KOLYVAGIN’S METHOD FOR CHOW GROUPS OF KUGA-SATO VARIETIES OVER RING CLASS FIELDS

Yara Elias

Department of Mathematics, McGill University
yara.elias@mail.mcgill.ca

Abstract

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 field character. This is an extension of Nekovar’s result [5] that uses Bertolini and Darmon’s refinement of Kolyvagin’s ideas, as described in [1].

Acknowledgments. I am very grateful to my advisor Henri Darmon who suggested this beautiful problem and guided me through its resolution and whose feedback was crucial to the writing of this article.

1 Introduction

Let $f$ be a normalized form of level $N \geq 5$ 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 $p$ satisfying

$$(p, ND\phi(N)(2r - 2)!) = 1.$$
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 $F = \mathbb{Q}(a_1, a_2, \ldots, \mu_e)$ be the field generated over $\mathbb{Q}$ by the coefficients of $f$ and $\mu_e$. We denote by $A$ the $p$-adic étale realization of the motive associated to $f$ as in [5, section 3]. It gives rise (by extending scalars appropriately) to 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 localization of $\mathcal{O}_F$ at $\wp$. The Selmer group

$$S \subseteq H^1(H, A_{\wp}/pA_{\wp})$$

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

$$H^1(H^w_v/H_v, A_{\wp}/pA_{\wp}) \quad \text{for } v \text{ not dividing } Np$$

$$H^1_f(H_v, A_{\wp}/pA_{\wp}) \quad \text{for } v \text{ dividing } p$$

where $H^1_f(H_v, A_{\wp}/pA_{\wp})$ is the finite part of $H^1(H_v, A_{\wp}/pA_{\wp})$ as in [4, part 1]. The Galois group

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

acts on $H^1(H, A_{\wp}/pA_{\wp})$ hence it acts on $S$. 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 $\hat{G}$. 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 $H^1(H, A_{\wp}/pA_{\wp})$. We denote by $Fr(v)$ the Frobenius element generating $\text{Gal}(H^w_v/H_v)$. This article is dedicated to the proof of the following statement:
Theorem 1.1. Assume that $p$ is such that

$$\text{Gal}\left(\mathbb{Q}(A_p/p)/\mathbb{Q}\right) \simeq \text{GL}_2(\mathcal{O}_p/p), \quad (p, ND\phi(N)(2r - 2)!)=1, \quad \text{and} \quad p \nmid |G|.$$

Suppose further that the eigenvalues of $Fr(v)$ acting on $A_p$ are not equal to 1 modulo $p$ for $v$ dividing $N$. Let $\chi \in \hat{G}$ be such that $\chi e^N$ is not divisible by $p$. Then the $\chi$-eigenspace of the Selmer group $S^\chi$ is one-dimensional over $\mathcal{O}_p$.

2 Heegner cycles

Consider the congruence subgroups $\Gamma(N)$ and $\Gamma_0(N)$ of the modular group $\text{SL}_2(\mathbb{Z})$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid a \equiv d \equiv 1, \quad b \equiv c \equiv 0 \mod{N} \right\},$$

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

Let $Y(N)$ be the smooth irreducible affine curve that is the coarse moduli space classifying elliptic curves with $\Gamma(N)$ level structure, that is elliptic curves $E$ with a pair of points $(P_1, P_2)$ of $E[N]$ satisfying

$$e_N(P_1, P_2) = \zeta_N,$$

where $e_N$ is the Weil pairing and $\zeta_N$ is some $N$-th root of unity. We denote by $Y_0(N)$ the smooth irreducible affine curve that is the coarse 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

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

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

The compactification of $Y(N)$ and $Y_0(N)$ viewed as Riemann surfaces will be denoted by $X(N)$ and $X_0(N)$. Let

$$\pi : Y_0(N) \longrightarrow X_0(N)$$

be the projection from $Y_0(N)$ to $X_0(N)$ where $X_0(N)$ is viewed as the quotient of $X(N)$ by the Borel subgroup of $SL_2(\mathbb{Z})$ acting on $X(N)$. Denote by $H = K_c$ the ring class field of $K$ of conductor $c$, and by $H_m = K_{cm}$ the ring class field of $K$ of conductor $cm$ for $m > 1$. Consider coprime integers $c$ and $m$ such that $(cm, NDp) = 1$. By the Heegner hypothesis, there is an ideal $\mathcal{N}$ of $\mathcal{O}_{cm}$, the order of $K$ of conductor $cm$, such that

$$\mathcal{O}_{cm}/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}.$$

Therefore, $\mathbb{C}/\mathcal{O}_{cm}$ and $\mathbb{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic $N$-isogeny. As points of $X_0(N)$ correspond to elliptic curves 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 of $K$ of conductor $cm$. Pick $x \in \pi^{-1}(x_m)$. And let $E$ be the corresponding elliptic curve. Then $E$ has complex multiplication by $\mathcal{O}_{cm}$. Letting $\text{graph}(\sqrt{-D})$ be the graph of the multiplication of $E$ by $\sqrt{-D}$, we denote by $Z_E$ the image of the divisor

$$(\text{graph}(\sqrt{-D}) - E \times 0 - D(0 \times E))$$
in the Néron-Severi group $NS(E \times E)$ of $E \times E$, that is, the group of divisors of $E \times E$ modulo algebraic equivalence. Let
\[
\mathcal{E} = \mathbb{Z}^2 \setminus (\mathbb{C} \times \mathbb{H})
\]
be the universal generalized elliptic curve where $(m,n)$ in $\mathbb{Z}^2$ acts on $\mathbb{C} \times \mathbb{H}$ by
\[
(z, \tau) \mapsto (z + m \tau + n, \tau).
\]
Consider the inclusion
\[
i : E^{2r-2} \rightarrow W_{2r-2},
\]
where $W_{2r-2}$ is the Kuga-Sato variety of dimension $2r-1$, that is, the smooth compactification of the $2r-2$-fold fibre product
\[
\mathcal{E} \times_{X(N)} \cdots \times_{X(N)} \mathcal{E}.
\]
Then $i_* (Z_E^{r-1})$ belongs to the Chow group $\text{CH}^r(W_{2r-2}/H_m)_0$ of homologically trivial subvarieties of $W_{2r-2}$ of codimension $r$ defined over $H_m$ modulo rational equivalence. Denote by $y_m$ the image of $i_* (Z_E^{r-1})$ by the étale Abel-Jacobi map
\[
\Phi : \text{CH}^r(W_{2r-2}/H_m)_0 \rightarrow H^1(H_m, A)
\]
as described in [3]. We consider two crucial properties of the Galois cohomology classes thus obtained from Heegner cycles.

**Proposition 2.1.** 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 $x \in \pi^{-1}(x_m)$. Then, we have

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

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

$$\text{Gal}(H_n/H_m) \simeq \text{Gal}(K_n/K_m) \simeq \text{Gal}(K_\ell/K_1) \simeq (\mathbb{Z}/((\ell + 1)/u_K)\mathbb{Z})^* \simeq (\mathbb{Z}/(\ell + 1)\mathbb{Z})^*,$$

where $u_K = |\theta_K^*|/2 = 1$. Let $E_n$ be the elliptic curve corresponding to $y \in \pi^{-1}(x_n)$. 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 $a_\ell$. (See [5, section 3]).

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

**Proposition 2.2.** 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

$$(y_n)_{\lambda_n} = Fr(\ell)(\text{res}_{K_{\lambda_m},K_{\lambda_n}}(y_m)_{\lambda_m}) \text{ in } H^1(K_{\lambda_n},A).$$
Proof. The proof can be found in [5 proposition 6.1(2)].

3 The Euler System

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

$$(\ell_i, DN pc) = 1 \text{ for } i = 1, \ldots, k.$$ 

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

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

the $\wp$-component of $y_n \in H^1(H_n, A)$. Let $Y_\wp = A_{\wp}/pA_{\wp}$ and let

$$L = H(Y_\wp(\overline{Q}))$$

be the smallest Galois extension of $H$ such that $\text{Gal}(\overline{Q}/L)$ acts trivially on $Y_\wp(\overline{Q})$. 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 $\text{Gal}(F_1/F_2)$. A prime $\ell$ will be referred to as a Kolyvagin prime if it is such that

$$(\ell, DN pc) = 1 \text{ and } \text{Frob}_\ell(L/Q) = \text{Frob}_\infty(L/Q),$$

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 $K$. Indeed, $\ell$ is not in the kernel of the Artin
map. Denote by $\lambda$ the unique prime in $K$ above $\ell$. Since $\lambda$ is unramified in $H$ and has the same image as $\text{Frob}_{\infty}(L/K) = \tau^2 = Id$ 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:

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

The Frobenius condition also implies that

$$a_\ell \equiv \ell + 1 \equiv 0 \mod p. \quad (1)$$

Indeed, the characteristic polynomial of $\text{Frob}(\ell)$ acting on $Y_p$ is

$$x^2 - a_\ell/\ell'x + 1/\ell,$$

while the characteristic polynomial of the complex conjugation is $x^2 - 1$. For the rest of the monograph, we assume that $p$ is such that

$$\text{Gal}(\mathbb{Q}(Y_p)/\mathbb{Q}) \simeq \text{GL}_2(O_{\wp}/p).$$

Let

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

These operators are related by

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

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

$$A_{\rho} \rightarrow Y_p = A_{\rho}/pA_{\rho}.$$ 

**Proposition 3.1.** We have

$$D_n\text{red}(y_{n, \rho}) \text{ belongs to } H^1(H_n, Y_p)^{G_n}.$$ 

**Proof.** It is enough to show that for all $\ell$ dividing $n$, $(\sigma_\ell - 1)D_n\text{red}(y_{n, \rho}) = 0$ in $H^1(H_n, Y_p)$. We have

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

Since $\text{res}_{H_n, H_n} \circ \text{cor}_{H_n, H_m} = \text{Tr}_\ell$, Proposition (2.1) implies

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

The latter is congruent to 0 modulo $p$ by Equation (1). 

**Proposition 3.2.** For $n$ such that $(n, cpND) = 1$, we have

$$Y_p(H_n) = Y_p(\mathbb{Q}) = 0,$$

and $\text{Gal}(H_n(Y_p)/H_n) \simeq \text{Gal}(H(Y_p)/H) \simeq \text{Gal}(K(Y_p)/K) \simeq \text{Gal}(\mathbb{Q}(Y_p)/\mathbb{Q})$. 

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

9
Proposition 3.3. The restriction map

$$\text{res}_{H,H_n} : H^1(H,Y_p) \longrightarrow H^1(H_n,Y_p)^{G_n}$$

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

Proof. This follows from the inflation-restriction sequence:

$$0 \rightarrow H^1(H_n/H,Y_p(H_n)) \xrightarrow{\text{inf}} H^1(H,Y_p) \xrightarrow{\text{res}} H^1(H_n,Y_p)^{G_n} \rightarrow H^2(H_n/H,Y_p(H_n))$$

using the fact that $Y_p(H_n) = 0$ by Proposition (3.2).

As a consequence, the cohomology classes $D_n \text{red}(y_n, \wp)$ can be lifted to cohomology classes $P(n)$ in $H^1(H,Y_p)$ such that

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

Proposition 3.4. Let $v$ be a prime of $H$. If $v \mid N$, then $P(n)_v$ is trivial. If $v \nmid Nnp$, then $P(n)_v$ lies in $H^1(H_{v}^{\text{ur}}/H_v,Y_p)$.

Proof. If $v$ divides $N$, we follow the proof in [5, lemma 10.1]. We denote by

$$Y_p^{\text{dual}} = \text{Hom}(Y_p, H_v(1))$$

the local Tate dual of $Y_p$. The local Euler characteristic formula yields

$$|H^1(H_v,Y_p)| = |H^0(H_v,Y_p)| \times |H^2(H_v,Y_p^{\text{dual}})|.$$

Local Tate duality then implies

$$|H^1(H_v,Y_p)| = |H^0(H_v,Y_p)|^2.$$
where

\[ H^0(H_v, Y_p) = Y_p(H_v). \]

The Weil conjectures and the assumption on \( Fr(v) \) imply that \( Y_p^{Fr(v)} = 0 \) where

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

We have the exact sequence

\[ 0 \rightarrow (Y_p^I)^{G(H_v^{ur}/H_v)} \rightarrow (Y_p)^{G(H_v^{ur}/H_v)} \rightarrow H^1(H_v^{ur}, A_\wp)^{G(H_v^{ur}/H_v)}, \]

where \( I = \text{Gal}(\overline{H_v}/H_v^{ur}) \) is the inertia group. Since \( (Y_p)^{Fr(v)} = 0 \) and

\[ H^1(I, A_\wp)^{Fr(v)} \subseteq (A_\wp/(I - 1))^{Fr(v)} = 0, \]

we conclude that \( (Y_p)^{G(H_v^{ur}/H_v)} = 0. \)

If \( v \) does not divide \( Nnp \), then

\[ \text{res}_{H_n} P(n)_v = D_n \text{red}(y_{n, \wp})_v \]

belongs to \( H^1(H_n^{ur}/H_n^{ur}, Y_p) \) and \( H_n^{ur}/H_v \) is unramified for \( v' \) in \( H_n \) above \( v \).

\[ \square \]

4 Localization of Kolyvagin classes

Nekovar [5] studied the localization of Kolyvagin cohomology classes by explicitly computing cocycles using the Euler system properties. We briefly explain his development in this section.

Consider the following setting where \( L_1 \) and \( L_\ell \) are either ring class fields of an imaginary quadratic field with conductors \( c \) and \( \ell c \) or the compositum of such ring class fields with a Ray class field of
fixed conductor. We denote by

\[ G = \text{Gal}(\overline{Q}/L_1), \quad H = \text{Gal}(\overline{Q}/L_\ell), \quad \tilde{G} = \text{Gal}(\overline{Q}/L_1^\perp), \]

and \( G_0 = \text{Gal}(\overline{Q}_\ell/L_{1,\lambda_1}), \quad H_0 = \text{Gal}(\overline{Q}_\ell/L_{\ell,\lambda_\ell}), \quad \tilde{G}_0 = \text{Gal}(\overline{Q}_\ell/Q_{\ell}) \),

where \( L_1^\perp \) is the maximal real subfield of \( L_1 \). Then

\[ G/H = \langle \sigma \rangle, \quad \tilde{G}/G = \langle \tau \rangle, \quad \tilde{G}/H = \text{Gal}(L_{\ell}/L_1^\perp) = \langle \sigma \rangle \rtimes \langle \tau \rangle \]

for some \( \sigma \) and \( \tau \). There is a surjective homomorphism

\[ \pi : \tilde{G}_0 \xrightarrow{\text{res}} \text{Gal}(\overline{Q}_\ell'/Q_{\ell}) = \hat{\mathbb{Z}}'(1) \times 2\hat{\mathbb{Z}}, \]

where

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

is generated by an element \( \tau \) and

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

is generated by the Frobenius element \( \phi \) at \( \ell \) and \( \phi \tau \phi^{-1} = \tau^\ell \). Let \( A \) be a free \( \mathbb{Z}_p \)-module of finite rank with a continuous action of \( \tilde{G} \) such that

\[ (A/pA)^G = 0. \]

and such that \( \tilde{G}_0 \) acts on \( A \) through its quotient \( \hat{\mathbb{Z}} \). One can show that

\[ H^1(G_0,A) = H^1(H_0,A) \simeq H^1(2\hat{\mathbb{Z}},A) \simeq A/(\phi^2-1)A \]
and a cocycle $F$ in $Z^1(\hat{\mathbb{Z}}(1) \times \hat{\mathbb{Z}}, A)$ acts by

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

where $[F] = a \mod (\phi^2 - 1)A$. Consider cohomology classes

$$x \in H^1(G, A), \ y \in H^1(H, A), \text{ with } \cor_{H,G}(y) = M_1x \text{ for some } M_1 \text{ divisible by } p.$$

Here, $M_1$ is implied by the first Euler system property. There exists $z \in H^1(G, A/pA)$ such that

$$\res_{G,H}(z) = D_\ell \red_M(y) \in H^1(H, A/pA).$$

For $a$ in $A$,

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

Therefore, $\res_{G,H_0}(z) = 0$. Hence, using the inflation-restriction sequence

$$0 \rightarrow H^1(G_0/H_0, A) \rightarrow H^1(G_0, A) \rightarrow H^1(H_0, A) \rightarrow 0,$$

we obtain

$$\res_{G,G_0}(z) = \inf_{G_0/H_0, G_0}(z_0)$$

for some

$$z_0 \in H^1(G_0/H_0, A/pA) = \Hom(<\sigma_0>, A/pA).$$

There is an element $a$ in $A$ such that

$$\cor_{H,G}(y)(g) - M_1x(g) = (g - 1)a$$
for $g \in G$. Note that

$$a = z_0(\sigma_0).$$

(See [5, section 7] for more details). Restricting $g$ to $g_0 \in G_0$ where $\pi(g_0) = \sigma_0^\ell \phi^{2v}$, we obtain

$$\sum_{i=0}^{\ell} y(\tilde{\sigma}_0^{-i}g_0\tilde{\sigma}_0^i) - M_1x(g_0) = (g_0 - 1)a,$$

where $\tilde{\sigma}$ is a lift of $\sigma \in G/H$ to $G$. We have

$$x(g_0) = (1 + \phi + \cdots + \phi^{v-1})a_x + (\phi^2 - 1)b_x, \quad a_x = \text{res}_{G,G_0}(x),$$

$$\& \quad y(g_0) = (1 + \phi + \cdots + \phi^{v-1})a_y + (\phi^2 - 1)b_y, \quad a_y = \text{res}_{H,H_0}(y).$$

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

$$((\ell + 1)y(g_0) - M_1x(g_0) = (\phi^2 - 1)a + (\phi^2 - 1)(M_1b_x - (\ell + 1)b_y),$$

where

$$(\phi^2 - 1)(M_1b_x - (\ell + 1)b_y) = 0 \mod p$$

as $\phi^2 - 1$ acts trivially on $A/p$ and $M_1 \equiv \ell + 1 \equiv 0 \mod p$. The second property of an Euler system

$$a_y = \phi(a_x) \mod (\phi^2 - 1)A$$

implies that

$$\frac{\ell + 1}{p} y(g_0) - \frac{M_1}{p} x(g_0) = \left(\frac{\ell + 1}{p} - \frac{M_1}{p}\right)x(g_0)$$

14
where $\varepsilon$ is such that $\phi = \tau$ acts by $\varepsilon$ on $a_x$. Therefore,

$$\left(\frac{\ell + 1}{p} \varepsilon - \frac{M_1}{p}\right) x(g_0) = \frac{\phi^2 - 1}{p} a \mod p.$$ 

The characteristic polynomial of $\phi$ implies that

$$\phi^2 - a \frac{\phi}{\ell^r} + 1/\ell = 0 \text{ on } A.$$

Therefore,

$$\left(\frac{\ell + 1}{p} \varepsilon - \frac{a_\ell}{p}\right) x(g_0) = \frac{a_\ell \phi / \ell^r + 1/\ell - 1}{p} = \frac{a_\ell \varepsilon / \ell^r + 1/\ell - 1}{p}.$$

We seek $\inf_{G_0/H_0,G_0}(z_0)$ where the generator $\sigma_0$ of $G_0/H_0$ can be lifted to the generator $\tau_\ell$ of $\text{Gal}(K_1/K_1^\mu)$. It is therefore enough to apply $\Phi$ to $z_0$ since $\Phi$ switches cocycles with same values on $\text{Frob}(\ell)$ and $\tau_\ell$. Finally, applying the formulas obtained to $x = D_{m} y_m$ and $y = D_{m} y_{\ell m}$ yields the relations we refer to in the next sections. Furthermore, the equation $\text{res}_{G,H_0}(z) = 0$ implies that $z$ vanishes on $\text{Frob}(\ell)$ and is hence ramified at $\ell$.

## 5 Statement

The Galois group $G = \text{Gal}(H/K)$ acts on $H^1(H,Y_p)$. Recall that 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 $\hat{G}$. We denote by

$$\delta = \text{red}(y_1) \quad \text{in} \quad H^1(H,Y_p).$$

Then $e_\chi \delta$ belongs to the $\chi$-eigenspace of $H^1(H,Y_p)$. We prove the following theorem.

**Theorem 5.1.** Assume that $p$ is such that

$$\text{Gal}(\mathbb{Q}(A_{\mathfrak{p}}/p)/\mathbb{Q}) \simeq \text{GL}_2(\mathcal{O}_{\mathfrak{p}}/p), \quad (p,ND\phi(N)(2r-2)!)=1, \quad \text{and} \quad p \nmid |G|. \quad (2)$$

Suppose further that the eigenvalues of $\text{Fr}(v)$ acting on $A_{\mathfrak{p}}$ are not equal to 1 modulo $p$ for $v$ dividing $N$. Let $\chi \in \hat{G}$ be such that $e_\chi \delta$ is non-zero. Then the $\chi$-eigenspace of the Selmer group $S^\chi$ is one-dimensional over $\mathcal{O}_{\mathfrak{p}}$.

Let $\lambda'$ be a prime of $H$ above $\lambda$. The self-duality of $Y_p$ given by

$$Y_p \simeq Y'_p,$$

(see [5] section 8) for more details) and local Tate duality gives a perfect pairing

$$\langle \cdot , \cdot \rangle_{\lambda'} : H^1(H^\text{ur}_{\lambda'}/H_{\lambda'/p},Y_p) \times H^1(H^\text{ur}_{\lambda'}Y_p) \longrightarrow \mathbb{Z}/p,$$

and $\mathcal{O}_{\mathfrak{p}}$-linear isomorphisms

$$\{H^1(H^\text{ur}_{\lambda'}/Y_p)\}^\text{dual} \simeq H^1(H^\text{ur}_{\lambda'}/Y_p) \simeq Y_p(Y_{\lambda'}), \quad (3)$$

where the last isomorphism is obtained by evaluation at the Frobenius element generating $\text{Gal}(H^\text{ur}_{\lambda'}/H_{\lambda'})$. Recall that the Selmer group $S \subseteq H^1(H,Y_p)$ consists of the cohomology classes whose localizations lie in $H^1(H^\text{ur}/H_{\nu},Y_p)$ for $\nu$ not dividing $Np$ and in $H^1_f(H_{\nu},Y_p)$ for $\nu$ dividing $p$. Here, $H^1_f(H_{\nu},Y_p)$ is
the finite part of $H^1(H_v, Y_p)$ as in [4, part 1]. We denote by

$$\text{res}_\lambda : H^1(H, Y_p) \longrightarrow \oplus_{\lambda' | \lambda} H^1(H_{\lambda'}, Y_p)$$

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

$$\text{res}_\lambda : S \longrightarrow \oplus_{\lambda' | \lambda} Y_p(H_{\lambda'}).$$

Taking the $(\mathbb{Z}/p)$-linear dual of the previous map and using isomorphism (3), we obtain a homomorphism

$$\psi_\ell : \oplus_{\lambda' | \lambda} H^1(H_{\lambda'}^{\text{ur}}, Y_p) \longrightarrow S^\text{dual}.$$ 

Let $X_\ell$ be the image of $\psi_\ell$ in $S^\text{dual}$. We aim to describe $S^\text{dual}$ by studying the $X_\ell$’s.

6 Generating the dual of the Selmer group

**Lemma 6.1.** For a module $M$, we have

$$H^1(\text{Aut}(M), M) = 0.$$ 

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

$$g = 2I \in \text{Aut}(M) \subseteq \text{Center(\text{Aut}(M))},$$

we have that $g - I = I$ is the zero map on $H^1(\text{Aut}(M), M)$ and the result follows.
**Proposition 6.2.** There exists a prime $q$ such that $q$ is a Kolyvagin prime, and such that

$$\text{res}_p e\delta \neq 0,$$

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

**Proof.** For the purpose of this proof, we denote the cocycle $e\delta$ by $c_1$ and the Galois group $G(L/H)$ by $G$. By Proposition (5.4), $c_1$ belongs to $S\varnothing$. The restriction map

$$r : H^1(H, Y_p) \rightarrow H^1(L, Y_p)^G = \text{Hom}_G(L, Y_p)$$

is injective. Indeed, Proposition (3.2) and Proposition (6.1) imply that

$$\text{Ker}(r) = H^1(H(Y_p)/H, Y_p) = 0.$$ 

Consider the evaluation pairing

$$r(S\varnothing) \times \text{Gal}(\overline{Q}/L) \rightarrow Y_p(L)$$

and let $\text{Gal}_{S}(\overline{Q}/L)$ be the annihilator of $r(S\varnothing)$. Let $L^S$ be the extension of $L$ fixed by $\text{Gal}_{S}(\overline{Q}/L)$ 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

$$r(S\varnothing) \hookrightarrow \text{Hom}_G(G_S, Y_p(L)).$$

We denote by $s$ the image of $r(c_1)$ in $\text{Hom}_G(G_S, Y_p(L))$.

If $s(G^+_S) = 0$, then as $s$ belongs to $S^\perp$, we have

$$s : G^-_S \rightarrow Y_p(L)^\perp,$$
where $Y_p(L)^\pm$ are the $\pm$ eigenspaces of $Y_p$ with respect to the action of $\tau$. On the one hand, the eigenspace $Y_p^\pm$ is of rank one over $O_{F_p}/p$. On the other hand, by Proposition (3.2) and Assumption (2),

$$G = G(L/H) \cong \text{GL}_2(O_{F_p}/p).$$

Hence, $Y_p(L)^\pm$ 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 $S^\times$ as $c_1$ is not divisible by $p$ in $S^\times$. As a consequence, we have that $s(G_S^+) \neq 0$, where

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

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 implies the existence of $q$ in $\mathbb{Q}$ such that

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

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

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

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

$\square$
Consider the following extensions

\[
\begin{align*}
I_0 & = F(\text{red}(y_1, \wp))^{\text{Gal}} \\
I_1 & = F(D_q \text{red}(y_q, \wp))^{\text{Gal}}
\end{align*}
\]

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

\[
V_0 = \text{Gal}(I_0/F), \quad V_1 = \text{Gal}(I_1/F), \quad \text{and} \quad V = \text{Gal}(I_0I_1/F).
\]

We have \( V_0 \simeq V_1 \simeq Y_p \). Let

\[
\begin{align*}
I_0^\varpi & = F(e^{\varpi \text{red}(y_1, \wp)})^{\text{Gal}} \\
I_1^\varpi & = F(e^{\varpi D_q \text{red}(y_q, \wp)})^{\text{Gal}}
\end{align*}
\]

We denote by \( V_0^\varpi \) and \( V_1^\varpi \) their respective Galois groups over \( F \). We will show that

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

**Proposition 6.3.** The extensions \( I_0^\varpi \) and \( I_1^\varpi \) are linearly disjoint over \( F \).

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

\[
H^1(H_q, Y_p)^{\text{Gal}(F/H_q)} \xrightarrow{(\cdot)} H^1(F, Y_p)^{\text{Gal}(F/H_q)}
\]
is injective. Indeed, combining Proposition (3.2) with Proposition (6.1) that implies that

\[ H^1(K(Y_p)/K, Y_p) = 0, \]

we obtain that

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

Furthermore, cocycles of \( H^1(F,Y_p)^{\text{Gal}(F/H_q)} \) factor through

\[ H^1(I_{01}/F,Y_p)^{\text{Gal}(F/H_q)} = \text{Hom}_{\text{Gal}(F/H_q)}(I_{01}/F,Y_p). \]

Consider the extension \( I^\tau \cap I_1^\tau \) of \( F \). It is a \( \text{Gal}(F/H_q) \)-submodule of \( Y_p \). The hypothesis \( \text{res}_{\beta'}e_{\chi}^{\text{red}}(y_{1,\ell}) \neq 0 \) implies that

\[ \text{res}_{\beta'}e_{\chi}^{\text{red}}(D_q y_{q,\ell}) \neq 0 \]

by [5, proposition 10.2(4)]. On the one hand, since \( \text{res}_{\beta'}e_{\chi}^{\text{red}}(D_q y_{q,\ell}) \) is ramified, \( e_{\chi}^{\text{red}}(y_{1,\ell}) \) does not belong to \( S^\tau \). On the other hand, \( e_{\chi}^{\text{red}}(y_{1,\ell}) \neq 0 \) belongs to \( S^\tau \) by Proposition (3.4). Therefore \( I^\tau_0 \cap I_1^\tau = 0 \) since \( Y_p \) is a simple \( \text{Gal}(F/H_q) \)-module. Note that the cocycles \( c_1 \) and \( c_2 \) cannot be linearly dependent either since one of them belongs to \( S^\tau \) while the other one does not.

For a subset \( U \subseteq V \), we denote by

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

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

\[ \text{Frob}_{\ell}(H(Y_p)/\mathbb{Q}) = \text{res}_{\ell}|_{H(Y_p)} \text{Frob}_{\ell}(I_{01}/\mathbb{Q}) = \tau \]

21
since \(a \in U\). In fact, it satisfies
\[
\text{Frob}_\ell(H_q(Y_p)/\mathbb{Q}) = \text{res}_{|H_q(Y_p)}\text{Frob}_\ell(I_{01}/\mathbb{Q}) = \tau.
\]
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
\[
\text{Frob}_\ell(H_q/H) = \tau^{|D(H/\mathbb{Q})|} = \tau^2 = \text{Id},
\]
where \(|D(H/\mathbb{Q})|\) is the order of the decomposition group \(D(H/\mathbb{Q})\), also the order of the residue extension. Similarly, a prime above \(\ell\) in \(H_q\) splits completely in \(H_q(Y_p)\); it lies in the kernel of the Artin map because of the Frobenius condition
\[
\text{Frob}_\ell(H_q(Y_p)/H_q) = \tau^{|D(H_q/\mathbb{Q})|} = \tau^2 = \text{Id}.
\]

**Proposition 6.4.** Assume \(U^+\) generates \(V^+\). Then \(\{X_\ell\}_{\ell \in L(U)}\) generates \(S^{\text{dual}}\).

**Proof.** The proof consists of the following steps:

1. An element \(s\) of \(S\) can be identified with an element \(h\) of \(\text{Hom}_G(F, Y_p)\).
2. To show the statement of the theorem, it is enough to show that \(\text{res}_\lambda(s) = 0\) for all \(\ell \in L(U)\) implies \(s = 0\).
3. The assumption \(\text{res}_\lambda(s) = 0\) for all \(\ell \in L(U)\) implies that \(h\) vanishes on \(U^+\).
4. The assumption \(U^+\) generates \(V^+\) implies \(h = s = 0\).

1. Let \(s\) be an element of \(S\). For the purpose of this proof, we denote
\[
G = \text{Gal}(H(Y_p)/H) \simeq \text{GL}_2(\mathcal{O}_p/p).
\]
We denote by $h$ the image of $s$ by restriction in

$$H^1(F, Y_p)^G \subset \text{Hom}_G(F, Y_p).$$

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

$$H^1(H, Y_p) \xrightarrow{(r_1)} H^1(H(Y_p), Y_p)^G \xrightarrow{(r_2)} H^1(F, Y_p)^G.$$

Combining Proposition (3.2) and (6.1) we obtain that

$$\text{Ker}(r_1) = H^1(H(Y_p)/H, Y_p) = 0.$$

Since $Y_p(H_q) = Y_p(H)$ by Proposition (3.2), we have

$$\text{Gal}(H_q(Y_p)/H(Y_p)) \simeq \text{Gal}(H_q/H) \simeq \mathbb{Z}/(q + 1)\mathbb{Z}.$$

Note that $q + 1$ is not a power of $p$. Indeed, if $q + 1 = p^\alpha$ for some $\alpha$, then $p^\alpha - 1$ divides $q$ implying that $p - 1$ divides the prime number $q$, a contradiction. Since $q + 1$ is not a power of $p$, $Y_p$ has no $G$-submodules of order $q + 1$. Hence,

$$\text{Ker}(r_2) = \text{Hom}_G(F/H(Y_p), Y_p) \simeq \text{Hom}_G(H_q/H, Y_p) = 0.$$ 

2. Local Tate duality identifies $\bigoplus_{\lambda} H^1(H^{ar}_\lambda, Y_p)$ with $\bigoplus_{\lambda} Y_p(H_{\lambda'})^{\text{dual}}$. So if we show that

$$\{\text{res}_\lambda\}_{\ell \in L(U)} : \mathcal{S} \rightarrow \bigoplus_{\lambda \in \Lambda} Y_p(H_{\lambda'})_{\ell \in L(U)}$$

23
is injective, then the induced map between the duals
\[
\left\{ \oplus_{\lambda'} \lambda Y_p(H_{\lambda'}) \right\}_{\ell \in L(U)}^{dual} = \left\{ \oplus_{\lambda'} \lambda H^1(H_{\lambda'}^{ur}, Y_p) \right\}_{\ell \in L(U)} \rightarrow S^{dual}
\]
would be surjective. Hence, it is enough to show that \( \text{res}_\lambda(s) = 0 \) for all \( \ell \in L(U) \) implies \( s = 0 \).

3. Consider \( I_{01} \), the minimal Galois extension of \( Q \) 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 \( x|_{l_0} \) belongs to \( U \). By Cebotarev’s density theorem, there exists \( \ell \in L(U) \) such that \( \text{Frob}_\ell(I_{01}/Q) = [\tau x] \). The hypothesis \( \text{res}_\lambda(s) = 0 \) implies that \( h(\text{Frob}_\lambda(I_{01}/F)) = 0 \) for \( \lambda'' \) above \( \ell \) in \( F \) since \( h(\text{Frob}_\lambda(I_{01}/F)) \) is a generator of the local extension of \( \text{Gal}(I_{01}/F) \) at \( \lambda'' \). In fact,

\[
\text{Frob}_\lambda(I_{01}/F) = (\tau x)^{|D(F/Q)|} = (\tau x)^2 = x^2 = 2x^+,
\]

where \( |D(F/Q)| \) is the order of the decomposition group \( D(F/Q) \), and is also the order of the residue extension and \( x^+ = \frac{1}{2} x^2 x \). Therefore, \( h(x^+) = 0 \) for all \( x \in \text{Gal}(I_{01}/F) \) such that \( x|_{l_0} \) 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 \( Y_p^- \), the minus eigenspace of \( Y_p \) for the action of \( \tau \) which is a free \( \mathcal{O}_\mathcal{P}/p \)-module of rank 1. In particular, it cannot be a proper non-trivial \( G \)-submodule of \( Y_p \). Therefore, \( h = 0 \) which implies \( s = 0 \).

\[ \square \]

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

**Proposition 6.5.** There is an element \( \sigma_0 \) in \( \text{Gal}(H_q/K) \) such that

\[
\tau e_{\mathcal{X}} y_{q,q'} = e_{\mathcal{X}}(\sigma_0)e_{\mathcal{X}} y_{q,q'}.
\]

24
where $-\varepsilon$ is the sign of the functional equation of $L(f,s)$.

Proof. [5, proposition 6.2] that uses a result in [2] states that

$$\tau y_{q,\rho} = \varepsilon \sigma_0 y_{q,\rho}$$

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

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

we have

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

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 (4) yields

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

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

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

$$\tau v_1 \tau(e\chi D_q y_{q,\rho}) = -\tau v_1 D_q \tau(e\chi y_{q,\rho}) = -\varepsilon \chi(\sigma_0)\tau v_1(e\chi D_q y_{q,\rho}).$$
When $\chi = \overline{\chi}$, for $(x, y)$ in $V_0^\chi V_1^\chi$,

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

In this case, we define

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

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

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

In this case, we define

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

In both cases, Proposition (6.3) and Congruence (1) imply that $U^+$ generates

$$V^+ \simeq V_0^+ \times V_1^+ \simeq \mathcal{O}_p/p \times \mathcal{O}_p/p \simeq Y_p.$$  

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

**Proposition 6.6.** The elements

$$\text{res}_\lambda e\overline{\chi}P(\ell) \text{ and } \text{res}_\lambda e\overline{\chi}P(\ell q)$$

*generate* $\oplus_{\lambda' | \lambda} H^1(H^\text{ar}_{\lambda'}, Y_p)^\chi$.

26
Proof. We have

$$\bigoplus_{\lambda' | \lambda} H^1(H_{\lambda'}^{ur}, Y_p)^{\mathfrak{F}} \simeq \bigoplus_{\lambda' | \lambda} Y_p(H_{\lambda'})^{\mathfrak{F}}$$

since the former is isomorphic to its dual as in [5, section 10]. The module $\bigoplus_{\lambda' | \lambda} Y_p(H_{\lambda'})^{\mathfrak{F}}$ is of dimension 2 over $\mathcal{O}_\rho/p$, hence, so is $\bigoplus_{\lambda' | \lambda} H^1(H_{\lambda'}^{ur}, Y_p)^{\mathfrak{F}}$. The Frobenius condition on $\ell$ implies that

$$\text{res}_\lambda e_{\mathcal{F}\text{red}}(y_1, \mathfrak{p}) \text{ and } \text{res}_\lambda e_{\mathcal{D}\text{red}}(y_q, \mathfrak{p})$$

are linearly independent over $\bigoplus_{\lambda' | \lambda} Y_p(H_{\lambda'})$. Indeed, if they were linearly dependent then, in the case $\chi = \overline{\chi}$,

$$(\text{res}_\lambda e_{\mathcal{F}\text{red}}(y_1, \mathfrak{p}))^{(\tau x)^2} - \text{res}_\lambda e_{\mathcal{F}\text{red}}(y_1, \mathfrak{p})$$

and

$$(\text{res}_\lambda e_{\mathcal{D}\text{red}}(y_q, \mathfrak{p}))^{(\tau y)^2} - \text{res}_\lambda e_{\mathcal{D}\text{red}}(y_q, \mathfrak{p})$$

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

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

generate $Y_p$, which yields a contradiction as $(\tau x)^2$ acts on the element $\text{res}_\lambda e_{\mathcal{F}\text{red}}(y_1, \mathfrak{p})$ generating the local extension of $I_0^{\mathfrak{F}}$ over $F$ by

$$(\text{res}_\lambda e_{\mathcal{F}\text{red}}(y_1, \mathfrak{p}))^{(\tau x)^2} - \text{res}_\lambda e_{\mathcal{F}\text{red}}(y_1, \mathfrak{p})$$

and $(\tau y)^2$ acts on the element $\text{res}_\lambda e_{\mathcal{D}\text{red}}(y_q, \mathfrak{p})$ generating the local extension of $I_1^{\mathfrak{F}}$ over $F$ by

$$\text{res}_\lambda e_{\mathcal{D}\text{red}}(y_q, \mathfrak{p})^{(\tau y)^2} - \text{res}_\lambda e_{\mathcal{D}\text{red}}(y_q, \mathfrak{p})$$
Similarly, in the case $\chi \neq \overline{\chi}$,

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

and

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

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

$$\text{Frob}_\ell(I_0^L/F) = x^y = (\tau_x)(\tau_y) \quad \text{and} \quad \text{Frob}_\ell(I_q^L/F) = z^w = (\tau_z)(\tau_w)$$

generate $Y_\rho$, which yields a contradiction.

In [5, section 9], Nekovar develops the localization of the so-called Kolyvagin corestriction which coincides with our definition of $P(n)$. Therefore, we can use the formula in [5, proposition 10.2(4)] with parameter $M_1 = 0$ which establishes an isomorphism relating

$$c_1(\ell)P(n)_{\lambda'} \quad \text{and} \quad c_2(\ell)P\left(\frac{n}{\ell}\right)_{\lambda'},$$

where $c_1(\ell)$ and $c_2(\ell)$ only depend on $\ell$. Note that this uses Proposition (2.2). Hence, if $\text{res}_\lambda e_{\overline{\chi}}P(q)$ and $\text{res}_\lambda e_{\overline{\chi}}P(\ell)$ were linearly dependent then

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

would be so as well.

7 Bounding the size of the dual of the Selmer group

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

28
Proposition 7.1. We have
\[ \sum_{\lambda' \mid \ell} \langle s_{\lambda'}, \text{res}_{\lambda'} P(n) \rangle_{\lambda'} = 0. \]

Proof. The proof follows [5, proposition 11.2(2)] where both the reciprocity law and the ramification properties of \( P(n) \) in Proposition (3.4) are used.

Proposition 7.2. The element \( \psi_{\ell}(\text{res}_{\lambda} e_{\chi} P(\ell q)) \) generates \( X^X_\ell \) over \( O_{P}/p \) for \( \ell \in L(U) \).

Proof. The image of \( \text{res}_{\lambda} e_{\chi} P(\ell) \) by the map
\[ \psi_{\ell} : \bigoplus_{\lambda' \mid \lambda} H^1(H_{\lambda'}, Y_p)^X \longrightarrow X^X_\ell \]
is the homomorphism from \( S^X \) to \( \mathbb{Z}/p \) given by:
\[ e_{\chi} s_{\lambda'} \longrightarrow \sum_{\lambda' \mid \lambda} \langle e_{\chi} s_{\lambda'}, e_{\chi} P(\ell) \rangle_{\lambda'}. \]

Proposition 7.1 implies that
\[ \sum_{\lambda' \mid \lambda} \langle e_{\chi} s_{\lambda'}, e_{\chi} P(\ell) \rangle_{\lambda'} = 0. \]

Hence, the image by \( \psi_{\ell} \) of \( \text{res}_{\lambda} e_{\chi} P(\ell) \), one of the two generators of \( \bigoplus_{\lambda' \mid \lambda} H^1(H_{\lambda'}, Y_p)^X \) by Proposition (6.6), is trivial.

Proposition 7.3. The modules \( X^X_\ell \) that are non-zero are all equal for \( \ell \in L(U) \).

Proof. Proposition (7.1) implies that
\[ \sum_{\lambda' \mid \lambda} \langle e_{\chi} s_{\lambda'}, e_{\chi} P(\ell q) \rangle_{\lambda'} + \sum_{\beta' \mid \beta} \langle e_{\chi} s_{\beta'}, e_{\chi} P(\ell q) \rangle_{\beta'} = 0. \]

Hence,
\[ p^h \psi_{\ell}(\text{res}_{\lambda} e_{\chi} P(\ell q)) + p^h \psi_{q}(\text{res}_{\beta} e_{\chi} P(\ell q)) = 0. \]
If $p^h \psi_\ell(\text{res}_\lambda e_\mathcal{P}(\ell q)) = 0$, then by Proposition (7.2), $X^\mathcal{T}_\ell = 0$. Otherwise, since

$$\psi_\ell(\text{res}_\lambda e_\mathcal{P}(\ell q))$$

generates $X^\mathcal{T}_\ell$ over $\mathcal{O}_\rho/p$, we have that

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

is non-zero. Therefore, the non-trivial element $\psi_q(\text{res}_\beta e_\mathcal{P}(\ell q))$ generates the one dimensional module $X^\mathcal{T}_q$ over $\mathcal{O}_\rho/p$ and $X^\mathcal{T}_\ell = X^\mathcal{T}_q$. \hfill \Box

**Theorem 7.4.** Assume $p$ is such that $\text{Gal}(\mathbb{Q}(Y_p)/\mathbb{Q}) \simeq \text{GL}_2(\mathcal{O}_\rho/p)$. Let $\chi$ be a complex character of $G$ such that $e_\chi^{\text{red}}(y_1, \mathcal{P})$ is not divisible by $p$. Then, $S^\chi$ is of dimension 1 over $\mathcal{O}_\rho/p$.

**Proof.** By Proposition (6.4), the set $\{X^\mathcal{T}_\ell\}$ generates $S^{\text{dual}\chi}$ as $\ell$ ranges over $L(U)$. Hence, the set $\{X^\mathcal{T}_\ell\}$ generates $S^{\text{dual}\chi}$ as $\ell$ ranges over $L(U)$, where, by Proposition (7.2), the modules $X^\mathcal{T}_\ell$ that are non-zero are one-dimensional vector spaces over $\mathcal{O}_\rho/p$ and are all equal. Hence, $\dim(S^\chi) \leq 1$. Also, $e_\chi^{\text{red}}(y_1, \mathcal{P})$ belongs to $S^\chi$ by Proposition (3.4) and is not divisible by $p$ in $S^\chi$. Indeed, this follows from the hypothesis on $e_\chi^{\text{red}}(y_1, \mathcal{P})$ and Proposition (6.5) where $\chi(\sigma_0)$ is a root of unity since $\text{Gal}(H/K)$ is a finite group. This implies that $\dim(S^\chi) \geq 1$. Therefore,

$$\dim(S^\chi) = \dim(S^{\text{dual}\chi}) = 1.$$  \hfill \Box

**Remark 7.5.** Because the $p$-adic Abel-Jacobi map factors through the Selmer group

$$\Phi^\chi : \text{CH}^r(W_2r^{-2}/H)^0_0 \otimes \mathcal{O}_\rho/p \mathcal{O}_\rho \rightarrow S^\chi,$$
Theorem (7.4) implies that \( \dim_{\mathcal{O}_p/p}(\text{Im}(\Phi^X)) = 1. \)

**Remark 7.6.** In Kolyvagin’s argument for elliptic curves \( E \) and certain imaginary quadratic fields \( K \), the non-triviality of the Heegner point \( y_K \) in \( E(K)/pE(K) \) for acceptable 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 \( H^1(H_m,A) \).

**References**

[1] Massimo Bertolini and Henri Darmon. Kolyvagin’s descent and Mordell-Weil groups over ring class fields. *J. Reine Angew. Math.*, 412:63–74, 1990.

[2] Benedict H. Gross. Heegner points on \( X_0(N) \). In *Modular forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., pages 87–105. Horwood, Chichester, 1984.

[3] Uwe Jannsen. Continuous étale cohomology. *Math. Ann.*, 280(2):207–245, 1988.

[4] Barry Mazur and Karl Rubin. *Kolyvagin Systems*, volume 168. Amer. Math. Soc., 2004.

[5] Jan Nekovář. Kolyvagin’s method for Chow groups of Kuga-Sato varieties. *Invent. Math.*, 107(1):99–125, 1992.