture that

$$\dim_{\mathbb{Q}}(\mathrm{Im}(\Phi) \otimes \mathbb{Q}) = ord_{s=r+1} L(f \otimes \theta_\psi, s).$$

(See [9] for more details). Kolyvagin's results [34] combined with those of Gross and Zagier [28] prove the Birch and Swinnerton-Dyer conjecture for analytic rank less or equal to 1. This is the particular case where the modular form f is associated to an elliptic curve and ψ is the trivial character. Nekovář's results [39, 40] that correpond to the setting where ψ is trivial provide further evidence towards a p-adic analog of the Beilinson-Bloch conjecture of the form

$$\dim_{\mathbb{Q}_p}(\mathrm{Im}(\Phi)\otimes\mathbb{Q}_p) = ord_{s=r+1}L_p(f,s)$$

due to Perrin-Riou [15, section 2.8], [42]. In this thesis, we provide a sufficient condition for $\dim_{\mathbb{Q}_p}(\mathrm{Im}(\Phi)\otimes\mathbb{Q}_p) = 1$. Since Shnidman [49] relates the order of vanishing of the p-adic L-function $L_p(f\otimes\theta_\psi,s)$ at $s=r+1$ to the height of the image by the p-adic Abel-Jacobi map of a generalized Heegner cycle of conductor 1, we obtain a p-adic analog of the statement conjectured by Beilinson and Bloch in Corollary 4.9.4.

4.4 Generalized Heegner cycles

We describe the construction of generalized Heegner cycles following Bertolini, Darmon and Prasanna [5]. Consider pairs (φ_i, A_i) where A_i is an elliptic curve defined over K_1 with level N structure defined over L_1 and

$$\varphi_i : A \longrightarrow A_i$$

is an isogeny over $\overline{K}$. Two pairs $(\varphi_i,A_i),(\varphi_j,A_j)$ are said to be *isomorphic* if there is a $\overline{K}$-isomorphism $\alpha : A_i \longrightarrow A_j$ satisfying $\alpha\circ\varphi_i = \varphi_j$. Let $Isog^{\mathcal{N}}(A)$ denote the isomorphism classes of pairs (φ_i,A_i) with $ker(\varphi_i)\cap A[\mathcal{N}]$ trivial. For (φ_i,A_i) in $Isog^{\mathcal{N}}(A)$, we associate a codimension $r+1$ cycle on V

$$\Upsilon_{\varphi_i} = Graph(\varphi_i)^r \subset (A\times A_i)^r \simeq (A_i)^r\times A^r \subset W_r\times A^r$$

and define a *generalized Heegner cycle*

$$\Delta_{\varphi_i} = e_r \Upsilon_{\varphi_i}.$$

Denote by D_{A_i} the element

$$(graph(\varphi_i) - 0 \times A - \deg(\varphi_i)(A_i \times 0)) \text{ in } NS(A_i \times A),$$

where $NS(A_i \times A)$ is the Néron-Severi group of $A_i \times A$. Let us assume that the index i of A_i indicates that $\mathrm{End}(A_i)$, which is an order in $\mathscr{O}_K$, has conductor i. Then Δ_{φ_i} is defined over the compositum of the abelian extension $\widetilde{K}$ of K over which the isomorphism class of A is defined, with the ring class field K_i of conductor i. (See Chapter 2, Section 2.3 for more details). Since $\widetilde{K}$ is the smallest extension of K_1 over which $\mathrm{Gal}(\overline{K}/\widetilde{K})$ acts trivially on $A[\mathscr{N}]$, it is equal to the ray class field L_1 of K of conductor $\mathscr{N}$. Therefore, Δ_{φ_i} is defined over

$$L_i = L_1 K_i.$$

Then

$$\Delta_{\varphi_i} = D^r_{A_i} \text{ belongs to } \mathrm{CH}^{r+1}(W/L_i).$$

In fact, Δ_{φ_i} is homologically trivial on W as shown in [5, proposition 2.7].

In the rest of this section, we consider elements (φ_i, A_i) and (φ_j, A_j) in $Isog^{\mathscr{N}}(A)$.

Lemma 4.4.1. *Consider the map*

$$g \times I : A_i \times A \longrightarrow A_j \times A,$$

where g is an isogeny of elliptic curves and I is the identity map. Then

$$(g \times I)_* D_{A_i} = \deg(g) \sqrt{\frac{\deg(\varphi_i)}{\deg(\varphi_j)}}\, D_{A_j}.$$

Proof. We denote the intersection pairing of two divisors by a dot. We have

$$(g \times I)_* D_{A_i} \cdot (g \times I)_* D_{A_i} = \deg(g)^2 D_{A_i} \cdot D_{A_i},$$

where

$$\begin{aligned}
&D_{A_i} \cdot D_{A_i} \\
&= (\mathrm{graph}(\varphi_i) - 0 \times A - \deg(\varphi_i) A_i \times 0) \cdot (\mathrm{graph}(\varphi_i) - 0 \times A - \deg(\varphi_i) A_i \times 0) \\
&= \mathrm{graph}(\varphi_i) \cdot \mathrm{graph}(\varphi_i) + 0 \times A \cdot 0 \times A + \deg(\varphi_i) A_i \times 0 \cdot \deg(\varphi_i) A_i \times 0 \\
&- 2\mathrm{graph}(\varphi_i) \cdot 0 \times A - 2\mathrm{graph}(\varphi_i) \cdot \deg(\varphi_i) A_i \times 0 + 2\deg(\varphi_i) A_i \times 0 \cdot 0 \times A \\
&= 0 + 0 + 0 - 2\deg(\varphi_i) - 2\deg(\varphi_i) + 2\deg(\varphi_i) \\
&= -2\deg(\varphi_i).
\end{aligned}$$

In the previous computation, the equality $\mathrm{graph}(\varphi_i) \cdot \mathrm{graph}(\varphi_i) = 0$ follows from the implication

$$(x, \varphi_i(x)) = (x, \varphi_i(x) + P) \implies P = 0$$

for a translation of $\varphi_i(x)$ by some quantity P. Hence,

$$(g \times I)_* D_{A_i} \cdot (g \times I)_* D_{A_i} = -2\deg(g)^2 \deg(\varphi_i).$$

Since $(g \times I)_* D_{A_i} = k D_{A_j}$ where $A_j = g(A_i)$ and $k > 0$, we also have

$$(g \times I)_* D_{A_i} \cdot (g \times I)_* D_{A_i} = k^2 D_{A_j} \cdot D_{A_j} = -2k^2 \deg(\varphi_j).$$

The equality $-2\deg(g)^2\deg(\varphi_i) = -2k^2\deg(\varphi_j)$ then implies that

$$k = \deg(g)\sqrt{\frac{\deg(\varphi_i)}{\deg(\varphi_j)}},$$

and

$$(g\times I)_* D_{A_i} = \deg(g)\sqrt{\frac{\deg(\varphi_i)}{\deg(\varphi_j)}} D_{A_j}.$$

□

4.5 Euler system properties

We study certain global and local norm compatibilities of generalied Heegner cycles satisfying the properties of Euler systems.

We have $\mathscr{O}_F \otimes \mathbb{Z}_p = \oplus_{\wp_i|p}\mathscr{O}_{F,\wp_i}$ where $\mathscr{O}_{F,\wp_i}$ is the completion of $\mathscr{O}_F$ at the prime $\wp_i$ dividing p. Recall that $V_\wp = (V_f \otimes_{\mathscr{O}_F} V_\psi)_\wp$ where $\wp$ is a prime of F dividing p. Let

$$G_V = \mathrm{Aut}(V_\wp/p).$$

For a Galois representation V,

$$F(V)$$

will designate the smallest extension of F such that $\mathrm{Gal}(\overline{F}/F(V))$ acts trivially on V.

We denote by $\mathrm{Frob}_v(F_1/F_2)$ the conjugacy class of the Frobenius substitution of the prime $v \in F_2$ in $\mathrm{Gal}(F_1/F_2)$ and by $\mathrm{Frob}_\infty(F_1/\mathbb{Q})$ the conjugacy class of the complex conjugation τ in $\mathrm{Gal}(F_1/\mathbb{Q})$. A rational prime ℓ is called a *Kolyvagin prime* if

$$(\ell, NDN_A p) = 1 \text{ and } a_\ell b_\ell \equiv \ell+1 \equiv a_\ell^2 - b_\ell^2 + 2 \equiv 0 \mod p. \tag{4.2}$$

Let

$$L = K(V_{\wp}/p).$$

Condition (4.2) is equivalent to

$$\mathrm{Frob}_{\ell}\left(L(\mu_p)/\mathbb{Q}\right) = \mathrm{Frob}_{\infty}\left(L(\mu_p)/\mathbb{Q}\right), \tag{4.3}$$

where μ_p is the group of p-th roots of unity. Indeed, it is enough to compare the characteristic polynomial of the complex conjugation $(x^2-1)^2 = x^4 - 2x^2 + 1$ acting on $V_{\wp}/p$ with roots -1 and 1, each with multiplicity 2, with the twist by $r+1$ of the characteristic polynomial of the Frobenius substitution at ℓ acting on $V_{\wp}/p$ with roots

$$\alpha_1\alpha_3,\ \ \alpha_1\alpha_4,\ \ \alpha_2\alpha_3,\ \ \text{and}\ \ \alpha_2\alpha_4$$

satisfying

$$\alpha_1\alpha_2 = \ell^r,\ \ \alpha_1+\alpha_2 = b_\ell,\ \ \alpha_3\alpha_4 = \ell^{r+1},\ \ \alpha_3+\alpha_4 = a_\ell.$$

The characteristic polynomial of $\mathrm{Frob}(\ell)$ acting on $V_{\wp}/p$ is

$$\begin{aligned}
&(x-\alpha_1\alpha_3)(x-\alpha_1\alpha_4)(x-\alpha_2\alpha_3)(x-\alpha_2\alpha_4)\\
&= (x^2-(\alpha_1\alpha_3+\alpha_1\alpha_4)x+\alpha_1^2\alpha_3\alpha_4)(x^2-(\alpha_2\alpha_3+\alpha_2\alpha_4)x+\alpha_2^2\alpha_3\alpha_4)\\
&= \left(x^2-\alpha_1 a_\ell x+\ell^{r+1}\alpha_1^2\right)\left(x^2-\alpha_2 a_\ell x+\ell^{r+1}\alpha_2^2\right)
\end{aligned}$$

We use the equality $(\alpha_1+\alpha_2)^2=\alpha_1^2+\alpha_2^2+2\alpha_1\alpha_2$ that is $b_\ell^2-2\ell^r=\alpha_1^2+\alpha_2^2$ to conclude that the latter equals

$$\begin{aligned}
&x^4-(\alpha_2 a_\ell+\alpha_1 a_\ell)x^3+\left(\ell^{r+1}\alpha_1^2+\ell^{r+1}\alpha_2^2+\alpha_1\alpha_2 a_\ell^2\right)x^2\\
&-\ell^{r+1}\left(\alpha_1 a_\ell\alpha_2^2+\alpha_2 a_\ell\alpha_1^2\right)x+\ell^{2r+2}\alpha_1^2\alpha_2^2\\
=\;&x^4-a_\ell b_\ell x^3+\left(\ell^{r+1}b_\ell^2-2\ell^{2r+1}+a_\ell^2\ell^r\right)x^2-\ell^{2r+1}a_\ell(\alpha_1+\alpha_2)x+\ell^{4r+2}\\
=\;&x^4-a_\ell b_\ell x^3+\left(\ell^{r+1}b_\ell^2-2\ell^{2r+1}+a_\ell^2\ell^r\right)x^2-\ell^{2r+1}b_\ell a_\ell x+\ell^{4r+2}.
\end{aligned}$$

To twist this characteristic polynomial by ℓ^{r+1}, it is enough to map $x\mapsto\ell^{r+1}x$. We obtain

$$\begin{aligned}
&\ell^{4r+4}x^4-a_\ell b_\ell\ell^{3r+3}x^3+\ell^{2r+2}\left(\ell^{r+1}b_\ell^2-2\ell^{2r+1}+a_\ell^2\ell^r\right)x^2-\ell^{3r+2}b_\ell a_\ell x+\ell^{4r+2}\\
=\;&\ell^{4r+4}\left(x^4-\frac{a_\ell b_\ell}{\ell^{r+1}}x^3+\frac{\ell^{r+1}b_\ell^2-2\ell^{2r+1}+a_\ell^2\ell^r}{\ell^{2r+2}}x^2-\frac{b_\ell a_\ell}{\ell^{r+2}}x+\frac{1}{\ell^2}\right).
\end{aligned}$$

On the one hand, using the congruences

$$a_\ell b_\ell\;\equiv\;\ell+1\;\equiv\;a_\ell^2-b_\ell^2+2\;\equiv\;0\mod p,$$

we find that the characteristic polynomial

$$x^4-2x^2+1$$

of the complex conjugation τ acting on $V_\wp/p$ is congruent to the characteristic polynomial of $\mathrm{Frob}(\ell)$ acting on $V_\wp/p$. On the other hand, comparing the action of the Frobenius element Frob_ℓ and the complex conjugation τ on ζ_p, where ζ_p is a p-th root of unity, we obtain

$$\zeta_p^\ell=\mathrm{Frob}_\ell(\zeta_p)=\mathrm{Frob}_\infty(\zeta_p)=\zeta_p^{-1}.$$

This implies that $\ell \equiv -1 \mod p$. As a consequence, Condition (4.2) is necessary to satisfy Equality (4.3).

Let $n = \ell_1 \cdots \ell_k$ be a squarefree integer where ℓ_i is a Kolyvagin prime for $i = 1, \cdots, k$. Then the extensions L_1 and K_n are disjoint over K_1 and

$$G_n = \mathrm{Gal}(L_n/L_1) \simeq \mathrm{Gal}(K_n/K_1).$$

The Galois group $\mathrm{Gal}(K_n/K_1)$ is the product over the primes ℓ dividing n of the cyclic groups $G_\ell = \mathrm{Gal}(K_\ell/K_1)$ of order $\ell+1$. We denote by σ_ℓ a generator of G_ℓ. The Frobenius condition on ℓ implies that it is inert in K. Denote by λ the unique prime in K above ℓ. Writing n as $n = \ell m$, we have that λ splits completely in L_m since it is unramified in L_m and has the same image as $\mathrm{Frob}_\infty(L/K) = \tau^2 = Id$ by the Artin map. A prime λ_m of L_m above λ ramifies completely in L_n. We denote by λ_n the unique prime in L_n above λ_m. Consider the image of Δ_{φ_n} by the Abel-Jacobi map

$$\Phi : \mathrm{CH}^{r+1}(W/L_n)_0 \longrightarrow H^1(L_n, V).$$

Proposition 4.5.1. *Consider $(A_n, \varphi_n) \sim (A_m, \varphi_m) \in Isog^{\mathscr{N}}(A)$ where $n = \ell m$ for an odd prime ℓ. Then*

$$T_\ell \Phi(\Delta_{\varphi_m}) = \mathrm{cor}_{L_n, L_m} \Phi(\Delta_{\varphi_n}) = a_\ell b_\ell \Phi(\Delta_{\varphi_m}).$$

Proof. By [45, corollary 11.4],

$$T_\ell(\Delta_{\varphi_m}) = \sum_{n_i} \Delta_{\varphi_{n_i}},$$

where the generalized Heegner cycles $\Delta_{\varphi_{n_i}}$ correspond to elements $(A_{n_i}, \varphi_{n_i}) \sim (A_m, \varphi_m)$ in $Isog^{\mathscr{N}}(A)$ for elliptic curves A_{n_i} that are ℓ-isogenous to A_m respecting level N structure.

These elliptic curves A_{n_i} correspond to gA_m where

$$g \in \mathrm{Gal}(L_n/L_m) \simeq \mathrm{Gal}(K_n/K_m) \simeq \mathrm{Gal}(K_\ell/K_1).$$

Hence

$$\sum_{n_i} \Delta_{\varphi_{n_i}} = \sum_{g \in \mathrm{Gal}(L_n/L_m)} g\Delta_{\varphi_n} = \mathrm{cor}_{L_n,L_m}(\Delta_{\varphi_n}) = a_\ell b_\ell \Delta_{\varphi_m},$$

where the last equality follows from the action of T_ℓ on V. Finally, we apply Φ which commutes with T_ℓ to obtain $T_\ell\Phi(\Delta_{\varphi_m}) = \mathrm{cor}_{L_n,L_m}\Phi(\Delta_{\varphi_n})$. □

For an element $c \in H^1(F,M)$, we denote by $\mathrm{res}_v(c) \in H^1(F_v,M)$ the image of c by the restriction map $H^1(F,M) \longrightarrow H^1(F_v,M)$ induced from the inclusion

$$\mathrm{Gal}(\overline{F_v}/F_v) \hookrightarrow \mathrm{Gal}(\overline{F}/F).$$

Proposition 4.5.2. *Consider $(A_n,\varphi_n),(A_m,\varphi_m) \in Isog^{\mathscr{N}}(A)$ where $n = \ell m$. Then*

$$\mathrm{res}_{\lambda_n}\Phi(\Delta_{\varphi_n}) = k\mathrm{Frob}_\ell(L_n/L_m)\mathrm{res}_{\lambda_m}\Phi(\Delta_{\varphi_m})$$

for $k = \ell\sqrt{\dfrac{\deg(\varphi_i)}{\deg(\varphi_j)}}$.

Proof. The Eichler-Shimura relation consists of the local congruence

$$\mathrm{Frob}_\ell + \mathrm{Frob}_\ell^t \equiv T_\ell \mod \ell$$

on $X_0(N)$ where Frob_ℓ is the Frobenius morphism and Frob_ℓ^t is the morphism dual to Frob_ℓ. For elliptic curves over $\mathscr{O}_{L_n}$, we have

$$\mathrm{Frob}_\ell^t \equiv \ell\,\mathrm{Frob}_\ell^{-1} \equiv \ell\,\mathrm{Frob}_\ell \mod \lambda_n$$

because $|\mathcal{O}_{L_n}/\lambda_n| = \ell^2$. Since λ_m completely ramifies in L_n, we have $\mathcal{O}_{L_m}/\lambda_m \simeq \mathcal{O}_{L_n}/\lambda_n$. Hence,

$$T_\ell(A_m) = \sum_{\sigma \in G(L_n/L_m)} \sigma A_m \equiv \sum_{\sigma \in G(L_n/L_m)} A_n \equiv (\ell+1)A_n \mod \lambda_n.$$

Therefore, we have $\mathrm{Frob}_\ell(A_m) \equiv A_n \mod \lambda_n$. By Proposition 4.4.1, this implies

$$(\mathrm{Frob}_\ell \times I)_* D_{A_m} \equiv k D_{A_n} \mod \lambda_n$$

where $k = \ell \sqrt{\dfrac{\deg(\varphi_i)}{\deg(\varphi_j)}}$ from which the result follows. □

4.6 Kolyvagin cohomology classes

We denote by

$$\Phi(\Delta_{\varphi_n})_\wp \in H^1(L_n, V_\wp)$$

the image of $\Phi(\Delta_{\varphi_n}) \in H^1(L_n, V)$ by the map $H^1(L_n, V) \longrightarrow H^1(L_n, V_\wp)$ induced by the projection $V \to V_\wp$. Let

$$y_n = \mathrm{red}(\Phi(\Delta_{\varphi_n})_\wp) \in H^1(L_n, V_\wp/p)$$

be the image of $\Phi(\Delta_{\varphi_n})_\wp \in H^1(L_n, V_\wp)$ by the map $H^1(L_n, V_\wp) \longrightarrow H^1(L_n, V_\wp/p)$ induced by the projection $V_\wp \to V_\wp/p$. We use certain operators (4.4) defined by Kolyvagin in order to lift the cohomology classes $y_n \in H^1(L_n, V_\wp/p)$ to Kolyvagin cohomology classes $P(n) \in H^1(K, V_\wp/p)$, for appropriate n.

Lemma 4.6.1. *For all n,*

$$H^0(L_n, V_\wp/p) = H^0(L_1, V_\wp/p) = 0$$

$$\textit{and}\ \ \mathrm{Gal}(L_n(V_\wp/p)/L_n) \simeq \mathrm{Gal}(L_1(V_\wp/p)/L_1) \simeq \mathrm{Gal}(K(V_\wp/p)/K).$$

Proof. The extensions L_n/L_1 and $L_1(V_\wp/p)/L_1$ are unramified outside primes dividing nc and $N_A N p$. Therefore, $L_n \cap L_1(V_\wp/p)$ is unramified over L_1 and is hence contained in L_1, the maximal unramified extension of K of conductor $\mathscr{N}$. Hence,

$$H^0(L_n, V_\wp/p) = H^0(L_1, V_\wp/p).$$

The result follows by the assumption on p which implies that $H^0(L_1, V_\wp/p) = 0$. $\square$

Proposition 4.6.2. *The restriction map*

$$res_{L_1,L_n} : H^1(L_1, V_\wp/p) \longrightarrow H^1(L_n, V_\wp/p)^{G_n}$$

is an isomorphism.

Proof. This follows from the inflation-restriction sequence

$$0 \to H^1(L_n/L_1, V_\wp/p) \xrightarrow{inf} H^1(L_1, V_\wp/p) \xrightarrow{res} H^1(L_n, V_\wp/p) \to H^2(L_n/L_1, V_\wp/p),$$

since $H^0(L_n, V_\wp/p) = 0$ by Lemma 4.6.1. $\square$

Let

$$\mathrm{Tr}_\ell = \sum_{i=0}^{\ell} \sigma_\ell^i, \quad D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i. \tag{4.4}$$

They are related by

$$(\sigma_\ell - 1)D_\ell = \ell + 1 - \mathrm{Tr}_\ell. \tag{4.5}$$

Define

$$D_n = \prod_{\ell | n} D_\ell \in \mathbb{Z}[G_n].$$

Proposition 4.6.3.

$$D_n y_n \in H^1(L_n, V_\wp/p)^{G_n}.$$

Proof. It is enough to show that for all ℓ dividing n,

$$(\sigma_\ell - 1)D_n y_n = 0.$$

We have

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

where the last equality follows by Relation (4.5). Since $res_{L_m,L_n} \circ \mathrm{cor}_{L_n,L_m} = \mathrm{Tr}_\ell$,

$$\begin{aligned}
&(\ell + 1 - \mathrm{Tr}_\ell)D_m \mathrm{red}(\Phi(\Delta_{\varphi_n})_\wp) \\
&= (\ell + 1)D_m \mathrm{red}(\Phi(\Delta_{\varphi_n})_\wp) - D_m a_\ell b_\ell \mathrm{red}(\Phi(\Delta_{\varphi_m})_\wp) \\
&\equiv 0 \bmod p.
\end{aligned}$$

by Proposition 4.5.1 and Condition 4.2. □

As a consequence, the cohomology classes $D_n y_n \in H^1(L_n, V_\wp/p)^{G_n}$ can be lifted to cohomology classes $c(n) \in H^1(L_1, V_\wp/p)$ such that

$$\mathrm{res}_{L_1,L_n} c(n) = D_n y_n.$$

We define

$$P(n) = \mathrm{cor}_{L_1,K} c(n) \text{ in } H^1(K, V_\wp/p).$$

Proposition 4.6.4. *Let v be a prime of L_1.*

1. *If $v | N_A N$, then $\mathrm{res}_v(P(n))$ is trivial.*
2. *If $v \nmid N_A N n p$, then $\mathrm{res}_v(P(n))$ lies in $H^1(K_v^{ur}/K_v, V_\wp/p)$.*

Proof. 1. We follow the proof in Chapter 3 Proposition 3.4.4. We denote by

$$V_{\wp}/p^{dual} = \mathrm{Hom}(V_{\wp}/p, \mathbb{Z}/p\mathbb{Z}(1))$$

the local Tate dual of $V_{\wp}/p$. The local Euler characteristic formula [37, Section 1.2] yields

$$|H^1(K_v, V_{\wp}/p)| = |H^0(K_v, V_{\wp}/p)| \times |H^2(K_v, V_{\wp}/p)|.$$

Local Tate duality then implies

$$|H^1(K_v, V_{\wp}/p)| = |H^0(K_v, V_{\wp}/p)|^2.$$

The Weil conjectures and the assumption on $Fr(v)$ imply that $((V_{\wp}/p)^{I_v})^{Fr(v)} = 0$ where

$$< Fr(v) > = \text{ Gal}(K_v^{ur}/K_v)$$

and $I = \mathrm{Gal}(\overline{K_v}/K_v^{ur})$ is the inertia group. (See Section 2.6 for more details). Therefore, $H^0(K_v, V_{\wp}/p) = ((V_{\wp}/p)^{I_v})^{Fr(v)} = 0$.

2. If v does not divide $NnpN_A$, then

$$res_{L_{1,v},L_{n,v'}}\mathrm{res}_v c(n) = \mathrm{res}_{v'} D_n y_n \in H^1(\overline{L_{n,v'}}/L_{n,v'}, V_{\wp}/p)$$

for v' above v in L_n. The exact sequence

$$\cdots \to H^1(L_{n,v'}^{ur}/L_{n,v'}, (V_{\wp}/p)^{I_v}) \to H^1(L_{n,v'}, V_{\wp}/p) \xrightarrow{\mathrm{res}} H^1(\overline{L_{n,v'}}/L_{n,v'}^{ur}, V_{\wp}/p) \to \cdots$$

allows us to view the cohomology class $\mathrm{res}_{v'} D_n y_n$ that belongs to $\mathrm{Ker}(\mathrm{res})$ as an element in $H^1(L_{n,v'}^{ur}/L_{n,v'}, V_{\wp}/p)$. The isomorphism $L_{n,v'} \simeq L_{1,v}$ hence implies that $\mathrm{res}_v c(n)$ belongs to $H^1(L_{1,v}^{ur}/L_{1,v}, V_{\wp}/p)$.

□

4.7 Global extensions by Kolyvagin classes

We construct a global pairing of the Selmer group that will subsequently be used to relate local and global information about the elements of the Selmer group and we consider extensions of L by Kolyvagin cohomology classes c and $P(q)$, where $P(q)$ will play a crucial role in the proof of Theorem 1.2.1.

Lemma 4.7.1. *We have*

$$H^1(\mathrm{Aut}(V_\wp/p), V_\wp/p) = 0.$$

Proof. First note that if $p \nmid |\mathrm{Aut}(V_\wp/p)|$, then $H^1(\mathrm{Aut}(V_\wp/p), V_\wp/p) = 0$. If p divides $|G|$, then since $V_\wp/p$ is irreducible as an $\mathrm{Aut}(V_\wp/p)-$module, Dickson's lemma [52, Theorem 6.21] implies that $\mathrm{Aut}(V_\wp/p)$ contains $\mathrm{SL}_2(F_q)$ for some q. In particular, it contains $2I$ where I is the identity map. Therefore, by Lemma 3.7.1, the map $x \mapsto (2I - I)x = Ix$ is the zero map on $H^1(\mathrm{Aut}(V_\wp/p), V_\wp/p)$ and the result follows. □

We recall the statement of theorem 1.3.1.

Theorem 1.3.1. Let p be such that

$$\mathrm{Gal}\left(K(V_\wp/p)/K\right) \simeq \mathrm{Aut}_K(V_\wp/p), \text{ and } (p, ND\phi(N)N_A) = 1.$$

Suppose that $V_\wp/p$ is a simple $\mathrm{Aut}_K(V_\wp/p)$-module. Suppose further that the eigenvalues of $Fr(v)$ acting on $V_\wp^{I_v}$ are not equal to 1 modulo p for v dividing NN_A. If $P(1)$ is non-zero, then the Selmer group S has rank 1 over $\mathscr{O}_{F,\wp}/p$.

Local Tate duality and the reciprocity law translate local properties of Kolyvagin's cohomology classes into local properties of elements of the Selmer group. This local information will be transferred to global one using a global pairing of the Selmer group. One can then conclude using Cebotarev's density theorem.

We denote the Galois group $\mathrm{Gal}(L/K)$ by G. The restriction map

$$r : H^1(K, V_\wp/p) \longrightarrow H^1(L, V_\wp/p)^G = \mathrm{Hom}_G(\mathrm{Gal}(\overline{\mathbb{Q}}/L), V_\wp/p)$$

has kernel

$$\mathrm{Ker}(r) = H^1(K(V_\wp/p)/K, V_\wp/p) = H^1(Aut(V_\wp/p), V_\wp/p) = 0$$

by Lemma 4.7.1. Hence, we can identify an element $c \in H^1(K, V_\wp/p)$ with its image $r(c)$. Consider the evaluation pairing

$$[\ ,\ ]\ r(S) \times \mathrm{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow V_\wp/p. \tag{4.6}$$

We denote by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ the annihilator of $r(S)$. Let L^S be the extension of L fixed by $\mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$ and G_S the Galois group $\mathrm{Gal}(L^S/L)$.

We consider the restriction d of an element c of $H^1(K, V_\wp/p)$ to $H^1(L, V_\wp/p)$. Then d factors through some finite extension $\tilde{L}$ of L. We denote by

$$L(c) = \tilde{L}^{\ker(d)}$$

the subextension of $\tilde{L}$ fixed by $\ker(d)$. Note that $L(c)$ is an extension of L.

Remark 4.7.2. The element y_1 belongs to S by Proposition 4.6.4. Also, $L(y_1)$ is a subextension of L^S. Indeed, assume $\rho \in \mathrm{Gal}_S(\overline{\mathbb{Q}}/L)$, then $[s, \rho] = 0$ for all $s \in S$. Hence, y_1 defines a cocycle of S by

$$\rho \longrightarrow \rho(y_1) - y_1 = 0.$$

This implies that ρ fixes $L(y_1)$, a subfield of L^S.

We have $\mathrm{Gal}(L(y_1)/L) \simeq V_\wp/p$ and we denote by $I = \mathrm{Gal}(L^S/L(y_1))$.

$$\begin{tikzcd}
 & L^S \\
L(y_1) \arrow[ur, "I"] & \\
 & L = K(V_\wp/p) \arrow[ul, "V_\wp/p"] \arrow[uu, "G_S"']
\end{tikzcd}$$

Lemma 4.7.3. *There is an isomorphism of $\mathscr{O}_{F,\wp}/p$-modules mapping* $\mathrm{res}_\lambda P(m\ell)$ *where λ' divides ℓ in K to* $\mathrm{res}_\lambda P(m)$. *Also,* $\mathrm{res}_\lambda P(\ell)$ *is ramified for all such λ.*

Proof. This is an adaptation of Section 3.5 in Chapter 3 that uses the properties of the Euler system considered in Proposition4.5.1 and Proposition 4.5.2. □

Lemma 4.7.4. *There is a Kolyvagin prime q such that*

$$\mathrm{Frob}_q(L^S/\mathbb{Q}) = \tau h, \;\; h \in \mathrm{Gal}(L^S/L), \;\; h^{\tau+1} \notin I \textit{ and } \;\; \mathrm{res}_{\beta'} y_1 \neq 0$$

for some prime β' in K above q.

Proof. Let q be a Kolyvagin prime such that

$$\mathrm{Frob}_q(L^S/\mathbb{Q}) = \tau h, \;\; h \in \mathrm{Gal}(L^S/L), \;\; h^{\tau+1} \notin I.$$

Note that the restriction of τh to L is τ. Assume q splits completely in $L(y_1)$. Then for a prime β' of $L(y_1)$ above q, we would have that

$$\mathrm{Frob}_{\beta'}(L^S/L(y_1)) = (\tau h)^2,$$

a contradiction since $\mathrm{Frob}_{\beta'}(L^S/L(y_1))$ belongs to I while $h^{\tau+1} = (\tau h)^2 \notin I$. Hence q does not split completely in $L(y_1)$. Therefore, since q splits completely in L and does not ramify in $L(y_1)$, there is a prime β in L_1 above q such that $|L(y_1)_{\beta''} : L_{\beta'}| > 1$ for a prime β' of L above β and a prime β'' of $L(y_1)$ above β'. This implies that

$$res_{\beta} y_1 \neq 0.$$

$\square$

Consider the following extensions

$$\begin{tikzcd}
& H_2 = H_0H_1 & \\
H_0 = L(c) \arrow[ur] & & H_1 = L(P(q)) \arrow[ul] \\
& L = K(V_{\wp}/p) \arrow[ul, "V_{\wp}/p"] \arrow[ur, "V_{\wp}/p"'] &
\end{tikzcd}$$

We define $V_i = \mathrm{Gal}(H_i/L)$ for $i = 0, 1, 2$. We have an isomorphism of $\mathrm{Aut}(A_{\wp}/p)$-modules

$$V_0 \simeq V_1 \simeq V_{\wp}/p.$$

Lemma 4.7.5. *The extensions L^S and H_1 are linearly disjoint over L.*

Proof. It is enough to prove that $L^S \cap H_1 = L$ as linear disjointness for Galois extensions is equivalent to disjointness. The Frobenius substitution $\tilde{\rho}$ of q in $\mathrm{Gal}(L^t/L^{ur})$ is such that

$$[s, \tilde{\rho}] = 0 \text{ for all } s \in S,$$

since s is unramified at q.

Lemma 4.7.3 implies that $P(q)$ ramifies at q and $\mathrm{res}_\beta P(q)$ is mapped under an isomorphism to $\mathrm{res}_\beta y_1 \neq 0$. Hence

$$\tilde{\rho}(P(q)) \neq 0.$$

As a consequence, $L^S \cap L(P(q)) \neq L(P(q))$. For all c generating L^S over L, we have

$$\mathrm{Gal}(L(c) \cap L(P(q))/L) \text{ is a } G_V - \text{submodule of } V_1 \simeq V_\wp/p.$$

Therefore, $\mathrm{Gal}(L(c) \cap L(P(q))/L)$ is trivial.

$\square$

4.8 Complex conjugation and local Tate duality

We study the action of complex conjugation on the image by the p-adic Abel-Jacobi map of generalized Heegner cycles and consider the pairing induced by the action of the complex conjugation and the local Tate pairing.

Lemma 4.8.1. *There is an element σ in $\mathrm{Gal}(K_j/K)$ such that*

$$\tau\Phi(\Delta_{\varphi_j})_\wp = \varepsilon_L^r \sigma\Phi(\Delta_{\varphi_j})_\wp,$$

where $-\varepsilon_L$ is the sign of the functional equation of $L(f,s)$, and $k = 2\sqrt{\dfrac{\deg(\varphi_i)}{\deg(\varphi_j)}}$.

Proof. Using [26] which shows that $\tau A_j = W_N(\sigma A_j)$ for some σ in $G(K_j/K)$, we obtain by Proposition 4.4.1

$$(\tau \times I)_*(D^r_{A_j}) = kD^r_{\tau(A_j)} = kD^r_{W_N(\sigma A_j)}$$

where $k = 2\sqrt{\dfrac{\deg(\varphi_i)}{\deg(\varphi_j)}}$. Consider the map

$$W \times I : W_N \times A \longrightarrow W_N \times A : ((E,P),A) \longrightarrow ((E/\langle P\rangle,P'),A),$$

where P' is such that the Weil pairing $< P, P' >$ of P with P' satisfies $< P, P' >= \zeta_N$ for some choice ζ_N of an N-th root of unity ζ_N. Note that W has degree N. Also,

$$W_* f(\tau) d_\tau d_z = \varepsilon_L N f(\tau) d_\tau d_z.$$

This implies as in [39, Proposition 6.2] that

$$(W \times I)_* D^r_{W_N(\sigma A_j)} = \varepsilon_L^r N^r D^r_{W_N(\sigma A_j)},$$

while Proposition 4.4.1 implies that the former equals $N^r \sqrt{\frac{\deg(\varphi_i)}{\deg(\varphi_j)}}^r D^r_{\sigma A_j}$. Hence,

$$D^r_{W_N(\sigma A_j)} = k_1 \varepsilon_L^r D^r_{\sigma A_j},$$

where $k_1 = \sqrt{\frac{\deg(\varphi_i)}{\deg(\varphi_j)}}^r$. Applying Proposition 4.4.1 to the map $(\sigma \times I)$, we obtain

$$(\sigma \times I)_* (D^r_{A_j}) = k_2 D^r_{\sigma A_j},$$

where $k_2 = \deg(\sigma)^r \sqrt{\frac{\deg(\varphi_i)}{\deg(\varphi_j)}}^r = k_1$. Hence, $D^r_{W_N(\sigma A_j)} = \varepsilon_L^r (\sigma \times I)_* (D^r_{A_j})$ and

$$(\tau \times I)_* (D^r_{A_j}) = \varepsilon_L^r k (\sigma \times I)_* (D^r_{A_j}).$$

Therefore

$$\tau \Phi(\Delta_{\varphi_j})_{\wp} = \varepsilon_L^r k \sigma \Phi(\Delta_{\varphi_j})_{\wp}.$$

$\square$

Remark 4.8.2. The non-trivial Kolyvagin class $P(1)$ belongs to $S^{+\varepsilon}$ where

$$\varepsilon = \varepsilon_L^r.$$

Indeed, y_1 is non-zero by the hypothesis on $\Phi(\Delta_{\varphi_1})_{\wp}$ and belongs to $S^{+\varepsilon}$ by Lemma 4.8.1. Using the relation $\tau D_\ell = -D_\ell \tau \mod p$, it can also be deduced from Lemma 4.8.1 that $P(n)$ belongs to the $(-1)^{\omega(n)}\varepsilon-$eigenspace where $\omega(n)$ is the number of distinct prime factors of n.

Given a Kolyvagin prime ℓ, the Frobenius condition implies that is inert in K. We denote by λ the prime of K lying above ℓ. As explained in Chapter 2, Section 2.5 using local Tate duality, we have a perfect local pairing

$$\langle\ .\ ,\ .\ \rangle_\lambda : H^1(K_\lambda^{ur}/K_\lambda, (V_\wp/p)^{I_\lambda}) \times H^1(K_\lambda^{ur}, V_\wp/p) \longrightarrow \mathbb{Z}/p,$$

where $I_\lambda = \mathrm{Gal}(\overline{K_\lambda}/K_\lambda^{ur})$ and $\mathscr{O}_{F,\wp}$-linear isomorphisms

$$\{H^1(K_\lambda^{ur}, V_\wp/p)\}^{dual} \simeq H^1(K_\lambda^{ur}/K_\lambda, (V_\wp/p)^{I_\lambda}).$$

We denote by

$$res_\lambda : H^1(K, V_\wp/p) \longrightarrow H^1(K_\lambda, V_\wp/p)$$

the restriction map from $H^1(K, V_\wp/p)$ to $H^1(K_\lambda, V_\wp/p)$. When the complex conjugation τ acts on a module M, we denote by M^+ and M^- the $+$ and $-$ eigenspaces of M with respect to the action of τ.

Lemma 4.8.3. *The action of complex conjugation induces non-degenerate pairings of eigenspaces*

$$\langle .,. \rangle_\lambda^\pm : H^1(K_\lambda^{ur}/K_\lambda, (V_\wp/p)^{I_\lambda})^\pm \times H^1(K_\lambda^{ur}, V_\wp/p)^\pm \longrightarrow \mathbb{Z}/p.$$

Proof. It is enough to show that the $+$ and $-$ eigenspaces are orthogonal. For cocycles c_1 and c_2 in the $+$ and $-$ eigenspaces respectively, we have

$$\langle c_1, c_2\rangle^{\tau}_{\lambda'} = \langle c_1^{\tau}, c_2^{\tau}\rangle_{\lambda'} = \langle c_1, -c_2\rangle_{\lambda'} = -\langle c_1, c_2\rangle_{\lambda'}.$$

Furthermore, $\langle c_1, c_2\rangle^{\tau}_{\lambda'} = \langle c_1, c_2\rangle_{\lambda'}$ since τ acts trivially on $H^2(K_\lambda, \mu_p) = \mathbb{Z}/p$. The case where c_1 and c_2 are in the $-$ and $+$ eigenspaces is similar. $\square$

Lemma 4.8.4. *We have*

$$G_S^+ = \{(\tau h)^2,\ h \in G_S\}, \quad I^+ = \{(\tau i)^2,\ i \in I\}.$$

Proof. On the one hand, $G_S^{\tau+1} \subseteq G_S^+$ as

$$G_S^{(\tau+1)(\tau-1)} = G_S^{\tau^2-1} = Id.$$

On the other hand, since p is odd, 2 is an automorphism of G_S. Therefore, if $h \in G_S^+$, then

$$h = (h^{1/2})^{\tau+1} \in G_S^{\tau+1}.$$

Hence,

$$G_S^+ = G_S^{\tau+1} = \{h^{\tau+1} = (\tau h \tau^{-1})\, h,\ \ h \in G_S\}.$$

The same proof applies for I. $\square$

4.9 Reciprocity law and local triviality

We use the reciprocity law in Proposition 4.9.1, local Tate duality in Proposition 4.8.3, Cebotarev's density theorem 2.1, and the global pairing of the Selmer group (4.6) to prove theorem 1.3.1.

Lemma 4.9.1. *We have*

$$\sum_{\lambda|\ell|n} \langle s_\lambda, res_\lambda P(n)\rangle_\lambda = 0.$$

Proof. The proof follows [39, proposition 11.2(2)] where both the reciprocity law, (see Chapter 2, Section 2.4 for more details) and the ramification properties of $P(n)$ in proposition 4.6.4 are used. □

Proposition 4.9.2. *We have $S^{-\varepsilon}$ is of rank 0 over $\mathcal{O}_{F,\wp}/p$.*

Proof. Consider the Kolyvagin class $P(\ell)$ where ℓ is a Kolyvagin prime satisfying

$$\mathrm{Frob}_\ell(L^S/\mathbb{Q}) = \tau h, \;\; h \in G_S, \;\; h \notin \mathrm{Gal}(L^S/L(y_1)).$$

We have that $P(\ell)$ belongs to the $-\varepsilon-$eigenspace by Remark 4.8.2. Then by Lemma 4.7.3, there is an isomorphism sending $\mathrm{res}_\lambda P(\ell)$ to $\mathrm{res}_\lambda P(1)$. The same argument as the one for q implies that

$$\mathrm{res}_\lambda P(1) \neq 0.$$

Let s be an element of $S^{-\varepsilon}$. Lemma 4.9.1 and Lemma 4.8.3 imply

$$\sum_{\lambda|\ell} \langle \mathrm{res}_\lambda s, \mathrm{res}_\lambda P(\ell)\rangle_\lambda^{-\varepsilon} = 0.$$

Since $\mathrm{res}_\lambda P(\ell) \neq 0$, the non-degeneracy of the local Tate pairing implies that $\mathrm{res}_\lambda s = 0$. Hence, $[s, \mathrm{Frob}_\lambda(L^S/L_1)] = 0$, that is $[s, (\tau h)^2] = 0$. By Cebotarev's density theorem, (see Chapter 2, Theorem 2.1 for more details) and Lemma 4.8.4, this statement is true for all h in $G_S^+ - I^+$. The homomorphism $s : G_S \longrightarrow V_\wp/p$ induces a G_V-homomorphism of groups

$$s : G_S^+ \longrightarrow V_\wp/p.$$

Therefore, the vanishing of s on $G_S^+ - I^+$ implies the vanishing of s on G_S^+. As a consequence, we obtain a G_V-homomorphism

$$s : G_S^- \longrightarrow V_\wp/p^\pm.$$

The modules $V_\wp/p^\pm$ are of rank 2 over $\mathscr{O}_{F,\wp}/p$. Since $V_\wp/p$ has no non-trivial G_V-submodules, we have $s(G_S^-) = s = 0$. □

Proposition 4.9.3. *We have $S^{+\varepsilon}$ is of rank 1 over $\mathscr{O}_{F,\wp}/p$.*

Proof. Let ℓ be a Kolyvagin prime such that

$$\mathrm{Frob}_\ell(L^S/\mathbb{Q}) = \tau i, \;\; i \in \mathrm{Gal}(L^S/L(y_1))$$

and such that

$$\mathrm{Frob}_\ell(L(P(q))/\mathbb{Q}) = \tau j, \;\; j \in \mathrm{Gal}(L(P(q))/L), \;\; j^{\tau+1} \neq 1.$$

These two Frobenius conditions are compatible because the extensions L^S and $L(P(q))$ are linearly disjoint by Lemma 4.7.5. Consider the Kolyvagin class $P(\ell q)$ which belongs to the $\varepsilon-$eigenspace by Remark 4.8.2. We have

$$\mathrm{res}_\lambda P(q) \neq 0$$

for λ above ℓ in K. Indeed, the Frobenius condition

$$\mathrm{Frob}_\lambda(L(P(q))/K) = j^{\tau+1} = (\tau j)^2 \neq 1$$

implies that λ does not split completely in $L(P(q))$. By Lemma 4.7.3, this implies that

$$\mathrm{res}_\lambda P(\ell q) \neq 0.$$

The Frobenius condition in $L^S/\mathbb{Q}$ implies that ℓ splits completely in $L(y_1)$, so that

$$\mathrm{res}_\lambda y_1 = 0.$$

Then by Lemma 4.7.3, $\mathrm{res}_\lambda P(\ell) = 0$. Hence, $P(\ell)$ belongs to the Selmer group, in fact to $S^{-\varepsilon}$. As a consequence of Proposition 4.9.2, $P(\ell) = 0$ implying

$$\mathrm{res}_\beta P(\ell) = 0.$$

Therefore by Lemma 4.7.3,

$$\mathrm{res}_\beta P(\ell q) = 0.$$

Let $s \in S^{+\varepsilon}$. By Lemma 4.9.1 and Lemma 4.8.3,

$$\sum_{\lambda|\ell} \langle \mathrm{res}_\lambda s, \mathrm{res}_\lambda P(\ell q)\rangle_\lambda^{+\varepsilon} + \sum_{\beta|q} \langle \mathrm{res}_\beta s, \mathrm{res}_\beta P(\ell q)\rangle_\beta^{+\varepsilon} = 0.$$

Hence,

$$\sum_{\lambda|\ell} \langle \mathrm{res}_\lambda s, \mathrm{res}_\lambda P(\ell q)\rangle_\lambda^{+\varepsilon} = 0.$$

The non-degeneracy of the local Tate pairing implies that

$$\mathrm{res}_\lambda s = 0.$$

Therefore, $[s, \mathrm{Frob}_\lambda(L^S/K_\lambda)] = 0$, that is

$$[s, (\tau i)^2] = 0.$$

This is true for all $i \in I$ by Cebotarev's density theorem and Lemma 4.8.4. As a consequence, the homomorphism $s : I \longrightarrow V_{\wp}/p$ reduces to a G_V-homomorphism

$$s : I^- \longrightarrow V_{\wp}/p^{\pm},$$

where $V_{\wp}/p^+$ and $V_{\wp}/p^-$ are free of rank 2 over $\mathscr{O}_{F,\wp}/p$. Therefore, since $V_{\wp}/p$ have no non-trivial G_V-submodules, $s(I^-) = s(I) = 0$. This implies that

$$s \in \mathrm{Hom}_{G_V}(\mathrm{Gal}(L^S/L)/I, V_{\wp}/p) \simeq \mathrm{Hom}_{G_V}(V_{\wp}/p, V_{\wp}/p) \simeq \mathscr{O}_{F,\wp}/p.$$

Therefore by Remark 4.8.2,

$$\mathrm{rank}(S) = 1.$$

□

Corollary 4.9.4. *Assume that f is ordinary at p. Under the hypotheses of Theorem 1.3.1, if $L'_p(f \otimes \theta_\psi, r+1) \neq 0$ then S is of rank 1 over $\mathscr{O}_{F,\wp}/p$.*

Proof. By [49, Theorem 1], the non-vanishing of $L'_p(f \otimes \theta_\psi, r+1)$ implies the non-vanishing of the image by the p-adic Abel-Jacobi map of the generalized Heegner cycle $\Phi(\Delta_I)_{\wp}$ of conductor 1, where I is the identity map. Since corestriction is injective, this implies that $P(1) \neq 0$. Hence, by Theorem 1.3.1, S is of rank 1 over $\mathscr{O}_{F,\wp}/p$. □

CHAPTER 5
Conclusion

5.1 From analytic rank to algebraic rank

Let $\phi : X_0(N) \longrightarrow E$ be a modular parametrisation of an elliptic curve E over $\mathbb{Q}$ with conductor N which maps the cusp infinity of $X_0(N)$ to the identity on E. Let x_1 be a Heegner point of conductor 1 on $X_0(N)$ attached to K. By the theory of complex multiplication, x_1 belongs to the Hilbert class field K_1 of K. Let $y_k = Tr_{K_1/K} y_k$. Gross-Zagier [28] proved that y_K has infinite order if and only if

$$L(E/K,1) = 0 \text{ and } L'(E/K,1) \neq 0.$$

Combined with Kolyvagin's result that

$$y_K \text{ has infinite order } \Rightarrow \text{rank}(E(K)) = 1,$$

one can conclude that

$$L'(E/K,1) \neq 0 \Rightarrow \text{rank}(E(K)) = 1.$$

Nekovář [39] adapted Kolyvagin's method to modular forms f of higher even weight. In [40], he proved a p-adic version of the Gross-Zagier formula relating the first derivative of a p-adic L-function of f at the central point and the p-adic height of a Heegner cycle. This result is due to Perrin-Riou in weight 2. As a consequence, Nekovář obtains a p-adic form of the conjecture of Beilinson and Bloch.

In [49], Shnidman relates the order of vanishing of the p-adic L-function of a modular form f twisted by an algebraic Hecke character at central critical points to the height of associated generalized Heegner cycles. Combining this with theorem 1.3.1 of Chapter 4, we obtain a p-adic version of the Beilinson-Bloch conjecture in Corollary 4.9.4.

5.2 Future directions

In the context of elliptic curves, if we omit the Heegner hypothesis, then the modular parametrisation fails to produce a non-trivial Heegner system [17, chapter 4]. Instead, one uses Shimura curve parametrisations [24]. In this setting, there are results of Zhang [55] and Disegni [19] computing heights of Heegner points on Shimura curves.

In the context of modular forms, Brooks [10] adapts results of Bertolini, Darmon and Prasanna [5] to the situation where the Heegner hypothesis is dropped. It would be interesting to have parallel results to Chapter 4 in this situation. More precisely, one could adapt the construction of generalized Heegner cycles to modular forms over Shimura curves in order to construct an appropriate Euler system and apply Kolyvagin's machinery to bound the size of the Selmer group, (see [22] for developments in this direction).

Bertolini, Darmon and Prasanna describe the relation between Abel-Jacobi images of generalized Heegner cycles and special values of certain p-adic L-function attached to the modular form [5]. Castella extends their results to a setting allowing arbitrary ramification at p [13]. An interesting future direction would be to examine the connection between the adapted generalized Heegner cycles (to the context of modular forms over Shimura curves) and special values of the p-adic L-function attached to f.

One could also consider Hida theoretic or Iwasawa theoretic settings such as in [21], [29] and [30].

References

[1] Donu Arapura and Kyungho Oh. On the Abel-Jacobi map for non-compact varieties. *Osaka J. Math.*, 34(4):769–781, 1997.

[2] Alexander A. Beilinson. Higher regulators and values of L-functions. *Journal of Soviet Mathematics*, 30(2):2036–2070, 1985.

[3] Massimo Bertolini and Henri Darmon. Kolyvagin's descent and Mordell-Weil groups over ring class fields. *J. Reine Angew. Math.*, 412:63–74, 1990.

[4] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. Chow-Heegner points on CM elliptic curves and values of p-adic L-functions. *International Mathematics Research Notices*, 2012.

[5] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. Generalized Heegner cycles and p-adic Rankin L-series. *Duke Math. J.*, 162(6):1033–1148, 2013.

[6] Manjul Bhargava and Arul Shankar. The average size of the 5-Selmer group of elliptic curves is 6, and the average rank is less than 1. *arXiv:1312.7859*, 2013.

[7] Manjul Bhargava, Christopher Skinner, and Wei Zhang. A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture. *arXiv:1407.1826*, 2014.

[8] Spencer Bloch. The dilogarithm and extensions of Lie algebras. In *Algebraic K-Theory Evanston 1980*, pages 1–23. Springer, 1981.

[9] Spencer Bloch and Kazuya Kato. L-functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.

[10] Ernest Hunter Brooks. *Generalized Heegner cycles, Shimura curves, and special values of p-adic L-functions*. PhD thesis, The University of Michigan, 2013.

[11] Jean-Luc Brylinski. Heights for local systems on curves. *Duke Math. J.*, 59(1):1–26, 1989.

[12] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for L-functions of modular forms and their derivatives. *Invent. Math.*, 102(3):543–618, 1990.

[13] Francesc Castella. *On the p-adic variation of Heegner points*. PhD thesis, McGill University, 2014.

[14] John Coates and Andrew Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[15] Pierre Colmez. Fonctions L p-adiques. *Séminaire Bourbaki*, 41:21–58, 1998-1999.

[16] David Cox. Primes of the form x^2+ny^2 with conditions. *J. Number Theory*, 130(4):852–861, 2010.

[17] Henri Darmon. Rational points on modular elliptic curves. *CBMS Reg. Conf. Ser. Math.*, 101, 2004. Published for the Conference Board of the Mathematical Sciences, Washington, DC.

[18] Pierre Deligne. Formes Modulaires et Representations de GL(2). In *Modular Functions of One Variable II*, volume 349 of *Lecture Notes in Math.*, pages 55–105. Springer Berlin Heidelberg, 1973.

[19] Daniel Disegni. p-adic heights of Heegner points on Shimura curves. *arXiv:1304.5204*, 2013.

[20] Tim Dokchitser and Vladimir Dokchitser. Parity of ranks for elliptic curves with a cyclic isogeny. *J. Number Theory*, 128(3):662–679, 2008.

[21] Olivier Fouquet. Euler systems in the Iwasawa theory of ordinary modular forms. In *Algebraic number theory and related topics 2008*, RIMS Kôkyûroku Bessatsu, B19, pages 255–276. Res. Inst. Math. Sci. (RIMS), Kyoto, 2010.

[22] Olivier Fouquet. Dihedral Iwasawa theory of nearly ordinary quaternionic automorphic forms. *Compos. Math.*, 149(3):356–416, 2013.

[23] Francesca Gala. Heegner points on $X_0(N)$. Master's thesis, Universita Degli Studi Di Milano, 2011.

[24] Matthew Greenberg. Computing Heegner points arising from Shimura curve parametrizations. In *Arithmetic geometry*, volume 8 of *Clay Math. Proc.*, pages 115–124. Amer. Math. Soc., Providence, RI, 2009.

[25] Benedict H. Gross. *Arithmetic on Elliptic Curves with Complex Multiplication*. PhD thesis, Harvard University, 1980.

[26] Benedict H. Gross. Heegner points on $X_0(N)$. In *Modular forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., pages 87–105. Horwood, Chichester, 1984.

[27] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.

[28] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[29] Benjamin Howard. The Heegner point Kolyvagin system. *Compos. Math.*, 140(6):1439–1472, 2004.

[30] Benjamin Howard. Special cohomology classes for modular Galois representations. *J. Number Theory*, 117(2):406–438, 2006.

[31] Uwe Jannsen. Continuous étale cohomology. *Math. Ann.*, 280(2):207–245, 1988.

[32] Uwe Jannsen. Algebraic cycles, K-theory, and extension classes. In *Mixed Motives and Algebraic K-Theory*, volume 1400 of *Lecture Notes in Math.*, pages 57–188. Springer Berlin Heidelberg, 1990.

[33] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, (295):ix, 117–290, 2004. Cohomologies p-adiques et applications arithmétiques. III.

[34] Victor A. Kolyvagin. *Euler Systems*, volume 2 of *The Grothendieck Festschrift*. Birkhäuser Boston, Boston, MA, 1990.

[35] Serge Lang. *Fundamentals of Diophantine Geometry*. Springer, 1983.

[36] Barry Mazur. Eigenvalues of Frobenius. In *Algebraic Geometry, Arcata 1974*, Proc. Sympos. Pure Math., pages 231–262. American Mathematical Society, 1975.

[37] James S. Milne. *Arithmetic Duality Theorems*. Perspectives in mathematics. Academic Press, 1986.

[38] M. Ram Murty and V. Kumar Murty. Mean values of derivatives of modular L-series. *Ann. of Math. (2)*, 133(3):447–475, 1991.

[39] Jan Nekovář. Kolyvagin's method for Chow groups of Kuga-Sato varieties. *Invent. Math.*, 107(1):99–125, 1992.

[40] Jan Nekovář. On the p-adic height of Heegner cycles. *Math. Ann.*, 302(1):609–686, 1995.

[41] Jan Nekovář. On the parity of ranks of Selmer groups II. *Comptes Rendus de l'Académie des Sciences-Series I-Mathematics*, 332(2):99–104, 2001.

[42] Bernadette Perrin-Riou. Points de Heegner et dérivées de fonctions L p-adiques. *Invent. Math.*, 89(3):455–510, 1987.

[43] Takeshi Saito. Weight-monodromy conjecture for ℓ-adic representations associated to modular forms. In *The arithmetic and geometry of algebraic cycles*, pages 427–431. Springer, 2000.

[44] Peter Schneider. Introduction to the Beilinson conjectures. *Perspectives in Mathematics*, 4:1–36, 1988.

[45] Chad Schoen. On the computation of the cycle class map for nullhomologous cycles over the algebraic closure of a finite field. *Ann. Sci.éc. Norm. Supér.*, 28(1):1–50, 1995.

[46] Anthony J. Scholl. Motives for modular forms. *Invent. Math.*, 100(1):419–430, 1990.

[47] Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics. Springer New York, 1995.

[48] Jean-Pierre Serre. Groupes finis. *arXiv: 0503154*, 2005.

[49] Ariel Shnidman. p-adic heights of generalized Heegner cycles. *arXiv: 1407.0785v2*, pages 1–34, 2014.

[50] Christopher Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin. *arXiv:1405.7294*, 2014.

[51] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL2. *Invent. Math.*, 195(1):1–277, 2014.

[52] Michio Suzuki. *Group theory*. Number vol. 1 in Grundlehren der mathematischen Wissenschaften. Springer-Verlag, 1982.

[53] John Tate. Duality theorems in Galois cohomology over number fields. In *Proceedings of an International Congress on Mathematics Stockholm*, pages 288–295, 1962.

[54] Takeshi Tsuji. On p-adic Hodge theory for semi-stable families. *Sūrikaisekikenkyūsho Kōkyūroku*, (884):141–153, 1994. Moduli spaces, Galois representations and L-function.

[55] Shouwu Zhang. Heights of Heegner points on Shimura curves. *Ann. of Math.*, 153(1):27–147, 2001.

[56] Wei Zhang. Selmer groups and the divisibility of Heegner points. *Cambridge Journal of Mathematics*, 0(0), 2014.