On the Finiteness of Ш for Motives Associated to Modular Forms

Amnon Besser[1]

Received: February 1, 1996
Revised: January 15, 1997

Communicated by Don Blasius

Abstract. Let f be a modular form of even weight on $\Gamma_0(N)$ with associated motive $\mathcal{M}_f$. Let K be a quadratic imaginary field satisfying certain standard conditions. We improve a result of Nekovář and prove that if a rational prime p is outside a finite set of primes depending only on the form f, and if the image of the Heegner cycle associated with K in the p-adic intermediate Jacobian of $\mathcal{M}_f$ is not divisible by p, then the p-part of the Tate-Šafarevič group of $\mathcal{M}_f$ over K is trivial. An important ingredient of this work is an analysis of the behavior of "Kolyvagin test classes" at primes dividing the level N. In addition, certain complications, due to the possibility of f having a Galois conjugate self-twist, have to be dealt with.

1991 Mathematics Subject Classification: 11G18, 11F66, 11R34, 14C15.

1 Introduction

Let f be a new form of even weight $2r$ for the group $\Gamma_0(N)$, let $\mathcal{M}_f$ be the r-th Tate twist of the motive associated to f by Jannsen [Jan88b] and Scholl [Sch90]. For all but a finite number of primes p there is a canonical choice of free $\mathbb{Z}_p$-lattice $T_p(\mathcal{M}_f)$ with a continuous action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $T_p(\mathcal{M}_f)\otimes\mathbb{Q}$ is the p-adic realization of $\mathcal{M}_f$. In [Nek92], Nekovář showed that under certain assumption one could apply the Kolyvagin method of Euler systems to $\mathcal{M}_f$ and obtained, among other things, the following result:

Theorem 1.1. *Let K be a quadratic imaginary field of discriminant D in which all primes dividing N split, and let p be a prime not dividing $2N$. Let $T_p(\mathcal{M}_f)$ be the p-adic realization of $\mathcal{M}_f$ and let $P(1)$ be the image in $H^1(K,T_p(\mathcal{M}_f))$ of the Heegner cycle associated with K under the p-adic Abel-Jacobi map. If $P(1)$ is not torsion, then the p-part of the Tate-Šafarevič group of $\mathcal{M}_f$ over K, $\text{Ш}_p(\mathcal{M}_f/K)$, is finite.*

[1]Partially supported by an NSF grant

We remark that in [Nek92] there is a stronger condition on p for the theorem to hold which is removed in a remark on the last paragraph of [Nek95].

The purpose of this note is to give the following refinement of the above result:

THEOREM 1.2. *There is a finite set of primes $\Psi(f)$, depending only on f, such that for a prime p not in $\Psi(f)$ the following holds: for K as in theorem 1.1, if $P(1)$ is not torsion, then $p^{2\mathcal{I}_p}\text{Ш}_p(\mathcal{M}_f/K)=0$, where $\mathcal{I}_p$ is the smallest non-negative integer such that the reduction of $P(1)$ to $H^1(K,T_p(\mathcal{M}_f)/p^{\mathcal{I}_p+1})$ is not 0. In particular, if $\mathcal{I}_p=0$, then $\text{Ш}_p(\mathcal{M}_f/K)$ is trivial*

Remark 1.3. 1. The Tate-Šafarevič group discussed here is not exactly the same as the one that appears in [Nek92]. The main difference is in the local conditions at the primes of bad reduction. Nekovář makes no conditions at these primes, which is why Ш comes out too big. The local condition that we use is the one defined by Bloch and Kato. The analysis of this local condition is one of the main ingredient of this work.

2. The finite set $\Psi(f)$ contains the primes dividing $2N$ and primes with an exceptional image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(T_p(\mathcal{M}_f))$ (see definition 6.1).

It is our hope that the methods used here allow a complete analysis of the structure of $\text{Ш}_p(\mathcal{M}_f/K)$ in terms of various Kolyvagin classes following [Kol91, McC91]. Notice however that some difficulties are already visible in the fact that the power of p annihilating Ш is $2\mathcal{I}_p$ whereas in the elliptic curves case one gets annihilation by $p^{\mathcal{I}_p}$. This difficulty is caused by the more complicated structure of the image of the Galois representation associated to $\mathcal{M}_f$ (see remark 6.5).

A natural problem raised by theorem 1.2 is to bound the numbers $\mathcal{I}_p$. In particular, one would hope that $\mathcal{I}_p=0$ for all but a finite number of p's. This would show the finiteness of $\text{Ш}(\mathcal{M}_f/K)$ except for possible infinite contribution at primes dividing $2N$. It is useful to compare the situation to the case where the weight of f is 2, where the triviality of $\text{Ш}_p(\mathcal{M}_f/K)$ for almost all p has been previously established in [KL90]. In that case, the class $P(1)$ correspond to a point on the Jacobian of a modular curve, and $\mathcal{I}_p=0$ for almost all p whenever $P(1)$ is of infinite order. This last result uses essentially the injectivity of the Abel-Jacobi map (up to torsion) and the Mordell-Weil theorem, neither of which is known for greater than 1 codimension cycles. One possible way of getting some control over the indices $\mathcal{I}_p$ could be to use the results of Nekovář on the p-adic heights of Heegner cycles: According to [Nek95, corollary to theorem A] one has the equality $h(P(1),P(1))=\Omega_{f\otimes K,p}L_p'(f\otimes K,r)$ where $h(\ ,\ )$ is the p-adic height pairing defined by Nekovář and Perrin-Riou, $L_p(f\otimes K)$ is a p-adic L-function of f over K defined by Nekovář and $\Omega_{f\otimes K,p}$ is some p-adic period. The p-adic height of elements of $H^1_f(K,T)$ has a bounded denominator (it is integral for universal norms from a $\mathbb{Z}_p$ extension) and so the estimation of $\mathcal{I}_p$ is reduced to giving estimates on the p-divisibility of $L_p'(f\otimes K,r)$.

Another problem is to handle primes dividing $2N$. The difficulty here is that we do not understand yet the image of the Abel-Jacobi map with $\mathbb{Q}_p$ coefficients for varieties over an extension of $\mathbb{Q}_p$ and with bad reduction. Recently there has been some progress on that problem [Lan96] but the results do not yet cover the cases we need.

Here is a short description of the contents. After a few preliminary remarks and definitions in section 2 we will recall in section 3 some of the main points of [Nek92].

For brevity this will be far from a full account. We merely attempt to indicate the main changes that need to be made and explain where the local conditions at the bad primes come into play. These conditions are then discussed in sections 4 and 5. We then give the proof of the main theorem in section 6. It would have been nice to skip this section or make it shorter and refer instead to the corresponding sections in [Nek92]. However, it turns out that to get the result we want under weaker conditions than the ones stated there (see the remark in loc. cit. page 121), the proof has to be modified somewhat. I have therefore chosen to give the full details of the proof. In the appendix we give a proof of a Hochschild-Serre spectral sequence for continuous group cohomology which is used in section 5.

As the reader will notice, this work is closely related to [Nek92]. Familiarity with that paper is helpful for reading this one but not necessary, as one may choose to trust the results quoted from there.

I would like to thank Wayne Raskind, Don Blasius, Haruzo Hida, Dinakar Ramakrishnan and Jan Nekovář for helpful discussions and remarks. I would also like to thank Farshid Hajir for encouraging me to write down my ideas on this subject. Finally, I would like to thank the referee for some useful corrections and remarks.

2 Preliminaries

For this work, a motive is effectively equivalent to its set of realizations. We only need the p-adic realizations for the different p's and a brief mention of the Betti realization. Thus, a motive $\mathcal{M}$ has a Betti realization which is a $\mathbb{Q}$-vector space $V_\mathbb{Q}$ and p-adic realizations which are continuous representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on $V_p = V_\mathbb{Q} \otimes \mathbb{Q}_p$ for the different p's. By choosing a suitable $\mathbb{Z}$-lattice $T_\mathbb{Z}$ in $V_\mathbb{Q}$ we have in each V_p an invariant $\mathbb{Z}_p$-lattice $T_p = T_\mathbb{Z} \otimes \mathbb{Z}_p$. The p-part of the Tate-Šafarevič group of $\mathcal{M}$ depends on the choice of T_p but statements about the p-part for all but a finite number of p are clearly independent of the choice of $T_\mathbb{Z}$. In the cases we will be considering there is a standard choice (a Tate twist of a piece of the étale cohomology of a suitable Kuga-Sato variety, see [Nek92, §3]) and the theorem will be proved for this choice. To be more precise:

$$T_p \otimes \mathbb{Q}_p \cong \rho_{f,p} \otimes \mathbb{Q}_p(r), \tag{2.1}$$

where $\rho_{f,p}$ is the standard p-adic representation associated to f.

To define the p-part of Ш, we start with the free $\mathbb{Z}_p$-module of finite rank, $T = T_p(\mathcal{M})$, on which $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts continuously. Let $V = T \otimes \mathbb{Q}_p$ and $A = V/T$, so that there is a short exact sequence:

$$0 \to T \xrightarrow{i} V \xrightarrow{\mathrm{pr}} A \to 0.$$

Let ℓ be a prime, possibly ∞. Let F be a finite extension of $\mathbb{Q}_\ell$ and let $\bar{F}$ be an algebraic closure of F. In [BK90, (3.7.1)] Bloch and Kato define the finite part H^1_f of the first Galois cohomology of F with values in V, T or A as follows:

$$\begin{aligned} H^1_f(F,V) &:= \operatorname{Ker} H^1(F,V) \xrightarrow{\text{res}} H^1(F^{ur},V) \text{ when } \ell \neq p; \\ H^1_f(F,V) &:= \operatorname{Ker} H^1(F,V) \to H^1(F, V \otimes B_{cris}) \text{ when } \ell = p; \\ H^1_f(F,T) &:= i^{-1} H^1_f(F,V); \\ H^1_f(F,A) &:= \operatorname{Im} H^1_f(F,V) \hookrightarrow H^1(F,V) \xrightarrow{\text{pr}} H^1(F,A), \end{aligned}$$

where F^{ur} is the maximal unramified extension of F. The ring B_{cris} is defined by Fontaine. We will not need to use the definition directly in the case $\ell = p$.

Let now K be a number field. When B is a $\operatorname{Gal}(\bar{\mathbb{Q}}/K)$-module we have restriction maps for each place v of K: $H^1(K,B) \to H^1(K_v,B)$. When $x \in H^1(K,B)$ we will denote its restriction to $H^1(K_v,B)$ by x_v. The p-part of the Selmer group of $\mathcal{M}$ over K is now defined as

$$\operatorname{Sel}_p(\mathcal{M}/K) := \operatorname{Ker} H^1(K,A) \longrightarrow \prod_v H^1(K_v,A)/H^1_f(K_v,A),$$

where the product is over all places v of K. We also define

$$H^1_f(K,V) := \operatorname{Ker} H^1(K,V) \longrightarrow \prod_v H^1(K_v,V)/H^1_f(K_v,V).$$

The p-part of the Tate-Šafarevič group of $\mathcal{M}$ over K is the quotient of $\operatorname{Sel}_p(\mathcal{M}/K)$ by the image of $H^1_f(K,V)$. Nekovář defines the same group as the quotient of the Selmer group by the image of an appropriate Abel-Jacobi map. It follows easily from his result that in the case of interest here his definition coincides with the one we are using.

Let A_{p^k} be the p^k-torsion subgroup of A and let $\operatorname{red}_{p^k} : T \to A_{p^k}$ be the reduction mod p^k. We will use the same notation for the reduction map $A_{p^n} \to A_{p^k}$ which is given by multiplication by p^{n-k} when $n > k$ and we notice that all reduction maps commute with each other. We will abuse the notation further to denote by red_{p^k} the maps induced by the reduction on Galois cohomology groups.

To simplify the notation slightly, we assume the following:

ASSUMPTION 2.1. There is a Galois invariant bilinear pairing $T \times T \to \mathbb{Z}_p(1)$ such that the induced pairings on $T/p^k \cong A_{p^k}$ are non-degenerate for all k.

This condition is satisfied in the case we are considering by [Nek92, proposition 3.1]. It is mostly made at this point so that we do not have to consider both T and its Kummer dual. We have the following well known results:

PROPOSITION 2.2. *The pairing above induces local Tate pairings, for each place v of K:*

$$\begin{gathered} H^1(K_v,T) \times H^1(K_v,A) \to H^1(K_v, \mathbb{Q}_p/\mathbb{Z}_p(1)) \cong \mathbb{Q}_p/\mathbb{Z}_p; \\ H^1(K_v,A_{p^k}) \times H^1(K_v,A_{p^k}) \to H^1(K_v, \mathbb{Z}/p^k(1)) \cong \mathbb{Z}/p^k, \end{gathered}$$

which are both perfect and will be denoted by $\langle\ ,\ \rangle_v$ (for the torsion coefficients case see [Mil86, Chap. I, Cor. 2.3]*). The following properties hold:*

1. [BK90, Proposition 3.8] *The pairing* $\langle\ ,\ \rangle_v$ *makes* $H^1_f(K_v,T)$ *and* $H^1_f(K_v,A)$ *exact annihilators of each other (this is true even in the case* $p|v$*).*

2. *If* x *and* y *belong to* $H^1(K,A_{p^k})$ *then*

$$\sum_v \langle x_v, y_v\rangle_v = 0,$$

where the sum is over all places v *of* K *but is in fact a finite sum.*

We remark that it is possible to neglect the infinite places in all the discussions if we assume that $p \neq 2$ or if K is totally imaginary. Both conditions will in fact hold.

DEFINITION 2.3. Let F be a local field. We define $H^1_f(F,A_{p^k})$ to be the preimage in $H^1(F,A_{p^k})$ of $H^1_f(F,A)$. We define $H^1_{f^*}(F,A_{p^k})$ to be the annihilator of $H^1_f(F,A_{p^k})$ in $H^1(F,A_{p^k})$ under local Tate duality. We will call the classes in $H^1_{f^*}(F,A_{p^k})$ the *dual finite classes.* We define the singular part of the cohomology as

$$H^1_{sin}(F,A_{p^k}) = H^1(F,A_{p^k})/H^1_{f^*}(F,A_{p^k})$$

(this definition is due to Mazur). If $x \in H^1(F,A_{p^k})$ we denote by x_{sin} its projection on the singular part. When K is a number field we let

$$\mathrm{Sel}(K,A_{p^k}) := \mathrm{Ker}\, H^1(K,A_{p^k}) \longrightarrow \prod_v H^1(K_v,A_{p^k})/H^1_f(K_v,A_{p^k}).$$

LEMMA 2.4. *The group* $H^1_{f^*}(F,A_{p^k})$ *is the image of* $H^1_f(F,T)$ *under the canonical map* $H^1(F,T) \to H^1(F,A_{p^k})$*. There is a perfect pairing, induced by* $\langle\ ,\ \rangle_v$*:*

$$\langle\ ,\ \rangle_v : H^1_f(F,A_{p^k}) \times H^1_{sin}(F,A_{p^k}) \to \mathbb{Z}/p^k$$

Proof. This is a formal consequence of the preceding definition and proposition 2.2. □

For a $\mathrm{Gal}(\bar F/F)$-module B and $\bar F \supset K \supset F$ we denote $B^{\mathrm{Gal}(\bar F/K)}$ by $B(K)$. If B' is a subset of B we denote by $F(B)$ the fixed field of the subgroup of $\mathrm{Gal}(\bar F/F)$ fixing B'.

3 METHOD OF PROOF

The Kolyvagin method, as applied to $\mathcal{M}_f$ by Nekovář, works as follows: Let f have q-expansion $f = \sum a_n q^n$. Let E be the field generated over $\mathbb{Q}$ by the a_i. It is known that E is a totally real finite extension of $\mathbb{Q}$. Let $\mathcal{O}_E$ be the ring of integers of E. As explained in [Nek92, Proposition 3.1], the invariant lattice $T_p(\mathcal{M}_f)$ can be taken to be a free rank 2 module over $\mathcal{O}_E \otimes \mathbb{Z}_p = \prod \mathcal{O}_{E_\mathfrak{p}}$, where the product is over all primes $\mathfrak{p}$ of E dividing p. To prove the result about Ш it is sufficient to choose one such prime $\mathfrak{p}$ and consider only the direct summand of $T_p(\mathcal{M}_f)$ corresponding to $\mathfrak{p}$. This summand will be denoted $T_{f,\mathfrak{p}}$. For the rest of this section we fix $T = T_{f,\mathfrak{p}}$ and let as usual $V = T \otimes \mathbb{Q}_p$ and $A = V/T$.

As the Tate-Šafarevič group is (obvious with the above definition) p-torsion, we wish to show that its part killed by p^k is killed by the fixed power $p^{2\mathcal{I}_p}$ for each k. We look at the short exact sequence

$$0 \to A_{p^k} \to A \xrightarrow{p^k} A \to 0$$

and the induced sequence on cohomology

$$0 \to A(K)/p^k \to H^1(K, A_{p^k}) \to H^1(K, A)_{p^k} \to 0$$

The conditions we will impose on the prime p imply, as we will see in part 2 of proposition 6.3, that $A(K) = 0$, and hence $H^1(K, A)_{p^k} \cong H^1(K, A_{p^k})$. It follows that the preimage in $H^1(K, A_{p^k})$ of $\mathrm{Sel}_p(T/K)$ is $\mathrm{Sel}(K, A_{p^k})$. Since $P(1) \in H^1_f(K, V)$ it will be enough to show that $\mathrm{Sel}(K, A_{p^k})/(\mathcal{O}_{E_\mathfrak{p}}/p^k)P(1)$ is killed by $p^{2\mathcal{I}_p}$.

Choose once and for all a complex conjugation $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let $S(k)$ be the set of primes ℓ satisfying:

- $\ell \nmid NDp$;
- ℓ is inert in K;
- p^k divides a_ℓ and $\ell + 1$;
- $\ell + 1 \pm a_\ell$ are not divisible by p^{k+1}.

Remark 3.1. The first 3 conditions are equivalent to $\mathrm{Frob}(\ell)$ and τ being conjugates in $\mathrm{Gal}(K(A_{p^k})/\mathbb{Q})$. The last condition can be arranged for infinitely many ℓ's (see proposition 6.10).

Let n be a product of distinct primes $\ell \in S(k)$. Nekovář associates with n a cohomology class $y_n \in H^1(K_n, T)$, where K_n is the ring class field of K of conductor n. The classes y_n are defined as the images of certain CM cycles under the Abel-Jacobi map of $\mathcal{M}_f$. When $n = m\ell$ the relation

$$\mathrm{cor}_{K_n, K_m}(y_n) = a_\ell y_m$$

holds, as well as some local congruence condition which we will not discuss here.

Let $G_n := \mathrm{Gal}(K_n/K_1)$. Then $G_n = \prod_{\ell | n} G_\ell$. For each prime $\ell \in S(k)$ we associate the element $D_\ell \in \mathbb{Z}[G_\ell]$ which is given by

$$D_\ell = \sum_{i=1}^{\ell} i\sigma^i, \qquad G_\ell = \langle \sigma \rangle,$$

and let $D_n = \prod_{\ell | n} D_\ell \in \mathbb{Z}[G_n]$. One now notices, following Kolyvagin, that $D_n(\mathrm{red}_{p^k} y_n) \in H^1(K_n, A_{p^k})$ is G_n-invariant. By [Nek92, Proposition 6.3]

$$p^M A_{p^k}(K_n) = 0, \tag{3.1}$$

with some constant M independent of n and k. An application of the inflation restriction sequence shows that there is a canonically defined class $z_n \in H^1(K_1, A_{p^{k-2M}})$ such that

$$\mathrm{res}_{K_1, K_n} z_n = D_n(\mathrm{red}_{p^{k-2M}} y_n).$$

Indeed, one has the commutative diagram with exact inflation restriction rows:

$$\begin{array}{ccccc} H^1(K_1, A_{p^k}) & \xrightarrow{\operatorname{res}_{K_1,K_n}} & H^1(K_n, A_{p^k})^{G_n} & \longrightarrow & H^2(G_n, A_{p^k}(K_n)) \\ \downarrow{\scriptstyle \operatorname{red}_{p^{k-M}}} & & \downarrow{\scriptstyle \operatorname{red}_{p^{k-M}}} & & \downarrow{\scriptstyle \operatorname{red}_{p^{k-M}}} \\ H^1(K_1, A_{p^{k-M}}) & \xrightarrow{\operatorname{res}_{K_1,K_n}} & H^1(K_n, A_{p^{k-M}})^{G_n} & \longrightarrow & H^2(G_n, A_{p^{k-M}}(K_n)) \end{array}$$

and the rightmost vertical map is 0 by (3.1) because the reduction map kills p^M torsion. It follows that

$$\operatorname{red}_{p^{k-M}} y_n \in \operatorname{Im}\left(\operatorname{res}_{K_1,K_n} : H^1(K_1, A_{p^{k-M}}) \to H^1(K_n, A_{p^{k-M}})\right).$$

We get the canonical class z_n by further reduction as in [Nek92, §7]. Finally, define

$$P(n) := \operatorname{cor}_{K_1,K} z_n.$$

Note the important difference between Nekovář's definition of the same classes and ours: in Nekovář's definition $\operatorname{res}_{K_1,K_n} z_n = p^M D_n(\operatorname{red}_{p^{k-M}} y_n)$. To simplify the notation, we may notice that the definition is entirely independent of the value of M. To define classes in the cohomology of A_{p^r} we need to start with n whose prime divisors satisfy certain congruences depending on r and M and we may freely assume that we have chosen the n correctly whatever the congruences are. It will be convenient to make the change of variable $k = k - 2M$ here. Note that $P(1)$ can be considered mod p^k for any k and its definition is independent of M.

PROPOSITION 3.2. *The classes $P(n)$ enjoy certain fundamental properties:*

1. *$P(n)$ belongs to the $(-1)^{par(n)}\varepsilon_L$-eigenspace of the complex conjugation τ acting on $H^1(K, A_{p^k})$, where $par(n)$ is the parity of the number of prime factors in n and ε_L is the negative of the sign of the functional equation of $L(f,s)$.*

2. *For a place v of K such that $v \nmid Nn$, $P(n) \in H^1_{f^*}(K_v, A_{p^k})$.*

3. *If $n = m\cdot\ell$ and λ is the unique prime of K above ℓ, then there is an isomorphism between $H^1_f(K_\lambda, A_{p^k})$ and $H^1_{sin}(K_\lambda, A_{p^k})$ which takes $P(m)_\lambda$ to $P(n)_{\lambda,sin}$. In particular, if $P(m)_\lambda \neq 0$, then $P(n)_{\lambda,sin} \neq 0$.*

Proof. This is [Nek92, Proposition 10.2] with a couple of modifications. First of all we remark that there is a miss-print in [Nek92] and the eigenvalue of τ on $P(n)$ is indeed $(-1)^{par(n)}\varepsilon_L$ as can be seen from the proof. To get the second statement when $v \nmid p$ we note that if such a v is a prime of good reduction one has $H^1_{f^*}(K_v, A_{p^k}) = H^1_f(K_v, A_{p^k}) = H^1_{ur}(K_v, A_{p^k})$ (see lemma 4.4) and that the auxiliary power of p that appear in [Nek92] is not needed here because of the change in the definition of $P(n)$ alluded to above. The case $v|p$ follows from [Nek92, Lemma 11.1]. Here, two remarks are in place: First of all, Nekovář uses the comparison theorem of Faltings for open varieties [Fal89]. As is well known, this result is not universally accepted. However, in the last 2 years Nekovář himself [Nek96] and Nizioł [Niz97, Theorem 3.2] have supplied alternative proofs that the image of the Abel-Jacobi map lies inside H_f in the case of good reduction. The second remark is that this is all we need because our assumption $p \nmid 2N$ imply that $v|p$ is a place of good reduction. □

One of the main points of this work is to analyze the dual finite conditions at primes of bad reduction and to show that by further reduction (i.e. by possibly increasing M) one may assume that the classes $P(n)$ are dual finite at these primes (see corollary 5.2).

4 Finite and dual finite conditions at ℓ

Let F be a finite extension of $\mathbb{Q}_\ell$ ($\ell \neq p$) and let T be a free $\mathbb{Z}_p$-module of finite rank with a continuous action of $G = \mathrm{Gal}(\bar{F}/F)$. Again let $V = T \otimes \mathbb{Q}_p$ and $A = V/T$. Let $I = \mathrm{Gal}(\bar{F}/F^{ur})$ be the inertial group. We assume the following condition is satisfied (as is in the case at hand, see [Nek92, proposition 3.1]):

Condition 4.1. There is a Galois invariant, non-degenerate bilinear pairing $V \times V \to \mathbb{Q}_p(1)$ and $V_I(-1)$ has no nontrivial fixed vector with respect to any power of Frobenius (true if V_I has no part of weight -2).

Proposition 4.2. *Under the above condition there exists a constant M such that for any finite unramified extension L/F we have*

1. $p^M H^1(L^{ur}, T)^{\mathrm{Gal}(L^{ur}/L)} = 0$;
2. $H^1_f(L, V) = H^1(L, V)$;
3. $V(L) = 0$.

Proof. The second statement immediately follows from the first. For the first statement we begin by noticing that I is independent of L. By making a finite ramified extension we may assume that the action of I factors through the p-primary part of its tame quotient. It then follows that $H^1(I, T) \cong T_I(-1)$ as $\mathrm{Gal}(L^{ur}/L)$-modules. The condition now implies that $T_I(-1)$ is a direct sum of a torsion group and a $\mathbb{Z}_p$-free module on which Frobenius has no invariants. Finally, the third statement follows since by duality one gets that 1 is not an eigenvalue of any power of Frobenius on V^I. □

Remark 4.3. If T is the Tate module of an elliptic curve with split semi-stable reduction, then the constant M is essentially the p-adic valuation of the number of components of the special fiber of E.

It follows from part 2 of proposition 4.2 that for any finite unramified extension L/F we have $H^1_f(L, T) = H^1(L, T)$, and therefore by lemma 2.4 we get

$$H^1_{f^*}(L, A_{p^k}) = \mathrm{Im}\, H^1(L, T) \xrightarrow{\mathrm{red}} H^1(L, A_{p^k}).$$

Lemma 4.4. *If the G-module T is unramified, then for any L as above*

$$H^1_{f^*}(L, A_{p^k}) = H^1_f(L, A_{p^k}) = H^1_{ur}(L, A_{p^k}) := \mathrm{Ker}\, H^1(L, A_{p^k}) \to H^1(L^{ur}, A_{p^k}).$$

Proof. It is enough to show the second equality as the condition of being unramified is self dual. It is clear that any class in $H^1_f(L, A_{p^k})$ is unramified. Conversely, a class in $H^1_{ur}(L, A_{p^k})$ is inflated from $H^1(L^{ur}/L, A_{p^k})$. Since $\mathrm{Gal}(L^{ur}/L) \cong \hat{\mathbb{Z}}$, H^1 is just coinvariants. It follows that the reduction map $H^1(L^{ur}/L, T) \to H^1(L^{ur}/L, A_{p^k})$ is surjective. □

5 The local condition under restriction

Keeping the assumption of the previous section, suppose now that L/F is a finite unramified extension with Galois group Δ. The short exact sequence $0 \to T \xrightarrow{p^k} T \xrightarrow{\mathrm{red}_{p^k}} A_{p^k} \to 0$ gives rise to the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1(F,T)/p^k & \xrightarrow{\mathrm{red}_{p^k}} & H^1(F,A_{p^k}) & \longrightarrow & H^2(F,T)_{p^k} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{res}_{F,L}} & & \downarrow{\scriptstyle \mathrm{res}_{F,L}} & & \downarrow{\scriptstyle \mathrm{res}_{F,L}} & & \\ 0 & \longrightarrow & \left(H^1(L,T)/p^k\right)^\Delta & \xrightarrow{\mathrm{red}_{p^k}} & H^1(L,A_{p^k})^\Delta & \longrightarrow & H^2(L,T)^\Delta_{p^k} & & \end{array} \tag{5.1}$$

Given $x \in H^1(F,A_{p^k})$ such that $\mathrm{res}_{F,L}\, x$ is in $H^1_{f^*}(L,A_{p^k})$, we would like to know how far is x from being in $H^1_{f^*}(F,A_{p^k})$. In view of (5.1) the obstruction is given by

$$\operatorname{Ker} H^2(F,T)_{p^k} \xrightarrow{\mathrm{res}_{F,L}} H^2(L,T)^\Delta_{p^k}. \tag{5.2}$$

Proposition 5.1. *The kernel* (5.2) *is annihilated by a constant p^M independent of k and L.*

Proof. Since Δ is finite, there is a Hochschild-Serre spectral sequence

$$E_2^{i,j} = H^i(\Delta, H^j(L,T)) \Rightarrow H^{i+j}(F,T).$$

Note that the cohomology here is the continuous cohomology. The Hochschild-Serre spectral sequence does not exist in general for continuous cohomology. A proof that it does exits in our case is found in the appendix. For $i+j=2$ the spectral sequence converges to a filtration $F^0 \supset F^1 \supset F^2 \supset 0$ on $H^2(F,T)$ with

$$\begin{aligned} F^1 &= \operatorname{Ker} H^2(F,T) \xrightarrow{\mathrm{res}_{F,L}} H^2(L,T)^\Delta; \\ F^1/F^2 &\cong E_\infty^{1,1} = E_3^{1,1} = \operatorname{Ker}\left[H^1(\Delta,H^1(L,T)) \to H^3(\Delta,T(L))\right] \\ &= H^1(\Delta,H^1(L,T)); \\ F^2 &\cong E_\infty^{2,0} \subset E_2^{2,0} = H^2(\Delta,T(L)) = 0, \end{aligned}$$

since $T(L)=0$ by part 3 of proposition 4.2. Therefore,

$$\operatorname{Ker}\left(H^2(F,T)_{p^k} \xrightarrow{\mathrm{res}_{F,L}} H^2(L,T)^\Delta_{p^k}\right) \cong H^1(\Delta,H^1(L,T))_{p^k}.$$

Applying the inflation restriction sequence to $\mathrm{Gal}(L^{ur}/L) \triangleleft \mathrm{Gal}(\bar{L}/L)$ and T we find

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

The right exactness is a consequence of the fact that $\mathrm{Gal}(L^{ur}/L) \cong \hat{\mathbb{Z}}$ has cohomological dimension 1. Applying the Hochschild-Serre spectral sequence to $\mathrm{Gal}(L^{ur}/L) \triangleleft \mathrm{Gal}(L^{ur}/F)$ and $T(L^{ur})$ we find that $H^1(\Delta, H^1(L^{ur}/L, T(L^{ur})))$ injects into $H^2(L^{ur}/F, T(L^{ur}))$ and is therefore 0 since $\mathrm{Gal}(L^{ur}/F) \cong \hat{\mathbb{Z}}$. Therefore, $H^1(\Delta, H^1(L,T)) \hookrightarrow H^1(\Delta, H^1(L^{ur},T)^{\mathrm{Gal}(L^{ur}/L)})$ and the result follows from proposition 4.2 □

Corollary 5.2. *Let p^M be the constant given by proposition 5.1. Then, if $x \in H^1(F, A_{p^{k+M}})$ and $\operatorname{res}_{F,L} x \in H^1_{f^*}(L, A_{p^{k+M}})$, then $\operatorname{red}_{p^k} x \in H^1_{f^*}(F, A_{p^k})$.*

Proof. The commuting diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T & \xrightarrow{p^{k+M}} & T & \xrightarrow{\operatorname{red}_{p^{k+M}}} & A_{p^{k+M}} & \longrightarrow & 0 \\ & & {\scriptstyle p^M}\downarrow & & {\scriptstyle =}\downarrow & & {\scriptstyle \operatorname{red}_{p^k}}\downarrow & & \\ 0 & \longrightarrow & T & \xrightarrow{p^k} & T & \xrightarrow{\operatorname{red}_{p^k}} & A_{p^k} & \longrightarrow & 0 \end{array}$$

gives rise to

$$\begin{array}{ccccc} H^1(F,T) & \xrightarrow{\operatorname{red}_{p^{k+M}}} & H^1(F, A_{p^{k+M}}) & \longrightarrow & H^2(F,T)_{p^{k+M}} \\ {\scriptstyle =}\downarrow & & {\scriptstyle \operatorname{red}_{p^k}}\downarrow & & {\scriptstyle p^M}\downarrow \\ H^1(F,T) & \xrightarrow{\operatorname{red}_{p^k}} & H^1(F, A_{p^k}) & \longrightarrow & H^2(F,T)_{p^k} \end{array}$$

The corollary now follows by a diagram chase on this last diagram as well as on (5.1) with k replaced by $k + M$. □

6 Proof of theorem 1.2

In this section we give the proof of the main theorem using a variant of the Kolyvagin argument following mostly [Gro91]. By proposition 3.2 and corollary 5.2 we may assume that the class $P(n)$ is dual finite at all primes which do not divide n. Recall that this involves fixing some large integer M, constructing the classes modulo p^{k+M} and then reducing them mod p^k.

We will concentrate on the case where f has no CM. The CM case can be handled similarly (see the remark in [Nek92] page 121). Recall that E is the field generated by the Fourier coefficients of the form f. We first exclude primes p which are ramified in E. If p is not excluded, let $\mathfrak{p}$ be a prime of E above p and recall that we are considering $T = T_{f,\mathfrak{p}}$ which is a rank 2 free $\mathcal{O}_{E_\mathfrak{p}}$-module with an action of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Let again $\rho_{f,p}$ be the p-adic representation associated with f. Consider the $\mathfrak{p}$ component of $\rho_{f,p}$ which is a representation of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on a 2-dimensional $E_\mathfrak{p}$ vector space $V_{\rho_f,\mathfrak{p}}$. According to a result of Ribet [Rib85, theorem 3.1] if p is outside a finite set of primes then there is a subfield E' of $E_\mathfrak{p}$ such that in an appropriate basis the image of $\operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\operatorname{Aut}(V_{\rho_f,\mathfrak{p}}) \cong \operatorname{GL}_2(E_\mathfrak{p})$ contains

$$\{g \in \operatorname{GL}_2(\mathcal{O}_{E'}),\ \det g \in ((\mathbb{Z}_p^\times)^{2r-1})\}$$

(in fact, the result of Ribet is stronger and treats the image of Galois in all the completions of E above p simultaneously), and therefore contains in particular

$$\{g \in \operatorname{GL}_2(\mathbb{Z}_p),\ \det g \in ((\mathbb{Z}_p^\times)^{2r-1})\}. \tag{6.1}$$

We exclude all other primes and the prime 2. This concludes our exclusions which we may sum up in:

DEFINITION 6.1. The set $\Psi(f)$ of excluded primes for theorem 1.2 is the set containing the primes dividing $2N$, primes that ramify in $E=\mathbb{Q}(a_i)$ and primes where the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(V_{\rho_f,\mathfrak{p}})$ does not contains (6.1) (in some basis).

We consider non excluded primes from now onward.

LEMMA 6.2. *Let $\tilde{G}_p$ be the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(T)\cong \mathrm{GL}_2(\mathcal{O}_{E_\mathfrak{p}})$ (p not excluded). Then, $\tilde{G}_p$ contains a subgroup conjugate to $\mathrm{GL}_2(\mathbb{Z}_p)$.*

Proof. By (2.1), $T\otimes E_\mathfrak{p}$ is just the r-th Tate twist of $V_{\rho_f,\mathfrak{p}}$. From that and Ribet's theorem it follows easily that after fixing an appropriate basis for T every matrix $A\in \mathrm{GL}_2(\mathcal{O}_{E_\mathfrak{p}})$ has a scalar multiple in $\tilde{G}_p$. Since $\mathrm{SL}_2(\mathcal{O}_{E_\mathfrak{p}})$ is the commutator subgroup of $\mathrm{GL}_2(\mathcal{O}_{E_\mathfrak{p}})$, it follows that $\mathrm{SL}_2(\mathcal{O}_{E_\mathfrak{p}})\subset \tilde{G}_p$. The lemma follows because for almost all ℓ, $\mathrm{Frob}(\ell)$ has determinant ℓ^{-1} and because $\tilde{G}_p$ is closed. □

Let $\mathbb{F}=\mathcal{O}_{E_\mathfrak{p}}/p^k$. Let $G_{p^k}\cong \mathrm{Gal}(\mathbb{Q}(A_{p^k})/\mathbb{Q})$ be the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{Aut}(A_{p^k})\cong \mathrm{GL}_2(\mathbb{F})$. Then, G_{p^k} contains a group G'_{p^k} conjugate to $\mathrm{SL}_2(\mathbb{Z}/p^k)$.

PROPOSITION 6.3. *Let $L=K(A_{p^k})$.*

1. *When $k=1$, A_p is an irreducible $\mathbb{F}[\mathrm{Gal}(L/K)]$-module.*
2. *$H^i(\mathrm{Gal}(L/K),A_{p^k})=0$ for all $i\geq 0$.*
3. *There is a natural pairing $[\ ,\ ]: H^1(K,A_{p^k})\times \mathrm{Gal}(\bar{\mathbb{Q}}/L)\to A_{p^k}$ inducing an isomorphism of $\mathbb{F}$-modules $H^1(K,A_{p^k})\cong \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(\bar{\mathbb{Q}}/L),A_{p^k})$.*
4. *The $\mathbb{F}$-module A_{p^k} is the direct sum of its ± 1 eigenspaces with respect to the generator τ of $\mathrm{Gal}(K/\mathbb{Q})$, each free of rank 1.*

Proof. Since $\mathrm{SL}_2(\mathbb{F}_p)$ has no nontrivial $\mathbb{Z}/2$ quotients when $p>2$ and $\mathrm{Gal}(L/K)$ is of index at most 2 in G_p, it follows that $\mathrm{Gal}(L/K)$ contains G'_p and therefore that A_p is an irreducible $\mathbb{F}[\mathrm{Gal}(L/K)]$-module. It also follows that $\mathrm{Gal}(L/K)$, considered as embedded in $\mathrm{Aut}(A_{p^k})$, contains the central Subgroup of order 2 generated by -1. Since $p\neq 2$, $H^i(\pm 1,A_{p^k})=0$ for all $i\geq 0$ and the second assertion follows from the Hochschild-Serre spectral sequence $H^i(\mathrm{Gal}(L/K)/\pm 1, H^j(\pm 1,A_{p^k}))\Rightarrow H^{i+j}(\mathrm{Gal}(L/K),A_{p^k})$. An inflation restriction sequence now implies that

$$H^1(K,A_{p^k})\cong H^1(L,A_{p^k})^{\mathrm{Gal}(L/K)}\cong \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(\bar{\mathbb{Q}}/L),A_{p^k})$$

hence the third assertion. Finally, part 4 follows because the determinant of τ on T is -1. □

Let S be a finitely generated $\mathbb{F}$-submodule of $H^1(K,A_{p^k})$. We consider the elements of S as elements of $\mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(\bar{\mathbb{Q}}/L),A_{p^k})$ and let L_S be the field fixed by the common kernel of these elements. The following lemma is immediate:

LEMMA 6.4. *The pairing $[\ ,\ ]$ induces a pairing*

$$[\ ,\ ]_S: S\times \mathrm{Gal}(L_S/L)\to A_{p^k},$$

which in turn induces an injection

$$\mathrm{Gal}(L_S/L) \hookrightarrow \mathrm{Hom}_{\mathbb{F}}(S, A_{p^k}) \text{ as } \mathrm{Gal}(L/K)\text{-modules.} \tag{6.2}$$

This injection has the property that

$$x \in S \text{ and } [x, \mathrm{Gal}(L_S/L)]_S = 0 \Longrightarrow x = 0.$$

In addition, this pairing induces an injection

$$S \hookrightarrow \mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L_S/L), A_{p^k}) \text{ as } \mathbb{F}\text{-modules}$$

Remark 6.5. Unlike the situation for elliptic curves [Gro91, proposition 9.3] we can not in general expect the injection (6.2) to be an isomorphism. For instance, if G_{p^k} is contained in $\mathrm{GL}_2(\mathbb{Z}/p^k)$, then there might exist a homomorphism $\phi : \mathrm{Gal}(\bar{\mathbb{Q}}/L) \to A_{p^k}$ whose image is contained in $(\mathbb{Z}/p^k)^2$. If we take S to be the $\mathbb{F}$-span of ϕ, then $\mathrm{Gal}(L_S/L) \cong (\mathbb{Z}/p^k)^2$ and is not in general an $\mathbb{F}$-module whereas $\mathrm{Hom}_{\mathbb{F}}(S, A_{p^k})$ is. The failure of (6.2) to be an isomorphism forces some changes in the final arguments.

Our chosen complex conjugation τ acts on all the groups above. We will denote by $G^{\pm}$ the ± 1-eigenspace of τ acting on an abelian group G.

LEMMA 6.6. *Let $C \subset \mathrm{Hom}_{\mathbb{F}}(S, A_{p^k})$ be a $\mathrm{Gal}(L/K)$-submodule with the property that $x \in S$ and $[x, C]_S = 0$ imply $x = 0$. Let $0 \neq s \in S$ and let $a \in \mathrm{Hom}_{\mathbb{F}}(S, A_{p^k})^+$. Let*

$$C' = a + C^+, \ C'' = \{c \in C', \ [s, c]_S \neq 0\}.$$

Then, C' and C'' have the same property as C with respect to eigenvectors of τ in S, that is, if $x \in S^{\pm}$ and $[x, C']_S = 0$ or $[x, C'']_S = 0$, then $x = 0$.

Proof. Suppose first that $[x, C^+]_S = 0$. Then $\mathbb{F} \cdot [x, C]_S$ is an $\mathbb{F}[\mathrm{Gal}(L/K)]$-submodule of A_{p^k} which is contained in the proper submodule $A_{p^k}^{\mp}$. Considering p-torsion and using part 1 of proposition 6.3 one finds that $\mathbb{F} \cdot [x, C]_S$ is trivial. It follows in particular that $[s, C^+]_S$ is non trivial and since $p \geq 3$ it contains at least 3 elements. From that it follows that for any $c \in C^+$ one may always find $c_1, \ c_2 \in C^+$ such that $c = (a + c_1) - (a + c_2)$ and $[s, a + c_i]_S \neq 0$ for $i = 1, 2$. The lemma follows easily. □

LEMMA 6.7. *Let ℓ be a prime in $S(M+k)$. Then, ℓ is inert in K. Let λ be the unique prime of K above ℓ. Then, for any choice of $\mathrm{Frob}(\lambda)$ in a decomposition group of λ, $\mathrm{Frob}(\lambda)$ acts trivially on A_{p^k} and therefore λ splits completely in L.*

Proof. Both assertions follow from remark 3.1. In $\mathrm{Gal}(K/\mathbb{Q})$, $\mathrm{Frob}(\ell) = \tau$ hence ℓ is inert in K. It now follows that $\mathrm{Frob}(\lambda)$ is conjugate to τ^2 and is therefore the identity on A_{p^k}. □

Let ℓ and λ be as in the previous lemma, let λ' be a prime of L_S above λ and let $\mathrm{Frob}(\lambda') \in \mathrm{Gal}(L_S/L)$ be the associated Frobenius substitution. It is easy to see that the formula

$$\phi_{\lambda'}(x) := [x, \mathrm{Frob}(\lambda')]_S$$

defines an element of $\mathrm{Hom}_{\mathbb{F}}(S, A_{p^k})$ which depends only on ℓ up to conjugation on A_{p^k} by some element of $\mathrm{Gal}(L/K)$. Using lemma 6.7 one has:

LEMMA 6.8. *There is a* $\mathrm{Gal}(K/\mathbb{Q})$*-equivariant isomorphism*

$$H^1_f(K_\lambda, A_{p^k}) \cong H^1(K_\lambda^{ur}/K_\lambda, A_{p^k}) \cong A_{p^k}, \tag{6.3}$$

where the last step is evaluation at the Frobenius. If $x \in H^1(K, A_{p^k})$ *and* $x_\lambda \in H^1_f(K_\lambda, A_{p^k})$ *then, up to conjugation as before, the image of* x_λ *under this isomorphism is* $\phi_{\lambda'}(x)$.

LEMMA 6.9. *Let* λ *be as above.*

1. *The pairing* $\langle\ ,\ \rangle_\lambda$ *defined in lemma* 2.4 *induces nondegenerate pairings:*

$$\langle\ ,\ \rangle_\lambda^\pm : H^1_f(K_\lambda, A_{p^k})^\pm \times H^1_{sin}(K_\lambda, A_{p^k})^\pm \to \mathbb{Z}/p^k.$$

2. *Both* $H^1_f(K_\lambda, A_{p^k})$ *and* $H^1_{sin}(K_\lambda, A_{p^k})$ *are direct sums of their* ± 1 *eigenspaces with respect to* τ. *All eigenspaces are free of rank* 1 *over* $\mathbb{F}$.

Proof. The first assertion follows since $\langle\ ,\ \rangle_\lambda$ is $\mathrm{Gal}(L/K)$ equivariant. The second assertion follows for $H^1_f(K_\lambda, A_{p^k})$ by lemma 6.8 and part 4 of proposition 6.3 and the same now follows for $H^1_{sin}(K_\lambda, A_{p^k})^\pm$ by the first assertion. □

PROPOSITION 6.10. *Let* $x,\ y \in S$ *and suppose that* $y \neq 0$. *Then there exists some* $\ell \in S(M+k)$ *such that* $y_\lambda \neq 0$. *If for almost all* $\ell \in S(M+k)$ *with* $y_\lambda \neq 0$ *we have* $x_\lambda = 0$, *then* $x = 0$.

Proof. Let $L_M = K(A_{p^{M+k+1}})$. Let C be the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/L_M)$ in $\mathrm{Gal}(L_S/L)$. We first claim that when considered in $\mathrm{Hom}_{\mathbb{F}}(S, A_{p^k})$, C satisfies the assumption of lemma 6.6. To show that, we first notice that the same argument used to prove that $H^i(\mathrm{Gal}(L/K), A_{p^k}) = 0$ for all $i \geq 0$ in proposition 6.3 shows that $H^i(\mathrm{Gal}(L_M/K), A_{p^k}) = 0$ for all such i. An inflation restriction sequence now shows that

$$\mathrm{Hom}_{\mathrm{Gal}(L/K)}(\mathrm{Gal}(L_M/L), A_{p^k}) = H^1(\mathrm{Gal}(L_M/L), A_{p^k})^{\mathrm{Gal}(L/K)} = 0.$$

This implies that if $x \in S$ satisfies $[x, C]_S = 0$, then in fact $[x, \mathrm{Gal}(L_S/L)]_S = 0$ and the claim follows from lemma 6.4.

By lemma 6.2 the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ in $\mathrm{Aut}(A_{p^{M+k+1}}) \cong \mathrm{GL}_2(\mathcal{O}_{E_\mathfrak{p}}/p^{M+k+1})$ contains an element of the form $a \cdot I$ such that $a \in 1 + p^{M+k}(\mathbb{Z}/p)^\times$. One checks that this element defines $\rho' \in \mathrm{Gal}(L_M/L_{M-1})$ with the property that if $\mathrm{Frob}(\ell)$ contains $\tau\rho'$, then $\ell \in S(M+k)$.

Now let $L' = L_M \cap L_S$. Then $C = \mathrm{Gal}(L_S/L')$. Consider $\sigma \in C^+$. Since C has odd order we can find $\rho \in C$ such that $\sigma = \rho^\tau \rho$. Let $\rho \cdot \rho' \in \mathrm{Gal}(L_M \cdot L_S/K)$ be the element whose restriction to $\mathrm{Gal}(L_M/K)$ is ρ' and whose restriction to $\mathrm{Gal}(L_S/L')$ is σ. By Čebotarev's density theorem, we may find infinitely many primes ℓ whose Frobenius conjugacy class in $\mathrm{Gal}(L_M \cdot L_S/\mathbb{Q})$ contains $\tau \cdot \rho \cdot \rho'$. Every such ℓ is in $S(M+k)$. In addition, after projecting to $\mathrm{Gal}(L_S/L')$ we find $\mathrm{Frob}(\lambda) = (\tau\rho)^2 = \rho^\tau \cdot \rho = \sigma$. Thus, we are able to generate a full coset of C in $\mathrm{Gal}(L_S/L)$ with these $\mathrm{Frob}(\lambda)$. By lemma 6.8 we are also able to generate all elements σ of this coset for which $[y, \sigma]_S = 0$ with $\{\mathrm{Frob}(\lambda),\ y_\lambda \neq 0\}$. The proposition therefore follows from lemma 6.6. □

LEMMA 6.11. *Suppose $x \in \mathrm{Sel}(K, A_{p^k})$ and n is a product of primes in $S(M+k)$.*

1. $\sum_{\ell | n} \langle x_\lambda, P(n)_{\lambda,sin} \rangle_\lambda = 0.$

2. *If x and $P(n)$ are in the same eigenspace for τ, $p^{k-\mathcal{I}-1} P(n)_{\lambda,sin} \neq 0$ and we have $\langle \mathbb{F} x_\lambda, P(n)_{\lambda,sin} \rangle_\lambda = 0$, then $p^{\mathcal{I}} x_\lambda = 0$.*

Proof. 1. This follows from proposition 2.2, lemma 2.4 and the fact that the classes $P(n)$ are dual finite at primes not dividing n.
2. Consider first the case $k = 1$ and $\mathcal{I} = 0$. The conditions then imply that $\mathbb{F} x_\lambda$ is a proper subspace of an eigenspace of τ on $H^1_f(K_\lambda, A_p)$ which is 1-dimensional over $\mathbb{F}$ by lemma 6.9 and it follows that $\mathbb{F} x_\lambda = 0$. If k is arbitrary but $\mathcal{I} = 0$ then $P(n)_{\lambda,sin}$ has a non trivial image in p-cotorsion hence by the previous case $\mathbb{F} x_\lambda$ has trivial p-torsion but this can only happen if $x_\lambda = 0$. Finally, if $\mathcal{I} \neq 0$ the conditions imply that $P(n)_{\lambda,sin} = p^{\mathcal{I}'} P'$ with $\mathcal{I}' \leq \mathcal{I}$ and P' has a non trivial image in p-cotorsion. Since $\langle \mathbb{F} p^{\mathcal{I}'} x_\lambda, P' \rangle_\lambda = 0$ we get from the previous case $p^{\mathcal{I}'} x_\lambda = 0$. □

The proof of theorem 1.2 may now be completed as follows: Let $\mathcal{I} = \mathcal{I}_p$ and let $\mathcal{J} = \mathcal{I} + 1$. We assume that $k > \mathcal{I}$ and we want to prove that $p^{2\mathcal{I}}$ kills $\mathrm{Sel}(K, A_{p^k}) / \mathbb{F} P(1)$. Our assumption is that $\mathrm{red}_{p^{\mathcal{J}}} P(1) \neq 0$ in $H^1(K, A_{p^{\mathcal{J}}})$. On $H^1(K, A_{p^k})$, multiplication by $p^{k-\mathcal{J}}$ factors as the composition of $\mathrm{red}_{p^{\mathcal{J}}}$ with the map $H^1(K, A_{p^{\mathcal{J}}}) \to H^1(K, A_{p^k})$ induced by the inclusion in the short exact sequence $0 \to A_{p^{\mathcal{J}}} \to A_{p^k} \to A_{p^{k-\mathcal{J}}} \to 0$. Since $A_{p^{k-\mathcal{J}}}(K) = 0$, this induced map is injective and we conclude that $p^{k-\mathcal{J}} P(1) \neq 0$. Let $x \in \mathrm{Sel}(K, A_{p^k})$. Suppose first that x is in the opposite eigenspace to $P(1)$, hence in the same eigenspace as $P(\ell)$ for $\ell \in S(M+k)$ by proposition 3.2. Let S be the $\mathbb{F}$-submodule of $H^1(K, A_{p^k})$ generated by x and $P(1)$. Suppose $\ell \in S(M+k)$ is such that $(p^{k-\mathcal{J}} P(1))_\lambda \neq 0$. Then, by part 3 of proposition 3.2, $p^{k-\mathcal{J}} P(\ell)_{\lambda,sin} \neq 0$ and from that and lemma 6.11 it follows that $p^{\mathcal{I}} x_\lambda = 0$. Proposition 6.10 therefore implies that $p^{\mathcal{I}} x = 0$.

Suppose now that x is in the same eigenspace as $P(1)$ and we claim that $p^{2\mathcal{I}} x$ has to be a multiple of $P(1)$. By proposition 6.10 we may find $\ell \in S(M+k)$ such that $(p^{k-\mathcal{J}} P(1))_\lambda \neq 0$. As before, this implies that $p^{k-\mathcal{J}} P(\ell)_{\lambda,sin} \neq 0$ and hence that $p^{k-\mathcal{J}} P(\ell) \neq 0$. Let S be generated by x, $P(1)$ and $P(\ell)$. Since $p^{k-\mathcal{J}} P(1)_\lambda \neq 0$ and both $P(1)_\lambda$ and x_λ are in the free rank 1 $\mathbb{F}$-module $H^1_f(K_\lambda, A_{p^k})^{\pm}$, it is easy to see that we may find a combination $x' = \alpha P(1) + p^{\mathcal{I}} x \in S$, with $\alpha \in \mathbb{F}$, such that $x'_\lambda = 0$. Consider now $\ell \neq \ell_1 \in S(M+k)$ such that $p^{k-\mathcal{J}} P(\ell)_{\lambda_1} \neq 0$. Then $p^{k-\mathcal{J}} P(\ell\ell_1)_{\lambda_1,sin} \neq 0$, again by part 3 of proposition 3.2. Let $x'' \in \mathbb{F} x'$. Then

$$\langle x''_\lambda, P(\ell\ell_1)_{\lambda,sin} \rangle_\lambda + \langle x''_{\lambda_1}, P(\ell\ell_1)_{\lambda_1,sin} \rangle_{\lambda_1} = 0.$$

Since $x''_\lambda = 0$ we find $\langle x''_{\lambda_1}, P(\ell\ell_1)_{\lambda_1,sin} \rangle_{\lambda_1} = 0$. Lemma 6.11 implies that $p^{\mathcal{I}} x'_{\lambda_1} = 0$. From proposition 6.10 we get $p^{\mathcal{I}} x' = 0$ and so $p^{2\mathcal{I}} x = -\alpha p^{\mathcal{I}} P(1)$.

A The Hochschild-Serre spectral sequence in continuous cohomology

Here we prove the following result:

Proposition A.1. *Let G be a profinite group, M a continuous module of G which is the inverse limit of discrete G-modules M_n, $n \in \mathbb{N}$, and H a normal subgroup of G with a finite quotient group $\Delta = G/H$. Then there is a Hochschild-Serre spectral sequence*

$$E_2^{i,j} = H^i(\Delta, H^j(H, M)) \Rightarrow H^{i+j}(G, M), \tag{A.1}$$

where the cohomology of M is the continuous cohomology, i.e., the one computed with respect to continuous cochains as in [Tat76].

Proof. The spectral sequence will be derived from the Grothendieck spectral sequence for the composition of the functors $U : \mathcal{A} \to \mathcal{B}$ and $V : \mathcal{B} \to \mathcal{C}$ defined as follows:

- $\mathcal{A}$ is the category of inverse systems $(M_n)_{n\in\mathbb{N}}$ of discrete G-modules;
- $\mathcal{B}$ is the category of Δ-modules and $\mathcal{C}$ of abelian groups;
- U is the functor which takes an inverse system of G-modules (M_n) to $\varprojlim M_n^H$;
- V is the Δ invariants functor.

In this case, $U \circ V$ is the functor which takes (M_n) to $\varprojlim M_n^G$, because taking invariants commutes with taking limits. The i-th right derived functor of $(M_n) \to \varprojlim M_n^G$ was shown by Jannsen [Jan88a] to be the continuous cohomology $H^i(G, \varprojlim M_n)$ and the same holds with G replaced by H. The only thing left to check is that U takes $\mathcal{A}$ injectives to V acyclics, or even to injectives. For this fact, a proof can be given along the lines of the proof of the usual Hochschild-Serre spectral sequence (see for example [HS76, p.303]). One only needs to give a left adjoint $\bar{U}$ to U which preserves monomorphisms and this is easily done: for a Δ-module N, let $\bar{U}(N)$ be the constant inverse system of N considered as a G-module. Now it is very easy to check that

$$\mathrm{Hom}_{\mathcal{A}}(\bar{U}(N), (M_n)) = \mathrm{Hom}_{\mathcal{B}}(N, \varprojlim M_n^H)$$

and so the proof is complete. □

References

[BK90] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift I (Boston), Prog. in Math., vol. 86, Birkhäuser, 1990, pp. 333–400.

[Fal89] G. Faltings, *Crystalline cohomology and p-adic Galois representations*, Algebraic analysis, geometry and number theory (Baltimore) (J.I Igusa, ed.), Johns Hopkins University Press, 1989, pp. 25–80.

[Gro91] B. Gross, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Cambridge) (J. Coates and M.J. Taylor, eds.), Lond. Math. Soc. Lect. Note Ser., vol. 153, Cambridge University Press, 1991, pp. 235–256.

[HS76] P. J. Hilton and U. Stammbach, *A course in homological algebra*, GTM, vol. 4, Springer, New York Heidelberg Berlin, 1976.

[Jan88a] U. Jannsen, *Continuous étale cohomology*, Math. Ann. 280 (1988), 207–245.

[Jan88b] U. Jannsen, *Mixed motives and algebraic K-theory*, Lect. Notes in Math., vol. 1400, Springer, Berlin Heidelberg New York, 1988.

[KL90] V. Kolyvagin and D. Logachev, *Finiteness of the Shafarevich-Tate and the group of rational points for some modular abelian varieties*, Leningrad Math. J. 1 (1990), 1229–1253.

[Kol91] V. Kolyvagin, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago IL. 1989) (Berlin Heidelberg New York), Lect. Notes in Math., vol. 1479, Springer, Berlin Heidelberg New York, 1991, pp. 333–400.

[Lan96] A. Langer, *Local points of motives in semistable reduction*, Preprint, 1996.

[McC91] W. McCallum, *Kolyvagin's work on Shafarevich-Tate groups*, L-functions and arithmetic (Cambridge) (J. Coates and M.J. Taylor, eds.), Lond. Math. Soc. Lect. Note Ser., vol. 153, Cambridge University Press, 1991, pp. 295–316.

[Mil86] J.S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Boston, Mass., 1986.

[Nek92] J. Nekovář, *Kolyvagin's method for Chow groups of Kuga-Sato varieties*, Invent. Math. 107 (1992), no. 1, 99–125.

[Nek95] J. Nekovář, *On the p-adic height of Heegner cycles*, Math. Ann. 302 (1995), 609–686.

[Nek96] J. Nekovář, *Syntomic cohomology and p-adic regulators*, 1996, In preparation.

[Niz97] W. Nizioł, *On the image of p-adic regulators*, Invent. Math. 127 (1997), 375–400.

[Rib85] K. Ribet, *On l-adic representations attached to modular forms II*, Glasgow Math. J. 27 (1985), 185–194.

[Sch90] A. Scholl, *Motives associated to modular forms*, Invent. Math. 100 (1990), 419–430.

[Tat76] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. 36 (1976), 257–274.

Amnon Besser
Department of Mathematics
UCLA
Box 951555
Los Angeles, CA 90095-1555
U.S.A.