Kolyvagin's method for Chow groups of Kuga–Sato varieties

by

Jan Nekovář

Max–Planck–Institut
für Mathematik
Gottfried–Claren–Str. 26
5300 Bonn 3
BRD

Czechoslovak Academy of Science
Math. Institute
Žitná 25
115 67 Praha 1
ČSFR

MPI/90-78

A.5 Zum Gradienten

Wir zeigen: Sei $U \subseteq \mathbf{R}^n$ offen und zu je zwei Punkten P und Q gebe es einen Weg $c : [a, b] \to U$ mit $c(a) = P$ und $c(b) = Q$. Weiter seien $f_1, f_2 : U \to \mathbf{R}$ zwei Funktionen mit $\operatorname{grad} f_1 = \operatorname{grad} f_2$. Dann gibt es ein $k \in \mathbf{R}$ mit $f_1 = f_2 + k$.

Beweis. Wir definieren eine Funktion $h : U \to \mathbf{R}$ durch $h := f_1 - f_2$. Dann gilt wegen der Voraussetzung $\operatorname{grad} h = 0$. Zu zeigen ist, das $h \equiv k$ für ein $k \in \mathbf{R}$ gilt. Dazu betrachten wir zwei beliebige Punkte $P, Q \in U$ und einen Weg $c : [a, b] \to U$ in U zwischen P und Q. Die Kettenregel liefert wieder

$$(h \circ c)'(t) = \langle \operatorname{grad} h(c(t)), c'(t) \rangle .$$

Wegen $\operatorname{grad} h = 0$ ist nun $\langle \operatorname{grad} h(c(t)), c'(t) \rangle = 0$, also $h \circ c$ konstant. Daraus folgt, daß $h(P) = h(c(a)) = h(c(b)) = h(Q)$ gilt. Also ist für beliebige Punkte $P, Q \in U$ gezeigt, daß $h(P) = h(Q)$ gilt, also ist h konstant.

A.6 Stammfunktionen zu Vektorfeldern

Es sei U eine Teilmenge des $\mathbf{R}^n$ und $F : U \to \mathbf{R}^n$ ein gegebenes Vektorfeld. Eine Funktion $\phi : U \to \mathbf{R}$ mit $\operatorname{grad} \phi = F$ heißt *Stammfunktion* zu F.

Uns interessiert nun, wann es solch eine Stammfunktion gibt. Dazu betrachten wir zunächst folgenden Spezialfall:

- Es sei $n = 2$ und F gegeben durch die Funktionen $f, g : U \to \mathbf{R}$. Nehmen wir an, es gebe eine Funktion ϕ mit $\operatorname{grad} \phi = F$, also $F = \left(\frac{\partial \phi}{\partial x_1}, \frac{\partial \phi}{\partial x_2}\right)$. Dies bedeutet, daß gerade $f = \frac{\partial \phi}{\partial x_1}$ und $g = \frac{\partial \phi}{\partial x_2}$ ist. Dann ist aber $\frac{\partial f}{\partial x_2} = \frac{\partial^2 \phi}{\partial x_1 \partial x_2}$ und $\frac{\partial g}{\partial x_1} = \frac{\partial^2 \phi}{\partial x_2 \partial x_1}$. Wenn nun ϕ von der Klasse C^1 ist, dann ist $\frac{\partial^2 \phi}{\partial x_1 \partial x_2} = \frac{\partial^2 \phi}{\partial x_2 \partial x_1}$, also gilt dann $\frac{\partial f}{\partial x_2} = \frac{\partial g}{\partial x_1}$.

Analog zeigt man allgemein: Wenn es ein $\phi \in C^1$ mit $F = \operatorname{grad} \phi$ gibt, dann gilt $\frac{\partial f_j}{\partial x_i} = \frac{\partial f_i}{\partial x_j}$ für alle i, j.

Wir können uns nun fragen: Wenn umgekehrt $\frac{\partial f_j}{\partial x_i} = \frac{\partial f_i}{\partial x_j}$ gilt, gibt es dann eine Stammfunktion ?

Die Antwort liefert der folgende

Satz. *Es sei U ein Rechteck im $\mathbf{R}^n$, d.h ein kartesisches Produkt von offenen Intervallen in $\mathbf{R}$. Weiter sei* $F = \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} : U \to \mathbf{R}^n$ *mit $f_i : U \to \mathbf{R}$ eine differenzierbare Funktion mit* $\frac{\partial f_j}{\partial x_i} = \frac{\partial f_i}{\partial x_j}$. *Dann gibt es eine Stammfunktion $\phi : U \to \mathbf{R}$ mit $F = \operatorname{grad} \phi$.*

Beweis. Wir führen den Beweis für den Fall $n = 2$ mit $f_1 = f$ und $f_2 = g$. Im allgemeinen Fall schließt man ganz analog.

Kolyvagin's method for Chow groups of Kuga-Sato varieties

Jan Nekovář

MPI für Mathematik, Gottfried-Claren-Str. 26, 5300 Bonn 3, BRD
Czechoslovak Academy of Science, Math. Institute, Žitná 25, 115 67 Praha 1, ČSFR

1. Introduction

In a remarkable series of papers [14-17], V.A.Kolyvagin introduced a new descent method based on properties of "Euler systems", which enabled him to prove, among other things, the finiteness of the Tate-Šafarevič groups of certain elliptic curves.

In the present work we apply the method of Euler systems to modular forms of higher (even) weight, obtaining some information about algebraic cycles on the corresponding Kuga-Sato varieties

More precisely, one may associate to every newform $f \in S_{2r}^{\text{new}}(\Gamma_0(N))$ with rational coefficients a motive $M = M(f)$ of rank 2 over $\mathbf{Q}$ (U.Jannsen, A.J.Scholl).Its l-adic realization M_l is a two dimensional representation of $G(\overline{\mathbf{Q}}/\mathbf{Q})$ which appears as a factor of the cohomology group $H_{\text{et}}^{2r-1}(Y \otimes \overline{\mathbf{Q}}, \mathbf{Q}_l)$, where Y is a suitable smooth compactification of the $(2r-2)$-fold fibre product of the universal elliptic curve (with the full level N structure) over the modular curve $X(N)$. The l-adic Abel-Jacobi map (over any extension K of $\mathbf{Q}$)

$$CH^r(Y/K)_0 \longrightarrow H^1_{\text{cont}}(K, H_{\text{et}}^{2r-1}(Y \otimes \overline{\mathbf{Q}}, \mathbf{Q}_l)(r))$$

induces a map

$$\Phi : CH^r(Y/K)_0 \longrightarrow H^1_{\text{cont}}(K, M_l(r))$$

(here $CH^r(Y/K)_0$ denotes the group of homologically trivial cycles on Y defined over K, modulo rational equivalence).

If K is an imaginary quadratic field in which all primes dividing N split, we may define a Heegner cycle

$$y \in CH^r(Y/K)_0 \otimes \mathbf{Q}_l \quad .$$

Its image $y_0 = \Phi(y)$ lies in the $(-\varepsilon)$-eigenspace under the action of the non-trivial element of $G(K/\mathbf{Q})$, where $\varepsilon = \pm 1$ is the sign in the functional equation of the L-series $L(f, s)$.

Theorem. Suppose that l does not divide $2(2r-2)!N\varphi(N)$. If y_0 is non-zero, then

$$(\text{Im}(\Phi))^{\varepsilon} \otimes \mathbf{Q}_l = 0, \quad (\text{Im}(\Phi))^{-\varepsilon} \otimes \mathbf{Q}_l = \mathbf{Q}_l . y_0 \quad .$$

and an analogue of the l-primary part of the Tate-Šafarevič group is finite.

A similar statement is proved for newforms with not necessarily rational coefficients. This result gives a new piece of evidence in favour of Bloch-Beilinson's conjectures on the properties of motivic L-series at the centre of the critical strip (see [12]): the conjectures predict that the dimension of $\mathrm{Im}(\Phi)$ is equal to the order of vanishing of the L-function of the modular form f over the field K at the centre of the critical strip. The results of Gross-Zagier [10] and Brylinski [3] suggest that in our situation the order of vanishing is equal to one precisely when the "f-component" of the Heegner cycle y has non-trivial height. There are some grounds to the belief that the latter occurs if and only if y_0 is non-zero (cf. the discussion at the end of sec.13).

The proof follows rather closely the presentation of B.Gross in [9]. Some modifications are necessary, however, as the whole construction is to be carried out in terms of the Galois representation $M_l(r)$ alone. This is the reason why Kolyvagin's corestriction and its properties under localization are treated perhaps at greater length than necessary. The calculations made in sec.9 confirm that the construction of "derived Euler systems" works solely in terms of the associated "Tate module", as suggested in [21].

This work has been done in the Max-Planck-Institute für Mathematik. I would like to express my gratitude for its support and hospitality. My thanks are also due to U.Jannsen, N.Schappacher and C.Schoen for helpful discussions.

2. Kuga-Sato varieties

In [26], A.J.Scholl constructs motives attached to holomorphic cusp forms on congruence subgroups. In this section we briefly recall his results.

Fix integers $N \geq 3$, $w \geq 1$. Let M_N be the affine modular curve over $\mathbf{Q}$ parametrising elliptic curves with full level N structure and let $j : M_N \hookrightarrow \overline{M}_N$ be its smooth compactification classifying generalized elliptic curves.

Denote by $\pi : X_N \longrightarrow M_N$ the universal elliptic curve and by $\overline{\pi} : \overline{X}_N \longrightarrow \overline{M}_N$ the universal generalized elliptic curve, which is smooth and proper.

Consider the w-fold fibre product $\overline{\pi}_w : \overline{X}_N^w \longrightarrow \overline{M}_N$ of $\overline{X}_N$ with itself over $\overline{M}_N$ and put $X_N^w = \overline{\pi}^{-1}(M_N)$.

The level N structure on $\overline{X}_N$ gives a homomorphism of group schemes over $\overline{M}_N$

$$(\mathbf{Z}/N)^2 \times \overline{M}_N \hookrightarrow \overline{X}_N^* \quad ,$$

where $\overline{X}_N^*$ is the Néron model of X_N over $\overline{M}_N$, namely the open subscheme of $\overline{X}_N$ on which $\overline{\pi}$ is smooth. Therefore $(\mathbf{Z}/N)^2$ acts by translations on $\overline{X}_N$. Multiplication by -1 in the fibers defines an action of the semidirect product $(\mathbf{Z}/N)^2 \rtimes \mu_2$ on $\overline{X}_N$.

The symmetric group Σ_w on w letters acts on $\overline{X}_N^*$ by permuting the factors. Hence the semidirect product

$$\Gamma_w := ((\mathbf{Z}/N)^2 \rtimes \mu_2)^w \rtimes \Sigma_w$$

acts on $\overline{X}_N^*$ by fibre-preserving automorphisms.

Let $\varepsilon : \Gamma_w \longrightarrow \{\pm 1\}$ be the homomorphism which is trivial on $(\mathbf{Z}/N)^{2w}$, is the product map on μ_2^w and is the sign character on Σ_w. Let $\Pi_\varepsilon \in \mathbf{Z}[1/(2N.w!)][\Gamma_w]$ be the projector associated to ε.

Consider the canonical desingularization $\overline{\overline{X}}_N^w$ described in [5] and [26]. By its canonical nature the action of Γ_w extends to $\overline{\overline{X}}_N^w$. Fix a prime number p not dividing $2N.w!$. One of the main results of [26] is the description of the parabolic cohomology group

$$H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*\mathrm{Sym}^w(R^1\pi_*\mathbf{Z}/p^M))$$

in terms of the compactification $\overline{\overline{X}}_N^w$:

Proposition 2.1.[26,1.2.1] $H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*\mathrm{Sym}^w(R^1\pi_*\mathbf{Z}/p^M)) = \Pi_\epsilon H^*_{\mathrm{et}}(\overline{\overline{X}}_N^w \otimes \overline{\mathbf{Q}}, \mathbf{Z}/p^M)$.

Strictly speaking, the theorem stated in [26] deals only with $\mathbf{Q}_p$–coefficients, but its proof is valid in our situation as well. In fact, it will be crucial to consider cohomology with *finite* coefficients.

Lemma 2.2. Put $\mathcal{F}_M := \mathrm{Sym}^w(R^1\pi_*\mathbf{Z}/p^M)$ and let $\mathcal{F} := \varprojlim \mathcal{F}_M$ be the corresponding p–adic sheaf. Then the parabolic cohomology group $H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*\mathcal{F})$ is torsion free and

$$H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*\mathcal{F}_M) = H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*\mathcal{F})/p^M$$

(always under the assumption $p \not| 2N.w!$).

Proof. As M_N is not complete, $H^2_{\mathrm{et}}(M_N \otimes \overline{\mathbf{Q}}, \mathcal{F}_M) = 0$. The monodromy of $\mathcal{F}$ at cusps is given by

$$\mathrm{Sym}^w \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$$

and its $SL(2, \mathbf{Z})$–conjugates. The condition on p then implies that $H^0_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, \mathcal{F}_M) = 0$. The only nonvanishing cohomology group $H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, \mathcal{F}_M)$ must be, therefore, a free $\mathbf{Z}/p^M$–module of rank r independent of M (by SGA $4\frac{1}{2}$, Rapport sur la formule des traces, Th.4.9). Thus $H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, \mathcal{F}) \simeq \mathbf{Z}_p^r$ and its subgroup $H^1_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*\mathcal{F})$ is torsion free. By Poincaré duality,

$$H^2_{\mathrm{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*\mathcal{F}) = H^2_c(M_N \otimes \overline{\mathbf{Q}}, \mathcal{F}) = H^0_{\mathrm{et}}(M_N \otimes \overline{\mathbf{Q}}, \mathcal{F}(1-w))^\vee = 0$$

(as $\mathcal{F}^\vee = \mathcal{F}(-w)$) and the second statement follows from [18,V.1.11].

We now recall the definition of Hecke operators (cf. [5],[26]). Fix a prime l not dividing N. Let $M_{N,l}$ be the modular curve over $\mathbf{Q}$ classifying elliptic curves E with a level N structure and a subgroup $C \subset E$ of order l. The fibre product $X_{N,l} = X_N \times_{M_N} M_{N,l}$ is the universal elliptic curve over $M_{N,l}$ equipped with a level N structure and a subgroup scheme C of order l. Write $X^w_{N,l}$ for the fibre product $X^w_N \times_{M_N} M_{N,l}$.

Let Q be the quotient of $X_{N,l}$ by C, with the level structure coming from that on $X_{N,l}$ and let Q^w be its w-fold fiber product over $M_{N,l}$. Consider the diagram :

$$\begin{array}{ccccccc}
X^w_N & \xleftarrow{\phi_1} & X^w_{N,l} & \xrightarrow{\psi} & Q^w & \xrightarrow{\phi_2} & X^w_N \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
M_N & \longleftarrow & M_{N,l} & = & M_{N,l} & \longrightarrow & M_N
\end{array}$$

in which the first and third squares are cartesian. The Hecke correspondence T_l on X_N^w, defined by

$$T_l = \phi_{1*}\psi^*\phi_2^* \qquad ,$$

induces endomorphisms T_l of $H^*_{\text{et}}(X_N^w \otimes \overline{\mathbf{Q}}, \mathbf{Z}/p^M)$. Define the Hecke correspondence – still to be denoted by T_l – on $\overline{\overline{X}}_N^w$ as the closure of the graph of T_l on $\overline{\overline{X}}_N^w \times \overline{\overline{X}}_N^w$.

In order to deal with forms of level $N = 1, 2$ one replaces N by $3N$ and then takes invariants under the kernel of the reduction map $GL(2, \mathbf{Z}/3N) \longrightarrow GL(2, \mathbf{Z}/N)$. This can be done as far as p does not divide $6(2r-2)!$.

3. Modular forms and Galois representations

The parabolic cohomology group $H^1_{\text{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*F)$ contains p–adic Galois representations associated to all cusp forms of weight $w+2$ on the full congruence subgroup $\Gamma(N)$. We shall be interested, however, only in forms on $\Gamma_0(N)$ with the trivial character. Let $w + 2 = 2r \geq 4$ be even and suppose that

$$f = \sum_{n=1}^{\infty} a_n q^n \quad \in \quad S_{2r}^{\text{new}}(\Gamma_0(N))$$

is a normalized ($a_1 = 1$) newform of weight $2r$ on $\Gamma_0(N)$. Let $B = \Gamma_0(N)/\Gamma(N)$ be the Borel subgroup of $GL(2, \mathbf{Z}/N)$ and put $\Pi_B := (\sharp B)^{-1} \sum_{b \in B} b \in \mathbf{Z}_p[B]$ (assuming that p does not divide $N\varphi(N)$).

Consider

$$J := \Pi_B H^1_{\text{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*F)(r) = H^1_{\text{et}}(\overline{M}_N \otimes \overline{\mathbf{Q}}, j_*F)(r)^B \quad .$$

Let $\mathbf{T} \subset \text{End}(J)$ be the subalgebra generated by the endomorphisms induced by all Hecke operators T_l for primes l not dividing N. The field $F = \mathbf{Q}(a_1, a_2, \ldots)$ generated by the coefficients of f is a totally real field of finite degree over $\mathbf{Q}$ and the coefficients themselves lie in its ring of integers $\mathcal{O}_F$. Write I for the kernel of the morphism $\mathbf{T} \longrightarrow \mathcal{O}_F$ sending T_l to a_l for all primes l not dividing N. Put $A := \{x \in J | I.x = 0\}$, $A_{\mathbf{Q}} := A \otimes \mathbf{Q}$.

Since f is a newform, there exists a $\mathbf{T}[G(\overline{\mathbf{Q}}/\mathbf{Q})]$–equivariant map $r : J \longrightarrow A$ such that $r|_A = p^m$ for some $m \geq 0$. Fix such a map.One may take $m = 0$ if there is no congruence $f \equiv f^*(\text{mod}\, \wp)$ between f and another Hecke eigenform f^* on $\Gamma_0(N)$ modulo any prime $\wp$ dividing p.

Proposition 3.1.

(1) A is a free $\mathcal{O}_F \otimes \mathbf{Z}_p$–module of rank 2 equipped with a continuous $\mathcal{O}_F$–linear action of the Galois group $G(\overline{\mathbf{Q}}/\mathbf{Q})$.

(2) There exists a $G(\overline{\mathbf{Q}}/\mathbf{Q})$–equivariant skew-symmetric pairing

$$[\ ,\ ] : A \times A \longrightarrow \mathbf{Z}_p(1)$$

satisfying

$$[\lambda x, y] = [x, \lambda y], \qquad x, y \in A, \quad \lambda \in \mathcal{O}_F \otimes \mathbf{Z}_p \qquad ,$$

such that the induced pairings

$$[\ ,\ ]_M : A/p^M A \times A/p^M A \longrightarrow \mu_{p^M}$$

are non-degenerate for all $M \geq 0$.

(3) If l is a prime not dividing Np, then the characteristic polynomial of the *arithmetic* Frobenius element $Fr(l)$ acting on A is equal to

$$\det(1 - xFr(l)|A) = 1 - a_l/l^{r-1}x + lx^2 \quad .$$

(4) If $l|N$, then $\det(1-xFr(l)|A_I) = 1-a_l/l^{r-1}x$ and $a_l = 0$ or $-\varepsilon_{f,l}l^{r-1}$, where $\varepsilon_{f,l} = \pm 1$ is the eigenvalue of the Atkin-Lehner involution W_l acting on f : $f|W_l = \varepsilon_{f,l}.f$.

Proof. (1) Since f is a newform, $A_{\mathbf{Q}}$ is a free $F \otimes \mathbf{Q}_p$−module of rank 2 and we know that A is torsion free. As all T_l are defined over $\mathbf{Q}$, the Galois action is $\mathcal{O}_F$−linear.
(2) Poincaré duality furnishes us with a skew-symmetric $G(\overline{\mathbf{Q}}/\mathbf{Q})$−equivariant pairing

$$[\ ,\ ]^{(P)} : J \times J \longrightarrow \mathbf{Z}_p(1)$$

satisfying $[T_l x, y]^{(P)} = [x, T_l y]^{(P)}$. As $[\ ,\ ]_{\mathbf{Q}}^{(P)}$ is nondegenerate on $J_{\mathbf{Q}}$ and the same is true for its restriction on $A_{\mathbf{Q}}$, the dual of A

$$A^* := \{x \in A_{\mathbf{Q}} | [x, A]^{(P)} \subseteq \mathbf{Z}_p(1)\}$$

has the form $A^* = u^{-1}A$ for some $u \in \mathcal{O}_F \otimes \mathbf{Z}_p$ and we put $[x, y] = [u^{-1}x, y]_{\mathbf{Q}}^{(P)}$.
(3) is the Eichler-Shimura relation (see [5,4.9]).
(4) is a combination of [4,Th.A] and [1,Th.3].

The Galois module A is a higher weight analogue of the Tate module of a modular elliptic curve and the pairing $[\ ,\ ]$ replaces the usual Weil pairing.

According to [26], $A_{\mathbf{Q}}$ is the p−adic realization of a certain motive $M = M(f)$ over $\mathbf{Q}$ with coefficients in F. In this language, Prop. 3.1 simply says that $M^\vee = M(-1)$ and

$$L(M^\vee, s) = L(f, s + r - 1) = \sum_{n=1}^{\infty} a_n n^{-s-r+1}$$

(including the Euler factors at primes $l|N$).

This L−series satisfies the functional equation (see [28,3.66])

$$\Lambda(s) := N^{s/2}(2\pi)^{-s-r+1}\Gamma(s + r - 1)L(M^\vee, s) = \varepsilon_L \Lambda(2 - s) \quad ,$$

where $\varepsilon_L = (-1)^{r-1}\varepsilon_f$.

4. Algebraic cycles and Abel-Jacobi map

The value of the L-series $L(M^\vee, s)$ at the centre of the critical strip $s = 1$ is conjecturally related to the group of codimension r cycles on the Kuga-Sato variety. Before we describe the conjectural relationship, which is a natural generalization of Birch and Swinnerton-Dyer's conjecture, we recall some definitions.

If V is a smooth variety over a field K, p a prime number different from char(K), one may define an étale version of the Abel-Jacobi map

$$\Phi : CH^r(V/K)_0 \longrightarrow H^1_{\mathrm{cont}}(K, H^{2r-1}_{\mathrm{et}}(V \otimes \overline{K}, \mathbf{Z}_p(r))) \quad ,$$

where

$$CH^r(V/K)_0 = \mathrm{Ker}[CH^r(V/K) \longrightarrow H^{2r}_{\mathrm{et}}(V \otimes \overline{K}, \mathbf{Z}_p(r))]$$

is the group of homologically trivial cycles of codimension r on V defined over K, modulo rational equivalence. One definition of Φ uses the Hochschild-Serre spectral sequence

$$E_2^{p,q} = H^p_{\mathrm{cont}}(K, H^q_{\mathrm{et}}(V \otimes \overline{K}, \mathbf{Z}_p(r))) \Longrightarrow H^{p+q}_{\mathrm{cont}}(V, \mathbf{Z}_p(r))$$

and the fact that the cohomology class of $Z \in CH^r(V/K)_0$ lies in $F^1 H^{2r}_{\mathrm{cont}}(V, \mathbf{Z}_p(r))$: $\Phi(Z)$ is by definition its image in $E_2^{1,2r-1}$. Alternatively, the diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^{2r-1}_{\mathrm{et}}(\overline{V}, \mathbf{Z}_p(r)) & \longrightarrow & H^{2r-1}_{\mathrm{et}}(\overline{V} - \overline{Z}, \mathbf{Z}_p(r)) & \longrightarrow & H^{2r}_{|\overline{Z}|}(\overline{V}, \mathbf{Z}_p(r)) & \longrightarrow & . \\
 & & \| & & \uparrow & & \uparrow & & \uparrow \\
0 & \longrightarrow & H^{2r-1}_{\mathrm{et}}(\overline{V}, \mathbf{Z}_p(r)) & \longrightarrow & E & \longrightarrow & \mathbf{Z}_p \cdot \overline{Z} & \longrightarrow & 0
\end{array}$$

defines an extension of continuous $G(\overline{K}/K)$-modules $\mathbf{Z}_p$ and $H^{2r-1}_{\mathrm{et}}(V \otimes \overline{K}, \mathbf{Z}_p(r))$ and the class of this extension is $\Phi(Z)$. See [11,12] for more details on continuous étale cohomology and the Abel-Jacobi map. We shall need later on some information on its behavior over local fields, part of which is provided by the following lemma :

Lemma 4.1. Let K be a finite extension of $\mathbf{Q}_l$, V a proper smooth variety over K. Let

$$A = H^{2r-1}_{\mathrm{et}}(V \otimes \overline{K}, \mathbf{Z}_p(r)) = \varprojlim_n (A_n = H^{2r-1}_{\mathrm{et}}(V \otimes \overline{K}, \mathbf{Z}/p^n(r))) \quad .$$

If p is a prime different from l, then

$$H^1_{\mathrm{cont}}(K, A) = H^1_{\mathrm{cont}}(K^{ur}/K, A) \qquad ,$$

i.e. consists of unramified cohomology classes.

Proof. As $l \neq p$, one has

$$H^1_{\mathrm{cont}}(K, A) \simeq \varprojlim_n H^1(K, A_n) = \varprojlim_n H^1(K^t/K, A_n) \qquad ,$$

where K^t is the maximal tamely ramified extension of K. The Galois group $G(K^t/K)$ is generated by two elements φ, τ satisfying the relation $\varphi\tau\varphi^{-1} = \tau^{\lambda}$, where $\lambda = l^d$ is the cardinality of the residue field of K, τ generates $G(K^t/K^{ur}) \simeq \prod_{q\neq l} \mathbf{Z}_p(1)$ and φ is a lift of the arithmetic Frobenius $Fr(\lambda) \in G(K^{ur}/K)$.According to the proper and smooth base change theorems, the modules A_n are unramified, hence we get an exact sequence

$$0 \longrightarrow H^1_{\text{cont}}(K^{ur}/K, A) \longrightarrow H^1_{\text{cont}}(K^t/K, A) \longrightarrow H^1_{\text{cont}}(K^t/K^{ur}, A)^{G(K^{ur}/K)}$$

with $H^1_{\text{cont}}(K^t/K^{ur}, A) \simeq \text{Hom}_{\text{cont}}(G(K^t/K^{ur}), A) \simeq A$ (evaluation at τ) and

$$H^1_{\text{cont}}(K^t/K^{ur}, A)^{G(K^{ur}/K)} \simeq \{a \in A | (\varphi - \lambda)(a) = 0\} \quad ,$$

which is zero by Weil's conjectures.

Returning to the situation of previous sections, let $V = \overline{\overline{X}}_N^{2r-2}$ be the Kuga-Sato variety and p a fixed prime not dividing $2(2r-2)!N\varphi(N)$.The Abel-Jacobi map composed with the projections Π_ϵ, Π_B introduced in sec.2 and sec.3 induces a map

$$\Phi : CH^r(\overline{\overline{X}}_N^{2r-2}/K)_0 \longrightarrow H^1_{\text{cont}}(K, J)$$

(recall that J is the parabolic cohomology group for $\Gamma_0(N)$).
Since the Abel-Jacobi map commutes with automorphisms of the underlying variety, Φ factors through $\Pi_\epsilon(CH^r(\overline{\overline{X}}_N^{2r-2}/K)_0 \otimes \mathbf{Z}_p)$. According to Prop. 2.1,

$$\Pi_\epsilon H^{2r}(\overline{\overline{X}}_N^{2r-2} \otimes \overline{\mathbf{Q}}, \mathbf{Z}_p(r)) = 0 \quad ,$$

hence

$$\Pi_\epsilon(CH^r(\overline{\overline{X}}_N^{2r-2}/K)_0 \otimes \mathbf{Z}_p) = \Pi_\epsilon(CH^r(\overline{\overline{X}}_N^{2r-2}/K) \otimes \mathbf{Z}_p)$$

over any extension K of $\mathbf{Q}$.
Finally, composing with the map $r : J \longrightarrow A$, we obtain

$$\Phi_{f,K} : \Pi_\epsilon(CH^r(\overline{\overline{X}}_N^{2r-2}/K) \otimes \mathbf{Z}_p) \longrightarrow H^1_{\text{cont}}(K, A) \quad .$$

Proposition 4.2. The map $\Phi_{f,K}$ is $\mathbf{T}$−equivariant. If $K/\mathbf{Q}$ is Galois, $\Phi_{f,K}$ is also $G(K/\mathbf{Q})$−equivariant.
Proof. The Abel-Jacobi map commutes with correspondences and the Galois action.

Now we are ready to state the promised generalization of Birch and Swinnerton-Dyer's conjecture:

Conjecture 4.3. (A.A.Beilinson, S.Bloch, see [12]) For each number field K,

$$\dim_{\mathbf{Q}_p}(\mathrm{Im}(\Phi_{f,K})\otimes\mathbf{Q}_p) = \mathrm{ord}_{s=1}L(M^\vee\otimes K,s) = \mathrm{ord}_{s=r}L(f\otimes K,s) \quad .$$

In particular, if $K=\mathbf{Q}(\sqrt{-D})$ is an imaginary quadratic field with discriminant $-D$, then

$$\dim_{\mathbf{Q}_p}(\mathrm{Im}(\Phi_{f,K})^+\otimes\mathbf{Q}_p) = \dim_{\mathbf{Q}_p}(\mathrm{Im}(\Phi_{f,\mathbf{Q}})\otimes\mathbf{Q}_p) = \mathrm{ord}_{s=r}L(f,s)$$

$$\dim_{\mathbf{Q}_p}(\mathrm{Im}(\Phi_{f,K})^-\otimes\mathbf{Q}_p) = \mathrm{ord}_{s=r}L(f\otimes\chi,s) \quad ,$$

where the signs $\pm$ refer to (± 1)-eigenspaces with respect to the action of the non-trivial element in $G(K/\mathbf{Q})$ and χ is the Dirichlet character corresponding to $K/\mathbf{Q}$.

5. CM cycles.

In this section we define certain algebraic cycles of codimension r on $\overline{\overline{X}}_N^{2r-2}$ coming from elliptic curves with complex multiplication. Our construction is modelled on [23,25]. Let $x\in M_N(\mathbf{C})$ correspond to an elliptic curve $E=E_x$ with complex multiplication (equipped with a level N structure). Then $R=\mathrm{End}(E)$ is an order of discriminant $-D$ in the imaginary quadratic field $K=\mathbf{Q}(\sqrt{-D})$. Fix one of the square roots $\sqrt{-D}\in R$. Write $\Delta\subset E\times E$ for the diagonal and $\Gamma_a\subset E\times E$ for the graph of any $a\in R$. The Néron-Severi group $NS(E\times E)$ is a free abelian group of rank four. Define Z_E to be the image of the divisor $\Gamma_{\sqrt{-D}}-(E\times\{0\})-D(\{0\}\times E)$ in $NS(E\times E)$. It lies in the free rank one $\mathbf{Z}$-module $\langle E\times\{0\},\{0\}\times E,\Delta\rangle^\perp\subset NS(E\times E)$ and changes sign when $\sqrt{-D}$ is replaced by $-\sqrt{-D}$.

The choice of $\sqrt{-D}$ fixes not only Z_E, but also all $Z_{E'}$ for E' isogeneous to E : for an isogeny $f:E\longrightarrow E'$ we fix the sign of $Z_{E'}$ by requiring $(f\times f)_*Z_E=cZ_{E'}$ with $c>0$. To check that this is independent of f, by composing with the dual isogeny to f one is reduced to prove that $(h\times h)_*Z_E=cZ_E$ with $c>0$ for all $h\in\mathrm{End}(E)$. And indeed, $(h\times h)_*$ acts on $NS(E\times E)$ by $\deg(h)$. In more down-to-earth terms, we simply insist that $\sqrt{-D'}/\sqrt{-D}$ should be positive under the canonical identification $R\otimes\mathbf{Q}\simeq R'\otimes\mathbf{Q}$.

Proposition 5.1. Let $f:E\longrightarrow E'$ be an isogeny between CM-elliptic curves with $R=\mathrm{End}(E)$, $R'=\mathrm{End}(E')$, $-D=disc(R)$, $-D'=disc(R')$. Then
(1) $(f\times f)_*Z_E=(\deg(f))(D/D')^{1/2}Z_{E'}$.
(2) $(f\times f)^*Z_{E'}=(\deg(f))(D'/D)^{1/2}Z_E$.

Proof. One has $(f\times f)_*Z_E=cZ_{E'}$ for some $c>0$ (in $NS(E\times E)\otimes\mathbf{Q}$, possibly). The constant c can be computed from $(f\times f)_*Z_E\cdot(f\times f)_*Z_E=(\deg(f))^2$, $Z_E\cdot Z_E=-2D$ and $Z_{E'}\cdot Z_{E'}=-2D'$.
Similarly, $(f\times f)^*Z_{E'}=c'Z_E$ with $c'>0$, hence by the projection formula $c'(f\times f)_*Z_E=(\deg(f))^2Z_{E'}$ and we conclude by (1).

Corollary 5.2. Assume $\deg(f)=l$ is a prime.
(1) If $\left(\frac{-D}{l}\right)=-1$, then $D'=Dl^2$ and $(f\times f)_*Z_E=Z_{E'}$.
(2) If $\left(\frac{-D'}{l}\right)=-1$, then $D=D'l^2$ and $(f\times f)^*Z_{E'}=Z_E$.

Proof. In the first case, $\mathrm{Ker}(f)$ cannot be an R-module, hence $D' = Dl^2$. In the second case we apply the same argument to the dual isogeny of f.

We now apply the above construction to the elliptic curve $E = E_x$, which is supposed to have a complex multiplication. Suppose that $D_1, \ldots, D_{r-1}$ are divisors in $E \times E$. Let K be a common rationality field of E and all D_i. Let

$$i : \pi_{2r-2}^{-1}(x) = E^{2r-2} \hookrightarrow \overline{\overline{X}}_N^{2r-2}$$

be the inclusion of the fibre over x into the (desingularization of) Kuga-Sato variety. Then $i_*(D_1 \times \ldots \times D_{r-1})$ is a cycle of codimension r on $\overline{\overline{X}}_N^{2r-2}$.

Lemma 5.3. The Abel-Jacobi image of $\Pi_\varepsilon i_*(D_1 \times \ldots \times D_{r-1})$ under

$$\Phi : \Pi_\varepsilon(CH^r(\overline{\overline{X}}_N^{2r-2}/K) \otimes \mathbf{Z}_p) \longrightarrow H^1_{\mathrm{cont}}(K, A)$$

depends only on the classes of D_i in $NS(E \times E)$.

Proof. If D_i' has the same class as D_i in $NS(E \times E)$ $(1 \leq i \leq r-1)$, then the cycle $z := (D_1 \times \ldots \times D_{r-1}) - (D_1' \times \ldots \times D_{r-1}')$ is homologically trivial already in the fiber $\pi_{2r-2}^{-1}(x)$. The Abel-Jacobi image of $\Pi_\varepsilon i_* z$ lies, therefore, in the image of

$$H^1_{\mathrm{cont}}(K, H^{2r-3}_{\mathrm{et}}(\pi_{2r-2}^{-1}(x) \otimes \overline{\mathbf{Q}}, \mathbf{Z}_p(r-1)) \longrightarrow H^1_{\mathrm{cont}}(K, \Pi_\varepsilon H^{2r-1}_{\mathrm{et}}(\overline{\overline{X}}_N^{2r-2} \otimes \overline{\mathbf{Q}}, \mathbf{Z}_p(r))),$$

which is trivial by Prop. 2.1.

Let $K = \mathbf{Q}(\sqrt{-D}) \hookrightarrow \mathbf{C}$ be an imaginary quadratic field of discriminant $-D$, in which all prime factors of N split. Write $\mathcal{O}_K$ for the ring of integers of K. Choose an ideal $\mathcal{N}$ of $\mathcal{O}_K$ with $\mathcal{O}_K/\mathcal{N} \simeq \mathbf{Z}/N$. The inclusion $\mathcal{O}_K \hookrightarrow \mathcal{N}^{-1}$ induces a cyclic N-isogeny $\mathbf{C}/\mathcal{O}_K \longrightarrow \mathbf{C}/\mathcal{N}^{-1}$ between two complex tori, hence a point x_1 of the modular curve $X_0(N)$. By the theory of complex multiplication, x_1 is rational over K_1, the Hilbert class field of K.

Let $n \geq 1$ be an integer prime to N and $\mathcal{O}_n := \mathbf{Z} + n\mathcal{O}_K$. Again, one has a cyclic isogeny $\mathbf{C}/\mathcal{O}_n \longrightarrow \mathbf{C}/(\mathcal{O}_n \cap \mathcal{N})^{-1}$, which defines a point x_n on $X_0(N)$. The point x_n is rational over K_n, the ring class field of conductor n over K. In the tower of extensions

$$\mathbf{Q} \hookrightarrow K \hookrightarrow K_1 \hookrightarrow K_n$$

one has $G(K/\mathbf{Q}) = \{1, c\}$, $G(K_1/K) = Pic(\mathcal{O}_K)$, $G_n = G(K_n/K_1) = (\mathcal{O}_K/n)^*/\mathcal{O}_K^* (\mathbf{Z}/n)^*$. Here c is complex conjugation, which lifts to K_n and makes $G(K_n/\mathbf{Q})$ a semidirect product of $G(K_n/K)$ and $\{1, c\}$ with $c-$action on $G(K_n/K)$ by $c\sigma c^{-1} = \sigma^{-1}$. If l is a prime inert in K, then K_l/K is ramified only at l and $G_l = G(K_l/K_1)$ is cyclic of degree $(l+1)/u_K$, where $u_K = (\sharp\mathcal{O}_K^*)/2$ $(= 1$ for $D \neq -3, -4)$.

Using our fixed embedding of K into $\mathbf{C}$ we fix square roots of discriminants of all orders of $\mathcal{O}_K$ by insisting that their imaginary part should be positive. Let n be squarefree and prime to $N \cdot D \cdot p$. Write κ for the canonical projection $M_N \longrightarrow X_0(N)$. Choose any $x \in \kappa^{-1}(x_n)$. The corresponding elliptic curve E_x has endomorphism ring $\mathrm{End}(E_x) = \mathcal{O}_n$ with discriminant Dn^2. Let i_x be the inclusion of the fibre $\pi_{2r-2}^{-1}(x)$ into $\overline{\overline{X}}_N^{2r-2}$ and denote by y_n the Abel-Jacobi image of $\Pi_\varepsilon(i_x)_*(Z_{E_x}^{r-1})$ under

$$\Phi : \Pi_\varepsilon(CH^r(\overline{\overline{X}}_N^{2r-2}/K_n) \otimes \mathbf{Z}_p) \longrightarrow H^1_{\mathrm{cont}}(K_n, J) \quad .$$

Note that y_n is independent of the choice of x, since the averaging over all $x \in \kappa^{-1}(x_n)$ has been built into the definition of Φ.

Proposition 5.4. Assume that $n = l \cdot m$, where l is inert in K. Then

$$T_l\, y_m = u_K \cdot \mathrm{cor}_{K_n,K_m}(y_n) \quad .$$

Proof. We first compute the action of T_l ($= T_l^*$ in the notation of [25]) on $(i_x)_*(Z_{E_x}^{r-1})$ for $x \in \kappa^{-1}(x_m)$: according to Prop. 4.2, Cor. 5.2 and Lemma 5.3 it is equal to

$$\sum_y (i_y)_*(Z_{E_y}^{r-1}) \qquad ,$$

where $l+1$ points $y \in M_N$ correspond to l–isogenies $E_y \longrightarrow E_x$ compatible with level N structures. By the theory of complex multiplication, the set $\{\kappa(y)\}$ consists of u_K orbits of x_n under the action of $G(K_n/K_m) \simeq G(K_l/K_1) \simeq \mathbf{Z}/((l+1)/u_K)\mathbf{Z}$. As the Galois action on Z_E's comes from that on M_N, the claim follows.

6. The Euler system

In the last section we have constructed cohomology classes $y_n \in H^1_{\mathrm{cont}}(K_n, J)$. Using the map $r : J \longrightarrow A$ from sec.3, we obtain new classes, still to be denoted y_n, in $H^1_{\mathrm{cont}}(K_n, A)$. From now on, we shall consider only square-free n of the form $n = l_1 \ldots l_k$, where all l_i are primes inert in K not dividing $N \cdot D \cdot p$. We also assume that $D \neq -3, -4$, but the method applies for $D = -3, -4$ as well: sometimes the value u_K appears in the formulas and occasionally a factor p has to be taken into account to compensate for this if u_K is divisible by p, i.e. for $p = D = 3$. The main result, Theorem 13.1, remains unaffected, however.

Under these assumptions, we have $G_n = G(K_n/K_1) = \prod_{l|n} G_l$ with G_l cyclic of order $l+1$. Fix, once for all, a generator σ_l of G_l. If $n = m \cdot l$, then, by class field theory, λ splits completely in K_m/K and all its factors λ_m are totally ramified in K_n/K_m : $\lambda_m = (\lambda_n)^{l+1}$. Write $K_{\lambda_n}, K_{\lambda_m}$ for the corresponding completions of K_n at λ_n resp. K_m at λ_m.

Proposition 6.1. If $n = m \cdot l$, then
(1) $\mathrm{cor}_{K_n,K_m}(y_n) = a_l \cdot y_m$.
(2) The local components of y_n resp. y_m satisfy

$$y_{n,\lambda_n} = Fr(l)(\mathrm{res}_{K_{\lambda_m},K_{\lambda_n}}(y_{m,\lambda_m})) \in H^1_{\mathrm{cont}}(K_{\lambda_n}, A)$$

(the Frobenius $Fr(l) \in G(K_\lambda/\mathbf{Q}_l)$ acts on $H^1_{\text{cont}}(K_{\lambda_n}, A)$, as the latter group is unramified by Lemma 4.1.).

Proof. (1) Follows from Prop. 5.4, as T_l acts on A by the scalar a_l.
(2) Since l is inert in K, the reductions of elliptic curves E, E' corresponding to $x_m, x_n \in M_N$ at λ_m resp. λ_n are both supersingular. This implies that the canonical l−isogeny $E \longrightarrow E'$ reduces to the Frobenius and we conclude by Cor. 5.2.

Proposition 6.2. The complex conjugation acts on y_n as

$$cy_n = -\varepsilon_L \cdot \sigma y_n \qquad ,$$

where $\sigma \in G(K_n/K)$ and $\varepsilon_L = (-1)^{r-1}\varepsilon_f$ is the sign in the functional equation of $L(f,s)$.
Proof. We recall that the Fricke involution acts on the modular form f by $(f|W_N)(\tau) = N^{-r}\tau^{-2r}f(-1/N\tau)$. One associates to f the differential form $\omega = f(\tau)d\tau dz$ on $X^{2r-2}_{N,0}$, where $dz = dz_1 \ldots dz_{2r-2}$ and $X^{2r-2}_{N,0}$ is the Kuga-Sato variety over $X_0(N)$. Define $W : X^{2r-2}_{N,0} \longrightarrow X^{2r-2}_{N,0}$ by

$$W : (\lambda : E \longrightarrow E', z) \longmapsto (\lambda^\vee : E' \longrightarrow E, \lambda(z)) \quad .$$

A simple calculation shows that $W^*(f(\tau)d\tau dz) = N^{r-1}(f|W_N)d\tau dz$. From Prop. 5.1 and Lemma 5.3 we get $W^*(Z^{r-1}_{W_N(\tau)}) = N^{r-1}Z^{r-1}_\tau$. Since $f|W_N = \varepsilon_f \cdot f$, one has

$$\Phi(Z^{r-1}_{W_N(\tau)}) = \varepsilon_f \Phi(Z^{r-1}_\tau)$$

in $H^1_{\text{cont}}(*, A)$. Suppose that $\tau \in \mathcal{O}_n$. According to [9,5.3], one has $c(E_\tau) = \sigma(E_{W_N(\tau)})$ for some $\sigma \in G(K_n/K)$. As c sends Z_E into $-Z_{c(E)}$, we get

$$c\Phi(Z^{r-1}_\tau) = (-1)^{r-1}\varepsilon_f \cdot \sigma\Phi(Z^{r-1}_\tau) \quad .$$

The statement follows if we take $\tau = x_n$.

The ring $\mathcal{O}_F \otimes \mathbf{Z}_p$ has a canonical direct sum decomposition $\mathcal{O}_F \otimes \mathbf{Z}_p = \bigoplus_{\wp|p} \mathcal{O}_\wp$, where $\mathcal{O}_\wp$ is the completion of $\mathcal{O}_F$ at a prime $\wp$ dividing p. We fix such a prime $\wp$. The localization $A_\wp = A \otimes_{\mathcal{O}_F \otimes \mathbf{Z}_p} \mathcal{O}_\wp$ of A at $\wp$ is a free $\mathcal{O}_\wp$−module of rank 2. The $\wp$-component of $y_n \in H^1_{\text{cont}}(K_n, A)$ will be denoted by $y_{n,\wp} \in H^1_{\text{cont}}(K_n, A_\wp)$. Put $Y = A_\wp \otimes \mathbf{Q}_p/\mathbf{Z}_p$. Then $Y_{p^M} = A_\wp/p^M A_\wp$ for all $M \geq 0$. Let $L = K(Y_{p^M}(\overline{\mathbf{Q}}))$ be the extension of K trivializing Y_{p^M}.

Proposition 6.3. For all n, $Y_{p^M}(K_n) = Y_{p^M}(K_1)$ and this group is killed by a fixed power p^{M_1} independent of M.

Proof. The extensions K_n/K and L_M/K are unramified outside primes dividing n and Np respectively, which implies that $K_n \cap L$ is unramified over K, hence is contained in K_1 (note that for $p \nmid D$ the same argument over $\mathbf{Q}$ instead of K implies that $K_n \cap L = \mathbf{Q}$). The existence of M_1, i.e. the finiteness of $Y(K_1)$, follows from Weil's conjectures.

Corollary 6.4. The kernel and cokernel of the restriction map

$$\mathrm{res}_{K_1,K_n} : H^1(K_1, Y_{p^M}) \longrightarrow H^1(K_n, Y_{p^M})^{G_n}$$

are both killed by p^{M_1}.

Proof. Follows from the inflation-restriction sequence.

We shall now construct G_n–invariant elements in $H^1(K_n, Y_{p^M})$. We assume from now on that each prime factor l of n satisfies

$$Fr_{L_M/\mathbf{Q}}(l) = Fr_{L_M/\mathbf{Q}}(c) \quad ,$$

where the R.H.S. is the conjugacy class of the complex conjugation. By Prop. 3.1., this condition boils down to

$$\left(\frac{-D}{l}\right) = -1, \quad a_l \equiv l+1 \equiv 0 \,(\mathrm{mod}\, p^M) \quad .$$

We define $D_l, Tr_l \in \mathbf{Z}[G_l]$ by

$$D_l = \sum_{i=1}^{l} i\sigma_l^i, \quad Tr_l = \sum_{i=0}^{l} \sigma_l^i \quad .$$

They are related by

$$(\sigma_l - 1)D_l = l + 1 - Tr_l \quad .$$

For $n = \prod l$ we put $D_n = \prod D_l \in \mathbf{Z}[G_n]$.

For $x \in H^1_{\mathrm{cont}}(*, A_{\mathfrak{p}})$ we denote by $\mathrm{red}_M(x)$ the image of x in $H^1(*, Y_{p^M})$. Since $\mathrm{res}_{K_m,K_n} \circ \mathrm{cor}_{K_n,K_m} = Tr_l$, we get from Prop. 6.1.

$$D_n \mathrm{red}_M(y_{n,\mathfrak{p}}) \in H^1(K_n, Y_{p^M})^{G_n} \quad .$$

This means that possibly after a multiplication by p^{M_1} this elements lifts to $H^1(K_1, Y_{p^M})$. We shall examine this lifting, called "Kolyvagin's corestriction" in [21], more closely in the following section.

7. Kolyvagin's corestriction.

This is a purely group-theoretic construction and works in the following situation: H is a normal subgroup in G, G/H is a cyclic group of order N with a fixed generator σ, A is a G-module killed by N, $[x] \in H^1(H, A)$ a cohomology class with $\mathrm{cor}_{H,G}[x] = 0 \in H^1(G, A)$.

As before, put

$$D = \sum_{i=1}^{N-1} i\sigma^i, \quad Tr = \sum_{i=0}^{N-1} \sigma^i \quad .$$

One has $(\sigma - 1)D = N - Tr$, hence $D[x] \in H^1(H, A)^{G/H}$.

Choose a cocycle $x \in Z^1(H, A)$ representing $[x]$. Then $\mathrm{cor}[x]$ is represented by the cocycle

$$\begin{aligned} \mathrm{cor}(x) : h &\longmapsto \sum_{i=0}^{N-1} \tilde{\sigma}^i x(\tilde{\sigma}^{-i} h \tilde{\sigma}^i) \qquad (h \in H) \\ \tilde{\sigma} &\longmapsto x(\tilde{\sigma}^N) \quad , \end{aligned}$$

where $\tilde{\sigma} \in G$ is a fixed lift of σ into G. Since $\mathrm{cor}[x] = 0$, on the cocycle level

$$\mathrm{cor}(x) : g \longmapsto (g - 1)a \qquad (g \in G)$$

for some $a \in A$, which is determined modulo A^G.
Define a cocycle $Dx \in Z^1(H, A)$ by

$$Dx : h \longmapsto \sum_{i=1}^{N-1} i\tilde{\sigma}^i x(\tilde{\sigma}^{-i} h \tilde{\sigma}^i) \quad .$$

A short calculation then shows :
(1) $\tilde{\sigma}(Dx)(\tilde{\sigma}^{-1} h \tilde{\sigma}) - (Dx)(h) = -(h-1)\tilde{\sigma}a$
(2) the function

$$\begin{aligned} f : h &\longmapsto (Dx)(h) \\ \tilde{\sigma} &\longmapsto -\tilde{\sigma}a \end{aligned}$$

extends uniquelly to a 1-cocycle $f \in Z^1(G, A)$ (which satisfies, of course, $\mathrm{res}_{G,H} f = Dx$) .
(3) If $x' = x + \delta b$ for some $b \in A$, then the corresponding extension

$$\begin{aligned} f' : h &\longmapsto (Dx)(h) \\ \tilde{\sigma} &\longmapsto -\tilde{\sigma}a' \end{aligned}$$

(with $\mathrm{cor}(x') = \delta a'$) satisfies

$$f' - f - \delta(\sum_{i=1}^{N-1} i\tilde{\sigma}^i)b \in Z^1(G, A^G) \quad .$$

In particular, if A^G is killed by an integer m, then

$$m[f] = m[f'] \in H^1(G, mA)$$

is a lift of $mD[x]$ which depends only on $[x]$.

We apply this construction in our particular situation, with a slightly changed notation. Namely, we fix $M > 0$, put $M' = M + M_1$ (recall that p^{M_1} kills $Y(K_1)$) and require that $a_l \equiv l+1 \equiv 0 (\mathrm{mod}\ p^{M'})$ for all primes l diving n. Denote by $j : Y_{p^{M'}} \longrightarrow Y_{p^M}$ the multiplication by p^{M_1}.

We are now ready to define cohomology classes $P_M(n) \in H^1(K, Y_{p^M})$, which will play a key role in the descent.

(1) For $n = 1$, put $P_M(1) := \mathrm{cor}_{K_1,K}(\mathrm{red}_M(y_{1,\mathfrak{p}}))$.
(2) For $n = l$, we know that $D_l \mathrm{red}_{M'}(y_{l,\mathfrak{p}}) = \mathrm{res}_{K_1,K_l}(z_l)$ for some $z_l \in H^1(K_1, Y_{p^{M'}})$ and we define

$$P_M(l) := \mathrm{cor}_{K_1,K}(j_*(z_l)) \in H^1(K, Y_{p^M}) \quad .$$

This depends only on y_l, as two choices of z_l differ by an element in

$$\mathrm{Im}(H^1(K, Y_{p^{M_1}}) \longrightarrow H^1(K, Y_{p^{M'}})) \subseteq \mathrm{Ker}(j_*) \quad .$$

(3) For $n = l_1 \dots l_k$ with $k \geq 2$ we have $p^{M_1} D_n \mathrm{red}_{M'}(y_{n,\mathfrak{p}}) = \mathrm{res}_{K_1,K_n}(z_n)$ for some $z_n \in H^1(K_1, Y_{p^{M'}})$ and we put

$$P_M(n) := \mathrm{cor}_{K_1,K}(j_*(z_n)) \in H^1(K, Y_{p^M})$$

(this is again independent on the choice of z_n).

We shall need an information on the local behavior of the class $P_M(n)$ at the place λ of K corresponding to a prime factor l of n. For such a prime, fix a place λ_n of K_n over l, which in turn determines places $\lambda_m, \lambda_l, \lambda_1$ in K_m, K_l, K_1 respectively with corresponding completions $K_{\lambda_n} = K_{\lambda_l}$, $K_{\lambda_m} = K_{\lambda_1} = K_\lambda$ and isomorphisms

$$G(K_{\lambda_l}/K_\lambda) = G(K_{\lambda_n}/K_{\lambda_m}) \simeq G_l = \langle \sigma_l \rangle \quad .$$

Localizing the inflation-restriction sequence for K_n/K_1 we obtain the commutative diagram with exact rows and columns :

$$\begin{tikzcd}
 & & 0 \arrow[d] & 0 \arrow[d] \\
 & & H^1(K_{\lambda_n}/K_{\lambda_1}, Y_{p^{M'}}) \arrow[r, "\sim"] \arrow[d, "\mathrm{inf}"] & H^1(K_{\lambda_n}^{ur}/K_{\lambda_1}^{ur}, Y_{p^{M'}}) \arrow[d, "\wr\,\mathrm{inf}"] \\
0 \arrow[r] & H^1_{ur}(K_{\lambda_1}, Y_{p^{M'}}) \arrow[r] \arrow[d, "\wr"] & H^1(K_{\lambda_1}, Y_{p^{M'}}) \arrow[r] \arrow[d, "\mathrm{res}"] & H^1(K_{\lambda_1}^{ur}, Y_{p^{M'}}) \arrow[d, "\mathrm{res}=0"] \\
0 \arrow[r] & H^1_{ur}(K_{\lambda_n}, Y_{p^{M'}})^{\langle \sigma_l \rangle} \arrow[r] & H^1(K_{\lambda_n}, Y_{p^{M'}})^{\langle \sigma_l \rangle} \arrow[r] & H^1(K_{\lambda_n}^{ur}, Y_{p^{M'}})^{\langle \sigma_l \rangle}
\end{tikzcd}$$

All rows and columns come from various inf-res sequences; only the surjectivity of the inflation map in the upper right corner may require an explanation: as we shall see in Prop. 8.1, it corresponds to the map

$$\mathrm{Hom}(\mu_{l+1}, Y_{p^{M'}}) \longrightarrow \mathrm{Hom}(\hat{\mathbf{Z}}'(1), Y_{p^{M'}})$$

with $\hat{\mathbf{Z}}'(1) = \prod_{q \neq l} \mathbf{Z}_q$.

8. Tame duality

In order to compute the local cohomology groups in the above diagram, we shall recall some basic facts on tame duality (cf.[27,5.5]). Assume that K is a local field with the residue field $\mathbf{F}_q$.

Proposition 8.1. Suppose that A is a finite group with a trivial action of $G(\overline{K}/K)$, killed by an integer M dividing $q-1$ ($\Rightarrow \mu_M \subset K$). Put $A' = \mathrm{Hom}(A, \mu_M)$. Then

(1) One has the commutative diagram with exact rows and canonical isomorphisms in the vertical direction

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_{ur}(K,A) & \longrightarrow & H^1(K,A) & \longrightarrow & H^1(K^{ur},A) & \longrightarrow & 0 \\ & & \downarrow \wr\alpha & & \downarrow \wr & & \downarrow \wr\beta & & \\ 0 & \longrightarrow & A & \longrightarrow & \mathrm{Hom}(K^*,A) & \longrightarrow & \mathrm{Hom}(\mu_M,A) & \longrightarrow & 0 \end{array}$$

(2) The evaluation map $A \times A' \longrightarrow \mu_M$ yields the cup product pairing

$$H^1(K,A) \times H^1(K,A') \longrightarrow H^2(K,\mu_M) \simeq \mathbf{Z}/M \quad ,$$

which in turn induces a perfect pairing

$$\begin{array}{cccccc} \langle\ ,\ \rangle_M : & H^1_{ur}(K,A) & \times & H^1(K^{ur},A') & \longrightarrow & \mathbf{Z}/M \\ & \downarrow \wr\alpha & & \downarrow \wr\beta' & & \downarrow \wr \\ & A & \times & \mathrm{Hom}(\mu_M,A') & \longrightarrow & \mathrm{Hom}(\mu_M,\mu_M) \end{array}$$

Proof. All statements are well-known. The maps α, β are evaluations at the generators φ resp.τ of $G(K^{ur}/K)$ resp. $G(K^t/K^{ur})$ (notation as in the proof of Lemma 4.1). Non-degeneracy of the pairing is [27,5.5.19]. The commutativity of the last diagram is proved in [14,Prop.8]. In fact, it is clear that it is commutative up to a constant in $\mathbf{Z}/M$ and it is highly implausible that such an intrinsic constant could be different from ± 1.The truth is, however, that the value of this constant is irrelevant for the success of the descent, as long as we know that it is invertible in $\mathbf{Z}/M$, which is equivalent to the fact that the pairing $\langle\ ,\ \rangle_M$ is non-degenerate.

As we have seen, the choice of λ_n identifies σ_l with an element of $G(K_{\lambda_l}/K_\lambda)$, which can be lifted to a generator τ_l of $G(K^t_\lambda/K^{ur}_\lambda)$ (well-defined modulo $(l+1)\hat{\mathbf{Z}}'(1)$). Under the canonical projection $\hat{\mathbf{Z}}'(1) \longrightarrow \mu_{p^{M'}}$, τ_l gets mapped to certain primitive $p^{M'}$–th root of unity $\zeta_{\lambda,M'} \in \mu_{p^{M'}}(K_\lambda)$. Equivalently, $\zeta_{\lambda,M'}$ corresponds to $\sigma_l^{(l+1)/p^{M'}}$ via class field theory.

Using Prop. 8.1, we get canonical ($\mathcal{O}_p$−linear) isomorphisms

$$\alpha_{\lambda,M'} : H^1_{ur}(K_\lambda, Y_{p^{M'}}) \simeq Y_{p^{M'}}(K_\lambda) \qquad ,$$
$$\beta_{\lambda,M'} : H^1(K^{ur}_\lambda, Y_{p^{M'}}) \simeq \mathrm{Hom}(\mu_{p^{M'}}(K_\lambda), Y_{p^{M'}}(K_\lambda)) \simeq Y_{p^{M'}}(K_\lambda),$$

the last map being the evaluation at $\zeta_{\lambda,M'}$, and

$$\phi_{\lambda,M'} = \beta^{-1}_{\lambda,M'} \circ \alpha_{\lambda,M'} : H^1_{ur}(K_\lambda, Y_{p^{M'}}) \simeq H^1(K^{ur}_\lambda, Y_{p^{M'}}) \quad .$$

On the cocycle level, $\phi_{\lambda,M'}$ interchanges cocycles with the same values on $Fr(l)$ and $\tau_l(\mathrm{mod}\ p^{M'})$ respectively. The second statement of Prop. 8.1. can be written as

Corollary 8.2.

$$\zeta_{\lambda,M'}^{\langle x,\phi_{\lambda,M'}(y)\rangle_{\lambda,M'}} = [\alpha_{\lambda,M'}(x), \alpha_{\lambda,M'}(y)]_{M'} \quad ,$$

provided we identify $Y_{p^{M'}}$ with $(Y_{p^{M'}})'$ via $[\ ,\ ]_{M'}$.

The diagram in sec.7 defines a canonical splitting

$$H^1(K_\lambda, Y_{p^{M'}}) = H^1_{ur}(K_\lambda, Y_{p^{M'}}) \oplus H^1(K^{ur}_\lambda, Y_{p^{M'}})$$

with both pieces isomorphic to $Y_{p^{M'}}(K_\lambda)$ via $\alpha_{\lambda,M'}$ resp. $\beta_{\lambda,M'}$. We shall see bellow that the localization $P_M(n)_\lambda$ lies in the ramified part $H^1(K^{ur}_\lambda, Y_{p^M})$ and our aim will be to identify the element of Y_{p^M} to which it corresponds.

9. Localization of Kolyvagin's corestriction

In order to determine $P_M(n)_\lambda$, we return to the general context of Kolyvagin's corestriction as in sec.7, with some additional structures listed bellow:

(1) One starts with a profinite group $\tilde{G}$ and an odd prime number p. There is a chain of normal subgroups $H \triangleleft G \triangleleft \tilde{G}$ with $\tilde{G}/H = \langle\sigma\rangle \rtimes \langle c\rangle$ dihedral, where $\langle\sigma\rangle$ is a cyclic group of order N, $\langle c\rangle$ is a group of order two acting on $\langle\sigma\rangle$ by $c\sigma c^{-1} = \sigma^{-1}$, $G/H = \langle\sigma\rangle$, $\tilde{G}/G = \langle c\rangle$.

(2) One is given a closed subgroup $\tilde{G}_0 \subset \tilde{G}$ with $G_0/H_0 = \langle\sigma_0\rangle$ again cyclic of order N (where $G_0 = \tilde{G}_0 \cap G$, $H_0 = \tilde{G}_0 \cap H$). This implies that $\tilde{G}_0/H = \langle\sigma_0\rangle \rtimes \mathbf{Z}/f\mathbf{Z}$ with $f = 1, 2$.

(3) The group $\tilde{G}_0$ is equipped with a surjective homomorphism

$$\pi : \tilde{G}_0 \longrightarrow \hat{\mathbf{Z}}'(1) \rtimes f\hat{\mathbf{Z}} \quad ,$$

where $\hat{\mathbf{Z}}'(1) = \prod_{l\neq p} \mathbf{Z}_l(1)$ and $\hat{\mathbf{Z}}$ have fixed generators τ and φ respectively, satisfying the usual relation $\varphi\tau\varphi^{-1} = \tau^d$ for some integer d prime to p. One also requires π to induce surjections

$$G_0 \longrightarrow \hat{\mathbf{Z}}'(1) \rtimes f\hat{\mathbf{Z}}, \quad H_0 \longrightarrow N\hat{\mathbf{Z}}'(1) \rtimes f\hat{\mathbf{Z}} \quad ,$$

under which the generator σ_0 of G_0/H_0 corresponds to τ modulo N.

(4) $A = \varprojlim A/p^n A$ is a torsion-free $\mathbf{Z}_p$-module of finite rank with a continuous action of $\tilde{G}$.

(5) $\tilde{G}_0$ acts on A through its quotient $\hat{\mathbf{Z}}$.

(6) $\mathrm{Ker}(\pi)$ has order prime to p (as a profinite group).

(7) φ acts on $A \otimes \overline{\mathbf{Q}}$ in a semisimple way, all its eigenvalues are algebraic and their archimedean absolute values are equal to $d^{1/2}$ under all embeddings $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$.

(8) Let M be a given power of p dividing N. Then $(\varphi^f - 1)^{2/f}$ kills A/MA.

(9) One is given $y \in H^1_{\mathrm{cont}}(H, A)$, $x \in H^1_{\mathrm{cont}}(G, A)$ with $\mathrm{cor}_{H,G}(y) = M_1 x$ for some M_1 divisible by M.

(10) $(A/MA)^G$ is killed by an integer m.

The situation the reader should keep in mind is the following: $H = G(\overline{\mathbf{Q}}/K_l)$, $G = G(\overline{\mathbf{Q}}/K_1)$, $\tilde{G} = G(\overline{\mathbf{Q}}/K_1^+)$ (K_1^+ is the maximal real subfield of K_1), $\tilde{G}_0 = G(\overline{\mathbf{Q}}_l/\mathbf{Q}_l)$, $G_0 = G(\overline{\mathbf{Q}}_l/K_\lambda)$, $H_0 = G(\overline{\mathbf{Q}}_l/K_{\lambda_l})$, $A = A_{\mathfrak{p}}$, $f = 2$, $d = l$, $N = l + 1$, $x = y_{1,\mathfrak{p}}$, $y = y_{l,\mathfrak{p}}$. We have included the case $f = 1$ for the sake of completeness; it corresponds to a related construction using primes split in K (cf. [16]).

As we have seen in the proof of Lemma 4.1, (5)-(7) imply that

$$H^1_{\mathrm{cont}}(G_0, A) = H^1_{\mathrm{cont}}(H_0, A) \simeq H^1_{\mathrm{cont}}(f\hat{\mathbf{Z}}, A) \simeq A/(\varphi^f - 1)A \quad .$$

On the cocycle level, this means that each 1-cocycle $F \in Z^1(\hat{\mathbf{Z}}'(1) \rtimes f\hat{\mathbf{Z}}, A)$ has a form

$$F(\tau^u \varphi^{fv}) = (1 + \varphi^f + \ldots + \varphi^{(v-1)f})a + (\varphi^f - 1)b$$

and its cohomology class is

$$[F] = a(\mathrm{mod}(\varphi^f - 1)A) \in A/(\varphi^f - 1)A \quad .$$

Thank to the assumptions (9)-(10), we may define Kolyvagin's corestriction $z \in H^1(G, mA/MA)$ satisfying $\mathrm{res}_{G,H}(z) = mD\mathrm{red}_M(y) \in H^1(H, mA/MA)$ (as before, $\mathrm{red}_M(y)$ is the image of y in $H^1(H, A/MA)$). By (3) and (5), D acts on A as the scalar $N(N-1)/2$, which is divisible by M, hence $\mathrm{res}_{G,H_0}(z) = 0$ and $\mathrm{res}_{G,G_0}(z) = \mathrm{inf}_{G_0/H_0,G_0}(z_0)$ for some $z_0 \in H^1(G_0/H_0, mA/MA) = \mathrm{Hom}(\langle\sigma_0\rangle, mA/MA)$.

Our task is to compute $z_0(\sigma_0) \in mA/MA$. To achieve that, we must do calculations on the level of cocycles, to be denoted by the same letters : $y \in Z^1(H, A)$, $x \in Z^1(G, A)$. According to (9), there is an $a \in A$ satisfying

$$(\mathrm{cor}(y))(g) - M_1 x(g) = (g - 1)a \qquad (g \in G).$$

We know from sec.7 that $z_0(\sigma_0) = -ma(\mathrm{mod}\ MA)$, which means that it is the value of a modulo MA we have to compute. Restricting ourselves to $g = g_0 \in G_0$, we get

$$\sum_{i=0}^{N-1} y(\tilde{\sigma}_0^{-i} g_0 \tilde{\sigma}_0^i) - M_1 x(g_0) = (g_0 - 1)a \quad .$$

At the same time, the calculation of $H^1_{\text{cont}}(G_0, A)$ above implies that for $\pi(g_0) = \sigma_0^u \varphi^{fv}$ one has

$$x(g_0) = (1 + \varphi^f + \ldots + \varphi^{(v-1)f})a_x + (\varphi^f - 1)b_x$$
$$y(g_0) = (1 + \varphi^f + \ldots + \varphi^{(v-1)f})a_y + (\varphi^f - 1)b_y$$

for some $a_x, a_y, b_x, b_y \in A$. Putting the last three equations together, we obtain

$$(1 + \varphi^f + \ldots + \varphi^{(v-1)f})(Na_y - M_1 a_x) = (\varphi^f - 1)(a + M_1 b_x - N b_y) \quad .$$

For $v = 1$ this reads as

$$\frac{N}{M} a_y - \frac{M_1}{N} a_x = \frac{\varphi^f - 1}{M}(a + M \cdot sth.)$$

(as A is torsion-free).

In this formula,

$$a_x(\text{mod}(\varphi^f - 1)A) = \text{res}_{G,G_0}(x) \in H^1_{\text{cont}}(f\hat{\mathbf{Z}}, A)$$
$$a_y(\text{mod}(\varphi^f - 1)A) = \text{res}_{H,H_0}(y) \in H^1_{\text{cont}}(f\hat{\mathbf{Z}}, A)$$

are "local components" of x and y respectively.

We now impose the last two assumptions

(11) $\varphi^2 - M_2\varphi + d = 0$ on A

(12) $a_y = \varphi(a_x) \mod(\varphi^f - 1)A$.

Then we get from the previous discussion the

Key formula :

$$\frac{\varphi^f - 1}{M}(a + M \cdot sth.) = \left(\frac{N}{M}\varphi - \frac{M_1}{M}\right) a_x \quad .$$

The question is, under which circumstances this allows us to compute the value of $z_0(\sigma_0) = -ma\,(\text{mod } MA)$. We discuss several cases when this is possible.

(I) "Genuine" Euler systems (this is the most favourable case, which occurs for elliptic modular curves): $\frac{(\varphi^f - 1)^{2/f}}{M}$ divides $\frac{N}{M}\varphi - \frac{M_1}{M}$ in $\text{End}(A)$.

(Ia) $f = 1$, $M|(\varphi - 1)^2 \Rightarrow M|(d - 1)$, $M|(M_2 - 2)$. If $N = d - 1$, $M_1 = M_2 - 2$ (the case of elliptic curves), then

$$a = (\varphi - 1)a_x \ (\text{mod } MA) \quad .$$

(Ib) $f = 2$, $M|(\varphi^2 - 1) \Rightarrow M|(d + 1)$, $M|M_2$. If $N = d + 1$, $M_1 = M_2$, then

$$a = -\varphi a_x \ (\text{mod } MA) \quad .$$

(II) $\frac{\varphi^2 - 1}{M} = \frac{M_2}{M}\varphi - \frac{d+1}{M}$ is invertible in $\text{End}(A)$ (assuming $f = 2$): then

$$a = (\frac{M_2}{M}\varphi - \frac{d+1}{M})^{-1}(\frac{N}{M}\varphi - \frac{M_1}{M})\, a_x \ (\text{mod } MA) \quad .$$

In the situation we have in mind, when $M_2 = a_l/l^{r-1}$, $N = l+1$, $M_1 = a_l$, $d = l$, we neither have a "genuine" Euler system, thank to the factor l^{r-1} coming from the Tate twist, nor can we rely on $(\varphi^2 - 1)/M$ being invertible. As a result, we can not obtain in general the precise value of $P_M(n)_\lambda$, but as we shall see in 12.2.3, the loss of information is relatively mild.

10. The Euler system revisited

The complex conjugation $c \in G(K/\mathbf{Q}) = G(K_\lambda, \mathbf{Q}_l)$ acts on $Y_{p^M}(K_\lambda)$, $H^1(K_\lambda, Y_{p^M})$, $H^1(K, Y_{p^{M'}})$ and various other groups. Let $(\ldots)^\pm$ be the corresponding ± 1-eigenspaces. By our assumptions on l, one has $\mu_{p^{M'}}(K_\lambda) = \mu_{p^{M'}}(K_\lambda)^-$ and the eigenspaces $Y_{p^{M'}}(K_\lambda)^\pm$ are free $\mathcal{O}_\mathfrak{p}/p^{M'}$-modules of rank 1. As the pairing $\langle\ ,\ \rangle_{\lambda,M'}$ is c-equivariant, we get non-degenerate pairings

$$\langle\ ,\ \rangle^\pm_{\lambda,M'} : H^1_{ur}(K_\lambda, Y_{p^{M'}})^\pm \times H^1(K_\lambda^{ur}, Y_{p^{M'}})^\pm \longrightarrow \mathbf{Z}/p^{M'} \quad .$$

Note that the map $\phi_{\lambda,M'}$ is c-antiequivariant :

$$\phi_{\lambda,M'} : H^1_{ur}(K_\lambda, Y_{p^{M'}})^\pm \simeq H^1(K_\lambda^{ur}, Y_{p^{M'}})^\mp \quad .$$

Before we establish the main properties of the cohomology classes $P_M(n)$, we need a simple lemma.

Lemma 10.1. There exists a constant M_2 such that p^{M_2} annihilates all cohomology groups $H^1(K_v, A/p^M A)$ for primes $v|N$ in K and $M \geq 0$.

Proof. Let v be such a prime. Then $K_v = \mathbf{Q}_q$ for some rational prime $q|N$. The formula for the local Euler characteristic ([27,5.7]) gives $\sharp H^1(\mathbf{Q}_q, A/p^M A) = (\sharp H^0(\mathbf{Q}_q, A/p^M A))^2$. We are thus reduced to find a bound for the latter group. Let $I = G(\overline{\mathbf{Q}}_q/\mathbf{Q}_q^{ur})$ be the inertia group. We distinguish two possibilities:

(a) $A^I = 0 \Longrightarrow H^0(\mathbf{Q}_q, A \otimes \mathbf{Q}_p/\mathbf{Z}_p)$ is finite .

(b) $A^I \neq 0 \Longrightarrow$ according to Prop. 3.1, $\det(1 - Fr(q)x|A^I) = 1 + q\varepsilon_{f,l}x$. The exact sequence

$$0 \longrightarrow (A^I/p^M A^I)^{\langle Fr(q)\rangle} \longrightarrow H^0(\mathbf{Q}_q, A/p^M A) \longrightarrow H^1(I, A)_{p^M}^{\langle Fr(q)\rangle}$$

then shows that $H^0(\mathbf{Q}_q, A/p^M A)$ is killed by $1 + q\varepsilon_{f,l}$.

Proposition 10.2. Let v be a non-archimedean place of K. Then

(1) $P_M(n) \in H^1(K, Y_{p^M})^{\varepsilon_n}$ with $\varepsilon_n = (-1)^{n-1}\varepsilon_L$.

(2) If $v\nmid N \cdot n \cdot p$, then $P_M(n)_v \in H^1_{ur}(K, Y_{p^M})$.

(3) If $v|N$, then $p^{M_2} P_M(n)_v = 0$.

(4) If $n = m \cdot l$, then

$$\left(\frac{(-1)^{r-1}\varepsilon_n a_l}{p^{M'}} - \frac{l+1}{p^{M'}}\right)P_M(n)_\lambda = \left(\frac{l+1}{p^{M'}}\varepsilon_n - \frac{a_l}{p^{M'}}\right)p^{M_1 d}\phi_{\lambda,M}(P_M(m)_\lambda) \quad ,$$

where $d = 1$ if n is a product of two primes and $d = 0$ otherwise. In particular, if both $(a_l \pm (l+1))/p^{M'}$ are $\wp$-adic units, then

$$P_M(n)_\lambda = u_{l,\varepsilon_n} p^{M_1 d} \phi_{\lambda,M}(P_M(n)_\lambda)$$

with

$$u_{l,\varepsilon_n} = -\varepsilon \frac{a_l \varepsilon - (l+1)}{(-1)^{r-1} a_l \varepsilon - (l+1)} \in (\mathcal{O}_\wp / p^M)^*$$

(note that $u_{l,\varepsilon} = -\varepsilon$ for r odd).

Proof. (1) follows from Prop. 6.2 and the fact that $cD_n = (-1)^n D_n c$.
(2) Both K_n/K and y_n are unramified at v.
(3) Follows from Lemma 10.1.
(4) We apply the discussion in sec.9 first in the particular situation described there, i.e. $x = y_{1,\wp}$, $y = y_{l,\wp}$.Then $P_M(l) = cor_{K_1,K}(z)$. The formula $\mathrm{res}_{G,H_0} = 0$ implies that $P_M(l)_\lambda$ indeed lies in the ramified subspace $H^1(K_\lambda^{ur}, Y_{p^M})$ and the statement of the proposition is equivalent to the key formula of sec.9. If $m > 1$, we apply the same formula to $G = G(\overline{\mathbf{Q}}, K_n)$, $H = G(\overline{\mathbf{Q}}, K_n)$, $x = D_m y_{m,\wp} \in H^1_{\mathrm{cont}}(G, A_\wp)$, $y = D_m y_{n,\wp} \in H^1_{\mathrm{cont}}(H, A_\wp)$.

Corollary 10.3. Assume that both $l + 1 \pm a_l$ divide $p^{M'+k}$ in $\mathcal{O}_\wp$. Then

$$\zeta_{\lambda,M}^{\langle s_\lambda, p^k P_M(n)_\lambda \rangle_{\lambda,M}} = [\alpha_{\lambda,M}(s_\lambda), u_{l,\varepsilon_n} p^{M_1 d + k} \alpha_{\lambda,M}(P_M(n/l)_\lambda]_M$$

for all $s_\lambda \in H^1_{ur}(K_\lambda, Y_{p^M})$ (with $\zeta_{\lambda,M} = (\zeta_{\lambda,M'})^{p^{M_1}}$).

11. Selmer group

The reciprocity law tells us that for all $x, y \in H^1(K, Y_{p^M})$ one has

$$\sum_v \langle x_v, y_v \rangle_{v,M} = 0 \in \mathbf{Z}/p^M \quad ,$$

where the sum is finite, since the local product $\langle x_v, y_v \rangle_{v,M}$ vanishes whenever both x and y are unramified at v.

We have seen that $p^{M_2} P_M(n)$ is unramified at places not dividing $n \cdot p$. We shall now investigate its behaviour at a prime v of K dividing p. Let V be a finite dimensional vector space over $\mathbf{Q}_p$ equipped with a continuous action of $G(\overline{K_v}/K_v)$. In [2], Bloch and Kato defined

$$H^1_f(K_v, V) = \mathrm{Ker}(H^1_{\mathrm{cont}}(K_v, V) \longrightarrow H^1_{\mathrm{cont}}(K_v, V \otimes B_{cris}))$$
$$H^1_g(K_v, V) = \mathrm{Ker}(H^1_{\mathrm{cont}}(K_v, V) \longrightarrow H^1_{\mathrm{cont}}(K_v, V \otimes B_{DR})) \ ,$$

where B_{cris} and B_{DR} are rings originally defined by Fontaine (see also [2]). Put $V = A \otimes \mathbf{Q}$ and define (for $* = f, g$) $H^1_*(K_v, A)$ resp. $H^1_f(K_v, Y_{p^M})$ to be the preimage of $H^1_*(K_v, V)$ in $H^1_{\mathrm{cont}}(K_v, A)$ resp. the image of $H^1_*(K_v, A)$ in $H^1(K_v, Y_{p^M})$.

Lemma 11.1. Let v be a prime of K dividing p. Then
(1) For any finite extension K' of K_v one has $H^1_f(K', A) = H^1_g(K', A)$ and the Abel-Jacobi map over K' factors through $H^1_f(K', A)$.
(2) For all n, $P_M(n)_v$ lies in $H^1_f(K_v, Y_{p^M})$.

Proof. (1) It follows from the de Rham conjecture for open varieties proved in [6] that the Abel-Jacobi map factors through $H^1_g(K', A)$. As $V = A \otimes \mathbf{Q}$ is crystalline (again by [6]), we infere from [13] and Prop. 3.1.3 (where the roles of p and l are interchanged) that the characteristic polynomial of the crystalline Frobenius f on $H^0(K_v, V \otimes B_{cris})$ is equal to $1 - a_p/p^r x + x^2/p$, hence $f - 1$ acts invertibly and since $V^\vee(1) = V$, we get $H^1_f = H^1_g$ from [2;3.8,3.8.4].
(2) H^1_f depends only on the action of the inertia subgroup of $G(\overline{K_v}/K_v)$. As K_n/K is unramified at v, we conclude by (1).

Define the Selmer group $S^{(M)} \subseteq H^1(K, Y_{p^M})$ to consist of those cohomology classes whose localizations lie in $H^1_{ur}(K_v, Y_{p^M})$ for $v \not| N \cdot p$ and in $H^1_f(K_v, Y_{p^M})$ for $v|p$. It is an $\mathcal{O}_\wp$-submodule of $H^1(K, Y_{p^M})$.

Proposition 11.2. (1) The global Abel-Jacobi map factors through

$$\Phi : CH^r(\overline{\overline{X}}_N^{2r-2}/K)_0 \otimes \mathcal{O}_\wp/p^M\mathcal{O}_\wp \longrightarrow S^{(M)} .$$

(2) For all $s \in S^{(M)}$ one has

$$p^{M_2} \sum_{l|n} \langle s_\lambda, P_M(n)_\lambda\rangle_{\lambda, M} = 0 \in \mathbf{Z}/p^M .$$

Proof. (1) Follows from Lemma 4.1 and Lemma 11.1.
(2) According to [2,3.8], $H^1_f(K_v, Y_{p^M})$ is isotropic in $H^1(K_v, Y_{p^M})$ for all v dividing p. The statement follows from Prop. 10.2 and the reciprocity law alluded to at the beginning of this section.

Taking the inductive limit, one gets a map

$$\Phi : CH^r(\overline{\overline{X}}_N^{2r-2}/K)_0 \otimes K_\wp/\mathcal{O}_\wp \longrightarrow S^{(\infty)} .$$

Denote its cokernel by $Ш_{\wp^\infty}$ – the $\wp$–primary part of the Tate-Šafarevič group.

See also [2],[7] and [8] for a general cohomological treatment of Selmer and Tate-Šafarevič groups. Note that our $Ш_{\wp^\infty}$, defined as the factor of the Selmer group by the image of the Abel-Jacobi map can in principle differ from that defined in [2], which is the quotient of the Selmer group by its maximal divisible subgroup.

12. Globalization

We now consider the formula of Cor. 8.2 in the global context. Let $L = K(Y_{p^{M'}}(\overline{\mathbf{Q}}))$ and choose a primitive $p^{M'}$–th root of unity $\zeta_{M'} \in \mu_{p^{M'}}(L)$. For each l with $Fr_{L/\mathbf{Q}}(l) =$

$Fr(c)$ choose some place λ_L of L such that the corresponding embedding $L \hookrightarrow L_{\lambda_L} = K_\lambda$ maps $\zeta_{M'}$ to $\zeta_{\lambda,M'}$ and put $\zeta_M := (\zeta_{M'})^{p^{M_1}}$. This may not always be possible in the case $p|D$, when we might be forced to redefine σ_l. The remedy would be to choose λ_L and $\zeta_{M'}$ first and then define $\zeta_{\lambda,M'}$ and σ_l reversing the above procedure. The choice of λ_L enables one to identify $Y_{p^M}(K_\lambda) \simeq Y_{p^M}(L_{\lambda_L}) = Y_{p^M}(L)$. The maps $\alpha_{\lambda,M}$, $\phi_{\lambda,M}$ have obvious analogues over L_{λ_L}; call them $\alpha_{\lambda_L,M}$ and $\phi_{\lambda_L,M}$ respectively. Consider the restriction map

$$r : H^1(K, Y_{p^M}) \longrightarrow H^1(L, Y_{p^M})^{G(L/K)} = \mathrm{Hom}_{G(L/K)}(G(\overline{\mathbf{Q}}/L), Y_{p^M}(L)) \quad .$$

Define a map, still to be denoted $\alpha_{\lambda_L,M}$,

$$\alpha_{\lambda_L,M} : H^1(L, Y_{p^M}) \longrightarrow Y_{p^M}(L)$$

as the composition of the old $\alpha_{\lambda_L,M}$, the canonical projection from $H^1(L_{\lambda_L}, Y_{p^M})$ to its unramified part and the localization map at λ_L. It is simply the evaluation map at $Fr(\lambda_L)$.

Then the global version of the formula in 8.2 reads as follows:

Lemma 12.1. Let $x, y \in H^1(K, Y_{p^M})$ with $x_\lambda, y_\lambda \in H^1_{ur}(K_\lambda, Y_{p^M})$. Then

$$\zeta_M^{(x,\phi_{\lambda_L,M}(y))_{\lambda,M}} = [\alpha_{\lambda_L,M}(r(x)), \alpha_{\lambda_L,M}(r(y))]_M \quad .$$

Let T_0 be a finite $\mathcal{O}_\mathfrak{p}$−submodule of $H^1(K, Y_{p^M})$. Denote by T its image in $\mathrm{Hom}_{G(L/K)}(G(\overline{\mathbf{Q}}/L), Y_{p^M}(L))$. The evaluation pairing

$$T \times G(L^{ab}/L) \longrightarrow Y_{p^M}(L)$$

is $G(L/\mathbf{Q})$−equivariant (the action on T factors through $G(K/\mathbf{Q})$). Let L_T be the fixed field of the annihilator of T. Then one has a $G(L/\mathbf{Q})$−equivariant map

$$j : G_T = G(L_T/L) \hookrightarrow \mathrm{Hom}(T, Y_{p^M}(L))$$

and a c−equivariant map

$$T \hookrightarrow \mathrm{Hom}_{G(L/K)}(G_T, Y_{p^M}(L)) \quad ,$$

both being injective.

Proposition 12.2. There exist integers $a, b \geq 0$ with the following property: for all $M' \geq M \geq a$ and all finite $\mathcal{O}_\mathfrak{p}$−submodules $T_0 \subset H^1(K, Y_{p^M})$ one has

(1) $p^a\, H^1(K(Y_{p^{M'}})/K, Y_{p^M}) = 0$

(2) $L_T \cap K(Y_{p^\infty}) \subseteq K(Y_{p^{M'+a}})$

(3) For each $g \in G_T^+$ one can find infinitely many primes l inert in K with

$$Fr_{L_T/K}(\lambda) = g, \quad p^{M'} | l + 1 \pm a_l, \quad p^{M'+a+1} \nmid l + 1 \pm a_l$$

(4) $p^b\,\mathrm{Coker}[j : G_T \longrightarrow \mathrm{Hom}(T, Y_{p^M})] = 0$

Proof. (1) Fix an isomorphism $A_\wp \simeq \mathcal{O}_\wp^2$ so that c acts as a diagonal matrix (with eigenvalues ± 1, of course). According to [22,5.7],[19,4.1] and the theory of complex multiplication, the image of $G(\overline{\mathbf{Q}}/K)$ in $Aut_{\mathcal{O}_\wp}(A_\wp) \simeq GL_2(\mathcal{O}_\wp)$ contains the subgroup of scalar matrices

$$D = \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} |x \in 1 + p^a \mathbf{Z}_p \right\}$$

for some a. Then, by Sah's lemma, p^a kills all cohomology groups $H^q(K(Y_{p^{M'}})/K, Y_{p^M})$.
(2) Put $L_n := K(Y_{p^{M'+n}})$. The group D acts trivially on all groups $H_n := G(L_n/L)$.As $a \leq M'$, H_n is abelian for $n \leq M'$. Put $E = L_T \cap L_{M'}$. Then, again by Sah's lemma, p^a kills $\mathrm{Hom}_{G(L/K)}(G_T, G(E/L))$, which proves the claim, as H_n has exact exponent p^n for $a \leq n \leq M'$.
(3) Each element $h \in H_{M'}$ is of the form

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + p^{M'} \begin{pmatrix} A & B \\ C & D \end{pmatrix} \quad (\mathrm{mod}\, p^{2M'}) \quad .$$

If $ch = Fr_{L_{M'}/\mathbf{Q}}(l)$, then $p^{M'+n} \nmid l + 1 \pm a_l$ iff $p^n \nmid A, D$. We know that $G(L_{M'}/E)$ contains $p^a H_{M'}$, hence also

$$\left\{ \begin{pmatrix} 1 + p^{M'}x & 0 \\ 0 & 1 + p^{M'}x \end{pmatrix} |x \in p^a\mathbf{Z}/p^{M'}\mathbf{Z} \right\} \quad .$$

This means that by making a suitable choice of x we may extend every $h \in G_T$ to an element $h' \in G(L_T L_{M'}/L)$ with $p^{a+1} \nmid A, D$. By the Čebotarev density theorem one can find infinitely many primes l with $Fr(l) = ch'$. The statement follows, since each $g \in G_T^+$ is of the form $g = h^{c+1} = (ch)^2$ and $g = Fr_{L_T/K}(\lambda)$ if $Fr_{L_T/\mathbf{Q}}(l) = ch$.
(4) Let $\chi : G(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \{\pm 1\}$ be the quadratic character corresponding to $K/\mathbf{Q}$. Denote by $\rho : G(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow Aut_{\mathcal{O}_\wp}(A_\wp)$ the Galois action on $A_\wp$. Then $\rho \otimes \chi$ is the Galois representation associated to the modular form $f \otimes \chi$. Let Z_M be the subalgebra of scalar matrices in $M_2(\mathcal{O}_\wp/p^M)$.

Lemma 12.3. There exist integers $m, n \geq 0$ with the following property: let V be one of $A_\wp/p^M$ or $(A_\wp/p^M) \otimes \chi$. If V_1 resp. V_2 is a $G(\overline{\mathbf{Q}}/\mathbf{Q})$–submodule resp. factormodule of V with $V_1 \not\subseteq \wp V$, then

$$p^m\,(V/V_1) = 0, \quad p^n\,(\mathrm{Hom}_{G(\overline{\mathbf{Q}}/\mathbf{Q})}(V_1, V_2)/Z_M) = 0 \quad .$$

Proof of the lemma. The existence of m follows from the fact that ρ and $\rho \otimes \chi$ are irreducible ([22,2.3]): we may work with $V_0 = A_\wp$ or $V_0 = A_\wp \otimes \chi$ and the pull-backs of V_1,V_2 to V_0 at this point; if there was a sequence of $V_1 \subseteq V_0$ with m tending to infinity, we could choose a subsequence converging to an invariant subspace in V_0, a contradiction.

To establish the existence of n, we first note that $p^{m+k+1}V \subseteq V_2 \subseteq p^k V$ for some k. Then the kernels and cokernels of both maps

$$\mathrm{Hom}_G(V_1, V_2) \longrightarrow \mathrm{Hom}_G(V_1, V/p^k V) \longleftarrow \mathrm{Hom}_G(V, V/p^k V)$$

are killed by p^{m+1}, where we have put $G = G(\overline{\mathbf{Q}}/\mathbf{Q})$. But

$$\mathrm{Hom}_G(V, V/p^k V) = \mathrm{Hom}_G(V_0/p^{M-k}, V_0/p^{M-k})$$

and the existence of n again follows from the irreducibility of V_0.

We now continue the proof of 12.2. As a $G(K/\mathbf{Q})$-module,

$$T = \bigoplus_{i=1}^{k} T_i/\wp^{n_i} \quad ,$$

where each T_i is either $\mathcal{O}_\mathfrak{p}$ or $\mathcal{O}_\wp \otimes \chi$. Then

$$V := \mathrm{Hom}(T, Y_{p^M}) = \bigoplus_{i=1}^{k} V_i$$

with $V_i = A_\mathfrak{p}/\wp^{n_i}$ or $(A_\mathfrak{p}/\wp^{n_i}) \otimes \chi$. We know that $W = G_T$ is an $\mathcal{O}_\mathfrak{p}[G(L/\mathbf{Q})]$-submodule of V satisfying the following property:
(P) The composed map $T \longrightarrow \mathrm{Hom}(V, Y_{p^M}) \longrightarrow \mathrm{Hom}(W, Y_{p^M})$ is injective.

We shall prove by induction on k that V/W is killed by p^c with $c = \max(m, n)$. For $k = 1$ this follows from the definition of m. Let now $k \geq 2$ and assume that we know that p^c kills V/W in all situations with k replaced by $k-1$. Let

$$\pi : V \longrightarrow V' := \bigoplus_{i=1}^{k-1} V_i$$

be the projection on the first $k-1$ factors. Then $W \cap \mathrm{Ker}(\pi)$ is isomorphic to its projection on V_k, to be called W_k, and

$$\pi(W) =: W' = \oplus W_i$$

with $W_i \subseteq V_i$ (for $1 \leq i \leq k-1$) satisfying $W_i \not\subseteq \wp V_i$ due to the property (P). "Inverting" the projection $\pi|_W$ we get a G-map

$$f : W' \longrightarrow V_k/W_k$$

with $\mathrm{Im}(f)$ not contained in $\wp(V_k/W_k)$ again by (P). According to the lemma,

$$f(w_1, \ldots, w_{k-1}) = a_1 w_1 + \ldots + a_{k-1} w_{k-1}$$

modulo p^n-torsion. The condition (P) then implies that p^n must kill V_k/W_k ; otherwise a suitable multiple of $(a_1, \ldots, a_{k-1}, -1) \in T$ would be trivial on W: a contradiction. As

$W' \oplus W_k \subseteq W$ and p^c kills V'/W' by induction hypothesis, we get $p^c(V/W) = 0$ as claimed.

Remark. It follows from the proof that one can take $a = b = 0$ in the following two cases:
(1) If f is a CM-form (as $p \nmid N$ and K is not the field of complex multiplication, the Galois group $G(L/K)$ is equal to the normalizer of a Cartan subgroup).
(2) If in the non-CM case the Galois group $G(L/\mathbf{Q})$ is as big as possible, i.e. equal to $GL_2(\mathcal{O}_\wp/p^{M'})$, and p is unramified in F.

13. Main theorem.

We are now ready to prove our main result. Recall that $f \in S_{2r}^{\text{new}}(\Gamma_0(N))$ is a newform of weight $2r \geq 4$, p a prime not dividing $N\varphi(N)(2r-2)!$ ($\times 3$ if $N = 1, 2$), F the extension of $\mathbf{Q}$ generated by the Hecke eigenvalues of f, $\mathcal{O}_F$ the ring of integers of F, $\wp$ a prime of $\mathcal{O}_F$ over p, K an imaginary quadratic field in which all primes dividing N split, A the free $\mathcal{O}_F \otimes \mathbf{Z}_p-$module of rank 2 carrying the $p-$adic realization of the motive $M(f)$ satisfying $L(M(f), s) = L(f, s + r)$, $A_\wp$ the localization of A at $\wp$, $Y = \overline{\overline{X}}_N^{2r-2}$ the non-singular compactification of the $(2r-1)-$dimensional Kuga-Sato variety over the modular curve M_N, $\varepsilon_L = \pm 1$ the sign in the functional equation of the $L-$series $L(f, s)$,

$$\Phi : CH^r(Y/K)_0 \otimes \mathcal{O}_\wp \longrightarrow H^1_{\text{cont}}(K, A_\wp)$$

the $\wp-$localization of the $f-$component of the Abel-Jacobi map. Let

$$y_0 := \text{cor}_{K_1,K}(y_{1,\wp}) \in H^1_{\text{cont}}(K, A_\wp) \quad .$$

Theorem 13.1. Suppose that y_0 is not torsion. Then $\text{Ш}_{\wp^\infty}$ is finite and

$$(\text{Im}(\Phi))^{\varepsilon_L} \otimes F_\wp = 0, \quad (\text{Im}(\Phi))^{-\varepsilon_L} \otimes F_\wp = F_\wp \cdot y_0 \quad .$$

Proof. As before, we pick a sufficiently large $M >> 0$ and put $M' = M + M_1$. We shall give bounds for the Selmer group introduced in sec.11. According to [29,2.1.Cor] and [27,6.2.Th.7], $\varprojlim_M S^{(M)}$ is a finitely generated $\mathbf{Z}_p-$module. Put, as before, $L = K(Y_{p^{M'}})$ and for $m \geq 0$ let Λ_m be the set of primes l inert in K satisfying

$$p^{M'} | l + 1 \pm a_l, \quad p^{M'+m+1} \nmid l + 1 \pm a_l \, .$$

Put $T_0 = S^{(M)}$ and let T be its image under the restriction map

$$r : H^1(K, Y_{p^M}) \longrightarrow H^1(L, Y_{p^M}) \quad .$$

If n is a product of distinct primes from Λ_m we define

$$u(n) := r(P_M(n)) \in H^1(L, Y_{p^M}).$$

By hypothesis, y_0 is not torsion in $H^1_{\mathrm{cont}}(K, A_\wp)$. Then, according to [29,2.1], there exists $M_0 \geq 0$ such that y_0 is not divisible by p^{M_0+1} in $H^1_{\mathrm{cont}}(K, A_\wp)$/torsion (the torsion, of course, being killed by p^{M_1}). Denote $e(x) = \min\{m | p^m x = 0\}$ whenever x is an element of an abelian group of the group itself. In this notation,

$$e(P_M(1)) = M - M_0$$
$$e(u(n)) \geq e(P_M(n)) - a.$$

Consider first T^{ϵ_L}. Choose $f_1^{\pm} : T^{\pm} \longrightarrow Y^{\pm}_{p^M}$ satisfying

$$e(f_1^{\epsilon_L}) = e(\mathrm{Hom}(T^{\epsilon_L}, Y^{\epsilon_L}_{p^M})) = e(T^{\epsilon_L})$$
$$e(f_1^{-\epsilon_L}(u(1))) = e(u(1)) \quad (\geq M - M_0 - a).$$

According to Prop. 12.2, one can find $l \in \Lambda_a$ with

$$\alpha^{\pm}_{\lambda_L, M} = p^b f_1^{\pm} \quad .$$

Let $t \in T^{\epsilon_L}$. The reciprocity law (Prop. 11.2.2) yields

$$\langle t_\lambda, p^{M_2} P_M(l)_\lambda \rangle_{\lambda, M} = 0 \quad .$$

As $l \in \Lambda_a$, Cor. 10.3 tells us that

$$[\alpha_{\lambda_L, M}(t), p^{M_2+a+1} \alpha_{\lambda_L, M}(u(1)_\lambda)]_M = 1 \quad ,$$

hence

$$[f_1^{\epsilon_L}(t), p^{M_2+a+2b+1} f_1^{-\epsilon_L}(u(1))]_M = 1 \quad ,$$

which implies that

$$p^{M_0+M_2+2a+2b+1} T^{\epsilon_L} = 0 \quad \Longrightarrow p^{M_0+M_2+3a+2b+1} (S^{(M)})^{\epsilon_L} = 0.$$

Let us now turn to $T^{-\epsilon_L}$. We can find $f_2^{\pm} : T^{\pm} \longrightarrow Y^{\pm}_{p^M}$ satisfying

$$e(f_2^{\epsilon_L}(u(l))) = e(u(l))$$
$$e(f_2^{-\epsilon_L} \bmod \mathcal{O}_\wp \cdot f_1^{-\epsilon_L}) = e(\mathrm{Hom}(T^{-\epsilon_L}, Y^{-\epsilon_L}_{p^M}) / \mathcal{O}_\wp \cdot f_1^{-\epsilon_L}) = e(\mathrm{Ker}(f_1^{-\epsilon_L})).$$

According to our choice of l we have $e(u(l)) \geq e(P_M(l)) - a \geq e(P_M(l)_\lambda) - a \geq e(P_M(1)_\lambda) - 2a = e(p^b f_1^{-\epsilon_L}(u(1))) - 2a = e(u(1)) - 2a - b \geq M - M_0 - 3a - b$. We can again find $l' \in \Lambda_a - \{a\}$ with $p^b f_2 = \alpha_{\lambda'_L, M}$

Let $t \in \mathrm{Ker}(f_1^{-\epsilon_L}) \subseteq T^{-\epsilon_L}$. Then the reciprocity law

$$\sum_v \langle t_v, P_M(ll')_v \rangle_{v, M} = 0$$

implies by Lemma 12.1

$$[p^b f_2^{-\varepsilon_L}(t_{\lambda'}), p^{b+M_1+M_2+a+1} f_2^{\varepsilon_L}(u(l))]_{\lambda',M} = 1 ,$$

hence the kernel of

$$f_1^{-\varepsilon_L} : T^{-\varepsilon_L} \longrightarrow Y_{p^M}^{-\varepsilon_L}$$

is killed by $p^{M_0+M_1+M_2+4a+3b+1}$.

We know that $u(1) = p^{M_0}x + t$ with $x, t \in \mathrm{Im}(\Phi)$ and t killed by p^{M_1}. This implies that (for sufficiently big M)

$$e(f_1^{-\varepsilon_L}(x)) = e(x) \geq M - a.$$

In the exact sequence

$$0 \longrightarrow \frac{\mathrm{Ker}(f_1^{-\varepsilon_L})}{sth.} \longrightarrow \frac{T^{-\varepsilon_L}}{\mathcal{O}_\mathfrak{p} \cdot t + \mathcal{O}_\mathfrak{p} \cdot x} \xrightarrow{f_1^{-\varepsilon_L}} \frac{Y_{p^M}^{-\varepsilon_L}}{\mathcal{O}_\mathfrak{p} \cdot f_1^{-\varepsilon_L}(t) + \mathcal{O}_\mathfrak{p} \cdot f_1^{-\varepsilon_L}(x)}$$

the first term is killed by $p^{M_0+M_1+M_2+4a+3b+1}$ and the last one by p^a. This shows that

$$p^{M_0+M_1+M_2+6a+3b+1}(S^{(M)})^{-\varepsilon_L}/(\mathcal{O}_\mathfrak{p} \cdot t + \mathcal{O}_\mathfrak{p} \cdot x) = 0.$$

Letting M tend to infinity, we see that

$$p^c S^{(\infty)}/((F_\mathfrak{p}/\mathcal{O}_\mathfrak{p}) \cdot y_0) = 0$$

for some c. As the image of Φ in $S^{(\infty)}$ is divisible, this proves the statement about $\mathrm{Im}(\Phi)$, shows that $Ш_{\mathfrak{p}^\infty}^{\varepsilon_L} = (S^{(M)})^{\varepsilon_L}$ and that $(S^{(M)})^{-\varepsilon_L}/(\mathcal{O}_\mathfrak{p} \cdot x + \mathcal{O}_\mathfrak{p} \cdot t)$ surjects on $Ш_{\mathfrak{p}^\infty}^{-\varepsilon_L}$ for sufficiently big M. Theorem follows.

Remark. The bounds given in the course of the proof are by no means ideal. The power p^1 is not necessary if p is unramified in F and we suspect that the factor p^{M_1} could be eliminated by a more detailed analysis of Kolyvagin's corestriction. If the same could be done also for the remaining parasitic factor p^{M_2}, then in a situation with $a = b = 0$ (cf. remark at the end of sec.12) the methods of [17] would probably apply in a completely formal way and one could describe the structure of the Tate-Šafarevič group $Ш_{\mathfrak{p}^\infty}$ solely in terms of the classes $P_M(n)$.

Remark. It would be desirable to find a criterion to check whether y_0 is torsion. In the weight 2 case, such a criterion is provided by the theorem of Gross and Zagier [10], which asserts that the value of the first derivative of the corresponding $L-$series at 1 is a multiple of the height of y_0. In conjunction with [3], the result of Gross and Zagier suggests that the same is true also in the higher weight case. Unfortunately, our understanding of the relationship between the Abel-Jacobi map and the real-valued height pairing is unsatisfactory. We hope that $p-$adic methods will have some bearing on this problem: one may indeed define a $p-$adic height pairing which factors through the Abel-Jacobi map (this will be discussed in a future paper) and the hope is that a p-adic version of the Gross-Zagier theorem, relating the p-adic height of y_0 to the derivative of a p-adic L-function, is valid in our situation as well (the weight two case is treated in [20]). Note that In [24] C.Schoen investigates the transcendental Abel-Jacobi map on a threefold associated to the unique form $f \in S_4(\Gamma_0(9))$, which provides the simplest situation when the hypothetic criterion could prove useful.

References

1. Atkin, A.O.L., Lehner, J.: Hecke operators on $\Gamma_0(m)$, Math.Ann. **185** , 134-160 (1970)

2. Bloch, S., Kato, K.: L-functions and Tamagawa numbers of motives, to appear in the volume in honor of A.Grothendieck

3. Brylinski, J.-L.: Heights for local systems on curves, Duke Math. J. **59** , 1-26 (1989)

4. Carayol, H.: Sur les représentations l-adiques attachées aux formes modulaires de Hilbert, Ann. Sci. ENS **19** , 409-468 (1986)

5. Deligne, P.: Formes modulaires et représentations l-adiques; Séminaire Bourbaki 1968/69 exp.355, Lect.Notes Math. **179** , pp.139-172, Berlin-Heidelberg-New York: Springer 1971

6. Faltings, G.: Crystalline cohomology and p-adic Galois representations, preprint 1988

7. Flach, M.: A generalization of the Cassels-Tate pairing, preprint 1990

8. Greenberg, R.: Iwasawa Theory for p-adic Representations, In: Algebraic Number Theory (in honor of K.Iwasawa), Advanced Studies in Pure Mathematics **17** , pp. 97-137, Academic Press, 1989

9. Gross, B.: Kolyvagin's work on modular elliptic curves, to appear in Proc. Durham Conference on Arithmetic and L-functions 1989

10. Gross, B., Zagier, D.: Heegner points and derivatives of L-series, Invent. Math. **84** , 225-320 (1986)

11. Jannsen, U.: Continuous Étale cohomology, Math. Ann. **280** , 207-245 (1988)

12. Jannsen, U.: Mixed Motives and Algebraic K-Theory, Lect. Notes Math. **1400** , Berlin-Heidelberg-New-York: Springer 1990

13. Katz, N., Messing, W.: Some consequences of the Riemann hypothesis for varieties over finite fields, Invent. Math. **23** , 73-77 (1974)

14. Kolyvagin, V.A.: Finiteness of $E(\mathbf{Q})$ and $Ш(E, \mathbf{Q})$ for a subclass of Weil curves, Izv. Akad. Nauk SSSR, Math.series, **52** , No.3, 522-540 (1988)

15. Kolyvagin, V.A.: On Mordell-Weil and Šafarevič-Tate groups for Weil elliptic curves, Izv. Akad. Nauk SSSR, Math.series, **52** , No.6, 1154-1180 (1988)

16. Kolyvagin, V.A.: Euler systems, to appear in the volume in honor of A.Grothendieck

17. Kolyvagin, V.A.: On the structure of Šafarevič-Tate groups, preprint

18. Milne, J.S.: Étale cohomology, Princeton: Princeton Univ. Press 1980

19. Momose, F.: On the l-adic representations attached to modular forms, J. Fac. Sci. Univ. Tokyo, Sec.IA, **28** , 89-109 (1981)

20. Perrin-Riou, B.: Points de Heegner et dérivées de fonctions L p-adiques, Invent. Math. **89** , 455-510 (1987)

21. Perrin-Riou, B.: Travaux de Kolyvagin et Rubin, Sém.Bourbaki 1989/90, exp. 717

22. Ribet, K.: Galois representations attached to eigenforms with nebentypus, In: Modular Functions in one Variable V (ed.J.-P.Serre, D.B.Zagier), Lect. Notes Math. **601** , pp.17-52, Berlin-Heidelberg-New York: Springer 1977

23. Schoen, C.: Complex multiplication cycles on elliptic modular threefolds, Duke Math.J. **53** , No.3, 771-794 (1985)

24. Schoen, C.: Complex multiplication cycles and a conjecture of Beilinson and Bloch, preprint 1990

25. Schoen, C.: On the computation of the cycle class map for nullhomologous cycles over the algebraic closure of a finite field, preprint 1990

26. Scholl, A.J.: Motives for modular forms, Invent. Math. **100** , 419-430 (1990)

27. Serre, J.-P.: Cohomologie Galoisienne, Lect. Notes Math. **5** , Berlin-Göttingen-Heidelberg-New York: Springer 1964

28. Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions, Princeton Univ. Press: 1971

29. Tate, J.: Relations between K_2 and Galois Cohomology, Invent. Math. **36** , 257-274 (1976)

SGA $4\frac{1}{2}$: Cohomologie étale, Lect. Notes Math. **569** , Berlin-Heidelberg-New York: Springer 1977