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

© Yara Elias 2015
DEDICATION

To Gorka, Greta, Jean and Rayane
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

**DEDICATION** ................................................................. ii

**ACKNOWLEDGEMENTS** .................................................. iii

**ABSTRACT** ................................................................. iv

**RÉSUMÉ** ................................................................. v

1 **Introduction** ............................................................. 1
   
   1.1 **Introduction** .................................................. 1
   1.2 **First contribution** .......................................... 7
   1.3 **Second contribution** ......................................... 9

2 **Preliminaries** .......................................................... 14

   2.1 **Abel-Jacobi map** ............................................. 14
   2.2 **Frobenius substitution** ..................................... 16
   2.3 **Local class field theory** ................................. 19
   2.4 **Brauer group and local reciprocity** .................... 22
   2.5 **Local Tate duality** ....................................... 25
   2.6 **Weil conjectures** ......................................... 28

3 **Kolyvagin's method for Chow groups of Kuga-Sato varieties over ring class fields** ............................................... 29

   3.1 **Introduction** .................................................. 29
   3.2 **Motive associated to a modular form** .................... 32
   3.3 **Heegner cycles** ............................................. 35
   3.4 **The Euler system** .......................................... 38
   3.5 **Localization of Kolyvagin classes** ....................... 43
   3.6 **Statement** ................................................... 47
   3.7 **Generating the dual of the Selmer group** ................ 49
   3.8 **Bounding the size of the dual of the Selmer group** .... 60
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>On the Selmer group attached to a modular form and an algebraic Hecke character</td>
<td>64</td>
</tr>
<tr>
<td>4.1</td>
<td>Introduction</td>
<td>64</td>
</tr>
<tr>
<td>4.2</td>
<td>Motive associated to a modular form and a Hecke character</td>
<td>69</td>
</tr>
<tr>
<td>4.3</td>
<td>p-adic Abel-Jacobi map</td>
<td>72</td>
</tr>
<tr>
<td>4.4</td>
<td>Generalized Heegner cycles</td>
<td>74</td>
</tr>
<tr>
<td>4.5</td>
<td>Euler system properties</td>
<td>77</td>
</tr>
<tr>
<td>4.6</td>
<td>Kolyvagin cohomology classes</td>
<td>82</td>
</tr>
<tr>
<td>4.7</td>
<td>Global extensions by Kolyvagin classes</td>
<td>86</td>
</tr>
<tr>
<td>4.8</td>
<td>Complex conjugation and local Tate duality</td>
<td>90</td>
</tr>
<tr>
<td>4.9</td>
<td>Reciprocity law and local triviality</td>
<td>93</td>
</tr>
<tr>
<td>5</td>
<td>Conclusion</td>
<td>98</td>
</tr>
<tr>
<td>5.1</td>
<td>From analytic rank to algebraic rank</td>
<td>98</td>
</tr>
<tr>
<td>5.2</td>
<td>Future directions</td>
<td>99</td>
</tr>
<tr>
<td>References</td>
<td></td>
<td>100</td>
</tr>
</tbody>
</table>
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

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

\[ 0 \rightarrow E(K)/pE(K) \rightarrow \text{Sel}_p(E/K) \rightarrow \text{III}(E/K)_p \rightarrow 0 \]

relates the rank of \( E(K) \) to the size of the so-called Selmer group \( \text{Sel}_p(E/K) \). The Shafarevich-Tate conjecture on the finiteness of \( \text{III}(E/K) \), the Shafarevich group of \( E \) over \( K \), implies that \( \text{Sel}_p(E/K) \) 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

\[ r(E/F) \geq 1 \Rightarrow r_{an}(E/F) \geq 1. \]

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

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

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

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

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

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 $\mathbb{Q}$,

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

No assumptions are made about the primes for which $E$ has additive reduction. However, the 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

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

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

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

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 $X_1(N)$,

- $\text{CH}^r(X/K)_0$ 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 $\text{Gal}(\overline{K}/K)$ acting on $A$. 

5
The Beilinson-Bloch conjecture, which generalizes Birch and Swinnerton-Dyer’s, predicts that

$$\dim_{\mathbb{Q}_p}(\text{Im}(\Phi) \otimes \mathbb{Q}_p) = \text{ord}_{s=r}L(f \otimes K, s).$$  \hspace{1cm} (1.1)$$

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

In [39], Nekovář shows that

$$\dim_{\mathbb{Q}_p}(\text{Im}(\Phi) \otimes \mathbb{Q}_p) = 1$$ \hspace{1cm} (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 \( |\mathcal{O}_K^\times| = 2 \). 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 \( \text{Gal}(H/K) \). 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 \( \mu_e \) and let \( \mathcal{O}_F \) 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 \( \mathcal{O}_F \otimes \mathbb{Z}_p \) module of rank 2, equipped with a continuous \( \mathcal{O}_F \)-linear action of \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \). Let \( A_{\wp} \) be the localization of \( A \) at a prime \( \wp \) of \( \mathcal{O}_F \) dividing \( p \). Then \( A_{\wp} \) is a free module of rank 2 over \( \mathcal{O}_{\wp} \), the completion of \( \mathcal{O}_F \) at \( \wp \). For a \( p \)-torsion \( \text{Gal}(\overline{H}/H) \) 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

\[
\begin{cases}
H^1(H_v^{\text{nr}}/H_v,M) & \text{for } v \text{ not dividing } Np \\
H^1_f(H_v,M) & \text{for } v \text{ dividing } p
\end{cases}
\]
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

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

acts on $H^1(H,M)$ hence it acts on $S$. Assume that $p$ does not divide $|G|$. We denote by $\hat{G} = \text{Hom}(G,\mu_e)$ 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 $\chi$-eigenspace given a character $\chi$ of $\hat{G}$. By the Heegner hypothesis, there is an ideal $\mathcal{N}$ of $\mathcal{O}_c$, the order of $K$ of conductor $c$, such that

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

Therefore, $\mathbb{C}/\mathcal{O}_c$ and $\mathbb{C}/\mathcal{N}^{-1}$ 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 $\mathcal{O}_c$. The Heegner cycle of conductor $c$ is defined as

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

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 $\text{Gal}(H_{v}^{\text{ur}}/H_{v})$, and by $I_{v} = \text{Gal}(\overline{H}_{v}/H_{v}^{\text{ur}})$. In Chapter 3 which is submitted for publication, we prove the following statement.

**Theorem 1.2.1.** Assume that $p$ is such that

$$\text{Gal}(\mathbb{Q}(A_{\rho}/p)/\mathbb{Q}) \cong \text{GL}_2(\mathcal{O}_{\rho}/p), \quad (p, ND\phi(N)) = 1, \text{ and } p \nmid |G|.$$ 

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

$$e^{\chi}y_1 \neq 0.$$ 

Then the $\chi$-eigenspace $S^\chi$ of the Selmer group $S$ has rank 1 over $\mathcal{O}_{\rho}/p$.

### 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 $|O_K^\times| = 2$. Let

$$\psi : A_K^\times \longrightarrow \mathbb{C}^\times$$

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 $O_K$ such that $\psi$ is the Hecke character associated to $A$ \cite[Theorem 9.1.3]{25}. 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 $\text{Aut}(K_1)$. (See \cite[Section 11]{25}). 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 \cite{46} and Deligne \cite{18} twisted by $r+2$ and by $V_{\psi}$ the $p$-adic étale realization of the motive associated to $\psi$ twisted by $\frac{r}{2}$. More precisely, $V_{\psi}$ is the $\psi$-isotypic component of

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

where $A^\sigma$ is the $\sigma$-conjugate of $A$, (see Section 4.2 for more details). Let $\mathcal{O}_F$ 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

$$\theta_{\psi} = \sum_{a \in \mathcal{O}_K} \psi(a)q^{N(a)}$$
associated to \( \psi \). Then \( V_f \) and \( V_\psi \) will be viewed (by extending scalars appropriately) as free \( \mathcal{O}_F \otimes \mathbb{Z}_p \)-modules of rank 2. We denote by

\[
V = V_f \otimes \mathcal{O}_F \otimes \mathbb{Z}_p \ V_\psi
\]

the \( p \)-adic étale realization of the twisted motive associated to \( f \) and \( \psi \) and let \( V_\wp \) be its localization at a prime \( \wp \) in \( F \) dividing \( p \). Then \( V_\wp \) is a four dimensional representation of \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) with coefficients in \( \text{End}(A/\mathbb{Q}) = \bigoplus_{\sigma \in \text{Gal}(H/\mathbb{Q})} \text{Hom}(A,A^\sigma) \).

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

\[
\mathcal{O}_K/\mathcal{N} = \mathbb{Z}/N \mathbb{Z}.
\]

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 \( \mathcal{N} \). Consider a pair \( (\varphi_1,A_1) \) 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 \( V \)

\[
\Upsilon_{\varphi_1} = \text{Graph}(\varphi_1)^T \subset (A \times A_1)^T \simeq (A_1)^T \times A^r \subset W_r \times A^r
\]

and define a \textit{generalized Heegner cycle} of conductor 1

\[
\Delta_{\varphi_1} = e_r \Upsilon_{\varphi_1},
\]
where $e_r$ is an appropriate projector (4.1). Then $\Delta_{\phi_1}$ is defined over $L_1$. The Selmer group

$$S \subseteq H^1(K, V_{\phi}/p)$$

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

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

where $K_v$ is the completion of $K$ at $v$, and

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

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

**Theorem 1.3.1.** Let $p$ be such that

$$\text{Gal}(K(V_{\phi}/p)/K) \simeq \text{Aut}_K(V_{\phi}/p), \text{ and } (p, N\mathbb{D}(N)\mathbb{N}_A) = 1.$$ 

Suppose that $V_{\phi}/p$ is a simple $\text{Aut}(V_{\phi}/p)$-module. Suppose further that the eigenvalues of $Fr(v)$ acting on $V_{\phi}^{I_v}$ are not equal to 1 modulo $p$ for $v$ dividing $N\mathbb{N}_A$. Assume the corestriction $\text{cor}_{L_1,K}\Phi(\Delta_{\phi_1}) \neq 0$ where

$$\Phi(\Delta_{\phi_1}) \in H^1(K, V_{\phi}/p)$$

is the image by the $p$-adic Abel-Jacobi map of the generalized Heegner cycle $\Delta_{\phi_1}$. Then the Selmer group $S$ has rank 1 over $\mathcal{O}_{F,\phi}/p$. 

12
One could consider other flavours of Selmer groups. Instead of studying the Selmer group with coefficients in $V_{\psi}/p$, 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 $\alpha, \beta$ are rationally equivalent if there is $u_0 \neq u_1 \in U$ with $\gamma_{u_0} = \alpha$ 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 $\alpha, \beta$ are \textit{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 $\mathcal{F}$ be an étale sheaf on the étale site of $X$ and let $i^!$ be the right adjoint of $i_\ast$. The group of sections of $\mathcal{F}$ with support on $Z$ is

$$\Gamma(X, i_\ast i^! \mathcal{F}) = \Gamma(Z, i^! \mathcal{F}) = \ker(\mathcal{F}(X) \rightarrow \mathcal{F}(U)).$$

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

$$H^k_{\text{et}}(Z, \mathcal{F}) : \mathcal{F} \rightarrow R^k \Gamma(Z, i^! \mathcal{F}).$$

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

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

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

$$0 \rightarrow H^{2c-1}_{\text{et}}(X, \mathcal{F}) \rightarrow H^{2c-1}_{\text{et}}(U, \mathcal{F}) \rightarrow H^{2c}_{\text{et}}(X, \mathcal{F}) \xrightarrow{i^!} H^{2c}_{\text{et}}(X, \mathcal{F}) \rightarrow 0,$$

$$0 \rightarrow H^{2d}_{\text{et}}(X, \mathcal{F}) \rightarrow H^{2d}_{\text{et}}(U, \mathcal{F}) \rightarrow H^{2d}_{\text{et}}(U, \mathcal{F}) \rightarrow 0,$$

where

$$H^k_{\text{et}}(X, \mathcal{F}) \simeq H^{k-2c}_{\text{et}}(Z, i^! \mathcal{F}(-c)).$$

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

$$cl : CH^c(X) \rightarrow H^{2c}_{\text{et}}(\overline{X}, \mathbb{Z}_p(c))^G.$$
where $\overline{X} = X \otimes \overline{K}$. For $Z \in CH^c(X)_0$, consider the diagram

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

where

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

is the kernel of the Gysin map and

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

Here, $E_Z$ is identified with a subquotient of

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

The $p$-adic Abel-Jacobi map is the map

$$
AJ^p : CH^0(X) \rightarrow Ext^1(\mathbb{Z}_p, H^{2c-1}_{et}(\overline{X}, \mathbb{Z}_p(c))) = H^1(K, H^{2c-1}_{et}(\overline{X}, \mathbb{Z}_p(c)))
$$

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 $\text{Gal}(\overline{K}/K)$.

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

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

uniquely determined by the condition that

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

where $N(p) = |\mathcal{O}_F/p|$. 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

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

the Frobenius substitution of $p$. When $p$ is a real infinite place, $(p, L/F)$ is the complex conjugation $\tau$. 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 occurrence of a conjugacy class $[\sigma]$ of an element $\sigma \in \text{Gal}(L/F)$ 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

$$\frac{|[\sigma]|}{[L:F]} = \frac{|[\sigma]|}{|\text{Gal}(L/F)|}.$$  \hfill (2.1)

and is hence infinite. In particular, if $L/F$ is abelian, then the set of unramified primes such that $\text{Frob}_p(L/F)$ 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 $s\bar{x}$ is a representative of $sx$ in $X$, then there exists $h_{s,x} \in H$ such that
\[ s\bar{x} = \bar{x} h_{s,x}. \]

Consider the map
\[ \text{Ver} : G \rightarrow H^{ab} : s \mapsto \prod_{x \in \bar{X}} h_{s,x} \mod [H,H], \]
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 $\mathcal{O}_x$ the orbits of $X$ under the action of $C$ and by $f_\alpha$ the cardinality of $\mathcal{O}_x$. If $x_\alpha$ belongs to $\mathcal{O}_x$, then $s^{f_\alpha}x_\alpha = x_\alpha$. This implies that given a representative $g_\alpha$ of $x_\alpha$ in $G$, there exists $h_\alpha \in H$ such that
\[ s^{f_\alpha}g_\alpha = g_\alpha h_\alpha. \]

Therefore, it is enough to show that
\[ \text{Ver}(s) = \prod_\alpha h_\alpha = \prod_\alpha g_\alpha^{-1}s^{f_\alpha}g_\alpha \mod [H,H] \]

to conclude that the homomorphism $G^{ab} \rightarrow H^{ab} \rightarrow G^{ab}$ maps $s$ to $s^n$. Indeed,
\[ g_\alpha^{-1}s^{f_\alpha}g_\alpha = s^{f_\alpha} \mod [G,G], \quad \text{and} \quad s^{\sum f_\alpha} = s^n. \]
In particular, if $G$ is abelian, we obtain a homomorphism
\[ \text{Ver} : G \rightarrow H : s \mapsto s^n. \]

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
\[
\begin{cases}
  m_p \geq 0 & \text{is non-zero for finitely many places } p \\
  m_p = 0 & \text{or 1 for infinite real places} \\
  m_p = 0 & \text{for infinite complex places}
\end{cases}
\]
Writing $m$ as $m = m_0m_\infty$, 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

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

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

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

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

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

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. $P_{E,1}(m) \subseteq \text{ker}(\psi)$
3. $\ker(\psi) = P_{E,1}(m) N_{E/F}(I_E(m'))$, 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

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

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

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

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

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

where

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

$$\text{Pic}(\mathcal{O}_m) \simeq \text{Gal}(K_m/K).$$

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

$$\text{Gal}(K_m/K_1) \simeq \frac{I_K(m\mathcal{O}_K) \cap P_K(\mathcal{O}_K)}{P_{K,Z}(m\mathcal{O}_K)} \simeq \frac{(\mathcal{O}_K/m)^*}{(\mathbb{Z}/m)^*}.$$ \[
\text{This provides a formula for the ratio of the class numbers of a ring and a suborder. The complex conjugation } \tau \text{ which generates } \text{Gal}(K/\mathbb{Q}) \text{ acts on an element } \sigma \text{ of } \text{Gal}(K_m/K) \text{ by } \tau \sigma \tau^{-1} = \sigma^{-1} \text{ and we have}
\]

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

### 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

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

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

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

$$
0 \rightarrow B_k \rightarrow \bigoplus_v B_{k_v} \xrightarrow{\sigma} \mathbb{Q}/\mathbb{Z} \rightarrow 0,
$$

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

$$
\text{inv}_{k_v} : B_{k_v} \simeq \mathbb{Q}/\mathbb{Z}.
$$

(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

$$
\text{res}_{K,L} : B_K \rightarrow B_L
$$
be the canonical homomorphism of $B_K$ into $B_L$. Then

$$inv_L \circ res_{K,L} = n \cdot inv_K.$$  

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 $\mu_n$ of $n$-th roots of unity. We choose a primitive $n$-th root of unity $\omega$ identifying $\mu_n$ with the group $\mathbb{Z}/n\mathbb{Z}$. The exact sequence

$$0 \rightarrow \mu_n \rightarrow \mathbb{K}^n \xrightarrow{\nu} \mathbb{K}^n \rightarrow 0,$$

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

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

since $H^1(G, K^*) = 0$. Given elements $a, b$ of $K^*$ we can associate elements $\phi_a, \phi_b$ 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 $\omega$ by the corollary to [47] Proposition XIV.2.6. Assume $L = K\left(\frac{1}{\sqrt{n}}\right)$, 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
\[
(a, b)_v = (b, */K)(a^n)/a^n
\]
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 \(K_{\lambda}\) be a local field with residue field \(F_q\) and let \(A\) be a finite group with an unramified action of \(\text{Gal}(\overline{K_{\lambda}}/K_{\lambda})\) killed by a prime \(p\). Assume \(p\) divides \(q - 1\) so that \(\mu_p \subset K_{\lambda}\) and let \(A' = \text{Hom}(A, \mu_p)\). We denote by \(K_{\lambda}^{ur}\), the maximal unramified extension of \(K_{\lambda}\), by \(K_{\lambda}^{t}\), the maximal tamely ramified extension of \(K_{\lambda}\), and by \(H^1_{ur}(K_{\lambda}, *)\), the group \(H^1(K_{\lambda}^{ur}/K_{\lambda}, *)\).

The natural pairing \(A \times A' \rightarrow \mu_p\) yields the cup product pairing
\[
H^1(K_{\lambda}, A) \times H^1(K_{\lambda}, A') \rightarrow H^2(K_{\lambda}, \mu_p) = \mathbb{Z}/p\mathbb{Z}
\]
which induces a perfect local Tate pairing
\[
H^1(K_{\lambda}^{ur}/K_{\lambda}, A) \times H^1(K_{\lambda}, A')/H^1(K_{\lambda}^{ur}/K_{\lambda}, A) \rightarrow \mathbb{Z}/p\mathbb{Z}.
\]

Let
\[
\alpha : H^1(K_{\lambda}^{ur}/K_{\lambda}, A) \xrightarrow{\sim} A/(\phi - 1)A
\]
be the evaluation map at the Frobenius element \(\phi\) where
\[
\text{Gal}(K_{\lambda}^{ur}/K_{\lambda}) = \langle \phi \rangle.
\]
Then $\alpha$ is an isomorphism. The exact sequence of Galois groups

$$0 \to \text{Gal}(\overline{K_{\lambda}}/K_{\lambda}) \to \text{Gal}(\overline{K_{\lambda}}/K_{\lambda}^{ur}) \to \text{Gal}(K_{\lambda}^{ur}/K_{\lambda}^{ur}) \to 0$$

induces the exact sequence

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

where $H^1(K_{\lambda}^{ur}, A') = 0$ since $\text{Gal}(\overline{K_{\lambda}}/K_{\lambda})$ is a pro-$q$ group. Therefore,

$$H^1(K_{\lambda}^{ur}, A') \simeq H^1(K_{\lambda}^{ur}/K_{\lambda}^{ur}, A') \simeq \text{Hom}(\mathbb{Z}/p\mathbb{Z}(1), A') \simeq \text{Hom}(\mu_p, A').$$

Hence we have an isomorphism

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

The exact sequence of Galois cohomology groups

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

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

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

Hence, we obtain a perfect local pairing

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

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 $\phi$ 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 $K_{\ell}$ is its ring class field of conductor $\ell$. Since the extension $K_{\lambda}/K_{\lambda}$ is totally ramified, the generator $\sigma_{\ell}$ of $Gal(K_{\lambda}/K_{\lambda})$ can be lifted to a generator

$$\tau_{\ell} \in Gal(K_{\lambda}^{ur}/K_{\lambda}^{ur}) \simeq \hat{\mathbb{Z}}/(1) = \prod_{q \neq \ell} \mathbb{Z}_q(1).$$

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

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

We obtain the map $\beta$

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

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

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

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

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

(2.2)

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

27
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 $\bar{k}$ 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

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

where $\phi$ is the Frobenius endomorphism acting on the étale cohomology $H^j$ of $V$. (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 $\alpha$ is an eigenvalue of the geometric Frobenius acting on $H^j(V)$ for an étale cohomology $H^j$ and $| \cdot |$ is any archimedean absolute value then $|\alpha| = q^{\frac{j}{2}}$. 

28
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 $|\mathcal{O}_K^\times| = 2$. 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 $\text{Gal}(H/K)$. 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 $\mu_e$. 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 $\mathcal{O}_F \otimes \mathbb{Z}_p$ module of rank 2, equipped with a continuous $\mathcal{O}_F$-linear action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $A_{\wp}$ be the localization of $A$ at a prime $\wp$ of $\mathcal{O}_F$ dividing $p$. Then $A_{\wp}$ is a free module of rank 2 over $\mathcal{O}_{\wp}$, the completion of $\mathcal{O}_F$ 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

\[
\begin{cases}
H^1(H_v^{ur}/H_v, A_{\varphi}/p) \text{ for } v \text{ not dividing } Np \\
H^1_f(H_v, A_{\varphi}/p) \text{ for } v \text{ dividing } p
\end{cases}
\]

where \( H^1_f(H_v, A_{\varphi}/p) \) is the **finite part** of \( H^1(H_v, A_{\varphi}/p) \) as in [9]. In our setting, since \( A_{\varphi} \) 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 \( H^1(H_v^{ur}/H_v, A_{\varphi}/p) = 0 \) for \( v \) dividing \( N \). The Galois group

\[ G = \text{Gal}(H/K) \]

acts on \( H^1(H, A_{\varphi}/p) \) and preserves the unramified and cristalline classes, hence it acts on \( S \). Assume that \( p \) does not divide \( |G| \). We denote by \( \hat{G} = \text{Hom}(G, \mu_c) \) 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 \( \chi \)-eigenspace given a character \( \chi \) of \( \hat{G} \).

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

\[ \mathcal{O}_c/\mathcal{N} = \mathbb{Z}/N\mathbb{Z}. \]

Therefore, \( \mathbb{C}/\mathcal{O}_c \) and \( \mathbb{C}/\mathcal{N}^{-1} \) 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 \( \mathcal{O}_c \). The Heegner
cycle of conductor $c$ is defined as

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

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

**Theorem 1.2.1.** Assume that $p$ is such that

$$\text{Gal}\left(\mathbb{Q}(A_{\rho}/p)/\mathbb{Q}\right) \cong \text{GL}_2(\mathcal{O}_{\rho}/p), \quad (p, ND\phi(N)) = 1, \quad p \nmid |G|.$$  

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

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 $\chi$-eigenspace of the Selmer group $S^\chi$, 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 $S^\chi$ 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 $\chi$ is trivial, the complex conjugation $\tau$ does not act on $S^\chi$ as
it maps it to $S^\bar{\chi}$.

3.2 Motive associated to a modular form

In this section, we describe the $p$-adic étale realization $\mathcal{A}$ 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 $SL_2(\mathbb{Z})$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \mod N \right\}. $$

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

$$\pi : \mathcal{E} \longrightarrow X_0(N).$$
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 \(\mathcal{E}\) 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
\[ \mathcal{E} \times_{X_0(N)} \cdots \times_{X_0(N)} \mathcal{E}, \]
(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
\[ \mathcal{F} = \text{Sym}^{2r - 2}(R^1\pi_*\mathbb{Z}/p). \]
Let
\[ \Gamma_{2r-2} = (\mathbb{Z}/N \times \mu_2)^{2r - 2} \rtimes \Sigma_{r-2} \]
where \(\mu_2 = \{\pm 1\}\) and \(\Sigma_{r-2}\) is the symmetric group on \(2r - 2\) elements. Then \(\Gamma_{2r-2}\) 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 \(\Gamma_{2r-2}\), called Scholl’s projector, belongs to the group of zero correspondences \(\text{Corr}^0(W_{2r-2}, W_{2r-2})_\mathbb{Q}\) 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.

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

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]).

Define

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

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

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

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

Consider the étale $p$-adic Abel-Jacobi map

$$\Phi : CH^r(W_{2r-2}/H)_0 \to H^1(H, H^{2r-1}_{et}(W_{2r-2} \otimes \overline{H}, \mathbb{Z}_p(r)))$$
where $\text{CH}^r(W_{2r-2}/H)_{0}$ 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

$$\Phi : \text{CH}^r(W_{2r-2}/H)_{0} \longrightarrow H^1(H,J).$$

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

$$e_r(\text{CH}^r(W_{2r-2}/H)_{0} \otimes \mathbb{Z}_p).$$

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

$$\text{CH}^r(W_{2r-2}/H)_{0} = \text{Ker}(\text{CH}^r(W_{2r-2}/H) \longrightarrow H^{r+1}(W_{2r-2} \otimes \overline{H}, \mathbb{Z}_p)),$$

we have $e_r(\text{CH}^r(W_{2r-2}/H)_{0} \otimes \mathbb{Z}_p) = e_r(\text{CH}^r(W_{2r-2}/H) \otimes \mathbb{Z}_p)$. Composing the former map with the map $e_A : J \longrightarrow A$, we get

$$\Phi : e_r \text{CH}^r(W_{2r-2}/H)_{0} \longrightarrow H^1(H,A).$$

### 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 \( \mathcal{N} \) of \( \mathcal{O}_{cm} \), the order of \( K \) of conductor \( cm \), such that
\[
\mathcal{O}_{cm}/\mathcal{N} = \mathbb{Z}/N\mathbb{Z}.
\]
Therefore, \( \mathbb{C}/\mathcal{O}_{cm} \) and \( \mathbb{C}/\mathcal{N}^{-1} \) 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 \( \mathcal{O}_{cm} \). Letting \( \text{graph}(-D) \) be the graph of the multiplication by \( -D \) on \( E \), we denote by \( Z_E \) the image of the divisor
\[
(\text{graph}(-D) - E \times 0 - D(0 \times E))
\]
in the Néron-Severi group \( \text{NS}(E \times E) \) 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 \( \text{CH}^r(W_{2r-2}/H_m)_0 \). Denote by \( y_m \) the image of \( i_*(Z_E^{r-1}) \) by the \( p \)-adic étale Abel-Jacobi map
\[
\Phi : \text{CH}^r(W_{2r-2}/H_m)_0 \longrightarrow H^1(H_m,A)
\]
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 $\ell$ is a prime inert in $K$. Then

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

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

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

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

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

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

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

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

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

The equality

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

follows from the definition of $A$ on which Hecke operators $T_\ell$ act by $a_\ell$. \qed

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

37
Proposition 3.3.2. Consider cocycles $y_n$ and $y_m$ with $n = \ell m$, where $\ell$ is a prime inert in $K$. Let $\lambda_m$ be a prime above $\ell$ in $K_m$ and $\lambda_n$ the prime above $\lambda_m$ in $K_n$. Then

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

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 $\ell_i$ inert in $K$ satisfying

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

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

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

the $\varnothing$-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 $P(n) \in H^1(H,A_\varnothing/p)$ using the cohomology classes $y_n \in H^1(H_n,A)$ for appropriate $n$. Let

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

be the smallest Galois extension of $H$ such that $\Gal(\overline{\mathbb{Q}}/L)$ acts trivially on $A_\varnothing/p$. We will denote by $\text{Frob}_{F_1/F_2}(\alpha)$, the conjugacy class of the Frobenius substitution of the prime $\alpha$ of $F_2$ in $\Gal(F_1/F_2)$.
A prime \( \ell \) will be referred to as a \textit{Kolyvagin prime} if it is such that

\[
(\ell, DNpc) = 1 \text{ and } \text{Frob}_\ell(L/Q) = \text{Frob}_\infty(L/Q),
\]

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

\[
\text{Frob}_{\lambda'}(L/H) = \tau^2 = \text{Id}.
\]

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 \( A_p/p \) is \( x^2 - 1 \) while the characteristic polynomial of \( \text{Frob}(\ell) \) 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

$$\text{Tr}_\ell = \sum_{i=0}^\ell \sigma^i, \quad D_\ell = \sum_{i=1}^\ell i \sigma^i. \quad (3.2)$$

These operators are related by

$$(\sigma - 1)D_\ell = 1 + \text{Tr}_\ell.$$ 

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

$$A_{\varphi} \longrightarrow A_{\varphi}/p.$$

**Proposition 3.4.1.** We have

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

**Proof.** It is enough to show that for all $\ell$ dividing $n$,

$$(\sigma - 1)D_n \text{red}(y_{n, \varphi}) = 0$$

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

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

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

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

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

40
Proposition 3.4.2. For \( n \) such that \((n, cpND) = 1\), we have

\[
H^0(H_n, A_{\phi}/p) = H^0(\mathbb{Q}, A_{\phi}/p) = 0, \\
\text{and } \text{Gal}(H_n(A_{\phi}/p)/H_n) \simeq \text{Gal}(H(A_{\phi}/p)/H) \simeq \text{Gal}(K(A_{\phi}/p)/K) \simeq \text{Gal}(\mathbb{Q}(A_{\phi}/p)/\mathbb{Q}).
\]

Proof. Indeed, \( H_n/\mathbb{Q} \) and \( \mathbb{Q}(A_{\phi}/p)/\mathbb{Q} \) are unramified outside primes dividing \( cnD \) and \( Np \) respectively, so \( H_n \cap \mathbb{Q}(A_{\phi}/p) \) is unramified over \( \mathbb{Q} \). Since \( \mathbb{Q} \) has no unramified extensions, we obtain that \( H_n \cap \mathbb{Q}(A_{\phi}/p) = \mathbb{Q} \), and therefore \( H^0(H_n, A_{\phi}/p) = H^0(\mathbb{Q}, Y_p) \).

The hypothesis \( \text{Gal}(\mathbb{Q}(A_{\phi}/p)/\mathbb{Q}) \simeq \text{GL}_2(\mathcal{O}_{\phi}/p) \) further implies that \( H^0(\mathbb{Q}, A_{\phi}/p) = 0 \).

The result follows. \( \square \)

Proposition 3.4.3. The restriction map

\[
\text{res}_{H,H_n} : H^1(H, A_{\phi}/p) \longrightarrow H^1(H_n, A_{\phi}/p)^{G_n}
\]

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

Proof. This follows from the inflation-restriction sequence:

\[
0 \to H^1(H_n/H, A_{\phi}/p) \overset{\text{inf}}{\longrightarrow} H^1(H, A_{\phi}/p) \overset{\text{res}}{\longrightarrow} H^1(H_n, A_{\phi}/p)^{G_n} \to H^2(H_n/H, A_{\phi}/p)
\]

using the fact that \( H^0(H_n, A_{\phi}/p) = 0 \) by Proposition 3.4.2. \( \square \)

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

\[
\text{res}_{H,H_n}P(n) = D_{n\text{red}}(y_{n, \phi}).
\]
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 $H^1(H_{v,ur}^\text{ur}/H_v, A_\varphi/p)$.

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

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

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

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

Local Tate duality then implies

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

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

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

and $I_v = \text{Gal}(\overline{H_v}/H_v^{ur})$ is the inertia group. (See Section 2.6 for more details). Therefore,

$$((A_\varphi/p)_{I_v})^G(H_v^{ur}/H_v) = (A_\varphi/p)^G(\overline{H_v}/H_v) = H^0(H_v, A_\varphi/p) = 0.$$

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

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

belongs to $H^1(H_{n, v', ur}^\text{ur}/H_{n, v'}, A_\varphi/p)$ and $H_{n, v'}/H_v$ is unramified for $v'$ in $H_n$ above $v$. \qed
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 \( \ell \) by explicitly computing cocycles using the Euler system properties. We briefly explain his development in this section.

**Set up.** We denote by

\[
G_1 = \text{Gal}(\overline{Q}/H_1), \quad G_\ell = \text{Gal}(\overline{Q}/H_\ell), \quad \tilde{G}_1 = \text{Gal}(\overline{Q}/H_1^+),
\]

and

\[
G_{\lambda_1} = \text{Gal}(\overline{Q}_\ell/H_{1,\lambda_1}), \quad G_{\lambda_\ell} = \text{Gal}(\overline{Q}_\ell/H_{\ell,\lambda_\ell}), \quad \tilde{G}_{\lambda_1} = \text{Gal}(\overline{Q}_\ell/Q_\ell),
\]

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

\[
G_1 / G_\ell = < \sigma >, \quad \tilde{G}_1 / G_1 = < \tau >, \quad \tilde{G}_1 / G_\ell = \text{Gal}(H_\ell/H_1^+) = < \sigma > \times < \tau >
\]

for some \( \sigma \) and \( \tau \) of order \( \ell + 1 \) and 2 respectively. There is a surjective homomorphism

\[
\pi : \tilde{G}_{\lambda_1} \xrightarrow{\text{res}} \text{Gal}(Q'_\ell/Q_\ell) = \hat{\mathbb{Z}}' (1) \times 2\hat{\mathbb{Z}},
\]

where

\[
\text{Gal}(Q'_\ell/Q^\ur_\ell) \simeq \hat{\mathbb{Z}}' (1) = \prod_{q \neq \ell} \hat{\mathbb{Z}}_\ell
\]

is generated by an element \( \tau_\ell \) and

\[
\text{Gal}(Q^\ur_\ell/Q_\ell) \simeq \hat{\mathbb{Z}}
\]

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

\[
H^1(G_{\lambda_1}, A_\rho/p) = H^1(G_{\lambda_\ell}, A_\rho/p) \simeq H^1(2\hat{\mathbb{Z}}, A_\rho/p) \simeq (A_\rho/p)/((\phi^2 - 1)A_\rho/p)
\]
and a cocycle $F$ in $Z^1(\hat{\mathbb{Z}}', 1 \times 2\hat{\mathbb{Z}}, A_\varphi/p)$ acts by

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

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

**Proposition 3.5.1.** We have

$$\left( \frac{\ell + 1}{p} \cdot \varepsilon - \frac{a_i}{p} \right) \gamma(P(m)_{\lambda_i}) = \frac{a_i \varepsilon / \ell - 1/ \ell - 1}{p} P(\ell m)_{\lambda_i} \quad (3.3)$$

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

**Proof.** We denote by

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

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

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

For $a$ in $A_\varphi/p$, we have

$$D_{\ell} a = \sum_{i=1}^{\ell} i \sigma^i(a) = \sum_{i=1}^{\ell} i = \frac{\ell(\ell + 1)}{2} \equiv 0 \mod p.$$
we obtain
\[ P(\ell m)_{\lambda} = \text{res}_{G, G_{\lambda}}(z) = \inf_{G_{\lambda} / G_{\lambda_1}} (z_1) \]
for some
\[ z_1 \in H^1(G_{\lambda_1} / G_{\lambda}, A \phi / p) = \text{Hom}(\langle \sigma \rangle, A \phi / p). \]
Since \( \text{cor}_{G, G_1}(y) = a_\ell x \), there is an element \( a \) in \( A \phi / p \) such that
\[ \text{cor}_{G, G_1}(y)(g_1) - a_\ell x(g_1) = (g_1 - 1)a \] \hspace{1cm} (3.4)
for \( g_1 \) in \( G_1 \). It is shown in [39, section 7] that
\[ a = z_1(\sigma). \]
We let
\[ a_x = \text{res}_{G, G_{\lambda_1}}(x), \quad \text{and} \quad a_y = \text{res}_{H, G_{\lambda_1}}(y). \]
Restricting \( g_1 \) to \( g_{\lambda_1} \in G_{\lambda_1} \) in equation (3.4) where \( \pi(g_{\lambda_1}) = \sigma^u \phi^{2^v} \), we obtain
\[ \sum_{i=0}^{\ell} a_y(\bar{\sigma}^i g_{\lambda_1} \bar{\sigma}^{-i}) - a_\ell a_x(g_{\lambda_1}) = (\ell + 1)a_y(g_{\lambda_1}) - a_\ell a_x(g_{\lambda_1}) = (\phi^2 - 1)a, \]
where \( \bar{\sigma} \) is a lift of \( \sigma \) in \( G_1 / G_{\ell} \) to \( G_1 \). We have
\[ x(g_{\lambda_1}) = (1 + \phi^2 + \ldots + \phi^{2^{(v-1)}})a_x + (\phi^2 - 1)b_x, \]
\[ \& \quad y(g_{\lambda_1}) = (1 + \phi^2 + \ldots + \phi^{2^{(v-1)}})a_y + (\phi^2 - 1)b_y. \]
For \( u = 0, v = 1 \), we obtain from the last three equations
\[ (\ell + 1)y(g_{\lambda_1}) - a_\ell x(g_{\lambda_1}) = (\phi^2 - 1)a + (\phi^2 - 1)(-a_\ell b_x + (\ell + 1)b_y), \] \hspace{1cm} (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
\[
a_y = \phi(a_x) \mod (\phi^2 - 1) A_{\phi}/p
\]
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 \(\varepsilon\) is such that \(\phi \equiv \tau\) acts by \(\varepsilon\) 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 \(\phi\) implies that
\[
\phi^2 - a_\ell \phi / \ell^r + 1 / \ell = 0 \text{ on } A_{\phi}/p.
\]
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 \(P(\ell m)_{\lambda_1} = \inf_{G_{\lambda_1}/G_{\lambda_1}, G_{\lambda_1}(z_1)}\) where the generator \(\sigma\) of \(G_{\lambda_1}/G_{\lambda_i}\) can be lifted to the generator \(\tau_\ell\) of \(G_{\lambda_1} = \Gal(H_{\lambda_1}/H_{\lambda_1}^w)\). It is therefore enough to apply the map \(\gamma\) defined by (2.2) to \(a\) to obtain \(P(\ell m)_{\lambda_1}\) where \(\gamma\) switches cocycles with same values on \(\Frob(\ell)\) and \(\tau_\ell\). The result follows. \(\Box\)
3.6 Statement

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

$$\hat{G} = \text{Hom}(G, \mu_c)$$

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 $\chi$-eigenspace given a character $\chi$ of $\hat{G}$. We let

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

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

**Theorem [1.2.1]** Assume that $p$ is such that

$$\text{Gal} \left( \mathbb{Q}(A_p/p)/\mathbb{Q} \right) \simeq \text{GL}_2(\mathcal{O}_p/p), \quad (p, ND\phi(N)) = 1, \quad \text{and } p \mid |G|. \quad (3.6)$$

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

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

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

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

where $I_{\lambda'} = \text{Gal}(H^{ur}_{\lambda'}/H_{\lambda'})$ and $\mathcal{O}_{\rho'}$-linear isomorphisms

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

where $\phi$ is the arithmetic Frobenius element generating $\text{Gal}(H^{ur}_{\lambda'}/H_{\lambda'})$. Recall that the Selmer group $S \subseteq H^1(H,A_\rho/p)$ consists of the cohomology classes whose localizations lie in $H^1(H_v^{ur}/H_v,A_\rho/p)$ for $v$ not dividing $Np$ and in $H^1_f(H_v,A_\rho/p)$ for $v$ dividing $p$.

Here, $H^1_f(H_v,A_\rho/p)$ is the finite part of $H^1(H_v,A_\rho/p)$ as in [9]. We denote by

$$\text{res}_\lambda : H^1(H,A_\rho/p) \rightarrow \bigoplus_{\lambda' | \lambda} H^1(H_{\lambda'}/A_\rho/p)$$

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

$$\text{res}_\lambda : S \rightarrow \bigoplus_{\lambda' | \lambda} H^1(H^{ur}_{\lambda'}/H_{\lambda'}/A_\rho/p)^{I_{\lambda'}}).$$

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

$$\psi_\ell : \bigoplus_{\lambda' | \lambda} H^1(H^{ur}_{\lambda'}/A_\rho/p) \rightarrow S^{dual}.$$

Let

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

### 3.7 Generating the dual of the Selmer group

**Lemma 3.7.1.** We have

\[
H^1(\text{Aut}(A_{\phi}/p), A_{\phi}/p) = 0.
\]

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

\[
g = 2I \in \text{Aut}(A_{\phi}/p)
\]

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

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

\[
\text{res}_{\beta'} e_\chi \delta \neq 0,
\]

where \( \beta' \) is a prime dividing \( q \) in \( H \).

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

\[
r : H^1(H, A_{\phi}/p) \longrightarrow H^1(L, A_{\phi}/p)^G = \text{Hom}_G(L, A_{\phi}/p)
\]

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

\[
\text{Ker}(r) = H^1(H(A_{\phi}/p)/H, A_{\phi}/p) = 0.
\]
Consider the evaluation pairing

\[ r(S^\mathcal{X}) \times \text{Gal}(\overline{\mathbb{Q}}/L) \longrightarrow A_{\rho}/p \]

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

\[ r(S^\mathcal{X}) \hookrightarrow \text{Hom}_G(G_S, A_{\rho}/p). \]

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

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

\[ s : G_S^- \longrightarrow A_{\rho}/p^\pm, \]

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

\[ G = G(L/H) \simeq \text{GL}_2(\mathcal{O}_{\rho}/p). \]

Hence, \( A_{\rho}/p^\pm \) 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 \( S^\mathcal{X} \) as \( c_1 \) is not divisible by \( p \) in \( S^\mathcal{X} \). As a consequence, we have that \( s(G_S^+) \neq 0 \), where

\[ G_S^+ = G_S^{\tau+1} = \{ h^\sigma h \mid h \text{ in } G_S \} = \{ (\tau h)^2 \mid h \text{ in } G_S \}. \]
Therefore, there exists $h$ in $G_S$ such that $c_1((\tau h)^2) \neq 0$. Consider the element $\tau h$ in $\text{Gal}(L^S/Q)$. Cebotarev’s density theorem, (see Chapter 2, Theorem 2.1 for more details) implies the existence of $q$ in $Q$ such that

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

and such that $(q,c_{pND}) = 1$. In particular, $q$ is a Kolyvagin prime since $\text{res}_{L}(\tau h) = \tau$.

For $\beta$ in $L$ above $q$, we have that

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

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

We consider the restriction $d$ of an element $c$ of $H^1(H,A_{\phi}/p)$ to $H^1(F,A_{\phi}/p)$. 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

$$I_0 = F(\text{red}(y_{1,\phi}))^{\text{Gal}}$$

$$I_1 = F(D_q\text{red}(y_{q,\phi}))^{\text{Gal}}$$

$$I_{01} = I_0I_1$$

$$F = H_q(A_{\phi}/p)$$
where the abbreviation Gal indicates taking Galois closure over $\mathbb{Q}$. We define

\[ V_0 = \text{Gal}(I_0/F), \quad V_1 = \text{Gal}(I_1/F), \quad \text{and} \quad V = \text{Gal}(I_0 I_1/F). \]

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

\[ I_0^{\mathcal{X}} = F(e_{\mathcal{X}} \text{red}(y_{1,\varphi}))^{\text{Gal}} \quad \text{and} \quad I_1^{\mathcal{X}} = F(e_{\mathcal{X}} D_q \text{red}(y_{q,\varphi}))^{\text{Gal}}. \]

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

\[ V^{\mathcal{X}} = \text{Gal}(I_0^{\mathcal{X}} I_1^{\mathcal{X}}/F) \simeq V_0^{\mathcal{X}} \times V_1^{\mathcal{X}}. \]

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

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

\[ H^1(H_q, A_{\varphi}/p)^{\text{Gal}(F/H_q)} \xrightarrow{(r)} H^1(F, A_{\varphi}/p)^{\text{Gal}(F/H_q)} \]

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

\[ H^1(K(A_{\varphi}/p)/K, A_{\varphi}/p) = 0, \]

we obtain that

\[ \text{Ker}(r) = H^1(F/H_q, A_{\varphi}/p) = 0. \]

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

\[ H^1(I_{01}, F, A_{\varphi}/p)^{\text{Gal}(F/H_q)} = \text{Hom}_{\text{Gal}(F/H_q)}(I_{01}, F, A_{\varphi}/p). \]
Consider the extension $I_0^X \cap I_1^X$ of $F$. It is a Gal($F/H_q$)-submodule of $A_{\rho}/p$. The hypothesis $\text{res}_{\beta} e_{\chi,\text{red}}(y_{1,\rho}) \neq 0$ implies that

$$\text{res}_{\beta} e_{\chi,\text{red}}(D_qy_{q,\rho}) \neq 0$$

by (3.3.2). On the one hand, since $\text{res}_{\beta} e_{\chi,\text{red}}(D_qy_{q,\rho})$ is ramified, $e_{\chi,\text{red}}(y_{q,\rho})$ does not belong to $S^X$. On the other hand, $e_{\chi,\text{red}}(y_{1,\rho}) \neq 0$ belongs to $S^X$ by Proposition 3.4.4.

Therefore $I_0^X \cap I_1^X = 0$ since $A_{\rho}/p$ is a simple 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 $S^X$ while the other one does not. $\square$

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

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

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

$$\text{Frob}_{\ell}(H(A_{\rho}/p)/Q) = \text{res}_{H(A_{\rho}/p)}\text{Frob}_{\ell}(I_{01}/Q) = \tau$$

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

$$\text{Frob}_{\ell}(H_q(A_{\rho}/p)/Q) = \text{res}_{H_q(A_{\rho}/p)}\text{Frob}_{\ell}(I_{01}/Q) = \tau.$$ 

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

$$\text{Frob}_{\ell}(H_q/H) = \tau^{[D(H/Q)]} = \tau^2 = \text{Id}.$$ 

53
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 \(\ell\) 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

\[
\text{Frob}_\ell(H_q(A_\wp/p)/H_q) = \tau^{D(H_q/\mathbb{Q})} = \tau^2 = \text{Id}.
\]

**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 \(\text{Hom}_{G}(F,A_\wp/p)\).
2. To show the statement of the theorem, it is enough to show that \(\text{res}_\wp(s) = 0\) for all \(\ell \in L(U)\) implies \(s = 0\).
3. The assumption \(\text{res}_\wp(s) = 0\) 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

\[
G = \text{Gal}(H(A_\wp/p)/H) \simeq \text{GL}_2(O_\wp/p).
\]

We denote by \(h\) the image of \(s\) by restriction in

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

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

\[
\ker(r_1) = H^1(H(A_{p}/p)/H, A_{p}/p) = 0.
\]

By Proposition 3.4.2 we have

\[
\text{Gal}(H \varphi/p)/H(A_{p}/p)) \cong \text{Gal}(H \varphi/H) \cong \mathbb{Z}/(q+1)\mathbb{Z}.
\]

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

\[
\ker(r_2) = \text{Hom}_G(\text{Gal}(F/H(A_{p}/p)), A_{p}/p) \cong \text{Hom}_G(H \varphi/H, A_{p}/p) = 0
\]

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

2. By Isomorphism (3.7), local Tate duality identifies \( \bigoplus_{\lambda'} H^1(H_{\lambda}'(H_{\lambda}'; A_{p}/p)) \) with

\[
\bigoplus_{\lambda'} H^1(H_{\lambda}'(H_{\lambda}'; A_{p}/p)) \cong \bigoplus_{\lambda'} H^1(H_{\lambda}'(H_{\lambda}'; (A_{p}/p)^{l_{\lambda'}})).
\]

So if we show that

\[
\{\text{res}_{\lambda} \}_{\ell \in L(U)} : S \longrightarrow \{\bigoplus_{\lambda'} H^1(H_{\lambda}'(H_{\lambda}'; (A_{p}/p)^{l_{\lambda'}})) \}_{\ell \in L(U)}
\]

is injective, then the induced map between the duals

\[
\big\{\bigoplus_{\lambda'} H^1(H_{\lambda}'(H_{\lambda}'; A_{p}/p)) \big\}_{\ell \in L(U)} \longrightarrow S^{\text{dual}}
\]

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

55
3. Consider $I_{01}$, the minimal Galois extension of $\mathbb{Q}$ containing $I_{01}$ such that $h$ factors through $\text{Gal}(I_{01}/F)$. Let $x$ be an element of $\text{Gal}(I_{01}/F)$ such that $x|_{I_{01}}$ belongs to $U$. By Cebotarev’s density theorem, there exists $\ell$ in $L(U)$ such that $\text{Frob}_\ell(I_{01}/\mathbb{Q}) = [\tau x]$. The hypothesis $\text{res}_\lambda(s) = 0$ implies that $h(\text{Frob}_\lambda(I_{01}/F)) = 0$ for $\lambda''$ above $\ell$ in $F$ since $\text{Frob}_\lambda(I_{01}/F)$ is a generator of the local extension of $\text{Gal}(I_{01}/F)$ at $\lambda''$. In fact,

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

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

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

**Proposition 3.7.5.** There is an element $\sigma_0$ in $\text{Gal}(H_q/K)$ such that

$$\tau e^\chi y_{q,\rho} = \varepsilon \chi(\sigma_0) e^\chi y_{q,\rho}, \quad \text{where } -\varepsilon \text{ is the sign of the functional equation of } L(f,s).$$
Proof. [39, proposition 6.2] that uses a result in [26] states that

$$\tau y_{q, \phi} = \epsilon \sigma_0 y_{q, \phi}$$

(3.8)

for some $\sigma_0$ in $\text{Gal}(H_q/K)$. Since $\tau$ acts on an element $g$ of $G$ by

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

we have

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

Also,

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

Therefore, applying $e \chi$ to Equation (3.8) yields

$$\tau \epsilon \chi y_{q, \phi} = \epsilon \chi(\sigma_0) e \chi y_{q, \phi}.$$

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

$$\tau v_0 \tau(e \chi y_{1, \phi}) = \epsilon \chi(\sigma_0) \tau v_0(e \chi y_{1, \phi}).$$

$$\tau v_1 \tau(e \chi D_q y_{q, \phi}) = -\tau v_1 D_q \tau(e \chi y_{q, \phi}) = -\epsilon \chi(\sigma_0) \tau v_1(e \chi D_q y_{q, \phi}).$$
When $c = c$, for $(x, y)$ in $V_0 V_1$, 

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

In this case, we define 

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

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

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

In this case, we define 

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

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

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

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

**Proposition 3.7.6.** The elements 

$$
\operatorname{res} \chi \varepsilon \chi P(\ell) \text{ and } \operatorname{res} \chi \varepsilon \chi P(\ell q)
$$

generate $\oplus_{\ell \mid \ell} H^1(\mathcal{H}_{\ell}^{ur}, A_{\phi}/p)$. 

**Proof.** We have 

$$
\oplus_{\ell \mid \ell} H^1(\mathcal{H}_{\ell}^{ur}, A_{\phi}/p) \simeq \oplus_{\ell \mid \ell} ((A_{\phi}/p)^{\ell \ell'}/(\phi - 1))
$$

58
since the former is isomorphic to its dual by Isomorphism \([3,7]\). The module
\[\oplus_{\lambda'} \lambda \left( (A_{\lambda'}) / p \right)^{I_{\lambda'}} / (\phi - 1) \bar{\psi} \]
is of rank at most 2 over \(q_{\lambda'}/p\), hence, so is \(\oplus_{\lambda'} \lambda H^1(\mathcal{H}_{\lambda', A_{\lambda'}/p}) \bar{\psi}\). The Frobenius condition on \(\ell\) implies that
\[\text{res}_\lambda e_{\bar{\psi}} \text{red}(y_{1, \lambda}) \text{ and res}_\lambda e_{\bar{\psi}} \text{D}_{q_{\lambda'}} \text{red}(y_{q, \lambda})\]
are linearly independent over \(\oplus_{\lambda'} \lambda A_{\lambda'}/p\). Indeed, if they were linearly dependent then, in the case \(\chi = \bar{\psi}\),
\[(\text{res}_\lambda e_{\bar{\psi}} \text{red}(y_{1, \lambda}))^{(\tau_x)^2} - \text{res}_\lambda e_{\bar{\psi}} \text{red}(y_{1, \lambda})
\text{ and } (\text{res}_\lambda e_{\bar{\psi}} \text{D}_{q} \text{red}(y_{q, \lambda}))^{(\tau_y)^2} - \text{res}_\lambda e_{\bar{\psi}} \text{D}_{q} \text{red}(y_{q, \lambda})\]
where \(\text{Frob}_\ell(I_{01}/\mathbb{Q}) = \tau u = (\tau_x, \tau_y)\) would also be linearly dependent. The Frobenius condition implies that
\[\text{Frob}_\ell(I_{0}^\bar{\psi}/F) = x^\tau x = (\tau x)^2 \text{ and Frob}_\ell(I_{1}^\bar{\psi}/F) = y^\tau y = (\tau y)^2\]
generate \(A_{\lambda'}/p\), which yields a contradiction as \((\tau x)^2\) acts on the element \(\text{res}_\lambda e_{\bar{\psi}} \text{red}(y_{1, \lambda})\)
generating the local extension of \(I_{0}^\bar{\psi}\) over \(F\) by
\[(\text{res}_\lambda e_{\bar{\psi}} \text{red}(y_{1, \lambda}))^{(\tau_x)^2} - \text{res}_\lambda e_{\bar{\psi}} \text{red}(y_{1, \lambda})\]
and \((\tau y)^2\) acts on the element \(\text{res}_\lambda e_{\bar{\psi}} \text{D}_{q} \text{red}(y_{q, \lambda})\) generating the local extension of \(I_{1}^\bar{\psi}\) over \(F\) by
\[\text{res}_\lambda e_{\bar{\psi}} \text{D}_{q} \text{red}(y_{q, \lambda}))^{(\tau_y)^2} - \text{res}_\lambda e_{\bar{\psi}} \text{D}_{q} \text{red}(y_{q, \lambda}).\]
Similarly, in the case $\chi \neq \overline{\chi}$,

$$(\text{res}_\lambda e_{\overline{\chi}} \text{red}(y_{1,\varphi}))^{x^{\tau}y} - \text{res}_\lambda e_{\overline{\chi}} \text{red}(y_{1,\varphi})$$

and

$$(\text{res}_\lambda e_{\overline{\chi}} D_q \text{red}(y_{q,\varphi}))^{z^{\tau}w} - \text{res}_\lambda e_{\overline{\chi}} D_q \text{red}(y_{q,\varphi})$$

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

$$\text{Frob}_\ell(I_{01}^{\overline{\chi}}/F) = x^{\tau}y = (\tau x)(\tau y) \text{ and } \text{Frob}_\ell(I_{1}^{\overline{\chi}}/F) = z^{\tau}w = (\tau z)(\tau w)$$

generate $A_{\varphi}/p$, which yields a contradiction.

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

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

would be linearly dependent as well. \qed

### 3.8 Bounding the size of the dual of the Selmer group

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

**Proposition 3.8.1.** We have

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

*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. \qed

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

60
Proof. The image of $\text{res}_\lambda e_\mathcal{X}P(\ell)$ by the map

$$\psi_\ell : \bigoplus_{\lambda' | \lambda} H^1(H_{u_r}^{\ell'}, A_{\varphi}/p) \mathcal{X} \longrightarrow X_\ell^\mathcal{X}$$

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

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

Proposition 3.8.1 implies that

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

Hence, the image by $\psi_\ell$ of $\text{res}_\lambda e_\mathcal{X}P(\ell)$, one of the two generators of

$$\bigoplus_{\lambda' | \lambda} H^1(H_{u_r}^{\ell'}, A_{\varphi}/p) \mathcal{X}$$

by Proposition 3.7.6, is trivial.

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

Proof. Proposition 3.8.1 implies that

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

Hence,

$$\psi_\ell(\text{res}_\lambda e_\mathcal{X}P(\ell q)) + \psi_q(\text{res}_\beta e_\mathcal{X}P(\ell q)) = 0.$$

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

$$\psi_\ell(\text{res}_\lambda e_\mathcal{X}P(\ell q))$$
generates $X^\mathcal{F}_\ell$ over $\mathcal{O}_p/p$, we have that

$$-\psi_\ell(\text{res}_P e_{\mathcal{F}}P(\ell q)) = \psi_q(\text{res}_\beta e_{\mathcal{F}}P(\ell q)) \in X^\mathcal{F}_q$$

is non-zero. Therefore, the non-trivial element $\psi_q(\text{res}_\beta e_{\mathcal{F}}P(\ell q))$ generates a rank 1 module $X^\mathcal{F}_q$ over $\mathcal{O}_p/p$ and $X^\mathcal{F}_\ell = X^\mathcal{F}_q$.

In what follows, we prove theorem 1.2.1

**Proof.** By Proposition 3.7.4, the set $\{X^\mathcal{F}_\ell\}$ generates $S^{\text{dual}}_{\mathcal{F}}$ as $\ell$ ranges over $L(U)$. Hence, the set $\{X^\mathcal{F}_\ell\}$ generates $S^{\text{dual}}_{\mathcal{F}}$ as $\ell$ ranges over $L(U)$, where, by Proposition 3.8.2, the modules $X^\mathcal{F}_\ell$ that are non-zero are of rank 1 over $\mathcal{O}_p/p$ and are all equal. Hence, $\text{rank}(S^\mathcal{F}) \leq 1$.

Also, $e_{\mathcal{F}}\text{red}(y_1, \mathcal{F})$ belongs to $S^\mathcal{F}$ by Proposition 3.4.4 and is not divisible by $p$ in $S^\mathcal{F}$. Indeed, this follows from the hypothesis on $e_{\mathcal{F}}\text{red}(y_1, \mathcal{F})$ and Proposition 3.7.5 where $\overline{\sigma}(\sigma_0)$ is a root of unity since $\text{Gal}(H/K)$ is a finite group. This implies that $\text{rank}(S^\mathcal{F}) \geq 1$. Therefore,

$$\text{rank}(S^\mathcal{F}) = \text{rank}(S^{\text{dual}}_{\mathcal{F}}) = 1.$$ 

\[ \square \]

**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)

$$\Phi^\mathcal{F} : \text{CH}^r(W_{2r-2}/H)^{\mathcal{F}}_0 \otimes \mathcal{O}_p/p\mathcal{O}_p \rightarrow S^\mathcal{F},$$

Theorem 1.2.1 implies that $\text{rank}_{\mathcal{O}_p/p}(\text{Im}(\Phi^\mathcal{F})) = 1$.

**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 $\text{Sel}_p(E/K)$. 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 $H^1(H, A_p/p)$. 
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

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

and the Tate-Shafarevich group $\text{III}(E/K)$ 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 $\chi$ of $\text{Gal}(K_c/K)$ where $K_c$ is the ring class field of $K$ of conductor $c$,

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

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 $\Phi$ of Heegner cycles on the associated Kuga-Sato varieties, hence showing that

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

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

$$\dim_{Q_p}(\text{Im}(\Phi) \otimes Q_p) = 1$$

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 $\psi$ of infinity type $(r, 0)$. The case of a Hecke character of infinity type $(0, 0)$ corresponds to the setting of Nekovár’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

$$\dim_{Q}(\text{Im}(\Phi) \otimes Q) = \text{ord}_{s=r+1} L(f \otimes \theta_\psi, s),$$

where $\theta_\psi$ is the theta series associated to $\psi$ \[44\], \[32\].

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 $|\mathcal{O}_K^\times| = 2$. 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 $\mathcal{O}_K$ such that $\psi$ 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 $\text{Aut}(K_1)$. (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 $\frac{\ell + 2}{2}$ and by $V_\psi$ the $p$-adic étale realization of the motive associated to $\psi$ twisted by $\frac{\ell}{2}$.

More precisely, $V_\psi$ is the $\psi$-isotypic component of

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

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

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

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

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

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

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

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

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

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

66
By the Heegner hypothesis, there is an ideal \( \mathcal{N} \) of \( \mathcal{O}_K \) satisfying
\[
\mathcal{O}_K / \mathcal{N} = \mathbb{Z} / N \mathbb{Z}.
\]

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 \( \mathcal{N} \). Consider a pair \((\varphi_1, A_1)\) where \( A_1 \) is an elliptic curve defined over \( K_1 \) with level \( N \) structure and
\[
\varphi_1 : A \rightarrow A_1
\]
is an isogeny over \( \overline{R} \). We associate to it a codimension \( r + 1 \) cycle on \( V \)
\[
\gamma_{\varphi_1} = \text{Graph}(\varphi_1)^r \subset (A \times A_1)^r \cong (A_1)^r \times A^r
\]
and define a generalized Heegner cycle of conductor 1
\[
\Delta_{\varphi_1} = e_r \gamma_{\varphi_1},
\]
where \( e_r \) is an appropriate projector (4.1). Then \( \Delta_{\varphi_1} \) is defined over \( L_1 \). We consider the corestriction
\[
P(1) = \text{cor}_{L_1, K} \Phi(\Delta_{\varphi_1}) \in H^1(K, V_{\varphi}/p)
\]
where \( \Phi \) is the \( p \)-adic étale Abel-Jacobi map. The Selmer group
\[
S \subseteq H^1(K, V_{\varphi}/p)
\]
consists of the cohomology classes which localizations at a prime $v$ of $K$ lie in

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

where $K_v$ is the completion of $K$ at $v$, and

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

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

**Theorem 1.3.1.** Let $p$ be such that

$$\text{Gal}\left(\left(K(V_p/p)/K\right) \simeq \text{Aut}_K(V_p/p), \quad (p, ND\phi(N)NN_A) = 1. \right.$$ 

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

To prove Theorem 1.3.1, we first consider the $p$-adic étale realization of the twisted motive $V$ associated to $f$ and $\psi$ 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 were 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 \cite{39} and Gross’ exposition of Kolyvagin’s method of Euler systems \cite{27}. The main novelty is that the algebraic Hecke character $\psi$ 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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation

$$V_\rho = (V_f \otimes_{\rho_{f} \otimes \mathbb{Z}_p} V_{\psi}) \rho,$$

where $\rho$ 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 $\pi : \mathcal{E} \rightarrow X_1(N)$. Denote by $W_r$ the Kuga-Sato variety of dimension $r + 1$, that is a compact desingularization of the $r$-fold fiber product of $\mathcal{E}$ 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 $\text{End}_{\mathbb{K}_1}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ corresponding to an element $\alpha$ of $K$. Consider the projectors

$$e_{A}^{(1)} = \left(\frac{\sqrt{-D} + \lceil \sqrt{-D} \rceil}{2\sqrt{-D}}\right)^{\otimes r} + \left(\frac{\sqrt{-D} - \lfloor \sqrt{-D} \rfloor}{2\sqrt{-D}}\right)^{\otimes r}, \quad e_{A}^{(2)} = \left(\frac{1 - \lceil -1 \rceil}{2}\right)^{\otimes r},$$

and

$$e_A = e_{A}^{(1)} \circ e_{A}^{(2)}.$$
in $\mathbb{Q}[\text{End}(A)]^r$. These projectors $e_A^{(1)}$, $e_A^{(2)}$ and $e_A$ belong to the group of correspondences $\text{Corr}^0(A,A)_\mathbb{Q}$ 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 $\Sigma_r$ is the symmetric group on $r$ elements. Then $\Gamma_r$ acts on $W_r$, (see [46, Sections 1.1.0,1.1.1] for more details.) The projector $e_W$ in $\mathbb{Z} \left[ \frac{1}{2N^r!} \right] [\Gamma_r]$ associated to $\Gamma_r$, called Scholl’s projector, belongs to the group of zero correspondences $\text{Corr}^0(W_r,W_r)_\mathbb{Q}$ 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

$$e_r = e_w e_A,$$  \hfill (4.1)

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

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

**Proposition 4.2.1.** The étale cohomology group

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

is isomorphic to

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

70
and

\[ H^1_{et}(X_1(N) \otimes \overline{\mathbb{Q}}, \mathcal{E}) \otimes e_A H^1_{et}(\overline{\mathbb{A}}, \mathbb{Z}_p). \]

**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

\[ \widetilde{V} = e_B H^1_{et}(X_1(N) \otimes \overline{\mathbb{Q}}, \mathcal{E})(r + 1) \]

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

\[ I = \text{Ker}\{ \mathbb{T} \rightarrow \mathcal{O}_F : T_\ell \mapsto a_\ell b_\ell, \mathbb{N} \mathcal{P}_A \}, \]

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

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

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

\[ \text{End}(A/\mathbb{Q}) = \bigoplus_{\sigma \in \text{Gal}(H/\mathbb{Q})} \text{Hom}(A, A^\sigma). \]
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 \( \psi \) in the middle étale cohomology of the associated Kuga-Sato varieties.

Consider the \( p \)-adic étale Abel-Jacobi map

\[
\Phi : \text{CH}^{r+1}(W/L_n)_0 \longrightarrow H^1(L_n, H^{2r+1}_{\text{et}}(W \otimes \overline{\mathbb{Q}}, \mathbb{Z}_p(r+1))),
\]

where \( \text{CH}^{r+1}(W/L_n)_0 \) 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

\[
\Phi : \text{CH}^{r+1}(W/L_n)_0 \longrightarrow H^1(L_n, \tilde{V}).
\]

In fact, \( \Phi \) factors through \( e_r(\text{CH}^{r+1}(W/L_n)_0 \otimes \mathbb{Z}_p) \) 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

\[
\text{CH}^{r+1}(W/L_n)_0 = \ker(\text{CH}^{r+1}(W/L_n) \longrightarrow H^{2r+2}(W \otimes \overline{\mathbb{Q}}, \mathbb{Z}_p(r+1))),
\]

we deduce that

\[
e_r(\text{CH}^{r+1}(W/L_n)_0 \otimes \mathbb{Z}_p) = e_r(\text{CH}^{r+1}(W/L_n) \otimes \mathbb{Z}_p).
\]
Hence, composing $\Phi$ with $m : \tilde{V} \to V$, we obtain

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

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

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

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

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

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

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

(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 $\psi$ is the trivial character. Nekovár’s results \cite{39,40} that correspond to the setting where $\psi$ is trivial provide further evidence towards a $p$-adic analog of the Beilinson-Bloch conjecture of the form

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

due to Perrin-Riou \cite{15, section 2.8}, \cite{42}. In this thesis, we provide a sufficient condition for $\dim_{\mathbb{Q}_p}(\text{Im}(\Phi) \otimes \mathbb{Q}_p) = 1$. Since Shnidman \cite{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 \cite{5}. Consider pairs $(\phi_i, A_i)$ where $A_i$ is an elliptic curve defined over $K_1$ with level $N$ structure defined over $L_1$ and

$$\phi_i : A \longrightarrow A_i$$

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

$$\mathcal{Y}_{\phi_i} = \text{Graph}(\phi_i)^r \subset (A \times A_i)^r \simeq (A_i)^r \times A^r \subset W_r \times A^r$$

74
and define a *generalized Heegner cycle*

\[ \Delta_{\varphi_i} = e_r Y_{\varphi_i}. \]

Denote by \( D_{A_i} \) the element

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

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 \( \text{End}(A_i) \), which is an order in \( \mathcal{O}_K \), has conductor \( i \). Then \( \Delta_{\varphi_i} \) 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 \( \text{Gal}(\widetilde{K}/\overline{K}) \) acts trivially on \( A[\mathcal{N}] \), it is equal to the ray class field \( L_1 \) of \( K \) of conductor \( \mathcal{N} \). Therefore, \( \Delta_{\varphi_i} \) is defined over

\[ L_i = L_1 K_i. \]

Then

\[ \Delta_{\varphi_i} = D_{A_i}^\prime \text{ belongs to } \text{CH}^{r+1}(W/L_i). \]

In fact, \( \Delta_{\varphi_i} \) is homologically trivial on \( W \) as shown in [5 proposition 2.7].

In the rest of this section, we consider elements \((\varphi_i, A_i)\) and \((\varphi_j, A_j)\) in \( \text{Isog}^{\mathcal{N}}(A) \).

**Lemma 4.4.1.** Consider the map

\[ g \times I : A_j \times A \to A_j \times A, \]
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

$$D_{A_i} \cdot D_{A_i} = (\text{graph}(\varphi_i) - 0 \times A - \deg(\varphi_i)A_i \times 0) \cdot (\text{graph}(\varphi_i) - 0 \times A - \deg(\varphi_i)A_i \times 0)$$

$$= \text{graph}(\varphi_i) \cdot \text{graph}(\varphi_i) + 0 \times A \cdot 0 \times A + \deg(\varphi_i)A_i \times 0 \cdot \deg(\varphi_i)A_i \times 0$$

$$- 2\text{graph}(\varphi_i) \cdot 0 \times A - 2\text{graph}(\varphi_i) \cdot \deg(\varphi_i)A_i \times 0 + 2 \deg(\varphi_i)A_i \times 0 \cdot 0 \times A$$

$$= 0 + 0 - 2\deg(\varphi_i) - 2\deg(\varphi_i) + 2\deg(\varphi_i)$$

$$= -2\deg(\varphi_i).$$

In the previous computation, the equality $\text{graph}(\varphi_i) \cdot \text{graph}(\varphi_i) = 0$ 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 $(g \times I)_* D_{A_i} = kD_{A_j}$ 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 $-2 \deg(g)^2 \deg(\phi_i) = -2k^2 \deg(\phi_j)$ then implies that

$$k = \deg(g) \sqrt{\frac{\deg(\phi_i)}{\deg(\phi_j)}},$$

and

$$(g \times I)_s D_{A_i} = \deg(g) \sqrt{\frac{\deg(\phi_i)}{\deg(\phi_j)}} D_{A_j}.$$ 

\[\square\]

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 $\mathcal{O}_F \otimes \mathbb{Z}_p = \bigoplus_{\mathfrak{p} | p} \mathcal{O}_{F, \mathfrak{p}}$, where $\mathcal{O}_{F, \mathfrak{p}}$ is the completion of $\mathcal{O}_F$ at the prime $\mathfrak{p}$ dividing $p$. Recall that $V_\mathfrak{p} = (V_f \otimes_{\mathcal{O}_F} V_\psi)_{\mathfrak{p}}$, where $\mathfrak{p}$ is a prime of $F$ dividing $p$. Let

$$G_V = \text{Aut}(V_\mathfrak{p}/p).$$

For a Galois representation $V$,

$$F(V)$$

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

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

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

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

Condition (4.2) is equivalent to

\[ \text{Frob}_\ell(L(\mu_p)/\mathbb{Q}) = \text{Frob}_\infty(L(\mu_p)/\mathbb{Q}), \quad (4.3) \]

where \( \mu_p \) 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 \( \ell \) acting on \( V_{\wp}/p \) with roots

\[ \alpha_1 \alpha_3, \quad \alpha_1 \alpha_4, \quad \alpha_2 \alpha_3, \quad \text{and} \quad \alpha_2 \alpha_4 \]

satisfying

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

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

\[
\begin{align*}
(x - \alpha_1 \alpha_3)(x - \alpha_1 \alpha_4)(x - \alpha_2 \alpha_3)(x - \alpha_2 \alpha_4) &= (x^2 - (\alpha_1 \alpha_3 + \alpha_1 \alpha_4)x + \alpha_1^2 \alpha_3 \alpha_4)(x^2 - (\alpha_2 \alpha_3 + \alpha_2 \alpha_4)x + \alpha_2^2 \alpha_3 \alpha_4) \\
&= (x^2 - \alpha_1 a_\ell x + \ell^{r+1} \alpha_1^2)(x^2 - \alpha_2 a_\ell x + \ell^{r+1} \alpha_2^2)
\end{align*}
\]
We use the equality \((a_1 + a_2)^2 = a_1^2 + a_2^2 + 2a_1a_2\) that is \(b_\ell^2 - 2\ell^r = a_1^2 + a_2^2\) to conclude that the latter equals

\[
x^4 - (\alpha_2 a_\ell + \alpha_1 a_\ell) x^3 + \left(\ell^{r+1} \alpha_1^2 + \ell^{r+1} \alpha_2^2 + \alpha_1 \alpha_2 a_\ell^2\right) x^2 \\
- \ell^{r+1} \left(\alpha_1 a_\ell \alpha_2^2 + \alpha_2 a_\ell \alpha_1^2\right) x + \ell^{2r+2} \alpha_1^2 \alpha_2^2 \\
= x^4 - a_\ell b_\ell x^3 + \left(\ell^{r+1} b_\ell^2 - 2\ell^{2r+1} + a_\ell^2 \ell^r\right) x^2 - \ell^{2r+1} a_\ell (\alpha_1 + \alpha_2) x + \ell^{4r+2} \\
= x^4 - a_\ell b_\ell x^3 + \left(\ell^{r+1} b_\ell^2 - 2\ell^{2r+1} + a_\ell^2 \ell^r\right) x^2 - \ell^{2r+1} b_\ell a_\ell x + \ell^{4r+2}.
\]

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

\[
\ell^{4r+4} x^4 - a_\ell b_\ell \ell^{3r+3} x^3 + \ell^{2r+2} \left(\ell^{r+1} b_\ell^2 - 2\ell^{2r+1} + a_\ell^2 \ell^r\right) x^2 - \ell^{3r+2} b_\ell a_\ell x + \ell^{4r+2} \\
= \ell^{4r+4} \left(x^4 - \frac{a_\ell b_\ell}{\ell^{r+1}} x^3 + \frac{\ell^{r+1} b_\ell^2 - 2\ell^{2r+1} + a_\ell^2 \ell^r}{\ell^{2r+2}} x^2 - \frac{b_\ell a_\ell}{\ell^{r+2}} x + \frac{1}{\ell^2}\right).
\]

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 \(\tau\) acting on \(V_\ell/p\) is congruent to the characteristic polynomial of \(\text{Frob}(\ell)\) acting on \(V_\ell/p\). On the other hand, comparing the action of the Frobenius element \(\text{Frob}_\ell\) and the complex conjugation \(\tau\) on \(\zeta_p\), where \(\zeta_p\) is a \(p\)-th root of unity, we obtain

\[\zeta_p^\ell = \text{Frob}_\ell(\zeta_p) = \text{Frob}_\infty(\zeta_p) = \zeta_p^{-1}.
\]
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 $\ell_i$ is a Kolyvagin prime for $i = 1, \cdots, k$. Then the extensions $L_1$ and $K_n$ are disjoint over $K_1$ and

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

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

Consider the image of $\Delta_{\phi_n}$ by the Abel-Jacobi map

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

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

$$T_\ell \Phi(\Delta_{\phi_m}) = \text{cor}_{L_n, L_m} \Phi(\Delta_{\phi_n}) = a_\ell b_\ell \Phi(\Delta_{\phi_m}).$$

**Proof.** By [45, corollary 11.4],

$$T_\ell(\Delta_{\phi_m}) = \sum_{n_i} \Delta_{\phi_{n_i}},$$

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

$$ g \in \text{Gal}(L_n/L_m) \cong \text{Gal}(K_n/K_m) \cong \text{Gal}(K_L/K_1). $$

Hence

$$ \sum_{i} \Delta_{\varphi_i} = \sum_{g \in \text{Gal}(L_n/L_m)} g \Delta_{\varphi_n} = \text{cor}_{L_n/L_m}(\Delta_{\varphi_n}) = a_{\ell} b_{\ell} \Delta_{\varphi_m}, $$

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

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

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

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

$$ \text{res}_\lambda \Phi(\Delta_{\varphi_n}) = k \text{Frob}_\ell(L_n/L_m) \text{res}_\lambda \Phi(\Delta_{\varphi_m}) $$

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

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

$$ \text{Frob}_\ell + \text{Frob}_\ell' \equiv T_\ell \mod \ell $$

on $X_0(N)$ where $\text{Frob}_\ell$ is the Frobenius morphism and $\text{Frob}_\ell'$ is the morphism dual to $\text{Frob}_\ell$. For elliptic curves over $\mathcal{O}_{L_n}$, we have

$$ \text{Frob}_\ell' \equiv \ell \text{Frob}_\ell^{-1} \equiv \ell \text{Frob}_\ell \mod \lambda_n $$

81
because $|\mathcal{O}_L/\lambda_n| = \ell^2$. Since $\lambda_m$ completely ramifies in $L_n$, we have $\mathcal{O}_L/\lambda_m \simeq \mathcal{O}_L/\lambda_n$.

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

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

where $k = \ell \sqrt{\frac{\deg(\phi)}{\deg(\phi_j)}}$ from which the result follows.

\[ \square \]

4.6 Kolyvagin cohomology classes

We denote by

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

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

$$y_n = \text{red}(\Phi(\Delta_{\phi_n})_{\phi}) \in H^1(L_n,V_{\phi}/p)$$

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

**Lemma 4.6.1.** For all $n$,

$$H^0(L_n,V_{\phi}/p) = H^0(L_1,V_{\phi}/p) = 0$$

and $\text{Gal}(L_n(V_{\phi}/p)/L_n) \simeq \text{Gal}(L_1(V_{\phi}/p)/L_1) \simeq \text{Gal}(K(V_{\phi}/p)/K)$. 

82
Proof. The extensions $L_n/L_1$ and $L_1(V_{\varphi}/p)/L_1$ are unramified outside primes dividing $nc$ and $N_A N p$. Therefore, $L_n \cap L_1(V_{\varphi}/p)$ is unramified over $L_1$ and is hence contained in $L_1$, the maximal unramified extension of $K$ of conductor $\mathcal{N}$. Hence,

$$H^0(L_n, V_{\varphi}/p) = H^0(L_1, V_{\varphi}/p).$$

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

**Proposition 4.6.2.** The restriction map

$$\text{res}_{L_1,L_n} : H^1(L_1, V_{\varphi}/p) \longrightarrow H^1(L_n, V_{\varphi}/p)^{G_n}$$

is an isomorphism.

**Proof.** This follows from the inflation-restriction sequence

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

since $H^0(L_n, V_{\varphi}/p) = 0$ by Lemma 4.6.1 \hfill \square

Let

$$\text{Tr}_\ell = \sum_{i=0}^\ell \sigma_i^i, \quad D_\ell = \sum_{i=1}^\ell i \sigma_i^i. \quad (4.4)$$

They are related by

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

Define

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

83
Proposition 4.6.3.

\[ D_n y_n \in H^1(L_n, V_{\varphi}/p)^{G_n}. \]

Proof. It is enough to show that for all \( \ell \) dividing \( n \),

\[ (\sigma_{\ell} - 1)D_n y_n = 0. \]

We have

\[ (\sigma_{\ell} - 1)D_n = (\sigma_{\ell} - 1)D\ell D_m = (\ell + 1 - \text{Tr}_{\ell})D_m, \]

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

\[ (\ell + 1 - \text{Tr}_{\ell})D_m \text{red}(\Phi(\Delta_{\varphi_n}, \varphi)) \]

\[ = (\ell + 1)D_m \text{red}(\Phi(\Delta_{\varphi_n}, \varphi)) - D_m a_\ell b_\ell \text{red}(\Phi(\Delta_{\varphi_m}, \varphi)) \]

\[ \equiv 0 \text{ mod } p. \]

by Proposition 4.5.1 and Condition 4.2. \( \square \)

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

\[ \text{res}_{L_1, L_n} c(n) = D_n y_n. \]

We define

\[ P(n) = \text{cor}_{L_1, K} c(n) \text{ in } H^1(K, V_{\varphi}/p). \]

Proposition 4.6.4. Let \( v \) be a prime of \( L_1 \).

1. If \( v \nmid N_A N \), then \( \text{res}_v (P(n)) \) is trivial.

2. If \( v \mid N_A N p \), then \( \text{res}_v (P(n)) \) lies in \( H^1(K_{v}^{ur} / K_v, V_{\varphi}/p) \).
Proof. 1. We follow the proof in Chapter 3 Proposition 3.4.4. We denote by

$$V_p/p^\text{dual} = \text{Hom}(V_p/p, \mathbb{Z}/p\mathbb{Z}(1))$$

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

$$|H^1(K_v, V_p/p)| = |H^0(K_v, V_p/p)| \times |H^2(K_v, V_p/p)|.$$ 

Local Tate duality then implies

$$|H^1(K_v, V_p/p)| = |H^0(K_v, V_p/p)|^2.$$ 

The Weil conjectures and the assumption on $Fr(v)$ imply that $(V_p/p)^{L_v} Fr(v) = 0$ where

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

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

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

$$\text{res}_{L_{1,v},L_{n,v}} c(n) = \text{res}_v D_n y_n \in H^1(L_{n,v}/L_{n,v}, V_p/p)$$

for $v'$ above $v$ in $L_n$. The exact sequence

$$\cdots \rightarrow H^1(L_{n,v}/L_{n,v}, (V_p/p)^{L_v}) \rightarrow H^1(L_{n,v}, V_p/p) \rightarrow \text{res} \rightarrow H^1(L_{n,v}/L_{n,v}, V_p/p) \rightarrow \cdots$$

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

85
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

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

**Proof.** First note that if $p \nmid |\text{Aut}(V_{\varphi}/p)|$, then $H^1(\text{Aut}(V_{\varphi}/p), V_{\varphi}/p) = 0$. If $p$ divides $|G|$, then since $V_{\varphi}/p$ is irreducible as an $\text{Aut}(V_{\varphi}/p)$-module, Dickson’s lemma [52, Theorem 6.21] implies that $\text{Aut}(V_{\varphi}/p)$ contains $\text{SL}_2(F_q)$ 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 $H^1(\text{Aut}(V_{\varphi}/p), V_{\varphi}/p)$ and the result follows. □

We recall the statement of theorem 1.3.1.

**Theorem 1.3.1.** Let $p$ be such that

$$\text{Gal}(K(V_{\varphi}/p)/K) \simeq \text{Aut}_K(V_{\varphi}/p), \quad (p, N\phi(N)N_A) = 1.$$ 

Suppose that $V_{\varphi}/p$ is a simple $\text{Aut}_K(V_{\varphi}/p)$-module. Suppose further that the eigenvalues of $Fr(v)$ acting on $V_{\varphi}^{I_v}$ 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 $O_{F,\varphi}/p$.

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 \( \text{Gal}(L/K) \) by \( G \). The restriction map

\[
r : H^1(K, V_{\rho}/p) \rightarrow H^1(L, V_{\rho}/p)^G = \text{Hom}_G(\text{Gal}(\overline{Q}/L), V_{\rho}/p)
\]

has kernel

\[
\text{Ker}(r) = H^1(K(V_{\rho}/p)/K, V_{\rho}/p) = H^1(\text{Aut}(V_{\rho}/p), V_{\rho}/p) = 0
\]

by Lemma 4.7.1. Hence, we can identify an element \( c \in H^1(K, V_{\rho}/p) \) with its image \( r(c) \).

Consider the evaluation pairing

\[
[\cdot, \cdot] \colon r(S) \times \text{Gal}(\overline{Q}/L) \rightarrow V_{\rho}/p.
\] (4.6)

We denote by \( \text{Gal}_S(\overline{Q}/L) \) the annihilator of \( r(S) \). Let \( L^S \) be the extension of \( L \) fixed by \( \text{Gal}_S(\overline{Q}/L) \) and \( G_S \) the Galois group \( \text{Gal}(L^S/L) \).

We consider the restriction \( d \) of an element \( c \) of \( H^1(K, V_{\rho}/p) \) to \( H^1(L, V_{\rho}/p) \). 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 \( \rho \in \text{Gal}_S(\overline{Q}/L) \), then \( [s, \rho] = 0 \) for all \( s \in S \). Hence, \( y_1 \) defines a cocycle of \( S \) by

\[
\rho \mapsto \rho(y_1) - y_1 = 0.
\]
This implies that $\rho$ fixes $L(y_1)$, a subfield of $L^S$.

We have $\text{Gal}(L(y_1)/L) \simeq V_\rho/p$ and we denote by $I = \text{Gal}(L^S/L(y_1))$.

![Diagram]

**Lemma 4.7.3.** There is an isomorphism of $\mathcal{O}_{F,\delta}/p$-modules mapping $\text{res}_\lambda P(m\ell)$ where $\lambda'$ divides $\ell$ in $K$ to $\text{res}_\lambda P(m)$. Also, $\text{res}_\lambda P(\ell)$ is ramified for all such $\lambda$.

*Proof.* This is an adaptation of Section 3.5 in Chapter 3 that uses the properties of the Euler system considered in Proposition 4.5.1 and Proposition 4.5.2. \hfill $\Box$

**Lemma 4.7.4.** There is a Kolyvagin prime $q$ such that

$$\text{Frob}_q(L^S/\mathbb{Q}) = \tau h, \ h \in \text{Gal}(L^S/L), \ h^{\tau+1} \notin I \text{ and } \text{res}_{\beta'}y_1 \neq 0$$

for some prime $\beta'$ in $K$ above $q$.

*Proof.* Let $q$ be a Kolyvagin prime such that

$$\text{Frob}_q(L^S/\mathbb{Q}) = \tau h, \ h \in \text{Gal}(L^S/L), \ h^{\tau+1} \notin I.$$ 

Note that the restriction of $\tau h$ to $L$ is $\tau$. Assume $q$ splits completely in $L(y_1)$. Then for a prime $\beta'$ of $L(y_1)$ above $q$, we would have that

$$\text{Frob}_{\beta'}(L^S/(L(y_1))) = (\tau h)^2,$$
a contradiction since \( \text{Frob}_{\beta'}(L^S/L(y_1)) \) belongs to \( I \) while \( h^{e+1} = (\tau h)^2 \notin I \). 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 \( \beta \) in \( L_1 \) above \( q \) such that \( |L(y_1)_{\beta'} : L_{\beta'}| > 1 \) for a prime \( \beta' \) of \( L \) above \( \beta \) and a prime \( \beta'' \) of \( L(y_1) \) above \( \beta' \). This implies that
\[
\text{res}_{\beta y_1} \neq 0.
\]

Consider the following extensions

\[
\begin{align*}
H_2 &= H_0H_1 \\
H_0 &= L(c) \\
H_1 &= L(P(q)) \\
L &= K(V_{\phi}/p)
\end{align*}
\]

We define \( V_i = \text{Gal}(H_i/L) \) for \( i = 0, 1, 2 \). We have an isomorphism of \( \text{Aut}(A_{\phi}/p) \)-modules
\[
V_0 \simeq V_1 \simeq V_{\phi}/p.
\]

**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 \( \text{Gal}(L'/L_{ur}) \) is such that
\[
[s, \tilde{\rho}] = 0 \quad \text{for all } s \in S,
\]

since \( s \) is unramified at \( q \).
Lemma 4.7.3 implies that $P(q)$ ramifies at $q$ and $\text{res}_\beta P(q)$ is mapped under an isomorphism to $\text{res}_\beta y_1 \neq 0$. 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

$$\text{Gal}(L(c) \cap L(P(q))/L)$$

is a $G_V$ submodule of $V_1 \cong V_\rho/p$.

Therefore, $\text{Gal}(L(c) \cap L(P(q))/L)$ 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 $\sigma$ in $\text{Gal}(K_j/K)$ such that

$$\tau \Phi(\Delta_{\varphi_j})_{\rho} = \varepsilon'_L \sigma \Phi(\Delta_{\varphi_j})_{\rho},$$

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

$$k = 2 \sqrt{\frac{\text{deg}(\varphi_i)}{\text{deg}(\varphi_j)}}.$$ 

**Proof.** Using [26] which shows that $\tau A_j = W_N(\sigma A_j)$ for some $\sigma$ in $G(K_j/K)$, we obtain by Proposition 4.4.1

$$(\tau \times I)_*(D_{A_j}^r) = kD_{(A_j)}^r = kD_{W_N(\sigma A_j)}^r$$

where $k = 2 \sqrt{\frac{\text{deg}(\varphi_i)}{\text{deg}(\varphi_j)}}$. Consider the map

$$W \times I : W_N \times A \rightarrow W_N \times A : ((E, P), A) \rightarrow ((E/(P), P'), A),$$

90
where $P'$ is such that the Weil pairing $<P, P'>$ of $P$ with $P'$ satisfies $<P, P'> = \zeta_N$ for some choice $\zeta_N$ of an $N$-th root of unity $\zeta_N$. Note that $W$ has degree $N$. Also,

$$W_*f(\tau)d\tau dz = e_LNf(\tau)d\tau dz.$$ 

This implies as in [39, Proposition 6.2] that

$$(W \times I)_*D_{W_N(\sigma A_j)}^r = e_LN^rD_{W_N(\sigma A_j)}^r,$$

while Proposition 4.4.1 implies that the former equals $N^r \left\langle \frac{\deg(\phi)}{\deg(\phi_j)} \right\rangle D_{\sigma A_j}^r$. Hence,

$$D_{W_N(\sigma A_j)}^r = k_1e_L^rD_{\sigma A_j}^r,$$

where $k_1 = \sqrt{\frac{\deg(\phi)}{\deg(\phi_j)}}$. Applying Proposition 4.4.1 to the map $(\sigma \times I)$, we obtain

$$(\sigma \times I)_*(D_{A_j}^r) = k_2D_{\sigma A_j}^r,$$

where $k_2 = \deg(\sigma)^r \sqrt{\frac{\deg(\phi)}{\deg(\phi_j)}} = k_1$. Hence, $D_{W_N(\sigma A_j)}^r = e_L^r(\sigma \times I)_*(D_{A_j}^r)$ and

$$(\tau \times I)_*(D_{A_j}^r) = e_L^r(k(\sigma \times I)_*(D_{A_j}^r)).$$

Therefore

$$\tau \Phi(\Delta_{\phi_j})\varphi = e_L^r k\sigma \Phi(\Delta_{\phi_j})\varphi.$$

Remark 4.8.2. The non-trivial Kolyvagin class $P(1)$ belongs to $S^+\varepsilon$ where

$$\varepsilon = e_L^r.$$
Indeed, \( y_1 \) is non-zero by the hypothesis on \( \Phi(\Delta_{\phi_1})_{\wp} \) and belongs to \( S^+ \) by Lemma \ref{lem:4.8.1}

Using the relation \( \tau D_\ell = -D_\ell \tau \mod p \), it can also be deduced from Lemma \ref{lem:4.8.1} that \( P(n) \) belongs to the \(( -1 )^{\omega(n)} \) \( e \) eigenspace where \( \omega(n) \) is the number of distinct prime factors of \( n \).

Given a Kolyvagin prime \( \ell \), the Frobenius condition implies that is inert in \( K \). We denote by \( \lambda \) the prime of \( K \) lying above \( \ell \). As explained in Chapter \ref{ch:2} Section \ref{sec:2.5} using local Tate duality, we have a perfect local pairing

\[
\langle \cdot, \cdot \rangle_\lambda : H^1(\Kur_{\lambda}^\ur / K_{\lambda}, (V_{\wp} / p)^{I_{\lambda}}) \times H^1(\Kur_{\lambda}^\ur / V_{\wp} / p) \longrightarrow \mathbb{Z} / p,
\]

where \( I_{\lambda} = \text{Gal}(\overline{K}_{\lambda} / \Kur_{\lambda}^\ur) \) and \( \mathcal{O}_{F, \wp}\)-linear isomorphisms

\[
\{H^1(\Kur_{\lambda}^\ur / V_{\wp} / p)^\text{dual}\} \simeq H^1(\Kur_{\lambda}^\ur / K_{\lambda}, (V_{\wp} / p)^{I_{\lambda}}).
\]

We denote by

\[
\text{res}_\lambda : H^1(K, V_{\wp} / p) \longrightarrow H^1(K_{\lambda}, V_{\wp} / p)
\]

the restriction map from \( H^1(K, V_{\wp} / p) \) to \( H^1(K_{\lambda}, V_{\wp} / p) \). When the complex conjugation \( \tau \) acts on a module \( M \), we denote by \( M^+ \) and \( M^- \) the \( + \) and \( - \) eigenspaces of \( M \) with respect to the action of \( \tau \).

**Lemma 4.8.3.** The action of complex conjugation induces non-degenerate pairings of eigenspaces

\[
\langle \cdot, \cdot \rangle_\lambda^\pm : H^1(\Kur_{\lambda}^\ur / K_{\lambda}, (V_{\wp} / p)^{I_{\lambda}})^\pm \times H^1(\Kur_{\lambda}^\ur / V_{\wp} / p)^\pm \longrightarrow \mathbb{Z} / p.
\]
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

$$\langle c_1, c_2 \rangle^\tau_{\lambda} = \langle c_1^\tau, c_2^\tau \rangle_{\lambda^\tau} = \langle c_1, -c_2 \rangle_{\lambda^\tau} = -\langle c_1, c_2 \rangle_{\lambda^\tau}.$$  

Furthermore, $\langle c_1, c_2 \rangle^\tau_{\lambda} = \langle c_1, c_2 \rangle_{\lambda^\tau}$ since $\tau$ 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

$$G_S^{+} = \{(\tau h)^2, \ h \in G_S\}, \ I^+ = \{2i^2, \ i \in I\}.$$  

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
\[ \sum_{\lambda |\ell |n} \langle s_\lambda, \text{res}_\lambda P(n) \rangle_\lambda = 0. \]

Proof. The proof follows \[39, \text{prop}osition \ 11.2(2)\] 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 \( \mathcal{O}_{F, \wp}/\mathfrak{p} \).

Proof. Consider the Kolyvagin class \( P(\ell) \) where \( \ell \) is a Kolyvagin prime satisfying

\[ \text{Frob}_\ell(L^S/Q) = \tau h, \ h \in G_S, \ h \notin \text{Gal}(L^S/L(y_1)). \]

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 \( \text{res}_\lambda P(\ell) \) to \( \text{res}_\lambda P(1) \). The same argument as the one for \( q \) implies that

\( \text{res}_\lambda P(1) \neq 0 \).

Let \( s \) be an element of \( S^{-\varepsilon} \). Lemma 4.9.1 and Lemma 4.8.3 imply

\[ \sum_{\lambda |\ell} \langle \text{res}_\lambda s, \text{res}_\lambda P(\ell) \rangle_{\lambda}^{-\varepsilon} = 0. \]

Since \( \text{res}_\lambda P(\ell) \neq 0 \), the non-degeneracy of the local Tate pairing implies that \( \text{res}_\lambda s = 0 \).

Hence, \( [s, \text{Frob}_\lambda (L^S/L_1)] = 0 \), 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 \( s : G_S \rightarrow V_{\wp}/\mathfrak{p} \) induces a \( G_V \)-homomorphism of groups

\[ s : G_S^+ \rightarrow V_{\wp}/\mathfrak{p}. \]
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 \( \mathcal{O}_{F,\wp}/p \). Since \( V_\wp/p \) has no non-trivial \( G_V \)-submodules, we have \( s(G^-_S) = s = 0 \).

**Proposition 4.9.3.** We have \( S^{+\epsilon} \) is of rank 1 over \( \mathcal{O}_{F,\wp}/p \).

**Proof.** Let \( \ell \) be a Kolyvagin prime such that

\[
\text{Frob}_\ell(L^S/Q) = \pi i, \quad i \in \text{Gal}(L^S/L(y_1))
\]

and such that

\[
\text{Frob}_\ell(L(P(q))/Q) = \tau j, \quad j \in \text{Gal}(L(P(q))/L), \quad j^{\tau+1} \neq 1.
\]

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 \( P(\wp q) \) which belongs to the \( \epsilon \)-eigenspace by Remark 4.8.2. We have

\[
\text{res}_\lambda P(q) \neq 0
\]

for \( \lambda \) above \( \ell \) in \( K \). Indeed, the Frobenius condition

\[
\text{Frob}_\lambda(L(P(q))/K) = j^{\tau+1} = (\tau j)^2 \neq 1
\]
implies that $\lambda$ does not split completely in $L(P(q))$. By Lemma \[4.7.3\], this implies that

$$\text{res}_\lambda P(\ell q) \neq 0.$$  

The Frobenius condition in $L^S/Q$ implies that $\ell$ splits completely in $L(y_1)$, so that

$$\text{res}_\lambda y_1 = 0.$$  

Then by Lemma \[4.7.3\], $\text{res}_\lambda P(\ell) = 0$. Hence, $P(\ell)$ belongs to the Selmer group, in fact to $S^{-e}$. As a consequence of Proposition \[4.9.2\], $P(\ell) = 0$ implying

$$\text{res}_\beta P(\ell) = 0.$$  

Therefore by Lemma \[4.7.3\],

$$\text{res}_\beta P(\ell q) = 0.$$  

Let $s \in S^{+e}$. By Lemma \[4.9.1\] and Lemma \[4.8.3\],

$$\sum_{\lambda \mid \ell} \langle \text{res}_\lambda s, \text{res}_\lambda P(\ell q) \rangle^+ + \sum_{\beta \mid q} \langle \text{res}_\beta s, \text{res}_\beta P(\ell q) \rangle^+ = 0.$$  

Hence,

$$\sum_{\lambda \mid \ell} \langle \text{res}_\lambda s, \text{res}_\lambda P(\ell q) \rangle^+ = 0.$$  

The non-degeneracy of the local Tate pairing implies that

$$\text{res}_\lambda s = 0.$$  

Therefore, $[s, \text{Frob}_\lambda (L^S/K_\lambda)] = 0$, that is

$$[s, (\tau i)^2] = 0.$$  

96
This is true for all $i \in I$ by Cebotarev’s density theorem and Lemma 4.8.4. As a consequence, the homomorphism $s : I \to V_{\varphi}/p$ reduces to a $G_V$-homomorphism

$$s : I^- \to V_{\varphi}/p^\pm,$$

where $V_{\varphi}/p^+$ and $V_{\varphi}/p^-$ are free of rank 2 over $O_{F,\varphi}/p$. Therefore, since $V_{\varphi}/p$ have no non-trivial $G_V$-submodules, $s(I^-) = s(I) = 0$. This implies that

$$s \in \text{Hom}_{G_V}(\text{Gal}(L^S/L)/I, V_{\varphi}/p) \simeq \text{Hom}_{G_V}(V_{\varphi}/p, V_{\varphi}/p) \simeq O_{F,\varphi}/p.$$

Therefore by Remark 4.8.2,

$$\text{rank}(S) = 1.$$

\[\square\]

**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 $O_{F,\varphi}/p$.

**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 $\Phi(\Delta_I)_{\varphi}$ 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 $O_{F,\varphi}/p$. \[\square\]
5.1 From analytic rank to algebraic rank

Let $\phi : X_0(N) \to E$ 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


