TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 369, Number 10, October 2017, Pages 7301–7342
http://dx.doi.org/10.1090/tran/6947
Article electronically published on May 5, 2017

A REFINED BEILINSON–BLOCH CONJECTURE FOR MOTIVES OF MODULAR FORMS

MATTEO LONGO AND STEFANO VIGNI

Abstract. We propose a refined version of the Beilinson–Bloch conjecture for the motive associated with a modular form of even weight. This conjecture relates the dimension of the image of the relevant p-adic Abel–Jacobi map to certain combinations of Heegner cycles on Kuga–Sato varieties. We prove theorems in the direction of the conjecture and, in doing so, obtain higher weight analogues of results for elliptic curves due to Darmon.

1. Introduction

Let $N \geq 3$ be an integer, let $k \geq 4$ be an even integer and let $f \in S_k^{\mathrm{new}}(\Gamma_0(N))$ be a normalized newform of weight k and level $\Gamma_0(N)$, whose q-expansion will be denoted by

$$f(q) = \sum_{n \geq 1} a_n q^n.$$

Let $p \nmid N$ be a prime number and let $\mathfrak{p} \,|\, p$ be a prime ideal of the ring of integers $\mathcal{O}_F$ of the totally real field F generated by the Fourier coefficients a_n of f. Finally, let K be a number field. To these data we may attach a p-adic Abel–Jacobi map

$$\mathrm{AJ}_K : \mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/K\big)_0 \otimes F_{\mathfrak{p}} \longrightarrow H^1_f(K, V_{\mathfrak{p}})$$

where $F_{\mathfrak{p}}$ is the completion of F at $\mathfrak{p}$, $\tilde{\mathcal{E}}_N^{k-2}$ is the Kuga–Sato variety of level N and weight k, $V_{\mathfrak{p}}$ is a twist of the $\mathfrak{p}$-adic representation associated with f and $H^1_f(K, V_{\mathfrak{p}})$ is its Bloch–Kato Selmer group over K (here the subscript "f" stands for "finite" and should not be confused with the modular form f). The Beilinson–Bloch conjectures ([1], [11]) connect the values of the L-functions of algebraic varieties over number fields to global arithmetic properties of these varieties (see, e.g., [52] for an introduction). In particular, they state that the $F_{\mathfrak{p}}$-dimension of the image $X_{\mathfrak{p}}(K)$ of AJ_K is equal to the order of vanishing of the complex L-function $L(f \otimes K, s)$ of f over K at its center of symmetry $s = k/2$. Moreover, if $\tilde{\rho}_{\mathfrak{p}}$ denotes this dimension, then the leading term of the derivative of order $\tilde{\rho}_{\mathfrak{p}}$ of $L(f \otimes K, s)$ at $s = k/2$ is predicted up to multiplication by elements of $\mathbb{Q}^\times$. When K is an imaginary quadratic field of discriminant coprime to Np or $K = \mathbb{Q}$, important results towards this conjecture (at least in low rank situations) have been obtained by combining Nekovář's generalization of Kolyvagin's theory to Chow groups of

Received by the editors February 1, 2016.
2010 *Mathematics Subject Classification.* Primary 14C25, 11F11.
Key words and phrases. Modular forms, Beilinson–Bloch conjecture, Heegner cycles.
The authors were partially supported by PRIN 2010–11 "Arithmetic Algebraic Geometry and Number Theory". The first author was also partially supported by PRAT 2013 "Arithmetic of Varieties over Number Fields". The second author was also partially supported by PRA 2013 "Geometria Algebrica e Teoria dei Numeri".

Kuga–Sato varieties ([39]) with Zhang's formula of Gross–Zagier type for higher weight modular forms ([55]). More recently, the Beilinson–Bloch conjectures have been subsumed within the Tamagawa number conjecture of Bloch and Kato ([12]), which predicts (by using Fontaine's theory of p-adic representations) the value of the non-zero rational factor that was not made explicit in the original conjectures.

The goal of the present article is to investigate refined – or equivariant – analogues of these conjectures in which, roughly speaking, L-functions are replaced by Heegner cycles.

To better explain our work, let us recall that refined versions of the Birch and Swinnerton-Dyer conjecture (BSD conjecture, for short) for a rational elliptic curve E were first proposed by Mazur and Tate in [37]. In that article, the role of L-functions was played by certain combinations of modular symbols with coefficients in the group algebra $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})]$, called "theta elements" and denoted by $\theta_{E,M}$; here $M \geq 1$ is an integer and ζ_M is a primitive M-th root of unity. The Mazur–Tate refined conjecture of BSD type states that $\theta_{E,M}$ belongs to a power r of the augmentation ideal I of $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})]$ that can be predicted in terms of the rank of the Mordell–Weil group $E(\mathbb{Q})$ and the number of primes of split multiplicative reduction for E dividing M. This conjecture describes also the leading value of $\theta_{E,M}$, which is defined as the image of $\theta_{E,M}$ in the quotient I^r/I^{r+1}. We point out that the rank-part of the conjecture has been recently proved, under some relatively mild assumptions, by Ota in [47]. Extensions and analogues of this conjecture for Artin L-functions and for L-functions of more general motives have also been formulated, and partial results have been proved (see, e.g., [14], [15], [21], [23], [49] and the references therein).

Moving from [37] and the observation that modular symbols and Heegner points enjoy similar formal properties, Darmon proposed in [18] refined versions *à la* Mazur–Tate of the BSD conjecture, where modular symbols are replaced by Heegner points. Later on, Bertolini and Darmon began a systematic study of p-adic analogues of the BSD conjecture in which the relevant p-adic L-functions are defined in terms of distributions of Heegner (and Gross–Heegner) points on Shimura curves attached either to definite or to indefinite quaternion algebras (see [4], [5], [6], [7], [8]).

Our aim in this paper is to formulate and study refined versions of the Beilinson–Bloch conjecture for the motive associated with the modular form f; in this context, the role of the Heegner points appearing in [18] is played by higher-dimensional Heegner cycles in the sense of Nekovář ([39]). We hope that our work, offering an equivariant refinement of the above-mentioned conjectures in which the complex L-function of a modular form is replaced by an algebraically defined one, can be viewed as complementary to the results of Burns and of Burns–Flach on Stark's conjectures and Tamagawa numbers of motives (see, e.g., [14], [15]).

In order to state our main results more precisely, we need some notation. Let K be an imaginary quadratic field of discriminant coprime to Np in which all the primes dividing N split, let T be a square-free product of primes that are inert in K and do not divide Np and let K_T be the ring class field of K of conductor T. Write $\mathcal{O}_\mathfrak{p}$ for the completion of $\mathcal{O}_F$ at $\mathfrak{p}$. As recalled in §2.1 and §2.3, there is a natural way to introduce an $\mathcal{O}_\mathfrak{p}$-lattice $A_\mathfrak{p}$ inside $V_\mathfrak{p}$, and to all these data we may attach a Heegner cycle $y_{T,\mathfrak{p}} \in \Lambda_\mathfrak{p}(K_T) \subset H^1_{\mathrm{cont}}(K_T, A_\mathfrak{p})$ where $\Lambda_\mathfrak{p}(K_T)$ is the image of the $\mathcal{O}_\mathfrak{p}$-integral version of the Abel–Jacobi map AJ_{K_T} and H^1_{cont} denotes continuous cohomology (see §2.4 and §3.1). Set $G_T := \mathrm{Gal}(K_T/K_1)$ and $\Gamma_T := \mathrm{Gal}(K_T/K)$, consider the theta element

$$\theta_{T,\mathfrak{p}} := \sum_{\sigma\in G_T} \sigma(y_{T,\mathfrak{p}})\otimes\sigma \in \Lambda_{\mathfrak{p}}(K_T)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[G_T]$$

and let $\theta^*_{T,\mathfrak{p}}$ be the image of $\theta_{T,\mathfrak{p}}$ via the involution sending $\sigma\in G_T$ to σ^{-1}. Taking suitable trace-like operators to K we obtain elements $\zeta_{T,\mathfrak{p}}$ and $\zeta^*_{T,\mathfrak{p}}$ that may be naturally viewed as belonging to $\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$ whenever $T\mid S$.

Now let S be a square-free product of primes that are inert in K and do not divide Np, then define the arithmetic L-function attached to S and $\mathfrak{p}$ as

$$\mathcal{L}_{S,\mathfrak{p}} := \Bigg(\sum_{T\mid S} a_T\zeta_{T,\mathfrak{p}}\Bigg)\otimes\Bigg(\sum_{T\mid S} a^*_T\zeta^*_{T,\mathfrak{p}}\Bigg) \in \Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_S],$$

where a_T and a^*_T are explicit elements of $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$ that are defined in (61) below in terms of the Möbius function and the quadratic character of K.

The finite-dimensional $F_{\mathfrak{p}}$-vector space $X_{\mathfrak{p}}(K)$ splits under the action of the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ as a direct sum

$$X_{\mathfrak{p}}(K) = X_{\mathfrak{p}}(K)^+\oplus X_{\mathfrak{p}}(K)^-$$

of its eigenspaces. Set $\rho^{\pm}_{\mathfrak{p}} := \dim_{F_{\mathfrak{p}}}\big(X_{\mathfrak{p}}(K)^{\pm}\big)$ and

$$\rho_{\mathfrak{p}} := \begin{cases}\max\{\rho^+_{\mathfrak{p}},\rho^-_{\mathfrak{p}}\}-1 & \text{if } \rho^+_{\mathfrak{p}}\neq\rho^-_{\mathfrak{p}}, \\ \rho^+_{\mathfrak{p}} & \text{otherwise.}\end{cases}$$

As a consequence of the Beilinson–Bloch conjecture, the function $\mathfrak{p}\mapsto\rho_{\mathfrak{p}}$ is expected to be constant and, since the order of vanishing of $L(f\otimes K,s)$ at $s=k/2$ is odd, the case $\rho^+_{\mathfrak{p}}=\rho^-_{\mathfrak{p}}$ should never occur. Let I_{Γ_S} be the augmentation ideal of $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$ (to simplify our notation, we suppress dependence on $\mathfrak{p}$). Finally, write $J(S)$ for the cokernel of the map

$$H^1_f(K,A_{\mathfrak{p}}/pA_{\mathfrak{p}}) \longrightarrow \bigoplus_{\ell\mid S} H^1_f(K_\lambda,A_{\mathfrak{p}}/pA_{\mathfrak{p}})$$

where K_λ is the completion of K at the unique prime λ above ℓ. Our results apply to all prime numbers p outside a finite set Σ that we introduce in §3.5; in fact, one crucial feature that we require of the prime p is that the Galois representation $V_{\mathfrak{p}}$ be irreducible with non-solvable image.

Theorem 1.1. *Let p be a prime number such that $p\notin\Sigma$, let S be a product of primes that are inert in K and do not divide Np, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ above p.*

(1) $\mathcal{L}_{S,\mathfrak{p}}\in\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\otimes_{\mathcal{O}_{\mathfrak{p}}} I^{2\rho_{\mathfrak{p}}}_{\Gamma_S}$.

(2) *Suppose that $p\mid \ell+1$ for all prime numbers $\ell\mid S$. If $|\rho^+_{\mathfrak{p}}-\rho^-_{\mathfrak{p}}|=1$, then the image $\tilde{\mathcal{L}}^{(p)}_{S,\mathfrak{p}}$ of $\mathcal{L}_{S,\mathfrak{p}}$ in*

$$\big(\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}/p\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\big)\otimes_{\mathcal{O}_{\mathfrak{p}}}\big(I^{2\rho_{\mathfrak{p}}}_{\Gamma_S}/I^{2\rho_{\mathfrak{p}}+1}_{\Gamma_S}\big)$$

belongs to the natural image of

$$\big(\Lambda_{\mathfrak{p}}(K)^{\otimes 2}/p\Lambda_{\mathfrak{p}}(K)^{\otimes 2}\big)\otimes_{\mathcal{O}_{\mathfrak{p}}}\big(I^{2\rho_{\mathfrak{p}}}_{\Gamma_S}/I^{2\rho_{\mathfrak{p}}+1}_{\Gamma_S}\big).$$

(3) *Let* $\text{Ш}_p(K, A_\mathfrak{p} \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ *be the* p*-part of the Shafarevich–Tate group of* $A_\mathfrak{p} \otimes \mathbb{Q}_p/\mathbb{Z}_p$ *over* K *and assume that* $p \mid \ell + 1$ *for all prime numbers* $\ell \mid S$*. If* $|\rho^+_\mathfrak{p} - \rho^-_\mathfrak{p}| = 1$ *and* p *divides* $\big|\text{Ш}_p(K, A_\mathfrak{p} \otimes \mathbb{Q}_p/\mathbb{Z}_p)\big| \cdot |J(S)|$*, then* $\tilde{\mathcal{L}}^{(p)}_{S,\mathfrak{p}} = 0$.

Theorem 1.1, which corresponds to Corollary 4.16 in the main body of the text, provides a higher weight analogue of a theorem of Darmon for elliptic curves over $\mathbb{Q}$ ([18]), and at the same time may be viewed as a partial result towards a *refined Beilinson–Bloch conjecture* for modular forms. This perspective is approached in a series of conjectures (Conjectures 4.3, 4.10 and 5.1) that study the order of vanishing and the leading coefficient of $\mathcal{L}_{S,\mathfrak{p}}$. In particular, in Conjecture 5.1 we relate $\mathcal{L}_{S,\mathfrak{p}}$ to a theory of regulators of Mazur–Tate type that we call *Nekovář regulators*. These regulators can be explicitly defined using Nekovář's theory of p-adic height pairings ([40], [43, Ch. 11]) and represent a generalization to our setting of those introduced by Mazur and Tate in [36] and [37]. We plan to further investigate the theory of generalized regulators in future work.

In a related, albeit different, circle of ideas, Mazur and Rubin proved in [35] a refined class number formula for real quadratic fields (proposed by Darmon in [19]) that, in a very special case, is an analogue of Gross's conjecture ([23]) involving first derivatives of L-functions at $s = 0$. The techniques of Mazur and Rubin, which are based on their theory of Kolyvagin systems ([34]), do not seem to lend themselves to being extended directly to the context of [18] or to our Heegner cycle setting, and thus do not appear to suggest a proof of the conjectures formulated in [18] or in the present paper. Broadly speaking, the obstruction to such an extension is accounted for by the difference between the Euler systems used in [18] and the Kolyvagin systems of [34] and [35] arising from (or modeled on) circular units. It would be very interesting to understand how to modify the Mazur–Rubin approach to obtain a proof of the conjectures in [18] and in this paper.

Theorem 1.1 is a consequence of analogous results for the elements $\zeta_{S,\mathfrak{p}}$ (Theorem 4.15). It is worth pointing out that all these results are based on a congruence property enjoyed by Heegner cycles (Theorem 3.34); namely, generalized Kolyvagin derivatives (called *Darmon–Kolyvagin derivatives* here and studied in §3.4) of Heegner cycles are zero modulo p^m if their order is less than the $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-rank of $H^1_f(K, A_\mathfrak{p}/p^m A_\mathfrak{p})$. As a by-product of Theorem 3.34, if ℓ is a prime not dividing N, inert in K and such that $p \mid \ell + 1$, then in Theorem 4.18 we give a bound (in terms of p and the dimension of $H^1_f(K, A_\mathfrak{p}/pA_\mathfrak{p})$ over $\mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}$) on the $\mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}$-dimension of the Galois module generated by Heegner cycles inside $\Lambda_\mathfrak{p}(K_\ell)/p\,\Lambda_\mathfrak{p}(K_\ell)$.

We conclude by remarking that W. Zhang has recently obtained in [56] a converse to Kolyvagin's theorem on the rank of rational elliptic curves, thus providing a purely Galois-theoretic criterion (involving Selmer groups) for a Heegner point to be non-torsion. In a future project, building on the techniques developed in the present paper, we will investigate generalizations of Zhang's results to forms of higher weight and similar criteria for Heegner cycles of codimension greater than 1.

Notation and conventions. Unless specified otherwise, unadorned tensor products $\otimes$ are taken over $\mathbb{Z}$.

The cardinality of a (finite) set X is denoted either by $\#X$ or by $|X|$.

If K is a field, then set $G_K := \mathrm{Gal}(\bar{K}/K)$, where $\bar{K}$ is a fixed algebraic closure of K. For any continuous G_K-module M let $H^i(K, M)$ denote the i-th cohomology group of G_K with coefficients in M. If K/F is a field extension, then

$$\mathrm{res}_{K/F} : H^i(F, M) \longrightarrow H^i(K, M), \qquad \mathrm{cores}_{K/F} : H^i(K, M) \longrightarrow H^i(F, M)$$

denote the restriction and corestriction maps in cohomology, respectively. Recall that for K/F finite and Galois there is an equality

$$\mathrm{res}_{K/F} \circ \mathrm{cores}_{K/F} = \mathbf{N}_{K/F} \tag{1}$$

where $\mathbf{N}_{K/F} := \sum_{\sigma \in \mathrm{Gal}(K/F)} \sigma$ is the Galois norm (or trace) operator acting on $H^i(K, M)$.

Fix algebraic closures $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and $\bar{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ for any prime number ℓ, and then fix field embeddings $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ for every ℓ. Let $\mathbb{Q}_\ell^{\mathrm{nr}}$ be the maximal unramified extension of $\mathbb{Q}_\ell$ inside $\bar{\mathbb{Q}}_\ell$ and write F_ℓ for the arithmetic Frobenius in $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{nr}}/\mathbb{Q}_\ell)$. With an abuse of notation, when dealing with a $G_{\mathbb{Q}}$-module that is unramified at ℓ we shall often adopt the same symbol to denote a lift of F_ℓ to $G_{\mathbb{Q}_\ell}$ (and its image in $G_{\mathbb{Q}}$).

Finally, if L/E is a Galois extension of number fields, λ is a prime of E that is unramified in L andff λ' is a prime of L above λ, then $\mathrm{Frob}_{\lambda'/\lambda} \in \mathrm{Gal}(L/E)$ denotes the Frobenius substitution at λ'; the conjugacy class of $\mathrm{Frob}_{\lambda'/\lambda}$ in $\mathrm{Gal}(L/E)$ will be denoted by Frob_λ (notation not reflecting dependence on L).

2. Beilinson–Bloch conjecture for modular forms

As in the introduction, $f \in S_k(\Gamma_0(N))$ is a normalized newform of (even) weight k and level $\Gamma_0(N)$. Let F (respectively, $\mathcal{O}_f$) denote the totally real field (respectively, the commutative ring) generated over $\mathbb{Q}$ (respectively, over $\mathbb{Z}$) by the Fourier coefficients of f, and write $\mathcal{O}_F$ for the ring of integers of F. It follows that $\mathcal{O}_f$ is an order of F; let $c_f = [\mathcal{O}_F : \mathcal{O}_f]$ be the conductor of $\mathcal{O}_f$. Finally, let p be a prime number such that $p \nmid 2N(k-2)!\phi(N)c_f$, where ϕ is Euler's function.

Remark 2.1. For the arguments developed in this section, a more natural choice of p would simply require that $p \nmid 2Nc_f$ and $p > k-1$, as explained in [41, §6.5]. However, in this case the notation becomes more complicated, and some neatly stated results, for instance [39, Proposition 2.1], require substantial modifications to make them consistent. In order to emphasize the new aspects of our paper without indulging in unenlightening technicalities, we therefore decided to work under the simplifying assumption above.

2.1. **Galois representations.**

Denote by Y_N the affine modular curve over $\mathbb{Q}$ of level $\Gamma(N)$ and let $j : Y_N \hookrightarrow X_N$ be its proper smooth compactification.

For any integer $n \geq 1$ define the sheaves

$$\mathcal{F}_n := \mathrm{Sym}^{k-2}\big(R^1\pi_*(\mathbb{Z}/p^n\mathbb{Z})\big)(k/2-1), \qquad \mathcal{F} := \varprojlim_n \mathcal{F}_n$$

(both $\mathcal{F}_n$ and $\mathcal{F}$ depend on p, but we suppress this dependence to simplify the notation).

Let $B := \Gamma_0(N)/\Gamma(N)$, consider the projector $\Pi_B := (\#B)^{-1}\sum_{b\in B} b \in \mathbb{Z}_p[B]$ and define

$$J_p := \Pi_B H^1_{\text{ét}}(X_N \otimes \bar{\mathbb{Q}}, j_*\mathcal{F})(k/2).$$

Denote by $\mathbb{T}$ the Hecke algebra generated over $\mathbb{Z}$ by the standard Hecke operators T_ℓ for primes $\ell \nmid N$. Let $\theta_f : \mathbb{T} \to \mathcal{O}_F$ be the morphism of algebras associated with f. The Hecke algebra $\mathbb{T}$ acts on J_p, as explained in [39, pp. 101–102]. Set $I_f := \ker(\theta_f)$ and define

$$A_p := \{x \in J_p \mid I_f \cdot x = 0\}.$$

Then A_p, which should be regarded as a higher weight analogue of the Tate module of an abelian variety, is equipped with a continuous $\mathcal{O}_f$-linear action of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and is (isomorphic to) the $k/2$-twist of the representation attached to f by Deligne ([20]). More precisely, A_p is a free $\mathcal{O}_F \otimes \mathbb{Z}_p$-module of rank 2 such that for every prime $\ell \nmid Np$ the arithmetic Frobenius F_ℓ at ℓ acting on A_p satisfies

$$\det\bigl(1 - XF_\ell \,|\, A_p\bigr) = 1 - \frac{a_\ell}{\ell^{\frac{k}{2}-1}}X + \ell X^2. \tag{2}$$

Here we are implicitly using the canonical identification $\mathcal{O}_f \otimes \mathbb{Z}_p = \mathcal{O}_F \otimes \mathbb{Z}_p$, which is a consequence of the fact that, by assumption, $p \nmid c_f$. As pointed out in [39, p. 102], there is a map $J_p \to A_p$ that is both $\mathbb{T}$-equivariant and $G_{\mathbb{Q}}$-equivariant.

2.2. **Kuga–Sato varieties.** In this subsection we briefly recall basic definitions and facts about Kuga–Sato varieties, along the lines of [20], [39, §2], [53, §1] (see also [9, Appendix A] by Conrad for a generalization to the relative situation).

Let $\pi : \mathcal{E}_N \to Y_N$ be the universal elliptic curve and $\bar{\pi} : \bar{\mathcal{E}}_N \to X_N$ the universal generalized elliptic curve, which is proper but not smooth. Define

$$\bar{\pi}_{k-2} : \bar{\mathcal{E}}_N^{k-2} \longrightarrow X_N$$

to be the fiber product of $k-2$ copies of $\bar{\mathcal{E}}_N$ over X_N. If $k \geq 4$, then $\bar{\mathcal{E}}_N^{k-2}$ is singular and we call its canonical desingularization $\tilde{\mathcal{E}}_N^{k-2}$ constructed by Deligne ([20]) the *Kuga–Sato variety* of level N and weight k. Then $\dim\bigl(\tilde{\mathcal{E}}_N^{k-2}\bigr) = k-1$, and there is a map $\tilde{\pi}_{k-2} : \tilde{\mathcal{E}}_N^{k-2} \to X_N$.

The level N structure on $\bar{\mathcal{E}}_N$ induces a homomorphism $(\mathbb{Z}/N\mathbb{Z})^2 \times X_N \hookrightarrow \mathscr{E}_N$ of group schemes over X_N, where $\mathscr{E}_N$ is the Néron model of $\bar{\mathcal{E}}_N$ over X_N. Therefore $(\mathbb{Z}/N\mathbb{Z})^2$ acts by translations on $\bar{\mathcal{E}}_N$. Moreover, $\mathbb{Z}/2\mathbb{Z}$ acts as multiplication by -1 in the fibers, and this gives an action of $(\mathbb{Z}/N\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z})$ on $\bar{\mathcal{E}}_N$. Finally, the symmetric group S_{k-2} on $k-2$ letters acts on $\bar{\mathcal{E}}_N^{k-2}$ by permutation of the factors, and this gives an action of

$$\Gamma_{k-2} := \bigl((\mathbb{Z}/N\mathbb{Z})^2 \rtimes (\mathbb{Z}/2\mathbb{Z})\bigr)^{k-2} \rtimes S_{k-2}$$

on $\bar{\mathcal{E}}_N^{k-2}$ by automorphisms on the fibers of $\bar{\pi}_{k-2}$, which extends canonically to an action of Γ_{k-2} on $\tilde{\mathcal{E}}_N^{k-2}$.

Now define the homomorphism $\epsilon : \Gamma_{k-2} \to \{\pm 1\}$ to be trivial on $(\mathbb{Z}/N\mathbb{Z})^{2(k-2)}$, the product map on $(\mathbb{Z}/2\mathbb{Z})^{k-2}$ and the sign character on S_{k-2}. Finally, let

$$\Pi_\epsilon \in \mathbb{Z}[1/2N(k-2)!][\Gamma_{k-2}]$$

be the projector associated with ϵ.

Then, by [39, Proposition 2.1] (see also [53, Theorem 1.2.1] and [41, II, Proposition 2.4] for the analogous result with coefficients in $\mathbb{Q}_p$), we have

$$H^1_{\text{ét}}(X_N \otimes \bar{\mathbb{Q}}, j_*\mathcal{F}_n)(1) = \Pi_\epsilon H^{k-1}_{\text{ét}}\bigl(\tilde{\mathcal{E}}_N^{k-2} \otimes \bar{\mathbb{Q}}, \mathbb{Z}/p^n\mathbb{Z}\bigr)(k/2).$$

Moreover, thanks to [39, Lemma 2.2], we know that $H^1_{\text{ét}}(X_N, j_*\mathcal{F})$ is torsion-free and that there is a canonical isomorphism

$$H^1_{\text{ét}}(X_N, j_*\mathcal{F}/p^m j_*\mathcal{F}) \simeq H^1_{\text{ét}}(X_N, j_*\mathcal{F})/p^m H^1_{\text{ét}}(X_N, j_*\mathcal{F})$$

for every integer $m \geq 1$. Combining these facts we obtain a map

$$H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}_N^{k-2} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_p(k/2)\big) \longrightarrow J_p \longrightarrow A_p \tag{3}$$

that factors through $\Pi_\epsilon H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}_N^{k-2} \otimes \bar{\mathbb{Q}}, \mathbb{Z}/p^n\mathbb{Z}\big)(k/2)$.

2.3. **Abel–Jacobi maps.** Fix a field L of characteristic 0, denote by $\bar{L}$ an algebraic closure of L and let

$$\Phi_{p,L} : \mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big)_0 \longrightarrow H^1_{\text{cont}}\Big(L, H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}_N^{k-2} \otimes \bar{L}, \mathbb{Z}_p(k/2)\big)\Big) \tag{4}$$

be the p-adic Abel–Jacobi map (see [25, §9]). Here $\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big)_0$ is the group of homologically trivial cycles of codimension $k/2$ on $\tilde{\mathcal{E}}_N^{k-2}$ defined over L modulo rational equivalence, and H^1_{cont} denotes continuous cohomology. Equivalently,

$$\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big)_0 = \ker\Big(\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big) \longrightarrow H^k_{\text{ét}}\big(\tilde{\mathcal{E}}_N^{k-2} \otimes \bar{L}, \mathbb{Z}_p(k/2)\big)\Big), \tag{5}$$

where $\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big)$ is the group of cycles of codimension $k/2$ on $\tilde{\mathcal{E}}_N^{k-2}$ defined over L modulo rational equivalence. Indeed, using the Lefschetz principle and comparison isomorphisms between étale and singular cohomology over $\mathbb{C}$, it can be proved that the right hand side of (5) does not depend on p (see, e.g., [42, §1.3] for details).

Composing (3) and (4) and extending $\mathbb{Z}_p$-linearly, if L is a number field, then we get a map

$$\mathrm{AJ}_{f,p,L} : \mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big)_0 \otimes \mathbb{Z}_p \longrightarrow H^1_{\text{cont}}(L, A_p). \tag{6}$$

Now we localize (or, rather, complete) the representation A_p at a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ dividing p. More precisely, if $\mathfrak{p}$ is such a prime, then denote by $\mathcal{O}_\mathfrak{p}$ the completion of $\mathcal{O}_F$ at $\mathfrak{p}$ and set $A_\mathfrak{p} := A_p \otimes_{\mathcal{O}_F \otimes \mathbb{Z}_p} \mathcal{O}_\mathfrak{p}$, which is a free $\mathcal{O}_\mathfrak{p}$-module of rank 2 equipped with a $G_\mathbb{Q}$-action. It follows that $A_p = \prod_{\mathfrak{p} \mid p} A_\mathfrak{p}$, the product being taken over all prime ideals of $\mathcal{O}_F$ above p. Fix once and for all a prime ideal $\mathfrak{p}$ as above. Composing the map $\mathrm{AJ}_{f,p,L}$ introduced in (6) with the one induced by the canonical projection $A_p \twoheadrightarrow A_\mathfrak{p}$, we get an $\mathcal{O}_\mathfrak{p}$-linear map

$$\mathrm{AJ}_{f,\mathfrak{p},L} : \mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big)_0 \otimes \mathcal{O}_\mathfrak{p} \longrightarrow H^1_{\text{cont}}(L, A_\mathfrak{p}). \tag{7}$$

If L is a Galois extension of L', then $\mathrm{AJ}_{f,\mathfrak{p},L}$ is $\mathrm{Gal}(L/L')$-equivariant with respect to the natural Galois actions on domain and codomain ([39, Proposition 4.2]). For simplicity, from here on we write AJ_L for $\mathrm{AJ}_{f,\mathfrak{p},L}$, understanding that we are fixing a prime $\mathfrak{p}$ of F above p.

Finally, let us introduce another map that will be used in §3.1. Since the Abel–Jacobi map commutes with automorphisms of the underlying variety, the map $\mathrm{AJ}_{f,p,L}$ in (6) factors through

$$\Pi_\epsilon\Big(\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big)_0 \otimes \mathbb{Z}_p\Big) = \Pi_\epsilon\Big(\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big) \otimes \mathbb{Z}_p\Big);$$

here the equality follows from [39, Proposition 2.1]; see also [39, p. 105]. Thus (7) yields a map

$$\Psi_{f,\mathfrak{p},L} : \Pi_B\Pi_\epsilon\Big(\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/L\big) \otimes \mathcal{O}_\mathfrak{p}\Big) \longrightarrow H^1_{\text{cont}}(L, A_\mathfrak{p}). \tag{8}$$

This map is $\mathbb{T}$-equivariant and if L is Galois over $\mathbb{Q}$, then it is $\mathrm{Gal}(L/\mathbb{Q})$-equivariant as well (use [39, Proposition 4.2] and apply the projection $A_p \twoheadrightarrow A_\mathfrak{p}$, which is both $\mathbb{T}$- and $\mathrm{Gal}(L/\mathbb{Q})$-equivariant).

2.4. **Selmer groups.** Let E be a number field and denote by $G_E := \mathrm{Gal}(\bar{E}/E)$ its absolute Galois group. Let $\mathcal{V}$ be a p-adic representation of G_E (i.e., a finite-dimensional $\mathbb{Q}_p$-vector space $\mathcal{V}$ equipped with a continuous action of G_E) unramified outside a finite set Ξ of places of E containing all the archimedean primes and the primes above p. If v is a prime of E above p, then, as in [12, §§3 and 5], define

$$H^1_f(E_v,\mathcal{V}) := \ker\Big(H^1_{\mathrm{cont}}(E_v,\mathcal{V}) \longrightarrow H^1_{\mathrm{cont}}\big(E_v,\mathcal{V}\otimes_{\mathbb{Q}_p} B_{\mathrm{cris}}\big)\Big),$$

where B_{cris} is Fontaine's crystalline ring of periods (see, e.g., [12, §1], and do not confuse the subscript "f" in H^1_f with our fixed modular form f!). If v is a prime of E not dividing p, then write $I_v := \mathrm{Gal}(\bar{E}_v/E_v^{\mathrm{ur}})$ for the inertia subgroup of $\mathrm{Gal}(\bar{E}_v/E_v)$, where E_v^{ur} denotes the maximal unramified extension of E_v. The unramified cohomology of $\mathcal{V}$ at v is defined as

$$H^1_{\mathrm{ur}}(E_v,\mathcal{V}) := H^1_{\mathrm{cont}}\big(\mathrm{Gal}(E_v^{\mathrm{ur}}/E_v),\mathcal{V}^{I_v}\big) \simeq \ker\Big(H^1_{\mathrm{cont}}(E_v,\mathcal{V}) \longrightarrow H^1_{\mathrm{cont}}(I_v,\mathcal{V})\Big),$$

the isomorphism coming from the inflation-restriction exact sequence (i.e., the exact sequence of low degree terms in the relevant Hochschild–Serre spectral sequence). Finally, for such a prime v of E set

$$H^1_f(E_v,\mathcal{V}) := H^1_{\mathrm{ur}}(E_v,\mathcal{V}).$$

Definition 2.2. The *Bloch–Kato Selmer group* $H^1_f(E,\mathcal{V})$ is the $\mathbb{Q}_p$-subspace of $H^1_{\mathrm{cont}}(E,\mathcal{V})$ consisting of those classes whose localizations lie in $H^1_f(E_v,\mathcal{V})$ for all primes v of E.

Let $G_{E,\Xi}$ denote the Galois group over E of the maximal extension of E unramified outside Ξ. Then $\mathcal{V}$ is a representation of $G_{E,\Xi}$ and $H^1_f(E,\mathcal{V})$ is a subspace of the finite-dimensional $\mathbb{Q}_p$-vector space $H^1_{\mathrm{cont}}(G_{E,\Xi},\mathcal{V})$; hence $H^1_f(E,\mathcal{V})$ has finite dimension over $\mathbb{Q}_p$.

Now we specialize the previous discussion to the case where

$$\mathcal{V} = H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}_N^{k-2}\otimes\bar{E},\mathbb{Q}_p(k/2)\big). \tag{9}$$

It is well known that $\mathcal{V}$ is unramified outside the primes of E dividing Np; in light of this, from here on we take

$$\Xi := \big\{v \text{ place of } E \;\big|\; v\,|\,Np \text{ or } v\,|\,\infty\big\}. \tag{10}$$

Remark 2.3. With $\mathcal{V}$ as in (9), the Selmer group $H^1_f(E,\mathcal{V})$ of Definition 2.2 is equal to the one originally defined in [12] and later studied, e.g., by Besser in [10]. In particular, it is smaller than the group considered by Nekovář in [39]; this is due to the fact that no local conditions at the places of E dividing N are imposed in [39] (cf. [39, p. 118]).

Let

$$\Phi_{p,E}\otimes\mathbb{Q}_p : \mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/E\big)_0\otimes\mathbb{Q}_p \longrightarrow H^1_{\mathrm{cont}}\Big(E,H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}_N^{k-2}\otimes\bar{E},\mathbb{Q}_p(k/2)\big)\Big) \tag{11}$$

be the map induced by the Abel–Jacobi map in (4).

Theorem 2.4 (Nizioł, Nekovář, Saito)**.** *There is an inclusion*

$$\mathrm{im}(\Phi_{p,E}\otimes\mathbb{Q}_p) \subset H^1_f\Big(E,H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}_N^{k-2}\otimes\bar{E},\mathbb{Q}_p(k/2)\big)\Big). \tag{12}$$

In particular, $\mathrm{im}(\Phi_{p,E}\otimes\mathbb{Q}_p)$ *is a finite-dimensional vector space over* $\mathbb{Q}_p$.

Proof. Let v be a prime of E and, for simplicity, set

$$\mathcal{V}_v := H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}^{k-2}_N \otimes \bar{E}_v, \mathbb{Q}_p(k/2)\big).$$

We need to show that there is an inclusion

$$\operatorname{im}(\Phi_{p,E_v} \otimes \mathbb{Q}_p) \subset H^1_f(E_v, \mathcal{V}_v),$$

where the map $\Phi_{p,E_v} \otimes \mathbb{Q}_p$ is defined as in (11) with E replaced by E_v. If $v \nmid p$, then the weight-monodromy conjecture ([51, p. 428]) is known to hold for compactified Kuga–Sato varieties over E_v ([50], [51]), and so $H^1_{\text{cont}}(E_v, \mathcal{V}_v) = 0$ by [42, Proposition 2.5]. On the other hand, if $v \mid p$, then $\tilde{\mathcal{E}}^{k-2}_N$ has good reduction at v (recall that $\tilde{\mathcal{E}}^{k-2}_N$ has good reduction outside N and $p \nmid N$), hence $\operatorname{im}(\Phi_{p,E_v} \otimes \mathbb{Q}_p) \subset H^1_f(E_v, \mathcal{V}_v)$ by [46, Theorem 3.2]. Finally, the last assertion follows from the finite dimensionality over $\mathbb{Q}_p$ of the right hand side of (12). $\square$

Remark 2.5. The result used above was proved in [46] under a projectivity assumption on the relevant algebraic varieties, but this stronger condition can be dispensed with, as explained in [42, Theorem 3.1].

We will now consider Selmer groups of $A_\mathfrak{p}$ and of quotients of it, and use Theorem 2.4 to describe them. For simplicity, assume that the prime number p does not ramify in F. Define the $F_\mathfrak{p}$-vector space $V_\mathfrak{p} := A_\mathfrak{p} \otimes_{\mathcal{O}_\mathfrak{p}} F_\mathfrak{p}$. For every integer $m \geq 1$ define $W_\mathfrak{p} := A_\mathfrak{p} \otimes \mathbb{Q}_p/\mathbb{Z}_p$, so that $W_\mathfrak{p}[p^m] = A_\mathfrak{p}/p^m A_\mathfrak{p}$. For any place v of E there are maps

$$\varphi_v : H^1(E_v, A_\mathfrak{p}) \longrightarrow H^1(E_v, V_\mathfrak{p}), \qquad \pi_v : H^1(E_v, A_\mathfrak{p}) \longrightarrow H^1(E_v, W_\mathfrak{p}[p^m])$$

induced by the canonical arrows $A_\mathfrak{p} \hookrightarrow V_\mathfrak{p}$ and $A_\mathfrak{p} \twoheadrightarrow W_\mathfrak{p}[p^m]$. Set

$$H^1_f(E_v, A_\mathfrak{p}) := \varphi_v^{-1}\big(H^1_f(E_v, V_\mathfrak{p})\big), \qquad H^1_f(E_v, W_\mathfrak{p}[p^m]) := \pi_v\big(H^1_f(E_v, A_\mathfrak{p})\big).$$

In the following definition M denotes either $A_\mathfrak{p}$ or $W_\mathfrak{p}[p^m]$.

Definition 2.6. The *Bloch–Kato Selmer group* $H^1_f(E, M)$ of M over E is the subgroup of $H^1_{\text{cont}}(E, M)$ consisting of the classes whose localizations lie in $H^1_f(E_v, M)$ for all v.

If Ξ is as in (10), then $A_\mathfrak{p}$ is a $G_{E,\Xi}$-module and $H^1_f(E, W_\mathfrak{p}[p^m])$ is a subgroup of the finite group $H^1(G_{E,\Xi}, W_\mathfrak{p}[p^m])$; hence $H^1_f(E, W_\mathfrak{p}[p^m])$ is a finite $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-module.

As in (9), set $\mathcal{V} := H^{k-1}_{\text{ét}}\big(\tilde{\mathcal{E}}^{k-2}_N \otimes \bar{E}, \mathbb{Q}_p(k/2)\big)$. To clarify the various relations between Abel–Jacobi maps and Selmer groups, observe that there is a commutative diagram

$$
\begin{tikzcd}
\mathrm{CH}^{k/2}(\tilde{\mathcal{E}}_N^{k-2}/E)_0 \otimes \mathbb{Q}_p \arrow[rr, "\Phi_{p,E}\otimes\mathbb{Q}_p"] \arrow[d] & & H^1_f(E,\mathcal{V}) \arrow[d, "\lambda"] \\
\mathrm{CH}^{k/2}(\tilde{\mathcal{E}}_N^{k-2}/E)_0 \otimes F_\mathfrak{p} \arrow[r, "\mathrm{AJ}_E\otimes F_\mathfrak{p}"] & H^1_{\mathrm{cont}}(E,V_\mathfrak{p}) & H^1_f(E,V_\mathfrak{p}) \arrow[l, hook'] \\
\mathrm{CH}^{k/2}(\tilde{\mathcal{E}}_N^{k-2}/E)_0 \otimes \mathcal{O}_\mathfrak{p} \arrow[r, "\mathrm{AJ}_E"] \arrow[u] \arrow[d, two heads] & H^1_{\mathrm{cont}}(E,A_\mathfrak{p}) \arrow[u, "\varphi"] \arrow[d, "\varpi"] & H^1_f(E,A_\mathfrak{p}) \arrow[l, hook'] \arrow[u, "\varphi"] \arrow[d, two heads, "\varpi"] \\
\mathrm{CH}^{k/2}(\tilde{\mathcal{E}}_N^{k-2}/E)_0 \otimes (\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}) \arrow[r, "\mathrm{AJ}_{E,m}"] & H^1_{\mathrm{cont}}(E,W_\mathfrak{p}[p^m]) & H^1_f(E,W_\mathfrak{p}[p^m]) \arrow[l, hook']
\end{tikzcd}
\tag{13}
$$

where

- the map λ comes from the map $\mathcal{V}\to V_\mathfrak{p}$ that is obtained by tensoring both sides of (3) by $\mathbb{Q}_p$ over $\mathbb{Z}_p$, noting that $A_p\otimes_{\mathbb{Z}_p}\mathbb{Q}_p=\prod_{\mathfrak{q}|p}V_\mathfrak{q}$ and then composing with the projection onto $V_\mathfrak{p}$;
- the maps φ and ϖ are induced by $A_\mathfrak{p}\hookrightarrow V_\mathfrak{p}$ and $A_\mathfrak{p}\twoheadrightarrow W_\mathfrak{p}[p^m]$, respectively;
- the unlabeled vertical arrows are induced by the natural maps $\mathbb{Q}_p\hookrightarrow F_\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}\hookrightarrow F_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}\twoheadrightarrow \mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$;
- the maps $\mathrm{AJ}_E\otimes F_\mathfrak{p}$ and $\mathrm{AJ}_{E,m}$ are induced by multiplication by elements of $F_\mathfrak{p}$ and of $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$, respectively.

Corollary 2.7. *There are inclusions*

(1) $\mathrm{im}(\mathrm{AJ}_E\otimes F_\mathfrak{p})\subset H^1_f(E,V_\mathfrak{p})$*;*
(2) $\mathrm{im}(\mathrm{AJ}_E)\subset H^1_f(E,A_\mathfrak{p})$*;*
(3) $\mathrm{im}(\mathrm{AJ}_{E,m})\subset H^1_f(E,W_\mathfrak{p}[p^m])$*.*

In particular, the $F_\mathfrak{p}$*-vector space* $\mathrm{im}(\mathrm{AJ}_E\otimes F_\mathfrak{p})$ *has finite dimension.*

Proof. All the inclusions follow easily from the definitions and the commutativity of diagram (13). To check the last assertion, note that $H^1_f(E,V_\mathfrak{p})$ is finite-dimensional over $F_\mathfrak{p}$ because $V_\mathfrak{p}$ is unramifed outside the finite set Ξ introduced in (10). □

For any number field E define

$$\Lambda_\mathfrak{p}(E):=\mathrm{im}(\mathrm{AJ}_E)\subset H^1_f(E,A_\mathfrak{p}) \tag{14}$$

and

$$X_\mathfrak{p}(E):=\varphi\big(\Lambda_\mathfrak{p}(E)\big)\otimes_{\mathcal{O}_\mathfrak{p}}F_\mathfrak{p}\subset H^1_f(E,V_\mathfrak{p}).$$

If E is Galois over $\mathbb{Q}$, then $\Lambda_\mathfrak{p}(E)$ and $X_\mathfrak{p}(E)$ are equipped with $\mathrm{Gal}(E/\mathbb{Q})$-actions.

Proposition 2.8. *There is an isomorphism*

$$\Lambda_\mathfrak{p}(E)/p^m\,\Lambda_\mathfrak{p}(E)\simeq \mathrm{im}(\mathrm{AJ}_{E,m})$$

of finite $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$*-modules.*

Proof. Taking continuous cohomology of the short exact sequence of Galois modules

$$0\longrightarrow A_\mathfrak{p}\xrightarrow{p^m}A_\mathfrak{p}\longrightarrow A_\mathfrak{p}/p^mA_\mathfrak{p}\longrightarrow 0,$$

where the second arrow is the multiplication-by-p^m map and the third arrow is the canonical projection, and using the identification $W_\mathfrak{p}[p^m] = A_\mathfrak{p}/p^m A_\mathfrak{p}$, yield an injection

$$i : H^1_{\mathrm{cont}}(E, A_\mathfrak{p}) \otimes_{\mathcal{O}_\mathfrak{p}} (\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}) \longhookrightarrow H^1(E, W_\mathfrak{p}[p^m])$$

of $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-modules. If $j : H^1_f(E, W_\mathfrak{p}[p^m]) \hookrightarrow H^1(E, W_\mathfrak{p}[p^m])$ denotes the natural inclusion, then part (3) of Corollary 2.7 implies that $\mathrm{AJ}_{E,m}$ factors through j, and therefore the diagram

$$\begin{tikzcd}
\mathrm{CH}^{k/2}\big(\tilde{\mathcal{E}}_N^{k-2}/E\big)_0 \otimes (\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}) \arrow[r, "\Psi"] \arrow[d, "\mathrm{AJ}_{E,m}"] & H^1_{\mathrm{cont}}(E, A_\mathfrak{p}) \otimes_{\mathcal{O}_\mathfrak{p}} (\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}) \arrow[d, hook, "i"] \\
H^1_f(E, W_\mathfrak{p}[p^m]) \arrow[r, hook, "j"] & H^1(E, W_\mathfrak{p}[p^m]),
\end{tikzcd}$$

where Ψ is the $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-linear extension of AJ_E, commutes. Thus $\mathrm{im}(i\circ\Psi)$ is equal to $\mathrm{im}(j \circ \mathrm{AJ}_{E,m})$, and the injectivity of i and j shows that $\mathrm{im}(\Psi) \simeq \mathrm{im}(\mathrm{AJ}_{E,m})$. On the other hand, $\mathrm{im}(\Psi) = \Lambda_\mathfrak{p}(E)/p^m\,\Lambda_\mathfrak{p}(E)$, and we are done. ☐

In particular, Proposition 2.8 implies that there is an injection

$$\Lambda_\mathfrak{p}(E)/p^m\,\Lambda_\mathfrak{p}(E) \longhookrightarrow H^1_f(E, W_\mathfrak{p}[p^m]) \tag{15}$$

of finite $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-modules; this map is Galois-equivariant if E is Galois over $\mathbb{Q}$.

Remark 2.9. By an abuse of notation, we will often adopt the same symbol to denote an element of $\Lambda_\mathfrak{p}(E)/p^m\,\Lambda_\mathfrak{p}(E)$ and its image in $H^1_f(E, W_\mathfrak{p}[p^m])$ via (15).

2.5. **Beilinson–Bloch conjecture.** Now we recall the Beilinson–Bloch conjecture in this setting. Let E be a number field and let $L(f\otimes E, s)$ be the complex L-function of f over E.

Conjecture 2.10 (Beilinson–Bloch, [1], [11])**.** $\dim_{\mathbb{F}_\mathfrak{p}}\big(X_\mathfrak{p}(E)\big) = \mathrm{ord}_{s=\frac{k}{2}} L(f\otimes E, s)$.

For details, see [25, pp. 158–168]. For generalizations to L-functions of motives, see [12]. The main result of [39], combined with the Gross–Zagier type formula for higher weight modular forms due to Zhang ([55]), gives the following result in the direction of the Beilinson–Bloch conjecture.

Theorem 2.11 (Nekovář, Zhang)**.** *Let K be an imaginary quadratic field in which all the prime numbers dividing N split and assume that the Abel–Jacobi map AJ_K is injective. If $\mathrm{ord}_{s=\frac{k}{2}} L(f \otimes K, s) = 1$, then $\dim_{\mathbb{F}_\mathfrak{p}}\big(X_\mathfrak{p}(K)\big) = 1$.*

See [55, §5.3] for other results on the Beilinson–Bloch conjecture, especially when the base field is $\mathbb{Q}$.

3. Divisibility properties of Heegner cycles

After reviewing the basic properties of Heegner cycles and the formalism of Darmon–Kolyvagin derivatives, we construct Kolyvagin classes attached to Heegner cycles and study their properties. The main result of this section (Theorem 3.34) is a congruence relation satisfied by these cohomology classes.

Fix throughout this paper an imaginary quadratic field K of discriminant D in which all the primes dividing N split (in other words, K satisfies the so-called "Heegner hypothesis" relative to N). Denote by $\mathcal{O}_K$ the ring of integers of K and by h_K its class number. For the sake of simplicity, assume also that $\mathcal{O}_K^\times = \{\pm 1\}$, i.e., that $K \neq \mathbb{Q}(\sqrt{-1})$ and $K \neq \mathbb{Q}(\sqrt{-3})$. Finally, fix an embedding $K \hookrightarrow \mathbb{C}$.

3.1. **Heegner cycles.** We review construction and basic properties of Heegner cycles on Kuga–Sato varieties. In doing this, we follow [39] and [41] closely (for Heegner-type cycles on more general varieties that are fibered over modular curves, see [9, §2]).

Fix an ideal $\mathcal{N} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$, which exists thanks to the Heegner hypothesis satisfied by K. For any integer $T \geq 1$ prime to NDp let $\mathcal{O}_T := \mathbb{Z} + T\mathcal{O}_K$ be the order of K of conductor T. Let $X_0(N)$ be the compact modular curve of level $\Gamma_0(N)$; the isogeny $\mathbb{C}/\mathcal{O}_T \to \mathbb{C}/(\mathcal{O}_T \cap \mathcal{N})^{-1}$ defines a Heegner point $x_T \in X_0(N)$ that, by the theory of complex multiplication, is rational over the ring class field K_T of K of conductor T (in particular, K_1 is the Hilbert class field of K).

Write $\kappa : X_N \to X_0(N)$ for the map induced by the inclusion $\Gamma(N) \subset \Gamma_0(N)$ and choose $\tilde{x}_T \in \kappa^{-1}(x_T)$. The elliptic curve E_T corresponding to $\tilde{x}_T$ has complex multiplication by $\mathcal{O}_T$. Fix the unique square root $\xi_T = \sqrt{-DT^2}$ of the discriminant of $\mathcal{O}_T$ with positive imaginary part under the chosen embedding of K into $\mathbb{C}$. For any $a \in \mathcal{O}_T$ let $\Gamma_{T,a} \subset E_T \times E_T$ denote the graph of a and let $i_{\tilde{x}_T} : \tilde{\pi}_{k-2}^{-1}(\tilde{x}_T) = E_T^{k-2} \hookrightarrow \tilde{\mathcal{E}}_N^{k-2}$ be the canonical inclusion. Then

$$\Pi_B\Pi_\epsilon(i_{\tilde{x}_T})_*\Big(\Gamma_{T,\xi_T}^{(k-2)/2}\Big) \in \Pi_B\Pi_\epsilon\Big(\mathrm{CH}^{k/2}(\tilde{\mathcal{E}}_N^{k-2}/K_T) \otimes \mathbb{Z}_p\Big), \tag{16}$$

and we define the *Heegner cycle*

$$y_{T,\mathfrak{p}} \in H^1_{\mathrm{cont}}(K_T, A_\mathfrak{p})$$

to be the image of the cycle in (16) via the map $\Psi_{f,\mathfrak{p},K_T}$ introduced in (8). This class is independent of the choice of $\tilde{x}_T$ ([39, p. 107]) and, by [41, Ch. II, §3.6], does not change if Γ_{T,ξ_T} is replaced by $\Gamma_{T,\xi_T} \smallsetminus [(E_T \times \{0\}) \cup (\{0\} \times E_T)]$ in (16), which is the choice made in [39, §5]. Finally, note that

$$y_{T,\mathfrak{p}} \in \Lambda_\mathfrak{p}(K_T)$$

because the Abel–Jacobi map AJ_{K_T} factors through $\Psi_{f,\mathfrak{p},K_T}$.

Define

$$\mathcal{S} := \big\{\ell \text{ prime number } \mid \ell \text{ is inert in } K \text{ and } \ell \nmid Np\big\}. \tag{17}$$

For each $\ell \in \mathcal{S}$ the extension K_ℓ/K_1 is cyclic of order $\ell + 1$ and unramified at primes different from ℓ. Also, if $\ell \neq \ell'$ are in $\mathcal{S}$, then K_ℓ and $K_{\ell'}$ are linearly disjoint over K_1. Fix a product $T = \prod_{i=1}^s \ell_i$ of distinct primes $\ell_i \in \mathcal{S}$, then put $G_T := \mathrm{Gal}(K_T/K_1)$ and $\Gamma_T := \mathrm{Gal}(K_T/K)$. The field K_T is the composite of the fields K_{ℓ_i}, which are linearly disjoint over K_1, and so there is a decomposition $G_T = \prod_{i=1}^s G_{\ell_i}$. In particular, if $T' \mid T$, then there is a canonical inclusion $G_{T'} \subset G_T$, using which we identify the elements of $G_{T'}$ with their images in G_T. Finally, set $\Gamma_1 := \mathrm{Gal}(K_1/K)$, so that $\Gamma_1 \simeq \mathrm{Pic}(\mathcal{O}_K)$ and $|\Gamma_1| = h_K$.

Let us recall two basic properties of Heegner cycles, which extend those of Heegner points and are due to Nekovář ([39]). Before stating them, we fix some notation that will be used in the rest of the paper.

Choose a complex conjugation $c \in G_\mathbb{Q}$ and use the same symbol to denote the images of c in quotients of $G_\mathbb{Q}$; in other words, c is a lift to $G_\mathbb{Q}$ of the generator of $\mathrm{Gal}(K/\mathbb{Q})$. We shall also write Frob_∞ for the conjugacy class of c in $\mathrm{Gal}(E/\mathbb{Q})$, relying on the context to make clear which number field E we are considering. Finally, recall that $\mathrm{cores}_{K_{T\ell}/K_T}$ denotes the corestriction map from $H^1(K_{T\ell}, A_\mathfrak{p})$ to $H^1(K_T, A_\mathfrak{p})$ and let ϵ be the sign of the functional equation of $L(f,s)$.

Proposition 3.1. *Let T be a square-free product of primes in $\mathcal{S}$.*

(1) *If $\ell \in \mathcal{S}$, $\ell \nmid T$, then* $\mathrm{cores}_{K_{T\ell}/K_T}(y_{T\ell,\mathfrak{p}}) = (a_\ell/\ell^{k/2-1}) \cdot y_{T,\mathfrak{p}}$.

(2) *There exists $\sigma \in \Gamma_T$ such that $c(y_{T,\mathfrak{p}}) = -\epsilon \cdot \sigma(y_{T,\mathfrak{p}})$.*

Proof. Upon applying the projection $A_p \twoheadrightarrow A_\mathfrak{p}$, part (1) is [39, Proposition 6.1, (1)], while part (2) is [39, Proposition 6.2]. (Note the misprint in loc. cit., since the Hecke action is twisted by $k/2-1$.) □

Remark 3.2. The relations stated in Proposition 3.1, together with the Key Formula appearing in [39, §9] (which will be used in the proof of Proposition 3.20 below), describe an *Euler system* for modular forms of weight $k > 2$. Euler systems for higher weight modular forms can also be constructed by using Howard's work [24] on the variation of Heegner points in Hida families, later extended to the case of indefinite Shimura curves in [22] and [32], by specialization to weight k. The relation between the two systems has been investigated by Castella in [16], and we expect that a similar approach could be adopted in the case of indefinite Shimura curves as well. We finally remark that, in yet another direction, it would be interesting to generalize to higher weight the Euler systems of Heegner points introduced by means of congruences between modular forms in [8] and developed in [26], [27], [28], [29], [30], [45]. In connection with this, see recent work by Chida and Hsieh ([17]).

3.2. **$\pm$-eigenspaces.** Recall that if M is an abelian group endowed with an action of an involution τ and 2 is invertible in $\mathrm{End}(M)$, then there is a decomposition $M = M^+ \oplus M^-$ where $M^\pm$ is the subgroup of M on which τ acts as ± 1.

Let p be a prime number as in the introduction and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ above p. Since $\mathrm{Gal}(K/\mathbb{Q})$ acts on $X_\mathfrak{p}(K)$, the formalism above applies and there is a decomposition

$$X_\mathfrak{p}(K) = X_\mathfrak{p}(K)^+ \oplus X_\mathfrak{p}(K)^-.$$

Define $\rho_\mathfrak{p}^\pm := \dim_{F_\mathfrak{p}}\big(X_\mathfrak{p}(K)^\pm\big)$ and

$$\rho_\mathfrak{p} := \begin{cases} \max\{\rho_\mathfrak{p}^+, \rho_\mathfrak{p}^-\} - 1 & \text{if } \rho_\mathfrak{p}^+ \neq \rho_\mathfrak{p}^-, \\ \rho_\mathfrak{p}^+ & \text{otherwise.} \end{cases} \tag{18}$$

Two remarks on these definitions, both related to the Beilinson–Bloch conjecture, are now in order.

Remark 3.3. (1) Conjecture 2.10 predicts, among other things, that the $F_\mathfrak{p}$-dimension of $X_\mathfrak{p}(E)$ does not depend on $\mathfrak{p}$, and therefore $\rho_\mathfrak{p}^+ + \rho_\mathfrak{p}^-$ is conjecturally independent of $\mathfrak{p}$. Moreover, let $f \otimes \epsilon_K$ be the twist of f by the quadratic Dirichlet character ϵ_K attached to the extension $K/\mathbb{Q}$. It can be shown (see [33, §6.1] for details; in [33] a p-ordinarity assumption is made, but this condition plays no role in the results about Selmer groups that we are interested in) that

$$X_\mathfrak{p}(K)^+ \simeq X_\mathfrak{p}(\mathbb{Q}) = \mathrm{im}(\Psi_{f,\mathfrak{p},\mathbb{Q}}) \otimes_{\mathcal{O}_\mathfrak{p}} F_\mathfrak{p}, \qquad X_\mathfrak{p}(K)^- \simeq \mathrm{im}(\Psi_{f\otimes\epsilon_K,\mathfrak{p},\mathbb{Q}}) \otimes_{\mathcal{O}_\mathfrak{p}} F_\mathfrak{p}.$$

Therefore Conjecture 2.10 (for f and $E = \mathbb{Q}$ or $f \otimes \epsilon_K$ and $E = \mathbb{Q}$) implies that $\rho_\mathfrak{p}^+$ and $\rho_\mathfrak{p}^-$ do not depend on p.

(2) As before, let $L(f \otimes K, s)$ denote the L-function of f over K, so that

$$L(f \otimes K, s) = L(f, s) \cdot L(f \otimes \epsilon_K, s). \tag{19}$$

Since the orders of vanishing of $L(f,s)$ and $L(f \otimes \epsilon_K, s)$ at $s = k/2$ have opposite parities (cf., e.g., [13, p. 543]), it follows from (19) that $L(f \otimes K, s)$ vanishes to odd order at $s = k/2$. Therefore Conjecture 2.10 predicts that the $F_\mathfrak{p}$-dimension $\rho_\mathfrak{p}^+ + \rho_\mathfrak{p}^-$ of $X_\mathfrak{p}(K)$ should be odd. Hence we expect the second possibility in (18) not to occur.

3.3. **Rank inequalities.** As a consequence of the structure theorem for finitely generated modules over principal ideal domains, a finite $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-module M can be decomposed as

$$M \simeq (\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p})^{r_{\mathfrak{p},m}(M)} \oplus \tilde{M} \tag{20}$$

where the exponent of $\tilde{M}$ divides p^m strictly and the integer $r_{\mathfrak{p},m}(M)$ does not depend on such a decomposition (see Lemma 3.4 below).

Let $\mathbb{F}_\mathfrak{p} := \mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}$ be the residue field of $\mathcal{O}_\mathfrak{p}$. In the sequel we will make use of the following auxiliary result.

Lemma 3.4. *Let M, M', M'' be finite $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-modules.*

(1) *If there is an injective homomorphism $M \hookrightarrow M'$, then $r_{\mathfrak{p},m}(M) \le r_{\mathfrak{p},m}(M')$.*
(2) *If there is a surjective homomorphism $M \twoheadrightarrow M'$, then $r_{\mathfrak{p},m}(M) \ge r_{\mathfrak{p},m}(M')$.*
(3) *If there is an exact sequence of $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-modules*
$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'',$$
then
$$r_{\mathfrak{p},m}(M) \le r_{\mathfrak{p},m}(M') + \dim_{\mathbb{F}_\mathfrak{p}}(M'' \otimes_{\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}} \mathbb{F}_\mathfrak{p}).$$

Proof. An injection $M \hookrightarrow M'$ of $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-modules induces an injection $p^{m-1}M \hookrightarrow p^{m-1}M'$ of $\mathbb{F}_\mathfrak{p}$-vector spaces, hence
$$r_{\mathfrak{p},m}(M) = \dim_{\mathbb{F}_\mathfrak{p}}(p^{m-1}M) \le \dim_{\mathbb{F}_\mathfrak{p}}(p^{m-1}M') = r_{\mathfrak{p},m}(M'),$$
which shows part (1). On the other hand, a surjection $M \twoheadrightarrow M'$ of $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-modules induces a surjection $p^{m-1}M \twoheadrightarrow p^{m-1}M'$ of $\mathbb{F}_\mathfrak{p}$-vector spaces, and part (2) follows similarly. Finally, part (3) can be proved as [18, Lemma 5.1]. $\square$

As before, let K be our imaginary quadratic field where all the prime factors of N split. With notation as in (20), set
$$\tilde{r}_{\mathfrak{p},m} := r_{\mathfrak{p},m}\big(H^1_f(K, W_\mathfrak{p}[p^m])\big).$$
Moreover, recall the integers $\rho_\mathfrak{p}^\pm$ introduced in §3.2 and define

$$\tilde{\rho}_\mathfrak{p} := \rho_\mathfrak{p}^+ + \rho_\mathfrak{p}^- = \dim_{F_\mathfrak{p}}\big(X_\mathfrak{p}(K)\big). \tag{21}$$

A direct computation proves the following.

Lemma 3.5. $2\rho_\mathfrak{p} \ge \tilde{\rho}_\mathfrak{p} - 1$, *with equality holding if and only if* $|\rho_\mathfrak{p}^+ - \rho_\mathfrak{p}^-| = 1$.

Observe that there is an obvious inequality

$$\tilde{\rho}_\mathfrak{p} \le r_{\mathfrak{p},m}\big(\Lambda_\mathfrak{p}(K)/p^m\Lambda_\mathfrak{p}(K)\big). \tag{22}$$

Proposition 3.6. $\tilde{\rho}_\mathfrak{p} \le \tilde{r}_{\mathfrak{p},m}$.

Proof. It follows from Proposition 2.8 and Lemma 3.4 that

$$r_{\mathfrak{p},m}\big(\Lambda_\mathfrak{p}(K)/p^m\Lambda_\mathfrak{p}(K)\big) = r_{\mathfrak{p},m}\big(\mathrm{im}(\mathrm{AJ}_{K,m})\big) \le r_{\mathfrak{p},m}\big(H^1_f(K, W_\mathfrak{p}[p^m])\big) = \tilde{r}_{\mathfrak{p},m}. \tag{23}$$

Combining (22) and (23) gives the desired inequality. $\square$

Since p is odd, there is a splitting

$$H^1_f(K, W_\mathfrak{p}[p^m]) = H^1_f(K, W_\mathfrak{p}[p^m])^+ \oplus H^1_f(K, W_\mathfrak{p}[p^m])^-$$

under the action of complex conjugation $c \in \mathrm{Gal}(K/\mathbb{Q})$. Set

$$\tilde{r}^{\pm}_{\mathfrak{p},m} := r_{\mathfrak{p},m}\big(H^1_f(K, W_\mathfrak{p}[p^m])^{\pm}\big)$$

and define

$$r_{\mathfrak{p},m} := \begin{cases} \max\big\{\tilde{r}^+_{\mathfrak{p},m}, \tilde{r}^-_{\mathfrak{p},m}\big\} - 1 & \text{if } \tilde{r}^+_{\mathfrak{p},m} \neq \tilde{r}^-_{\mathfrak{p},m}, \\ \tilde{r}^+_{\mathfrak{p},m} & \text{otherwise.} \end{cases}$$

Recall the integer $\rho_\mathfrak{p}$ defined in (18).

Proposition 3.7. $\rho_\mathfrak{p} \leq r_{\mathfrak{p},m}$.

Proof. Combine the $\mathrm{Gal}(K/\mathbb{Q})$-equivariance of the Abel–Jacobi map with Proposition 3.6. □

3.4. **Darmon–Kolyvagin derivatives.** In this subsection we consider the general formalism of Darmon–Kolyvagin derivatives in the case of ring class fields of square-free conductor.

Fix a square-free product $S = \prod_{i=1}^t \ell_i$ of primes ℓ_i in $\mathcal{S}_{p^m}$. For a prime $\ell \mid S$ let σ_ℓ be a generator of G_ℓ. For any integer k such that $0 \leq k \leq \ell = \#G_\ell - 1$ define the derivative operator

$$\mathbf{D}^k_\ell := \sum_{i=k}^{\ell} \binom{i}{k} \sigma^i_\ell \in \mathbb{Z}[G_\ell] \subset \mathcal{O}_\mathfrak{p}[G_\ell].$$

If $\kappa = (k_1, \dots, k_t) \in \mathbb{Z}^t$ with $0 \leq k_i \leq \ell_i$, then the *Darmon–Kolyvagin κ-derivative* is

$$\mathbf{D}_\kappa := \mathbf{D}^{k_1}_{\ell_1} \cdots \mathbf{D}^{k_t}_{\ell_t} \in \mathbb{Z}[G_S] \subset \mathcal{O}_\mathfrak{p}[G_S].$$

The *order*, the *support* and the *conductor* of $\mathbf{D}_\kappa$ are defined as

$$\mathrm{ord}(\mathbf{D}_\kappa) := \sum_{i=1}^t k_i, \quad \mathrm{supp}(\mathbf{D}_\kappa) := S, \quad \mathrm{cond}(\mathbf{D}_\kappa) := \prod_{k_i > 0} \ell_i,$$

respectively, and we set

$$\eta(\kappa) := \min\big\{\mathrm{ord}_p(n_i) \;\mid\; k_i > 0\big\}.$$

Finally, given $\kappa = (k_1, \dots, k_s)$ and $\kappa' = (k'_1, \dots, k'_s)$ we say that $\mathbf{D}_{\kappa'}$ is *less than* $\mathbf{D}_\kappa$ if $k'_i \leq k_i$ for all i, and we write $\kappa' \leq \kappa$ in this case. Moreover, we say that $\mathbf{D}_{\kappa'}$ is *strictly less than* $\mathbf{D}_\kappa$, written $\kappa' < \kappa$, if $\kappa' \leq \kappa$ and $\kappa' \neq \kappa$.

Now we collect some basic facts about these derivatives. Most of them will not be used until Section 4, but we prefer to gather them here for the sake of clarity. The proofs are straightforward computations and will be omitted; see [18, §3.1 and §4.1] for details.

3.4.1. *Taylor's formula.* The *resolvent element* associated with an element m of an $\mathcal{O}_\mathfrak{p}[G_S]$-module M is defined as

$$\theta_m := \sum_{\sigma \in G_S} \sigma(m) \otimes \sigma \in M \otimes_{\mathcal{O}_\mathfrak{p}} \mathcal{O}_\mathfrak{p}[G_S].$$

Then

$$\theta_m = \sum_{\kappa} \mathbf{D}_\kappa(m) \otimes (\sigma_1 - 1)^{k_1} \dots (\sigma_t - 1)^{k_t},$$

where the sum is taken over all t-tuples of integers $\kappa = (k_1, \dots, k_t)$, with the convention that only those κ with $0 \le k_i \le \ell_i$ for all i appear in the sum above.

3.4.2. *Divisibility criterion.* Let I_{G_S} be the augmentation ideal of $\mathcal{O}_\mathfrak{p}[G_S]$ and let $r \le p$ be an integer. If $\mathbf{D}_\kappa(m) \equiv 0 \pmod{p^{\eta(\kappa)}}$ for all κ with $\mathrm{ord}(\kappa) < r$, then θ_m belongs to the natural image of $M \otimes_{\mathcal{O}_\mathfrak{p}} I_{G_S}^r$.

3.4.3. *Action of complex conjugation.* The action of $c \in \mathrm{Gal}(K/\mathbb{Q})$ by conjugation on $\Gamma_S = \mathrm{Gal}(K_S/K)$ sends σ to σ^{-1}. This induces an action of c on $\mathcal{O}_\mathfrak{p}[G_S]$ by linearity, and the formula

$$c\,\mathbf{D}_\kappa\, c^{-1} = (-1)^{\mathrm{ord}(\mathbf{D}_\kappa)} \mathbf{D}_\kappa + \sum_{\kappa' < \kappa} \alpha_{\kappa'} \mathbf{D}_{\kappa'}$$

holds for suitable integers $\alpha_{\kappa'}$.

3.4.4. *Some formulas.* For any prime $\ell \,|\, S$ and any integer k with $0 \le k \le \ell$ we have

$$(\sigma_\ell - 1)\mathbf{D}_\ell^k = \binom{\ell+1}{k} - \sigma_\ell \mathbf{D}_\ell^{k-1}.$$

In particular, since $p^m \,|\, \ell + 1$, for all $0 < k < p$ we have

$$(\sigma_\ell - 1)\mathbf{D}_\ell^k \equiv -\sigma_\ell \mathbf{D}_\ell^{k-1} \pmod{p^m}. \tag{24}$$

3.4.5. *Special bases.* An element $\xi \in \mathbb{Z}[G_\ell]$, for a prime $\ell \,|\, S$, can be written as a $\mathbb{Z}$-linear combination of the derivatives $\mathbf{D}_\ell^k$ for $k = 0, \dots, \ell$. Since this is not justified in [18], we give a short proof. Write $\xi = \sum_{i=0}^{\ell} a_i \sigma_\ell^i$. By rearranging the sums, one can check that a linear combination $\sum_{k=0}^{\ell} \alpha_k \mathbf{D}_\ell^k$ of derivatives can be written as $\sum_{i=0}^{\ell} \left(\sum_{k=0}^{i} \alpha_k \binom{i}{k} \right) \sigma_\ell^i$. Therefore we have to prove that we can find coefficients $\alpha_k \in \mathbb{Z}$ such that $\sum_{k=0}^{i} \alpha_k \binom{i}{k} = a_i$ for all $i = 0, \dots, \ell$. The generic equation in this system is

$$\alpha_0 + i\alpha_1 + \binom{i}{2}\alpha_2 + \dots + \binom{i}{i-1}\alpha_{i-1} + \alpha_i = a_i,$$

and the desired solution can be found recursively.

3.5. **The set of exceptional primes.** The main result of this section, Theorem 3.34, applies to all primes p outside a finite set Σ that we describe below.

Let Σ be the set of prime numbers p satisfying at least one of the following conditions:

- $p \,|\, 6ND(k-2)!\phi(N)c_f$ and p ramifies in F;

- the image of the p-adic representation
$$\rho_{f,p} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_F \otimes \mathbb{Z}_p)$$
attached to f by Deligne ([20]) does not contain the set
$$\big\{ g \in \mathrm{GL}_2(\mathcal{O}_F \otimes \mathbb{Z}_p) \ \big|\ \det(g) \in (\mathbb{Z}_p^\times)^{k-1} \big\}.$$

Lemma 3.8. *The set Σ is finite.*

Proof. The only non-trivial fact to check is that there are only finitely many prime numbers satisfying the last condition, and this follows from [48, Theorem 3.1]. □

For a prime number $p \notin \Sigma$ and an integer $m \geq 1$ define

$$\mathcal{S}_{p^m} := \big\{ \ell \text{ prime number } \ \big|\ \ell \text{ is inert in } K,\ \ell \nmid N \text{ and } p^m \mid \ell + 1 \big\}. \tag{25}$$

Notice that $\mathcal{S}_{p^m} \subset \mathcal{S}$ with $\mathcal{S}$ defined in (17). As a piece of notation, when we write that a (non-zero) prime ideal of $\mathbb{Z}$ belongs to a set Θ of prime numbers we mean that the positive generator of this ideal belongs to Θ. Let $\boldsymbol{\mu}_{p^m}$ denote the p^m-th roots of unity in $\bar{\mathbb{Q}}$. By [18, Lemma 3.14], a prime ℓ belongs to $\mathcal{S}_{p^m}$ precisely when $\mathrm{Frob}_\ell = \mathrm{Frob}_\infty$ in $\mathrm{Gal}(K(\boldsymbol{\mu}_{p^m})/\mathbb{Q})$; hence $\mathcal{S}_{p^m}$ is infinite by Čebotarev's density theorem. Furthermore, there is an inclusion $\boldsymbol{\mu}_{p^m} \subset K_\lambda$ for every prime λ of K such that $\lambda \cap \mathbb{Z} \in \mathcal{S}_{p^m}$.

With Σ as above, fix from now to the end of this section a prime number $p \notin \Sigma$ and a quadruplet $(\mathfrak{p}^m, S, \mathbf{D}_\kappa, \ell)$ consisting of

- a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ above p;
- an integer $m \geq 1$;
- a square-free product $S = \prod_i \ell_i$ of primes ℓ_i in the set $\mathcal{S}_{p^m}$ introduced in (25);
- a derivative $\mathbf{D}_\kappa$ with $\mathrm{supp}(\mathbf{D}_\kappa) = S$;
- an auxiliary prime $\ell \in \mathcal{S}_{p^m}$.

3.6. **Kolyvagin classes attached to Heegner cycles.** In this subsection we introduce classes $d(\ell) \in H^1(K, W_\mathfrak{p}[p^m])$ depending on the data S, p^m, $\mathbf{D}_\kappa$ and ℓ.

Recall that $V_\mathfrak{p} = A_\mathfrak{p} \otimes_{\mathcal{O}_\mathfrak{p}} F_\mathfrak{p}$ and let
$$\vartheta_\mathfrak{p} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(A_\mathfrak{p}), \qquad \vartheta'_\mathfrak{p} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(V_\mathfrak{p})$$
be the Galois representations attached to $A_\mathfrak{p}$ and $V_\mathfrak{p}$, respectively. If $\gamma : \mathrm{Aut}(A_\mathfrak{p}) \hookrightarrow \mathrm{Aut}(V_\mathfrak{p})$ denotes the natural injection defined by extending $F_\mathfrak{p}$-linearly an automorphism of $A_\mathfrak{p}$, then $\vartheta'_\mathfrak{p} = \gamma \circ \vartheta_\mathfrak{p}$, which induces an inclusion $\mathrm{im}(\vartheta_\mathfrak{p}) \subset \mathrm{im}(\vartheta'_\mathfrak{p})$.

For every integer $m \geq 1$ the group $G_{\mathbb{Q}}$ acts on $W_\mathfrak{p}[p^m]$ via its action on $A_\mathfrak{p}$, and reducing $\vartheta_\mathfrak{p}$ modulo p^m gives a representation
$$\bar{\vartheta}_{\mathfrak{p},m} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(W_\mathfrak{p}[p^m]).$$
In particular, $\bar{\vartheta}_\mathfrak{p} := \bar{\vartheta}_{\mathfrak{p},1}$ is a residual representation of $G_{\mathbb{Q}}$ over the finite field $\mathbb{F}_\mathfrak{p}$.

For any subfield L of $\bar{\mathbb{Q}}$ and for $M \in \big\{ A_\mathfrak{p}, V_\mathfrak{p}, W_\mathfrak{p}[p^m] \big\}$ we write $M(L)$ as shorthand for $H^0_{\mathrm{cont}}(L, M)$; similar conventions apply when L is a completion of a number field.

Lemma 3.9. *If $p \notin \Sigma$, then $\vartheta'_\mathfrak{p}$ and $\bar{\vartheta}_\mathfrak{p}$ are irreducible and have non-solvable images.*

Proof. By [10, Proposition 6.3, (1)], the representation $\bar{\vartheta}_{\mathfrak{p}}$ is irreducible, and this implies the irreducibility of $\vartheta'_{\mathfrak{p}}$ ([31, Proposition 2.5]). Finally, by [10, Lemma 6.2], the image of $\vartheta_{\mathfrak{p}}$ in $\mathrm{Aut}(A_{\mathfrak{p}}) \simeq \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$ contains a subgroup that is conjugate to $\mathrm{GL}_2(\mathbb{Z}_p)$. But the groups $\mathrm{GL}_2(\mathbb{Z}_p)$ and $\mathrm{GL}_2(\mathbb{F}_p)$ are not solvable because $p > 3$; hence the images of $\vartheta_{\mathfrak{p}}$ and of $\bar{\vartheta}_{\mathfrak{p}}$ are not solvable. Since $\mathrm{im}(\vartheta_{\mathfrak{p}}) \subset \mathrm{im}(\vartheta'_{\mathfrak{p}})$, the claim follows. □

Lemma 3.10. *If $p \notin \Sigma$ and the extension $E/\mathbb{Q}$ is solvable, then*

(1) $V_{\mathfrak{p}}(E) = 0$;
(2) $W_{\mathfrak{p}}[p^n](E) = 0$ *for all* $n \geq 1$.

Proof. Let us prove part (1). Since $p \notin \Sigma$, Lemma 3.9 ensures that $\vartheta'_{\mathfrak{p}}$ is irreducible with non-solvable image. The submodule $V_{\mathfrak{p}}(E)$ of $V_{\mathfrak{p}}$ is $G_{\mathbb{Q}}$-stable; hence if $V_{\mathfrak{p}}(E) \neq 0$, then $V_{\mathfrak{p}}(E) = V_{\mathfrak{p}}$ by the irreducibility of $\vartheta'_{\mathfrak{p}}$. Thus $\vartheta'_{\mathfrak{p}}$ factors through $\mathrm{Gal}(E/\mathbb{Q})$, which is solvable by assumption. It follows that $\mathrm{im}(\vartheta'_{\mathfrak{p}})$ is solvable, which is a contradiction. Finally, in order to prove part (2) it is of course enough to prove the claim for $n = 1$, and this can be done *mutatis mutandis* in the same way, using again Lemma 3.9. □

Write $L_m := K(W_{\mathfrak{p}}[p^m])$ for the composite of K and the subfield of $\bar{\mathbb{Q}}$ fixed by $\ker(\bar{\vartheta}_{\mathfrak{p},m})$. With notation as in §3.1, define a set $\tilde{\mathcal{S}}_{p^m}$ of prime numbers as

$$\tilde{\mathcal{S}}_{p^m} := \big\{\ell \text{ prime number} \;\big|\; \ell \nmid NDp \text{ and } \mathrm{Frob}_\ell = \mathrm{Frob}_\infty \text{ in } \mathrm{Gal}(L_m/\mathbb{Q})\big\}.$$

Again by Čebotarev's density theorem, $\tilde{\mathcal{S}}_{p^m}$ is infinite.

Lemma 3.11. *A prime ℓ not dividing D belongs to $\tilde{\mathcal{S}}_{p^m}$ if and only if ℓ belongs to $\mathcal{S}_{p^m}$ and $\mathfrak{p}^m$ divides a_ℓ in $\mathcal{O}_F$.*

Proof. Equating the minimal polynomials of F_ℓ (see (2)) and of c acting on $W_{\mathfrak{p}}[p^m]$, one finds the divisibility relations $\mathfrak{p}^m \mid a_\ell$ and $\mathfrak{p}^m \mid \ell+1$ in $\mathcal{O}_F$. Since p is unramified in F, the second relation gives an inclusion $(\ell+1) \subset (p^m)$ of principal ideals of $\mathcal{O}_F$. This immediately implies that $p^m \mid \ell + 1$ in $\mathbb{Z}$, which concludes the proof. □

With notation as before, let $\ell \in \tilde{\mathcal{S}}_{p^m}$ and put $T := S\ell$. Define

$$\tilde{P}(\ell) := \mathbf{D}_\kappa \mathbf{D}_\ell^1(y_{T,\mathfrak{p}}) \in \Lambda_{\mathfrak{p}}(K_T),$$

then denote by

$$P(\ell) \in \Lambda_{\mathfrak{p}}(K_T)/p^m\,\Lambda_{\mathfrak{p}}(K_T)$$

the image of $\tilde{P}(\ell)$ under the canonical projection.

With the exception of §3.8, from here till the end of §3.9 we will work under the following technical assumption on $(\mathfrak{p}^m, S, \mathbf{D}_\kappa, \ell)$.

Assumption 3.12. *For all $\mathbf{D}_{\kappa'}$ strictly less than $\mathbf{D}_\kappa \mathbf{D}_\ell^1$ we have $\mathbf{D}_{\kappa'}(y_{T,\mathfrak{p}}) = 0$.*

With this condition in force, we can prove

Lemma 3.13. *The class $P(\ell)$ is fixed by the action of G_T.*

Proof. Let $\sigma = \sigma_{\ell_i}$ or $\sigma = \sigma_\ell$. Congruence (24) shows that

$$(\sigma - 1)\tilde{P}(\ell) \equiv -\sigma \mathbf{D}_{\kappa'}(y_{T,\mathfrak{p}}) \pmod{p^m}$$

for some $\mathbf{D}_{\kappa'}$ strictly less than $\mathbf{D}_\kappa \mathbf{D}_\ell^1$, which concludes the proof. □

Recall from (15) that there is an injective, Galois-equivariant map of $\mathcal{O}_{\mathfrak{p}}/p^m\mathcal{O}_{\mathfrak{p}}$-modules

$$\Lambda_{\mathfrak{p}}(K_T)/p^m\,\Lambda_{\mathfrak{p}}(K_T) \hookrightarrow H^1_f(K_T, W_{\mathfrak{p}}[p^m]) \subset H^1(K_T, W_{\mathfrak{p}}[p^m]).$$

By Lemma 3.13, the image of $P(\ell)$ via this map belongs to $H^1_f(K_T, W_{\mathfrak{p}}[p^m])^{G_T}$, hence to $H^1(K_T, W_{\mathfrak{p}}[p^m])^{G_T}$. Since $K_T/\mathbb{Q}$, being generalized dihedral, is solvable, part (2) of Lemma 3.10 and the inflation-restriction exact sequence give an isomorphism

$$\mathrm{res}_{K_T/K_1} : H^1(K_1, W_{\mathfrak{p}}[p^m]) \xrightarrow{\simeq} H^1(K_T, W_{\mathfrak{p}}[p^m])^{G_T}.$$

Let $\mathbf{N} = \mathbf{N}_{K_1/K} := \sum_{\sigma\in\Gamma_1}\sigma \in \mathbb{Z}[\Gamma_1]$ denote the norm operator from K_1 to K. The abelian group $H^1(K_1, W_{\mathfrak{p}}[p^m])$ is naturally a Γ_1-module, so $\mathbf{N}$ induces a map

$$\mathbf{N} : H^1(K_1, W_{\mathfrak{p}}[p^m]) \longrightarrow H^1(K_1, W_{\mathfrak{p}}[p^m])^{\Gamma_1}.$$

Since $p \nmid h_K$, inflation-restriction shows that there is an isomorphism

$$\mathrm{res}_{K_1/K} : H^1(K, W_{\mathfrak{p}}[p^m]) \xrightarrow{\simeq} H^1(K_1, W_{\mathfrak{p}}[p^m])^{\Gamma_1}.$$

Consider the diagram

$$\begin{tikzcd}
H^1(K_1, W_{\mathfrak{p}}[p^m]) \arrow[d, "\mathbf{N}"] & H^1(K_T, W_{\mathfrak{p}}[p^m])^{G_T} \arrow[l, "\mathrm{res}^{-1}_{K_T/K_1}"'] \arrow[d, dashed, "\beta"] \\
H^1(K_1, W_{\mathfrak{p}}[p^m])^{\Gamma_1} \arrow[r, "\mathrm{res}^{-1}_{K_1/K}"] & H^1(K, W_{\mathfrak{p}}[p^m])
\end{tikzcd}$$

where the broken arrow β is defined so as to make the resulting square commute. Thus we can attach to $P(\ell) \in H^1(K_T, W_{\mathfrak{p}}[p^m])^{G_T}$ a *Kolyvagin class*

$$d(\ell) := \beta\big(P(\ell)\big) \in H^1(K, W_{\mathfrak{p}}[p^m])$$

such that

$$\mathrm{res}_{K_T/K}\big(d(\ell)\big) = \mathbf{N}_T\big(P(\ell)\big) \tag{26}$$

where $\mathbf{N}_T \in \mathbb{Z}[\Gamma_T]$ is an arbitrary lift of $\mathbf{N}$ via the canonical projection $\Gamma_T \twoheadrightarrow \Gamma_1$ (if $\mathbf{N}'_T$ is another such lift, then $\mathbf{N}_T(P(\ell)) = \mathbf{N}'_T(P(\ell))$ by Lemma 3.13). Furthermore, since $\mathrm{res}_{K_T/K}$ is an isomorphism, $d(\ell)$ is the only class in $H^1(K, W_{\mathfrak{p}}[p^m])$ satisfying (26).

3.7. **Action of complex conjugation on Kolyvagin classes.** Recall that ϵ is the sign of the functional equation of $L(f,s)$ and set $\epsilon_\kappa := (-1)^{\mathrm{ord}(\mathbf{D}_\kappa)}\epsilon$.

Proposition 3.14. *The class $d(\ell)$ belongs to the ϵ_κ-eigenspace of $H^1(K, W_{\mathfrak{p}}[p^m])$ under the action of c.*

Proof. By §3.4.3 and Assumption 3.12, there is an equality

$$c\big(\tilde{P}(\ell)\big) = (-1)^{\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell)}\mathbf{D}_\kappa\mathbf{D}^1_\ell c(y_{T,\mathfrak{p}}).$$

Since the ring $\mathbb{Z}[\Gamma_T]$ is commutative, part (2) of Proposition 3.1 then shows that

$$c\big(P(\ell)\big) = -\epsilon(-1)^{\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell)}\sigma\big(P(\ell)\big)$$

for a suitable $\sigma \in \Gamma_T$. Applying any lift $\mathbf{N}_T = \sum_{i=1}^{h_K}\sigma_i \in \mathbb{Z}[\Gamma_T]$ of $\mathbf{N}$ on both sides gives

$$\mathbf{N}_T\big(c(P(\ell))\big) = -\epsilon(-1)^{\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell)}\mathbf{N}_T\big(\sigma(P(\ell))\big). \tag{27}$$

Now $\sum_{i=1}^{h_K}\sigma_i c = c\sum_{i=1}^{h_K}\sigma_i^{-1}$. Moreover, since $\mathbf{N}'_T := \sum_{i=1}^{h_K}\sigma_i^{-1}$ and $\mathbf{N}''_T := \sum_{i=1}^{h_K}\sigma_i\sigma$ are two lifts of $\mathbf{N}$, equality (26) implies that

$$\mathbf{N}'_T\big(P(\ell)\big) = \mathrm{res}_{K_T/K}\big(d(\ell)\big) = \mathbf{N}''_T\big(P(\ell)\big). \tag{28}$$

By definition of ϵ_κ, combining (27) and (28) gives

$$c\cdot \mathrm{res}_{K_T/K}\big(d(\ell)\big) = \epsilon_\kappa \mathrm{res}_{K_T/K}\big(d(\ell)\big),$$

and the conclusion follows from the $\mathrm{Gal}(K/\mathbb{Q})$-equivariance of the isomorphism $\mathrm{res}_{K_T/K}$. □

3.8. **Tate duality.** In this subsection we do not suppose that Assumption 3.12 holds. Let λ denote the unique prime of K above ℓ. By [39, Proposition 3.1, (2)], there is a $G_\mathbb{Q}$-equivariant skew-symmetric pairing

$$[\cdot\,,\cdot] : A_\mathfrak{p}\times A_\mathfrak{p} \longrightarrow \mathbb{Z}_p(1)$$

such that the induced pairing

$$[\cdot\,,\cdot]_m : W_\mathfrak{p}[p^m]\times W_\mathfrak{p}[p^m] \longrightarrow \boldsymbol{\mu}_{p^m}$$

is non-degenerate. With notation as before, combining cup product in cohomology with the map $W_\mathfrak{p}[p^m]\otimes W_\mathfrak{p}[p^m]\to\boldsymbol{\mu}_{p^m}$ induced by $[\cdot\,,\cdot]_m$ gives rise to a pairing

$$\langle\cdot\,,\cdot\rangle_\lambda : H^1(K_\lambda, W_\mathfrak{p}[p^m])\times H^1(K_\lambda, W_\mathfrak{p}[p^m]) \longrightarrow H^2(K_\lambda,\boldsymbol{\mu}_{p^m}) = \mathbb{Z}/p^m\mathbb{Z},$$

with the equality on the right coming from the invariant map of local class field theory. By a result of Tate, this pairing is non-degenerate (cf. [38, Ch. I, Corollary 2.3]).

Since $A_\mathfrak{p}$ is unramified at λ, the group $H^1_f(K_\lambda, W_\mathfrak{p}[p^m]) = H^1_{\mathrm{ur}}(K_\lambda, W_\mathfrak{p}[p^m])$ is its own annihilator in $H^1(K_\lambda, W_\mathfrak{p}[p^m])$ under Tate's pairing $\langle\cdot\,,\cdot\rangle_\lambda$ ([10, Lemma 4.4]). The *singular part* of the cohomology is then defined via the short exact sequence

$$0\longrightarrow H^1_f(K_\lambda, W_\mathfrak{p}[p^m])\longrightarrow H^1(K_\lambda, W_\mathfrak{p}[p^m])\longrightarrow H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])\longrightarrow 0,$$

and $\langle\cdot\,,\cdot\rangle_\lambda$ induces a $\mathrm{Gal}(K/\mathbb{Q})$-equivariant perfect pairing

$$\langle\cdot\,,\cdot\rangle_\lambda : H^1_f(K_\lambda, W_\mathfrak{p}[p^m])\times H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m]) \longrightarrow \mathbb{Z}/p^m\mathbb{Z}. \tag{29}$$

It follows that there are natural identifications

$$H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m]) = H^1(K_\lambda^{\mathrm{ur}}, W_\mathfrak{p}[p^m]) = \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}(\bar K_\lambda/K_\lambda^{\mathrm{ur}}), W_\mathfrak{p}[p^m]\big) \tag{30}$$

where K_λ^{ur} is the maximal unramified extension of K_λ. Let K_λ^{t} denote the maximal tamely ramified extension of K_λ. The wild inertia group $\mathrm{Gal}(\bar K_\lambda/K_\lambda^{\mathrm{t}})$ is a pro-ℓ-group and $\ell\neq p$; hence equalities (30) yield a further identification

$$H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m]) = \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}(K_\lambda^{\mathrm{t}}/K_\lambda^{\mathrm{ur}}), W_\mathfrak{p}[p^m]\big). \tag{31}$$

Fix a (topological) generator τ of $\mathrm{Gal}(K_\lambda^{\mathrm{t}}/K_\lambda^{\mathrm{ur}})$, so that τ and a lift to $\mathrm{Gal}(K_\lambda^{\mathrm{t}}/K_\lambda)$ of the Frobenius $F_\lambda\in\mathrm{Gal}(K_\lambda^{\mathrm{ur}}/K_\lambda)$ generate $\mathrm{Gal}(K_\lambda^{\mathrm{t}}/K_\lambda)$ topologically. In light of (31), evaluating homomorphisms at τ gives an isomorphism

$$\alpha_\lambda : H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m]) \xrightarrow{\simeq} W_\mathfrak{p}[p^m].$$

On the other hand, by [10, Lemma 6.8], if $\ell\in\tilde{\mathcal{S}}_{p^m}$, then evaluation at Frob_λ gives a $\mathrm{Gal}(K/\mathbb{Q})$-equivariant isomorphism

$$\beta_\lambda : H^1_f(K_\lambda, W_\mathfrak{p}[p^m]) \xrightarrow{\simeq} W_\mathfrak{p}[p^m].$$

It follows that for every $\ell \in \tilde{\mathcal{S}}_{p^m}$ there is an isomorphism

$$\nu_\lambda := \alpha_\lambda^{-1} \circ \beta_\lambda : H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m]) \xrightarrow{\simeq} H^1_{sin}(K_\lambda, W_{\mathfrak{p}}[p^m]) \tag{32}$$

of $\mathcal{O}_{\mathfrak{p}}/p^m\mathcal{O}_{\mathfrak{p}}$-modules.

As a piece of notation, for a $\mathbb{Z}/p^m\mathbb{Z}$-module M write

$$M^* := \mathrm{Hom}(M, \mathbb{Z}/p^m\mathbb{Z})$$

for the Pontryagin dual of M. Note that if M is endowed with a $\mathbb{Z}/p^m\mathbb{Z}$-linear action of an involution τ, then M^* inherits a $\mathbb{Z}/p^m\mathbb{Z}$-linear action of τ by setting

$$(\tau \cdot f)(m) := f(\tau \cdot m)$$

for all $f \in M^*$ and all $m \in M$. Letting the superscripts $\pm$ denote the $\pm$-eigenspaces under the actions of τ, there are canonical isomorphisms

$$(M^*)^\pm \xrightarrow{\simeq} (M^\pm)^* \tag{33}$$

of $\mathbb{Z}/p^m\mathbb{Z}$-modules.

With this notation in force, the pairing in (29) is equivalent to an isomorphism

$$H^1_{sin}(K_\lambda, W_{\mathfrak{p}}[p^m]) \xrightarrow{\simeq} H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])^*. \tag{34}$$

By composing isomorphism (34) with the dual of the natural (localization) map

$$H^1_f(K, W_{\mathfrak{p}}[p^m]) \longrightarrow H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m]),$$

we obtain a map

$$\phi_\lambda : H^1_{sin}(K_\lambda, W_{\mathfrak{p}}[p^m]) \longrightarrow H^1_f(K, W_{\mathfrak{p}}[p^m])^*.$$

Analogously, for every $\mathbb{Z}/p^m\mathbb{Z}$-submodule $\mathscr{S} \subset H^1_f(K, W_{\mathfrak{p}}[p^m])$ we obtain by restriction a map $H^1_{sin}(K_\lambda, W_{\mathfrak{p}}[p^m]) \to \mathscr{S}^*$, which will be denoted by the same symbol. Observe that ϕ_λ is $\mathrm{Gal}(K/\mathbb{Q})$-equivariant.

Remark 3.15. In light of the perfect pairing (29), when dealing with Tate's duality we shall often use the same symbol to denote $d(\ell)_\lambda$ and its image in $H^1_{sin}(K_\lambda, W_{\mathfrak{p}}[p^m])$.

3.9. **Local behaviour of Kolyvagin classes.** By class field theory, λ splits completely in K_S/K; choose a prime λ_S of K_S above λ. Furthermore, λ_S is totally ramified in K_T/K_S; write λ_T for the unique prime of K_T above it.

As before, if v is a place of K, then write K_v for the completion of K at v. There is a localization (restriction) map

$$\mathrm{res}_v : H^1(K, W_{\mathfrak{p}}[p^m]) \longrightarrow H^1(K_v, W_{\mathfrak{p}}[p^m]),$$

and if $s \in H^1(K, W_{\mathfrak{p}}[p^m])$, then we write s_v for $\mathrm{res}_v(s)$.

Proposition 3.16. *If v is an archimedean place of K, then $d(\ell)_v = 0$.*

Proof. The quadratic field K is imaginary, hence $K_v = \mathbb{C}$. The proposition follows because $\mathbb{C}$ is algebraically closed and so $H^1(\mathbb{C}, W_{\mathfrak{p}}[p^m]) = 0$. □

Now set $S' := \mathrm{cond}(\mathbf{D}_\kappa)$.

Proposition 3.17. *If v is a finite place of K not dividing $S'\ell$, then*

$$d(\ell)_v \in H^1_f(K_v, W_{\mathfrak{p}}[p^m]).$$

Proof. By construction, $P(\ell)$ belongs to $H^1_f(K_{S'\ell}, W_\mathfrak{p}[p^m])$. If $v \nmid p$ is a prime of K and v' is a prime of $K_{S'\ell}$ above it, then $P(\ell)$ belongs to $H^1_{\mathrm{un}}(K_{S'\ell,v'}, W_\mathfrak{p}[p^m])$. By definition, the restriction of $d(\ell)$ is $P(\ell)$. In particular, the restriction of $d(\ell)_v$ under the map

$$H^1(K_v, W_\mathfrak{p}[p^m]) \longrightarrow H^1(K_{S'\ell,v'}, W_\mathfrak{p}[p^m])$$

lies in $H^1_{\mathrm{un}}(K_{S'\ell,v'}, W_\mathfrak{p}[p^m])$. By inflation-restriction, the kernel of the map above is

$$H^1\big(K_{S'\ell,v'}/K_v, W_\mathfrak{p}[p^m](K_{S'\ell,v'})\big),$$

and the extension $K_{S'\ell,v'}/K_v$ is unramified; therefore $d(\ell)_v$ is unramified too. On the other hand, if $v \mid p$, then the claim follows from the de Rham conjecture for open varieties (now a theorem of Faltings), as explained in [39, Lemma 11.1, (2)]. □

Now we begin the study of $d(\ell)_\lambda$ (recall that λ is the unique prime of K above the prime number $\ell \in \tilde{\mathcal{S}}_{p^m}$). For this, we need some preliminaries.

Lemma 3.18. *If $\ell \in \tilde{\mathcal{S}}_{p^m}$, then there are isomorphisms of $\mathcal{O}_\mathfrak{p}$-modules*

$$H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])^\pm \simeq \mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}, \qquad H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^\pm \simeq \mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}.$$

Proof. This is [10, Lemma 6.9, (2)]. (Notice that the first three conditions listed on [10, p. 36] are equivalent to the condition $\ell \in \tilde{\mathcal{S}}_{p^m}$ by [10, Remark 3.1] and that the fourth condition on [10, p. 36] plays no role in the proof of [10, Lemma 6.9]). □

Lemma 3.19. *If $\ell \in \tilde{\mathcal{S}}_{p^m}$, then the expressions $\big(a_\ell \pm (\ell+1)\,\mathrm{Frob}_\lambda\big)/p^m$ define endomorphisms of $H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])$. Furthermore, if $\big(a_\ell \pm (\ell+1)\big)/p^m$ are both p-adic units, then the maps above are invertible.*

Proof. Since $\ell \in \tilde{\mathcal{S}}_{p^m}$, there is an equality $\mathrm{Frob}_\ell = \mathrm{Frob}_\infty$ of conjugacy classes in $\mathrm{Gal}(K/\mathbb{Q})$, so Frob_λ acts on $H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])^\pm$ as multiplication by ± 1. Then Lemma 3.11 shows that $\big(a_\ell \pm (\ell+1)\,\mathrm{Frob}_\lambda\big)/p^m$ are indeed well-defined endomorphisms of the $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-module $H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])$, and the last claim is obvious. □

In the proof of the next result we use the isomorphism ν_λ defined in (32) (keep Remarks 2.9 and 3.15 in mind for our notational conventions).

Proposition 3.20. *Suppose that $\ell \in \tilde{\mathcal{S}}_{p^m}$ and that $\big(a_\ell \pm (\ell+1)\big)/p^m$ are both p-adic units. Then $d(\ell)_\lambda \neq 0$ in $H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])$ if and only if $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})_\lambda \neq 0$ in $H^1_f(K_\lambda, W_\mathfrak{p}[p^m])$.*

Proof. Applying the Key Formula in [39, §9] with y a 1-cocycle that represents $\mathbf{D}_\kappa(y_{S\ell,\mathfrak{p}})$, and using Proposition 3.14 plus the relations $\ell+1 \equiv a_\ell \equiv 0 \pmod{\mathfrak{p}^m}$ to simplify the right hand side, we get

$$\frac{(-1)^{k/2-1}\epsilon_\kappa a_\ell - (\ell+1)}{p^m} d(\ell)_{\lambda,sin} \equiv \frac{a_\ell - (\ell+1)\,\mathrm{Frob}_\lambda}{p^m}\Big(\nu_\lambda\big(\mathbf{D}_\kappa(y_{S,\mathfrak{p}})_\lambda\big)\Big) \pmod{p^m}.$$

(Note the difference of sign with respect to loc. cit.; the correction can be found in [44, Proposition 5.16].) But $\frac{(-1)^{k/2-1}\epsilon_\kappa a_\ell - (\ell+1)}{p^m} \in (\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p})^\times$ by assumption, and the proposition follows because $\frac{a_\ell - (\ell+1)\,\mathrm{Frob}_\lambda}{p^m}$ is invertible on $H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])$ by Lemma 3.19. □

Recall that the data $(\mathfrak{p}^m, S, \mathbf{D}_\kappa, \ell)$ satisfy Assumption 3.12. As before, L_m is the field $K(W_\mathfrak{p}[p^m])$ and S' is the conductor of $\mathbf{D}_\kappa$. Define

$$H^1_{f,S'}(K, W_\mathfrak{p}[p^m]) := \ker\Big(H^1_f(K, W_\mathfrak{p}[p^m]) \longrightarrow \bigoplus_{v\,|\,S'} H^1_f(K_v, W_\mathfrak{p}[p^m])\Big). \tag{35}$$

Proposition 3.21. *The class $d(\ell)_\lambda$ lies in the kernel of*

$$\phi_\lambda : H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa} \longrightarrow \big(H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^*\big)^{\epsilon_\kappa}$$

for all $m \geq 1$.

Proof. To begin with, $d(\ell)_\lambda \in H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}$ by Proposition 3.14. Pick an element $s \in H^1_{f,S'}(K, W_\mathfrak{p}[p^m])$, so that $s_\lambda \in H^1_f(K_\lambda, W_\mathfrak{p}[p^m])$; we need to show that

$$\langle s_\lambda, d(\ell)_\lambda\rangle_\lambda = 0. \tag{36}$$

By [10, Proposition 2.2, (2)], one has

$$\sum_v \langle s_v, d(\ell)_v\rangle_v = 0, \tag{37}$$

where the sum is taken over all (finite) places of K. Now observe that if $v \nmid S'\ell$, then $\langle s_v, d(\ell)_v\rangle_v = 0$ by Proposition 3.17. On the other hand, if $v\,|\,S'$, then $s_v = 0$ because $s \in H^1_{f,S'}(K, W_\mathfrak{p}[p^m])$. Therefore (36) is an immediate consequence of (37). ☐

3.10. **Applications of Čebotarev's density theorem.** Recall that L_m is the composite of K and the field $\bar{\mathbb{Q}}^{\ker(\bar\vartheta_{\mathfrak{p},m})}$ fixed by $\ker(\bar\vartheta_{\mathfrak{p},m})$. Similarly, define $L_{S,m} := K_S(W_\mathfrak{p}[p^m])$ to be the composite of K_S and $\bar{\mathbb{Q}}^{\ker(\bar\vartheta_{\mathfrak{p},m})}$.

We need some cohomological lemmas.

Lemma 3.22. *For all $i \geq 0$ there is an isomorphism*

$$H^i\big(\mathrm{Gal}(L_m/K), W_\mathfrak{p}[p^m]\big) \simeq H^i\big(\mathrm{Gal}(L_{S,m}/K_S), W_\mathfrak{p}[p^m]\big).$$

Proof. The fields K and $\mathbb{Q}(W_\mathfrak{p}[p^m])$ are linearly disjoint over $\mathbb{Q}$, and the same is true of K_S and $\mathbb{Q}(W_\mathfrak{p}[p^m])$. This holds because $\mathbb{Q}(W_\mathfrak{p}[p^m]) \cap K$ and $\mathbb{Q}(W_\mathfrak{p}[p^m]) \cap K_S$ are extensions of $\mathbb{Q}$ that are everywhere unramified, which is a consequence of the fact that $\mathbb{Q}(W_\mathfrak{p}[p^m])/\mathbb{Q}$ is unramified outside Np while $K_S/\mathbb{Q}$ is unramified outside SD and $(pN, SD) = 1$. It follows that the restriction maps induce canonical isomorphisms

$$\mathrm{Gal}(L_m/K) \simeq \mathrm{Gal}(\mathbb{Q}(W_\mathfrak{p}[p^m])/\mathbb{Q}), \quad \mathrm{Gal}(L_{S,m}/K_S) \simeq \mathrm{Gal}(\mathbb{Q}(W_\mathfrak{p}[p^m])/\mathbb{Q}).$$

Therefore both groups appearing in the statement of the lemma are isomorphic to

$$H^i\big(\mathrm{Gal}(\mathbb{Q}(W_\mathfrak{p}[p^m])/\mathbb{Q}), W_\mathfrak{p}[p^m]\big),$$

and this concludes the proof. ☐

Lemma 3.23. *For all $i \geq 0$, $H^i\big(\mathrm{Gal}(L_m/K), W_\mathfrak{p}[p^m]\big) = 0$.*

Proof. This is [10, Proposition 6.3, (2)]. ☐

Lemma 3.24. *The restriction map*

$$H^1(K, W_\mathfrak{p}[p^m]) \longrightarrow H^1(K_S, W_\mathfrak{p}[p^m])$$

is injective.

Proof. By the inflation-restriction exact sequence, the kernel of this map is

$$H^1\big(\mathrm{Gal}(K_S/K), W_\mathfrak{p}[p^m](K_S)\big),$$

which is trivial because $W_\mathfrak{p}[p^m](K_S) = 0$ by part (2) of Lemma 3.10. $\square$

Lemma 3.25. *The restriction map*

$$H^1(K_S, W_\mathfrak{p}[p^m]) \longrightarrow H^1(L_{S,m}, W_\mathfrak{p}[p^m])$$

is injective.

Proof. The kernel of this map is $H^1\big(\mathrm{Gal}(L_{S,m}/K_S), W_\mathfrak{p}[p^m]\big)$, which is trivial by a combination of Lemmas 3.22 and 3.23. $\square$

Lemma 3.26. *The restriction map*

$$H^1(K, W_\mathfrak{p}[p^m]) \longrightarrow H^1(L_{S,m}, W_\mathfrak{p}[p^m])$$

is injective.

Proof. Combine Lemmas 3.24 and 3.25. $\square$

Keep the notation of (20). Now we can prove the following.

Proposition 3.27. *Suppose that*

- $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$ *is not trivial in* $H^1(K_S, W_\mathfrak{p}[p^m])$*;*
- $r_{\mathfrak{p},m}\big(H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}\big) \geq 1$.

Then there exist infinitely many prime numbers ℓ *such that*

(1) $\ell \nmid pNDS$ *and* $\mathrm{Frob}_\ell = \mathrm{Frob}_\infty$ *in* $\mathrm{Gal}(L_{S,m}/\mathbb{Q})$*;*
(2) $\ell + 1 \pm a_\ell \not\equiv 0 \pmod{\mathfrak{p}^{m+1}}$*;*
(3) *the image of* $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$ *in* $H^1_f(K_\lambda, W_\mathfrak{p}[p^m])$ *is not zero, where* λ *is the unique prime of* K *above* ℓ*;*
(4) *the map of* $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$*-modules*

$$H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa} \longrightarrow H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}$$

is surjective.

Proof. By assumption, $\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \neq 0$ in $H^1(K_S, W_\mathfrak{p}[p^m])$; hence Lemma 3.25 implies that the same is true of its image in $H^1(L_{S,m}, W_\mathfrak{p}[p^m])$, denoted by the same symbol. Since p is odd, $H^1(L_{S,m}, W_\mathfrak{p}[p^m])$ splits as the direct sum of its $\pm$-eigenspaces for the action of $c \in \mathrm{Gal}(K/\mathbb{Q})$, so there is $\delta \in \{\pm\}$ such that the projection of $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$ to the δ-eigenspace of $H^1(L_{S,m}, W_\mathfrak{p}[p^m])$ is non-zero. Let us fix such a sign δ and write d for the corresponding projection of $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$.

Let $s \in H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}$ be an element of exact order p^m, which exists by assumption. By Lemma 3.26, the image of s in $H^1(L_{S,m}, W_\mathfrak{p}[p^m])$ has order p^m as well. Since the relevant Galois action is trivial and $W_\mathfrak{p}[p^m]$ is abelian, there is a canonical identification

$$H^1(L_{S,m}, W_\mathfrak{p}[p^m]) = \mathrm{Hom}\big(\mathrm{Gal}(L^{\mathrm{ab}}_{S,m}/L_{S,m}), W_\mathfrak{p}[p^m]\big),$$

where $L^{\mathrm{ab}}_{S,m}$ is the maximal abelian extension of $L_{S,m}$. Denote by ψ and φ the homomorphisms corresponding to d and to the image of s in $H^1(L_{S,m}, W_\mathfrak{p}[p^m])$, respectively.

Denote by $\tilde{L}_{S,m}$ the smallest extension of $L_{S,m}$ that is cut out by ψ and φ and is Galois over $\mathbb{Q}$. There is an isomorphism

$$\mathrm{Gal}(\tilde{L}_{S,m}/K_S) \simeq \mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m}) \rtimes \mathrm{Gal}(L_{S,m}/K_S).$$

Complex conjugation c acts on $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})$ by inner automorphisms, and we denote by $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})^+$ the subgroup of $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})$ that is fixed by c. Set

$$\Phi := H^1\big(\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m}), W_\mathfrak{p}[p^m]\big) = \mathrm{Hom}\big(\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m}), W_\mathfrak{p}[p^m]\big).$$

By definition of $\tilde{L}_{S,m}$, the maps ψ and φ factor through $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})$ and so determine maps $\bar{\psi}$ and $\bar{\varphi}$ in Φ. The group $\mathrm{Gal}(L_{S,m}/K_S)$ acts canonically on Φ, and $\bar{\psi}$ and $\bar{\varphi}$ are fixed by this action as they are restrictions of classes in $H^1(K_S, W_\mathfrak{p}[p^m])$ and $H^1(K, W_\mathfrak{p}[p^m])$, respectively. There is also an action of c on Φ and, since s belongs to $H^1(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}$, the map $\bar{\varphi}$ belongs to Φ^{ϵ_κ}, while $\bar{\psi}$ belongs to Φ^δ by construction.

Now we claim that both $\bar{\psi}$ and $p^{m-1}\bar{\varphi}$ are non-zero on $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})^+$. To show this, let ϱ denote either $\bar{\psi}$ or $p^{m-1}\bar{\varphi}$. If $\varrho = 0$ on $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})^+$, then ϱ maps $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})$ to one of the eigenspaces $W_\mathfrak{p}[p^m]^\pm$. This is true because ϱ factors through the p-primary part of $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})$, which splits as the sum of the two eigenspaces for the action of c, and ϱ belongs to an eigenspace of Φ. Since ϱ is non-zero and fixed by $\mathrm{Gal}(L_{S,m}/K_S)$, it follows that $\mathrm{im}(\varrho)$ is a non-zero, proper submodule of $W_\mathfrak{p}[p^m]$ that is stable under the action of $\mathrm{Gal}(L_{S,m}/K_S) \simeq \mathrm{Gal}(\mathbb{Q}(W_\mathfrak{p}[p^m])/\mathbb{Q})$. Multiplying $\mathrm{im}(\varrho)$ by a suitable power of p, we obtain a non-zero, proper submodule of $W_\mathfrak{p}[p]$ that is stable under $\mathrm{Gal}(\mathbb{Q}(W_\mathfrak{p}[p^m])/\mathbb{Q})$, and this contradicts the irreducibility of $\bar{\vartheta}_\mathfrak{p}$ (Lemma 3.9). We conclude that both $p^{m-1}\bar{\varphi}$ and $\bar{\psi}$ are necessarily non-zero on $\mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})^+$.

It follows that we can find $g \in \mathrm{Gal}(\tilde{L}_{S,m}/L_{S,m})^+$ such that $\bar{\psi}(g) \neq 0$ and $\bar{\varphi}(g)$ has exact order p^m. Let ℓ be a prime number unramified in $\tilde{L}_{S,m}/\mathbb{Q}$ such that

$$\ell \nmid NDSp, \qquad \mathrm{Frob}_\ell = \mathrm{Frob}_\infty g. \tag{38}$$

Here $\mathrm{Frob}_\infty g$ denotes the conjugacy class of cg in $\mathrm{Gal}(\tilde{L}_{S,m}/\mathbb{Q})$. By Čebotarev's density theorem, the set of primes satisfying (38) is infinite.

Clearly, (1) is satisfied by any ℓ as in (38). In particular, ℓ is inert in K, and we denote by λ the unique prime of K above ℓ, which splits completely in $L_{S,m}$ ([10, Lemma 6.7]). Choose a prime $\tilde{\lambda}_{S,m}$ of $\tilde{L}_{S,m}$ above λ such that $\mathrm{Frob}_{\tilde{\lambda}_{S,m}/\ell} = cg$ and let $\lambda_{S,m}$ be the prime of $L_{S.m}$ below $\tilde{\lambda}_{S,m}$; the completion $L_{\lambda_{S,m}}$ of $L_{S,m}$ at $\lambda_{S,m}$ is then equal to K_λ.

Now we show that every prime ℓ satisfying (38) satisfies also (3) and (4) in the statement of the proposition. If $\varrho = \bar{\psi}$ or $\varrho = p^{m-1}\bar{\varphi}$, then, since $g^c = g$, one has

$$\varrho\big(\mathrm{Frob}_{\tilde{\lambda}_{S,m}/\lambda_{S,m}}\big) = \varrho\big(\mathrm{Frob}^2_{\tilde{\lambda}_{S,m}/\ell}\big) = \varrho(g^c g) = \varrho(g^2) \neq 0. \tag{39}$$

Therefore the restriction of ϱ to $\mathrm{Gal}\big(\tilde{L}_{\tilde{\lambda}_{S,m}}/L_{\lambda_{S,m}}\big)$ is non-zero and hence, since $L_{\lambda_{S,m}} = K_\lambda$, taking $\varrho = \bar{\psi}$ gives (3). As for (4), note that, by Lemma 3.18, it suffices to find an element of $H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}$ whose image in $H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}$ has exact order p^m. But it follows from (39) with $\varrho = p^{m-1}\bar{\varphi}$ that the order of the image of s in $H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}$ is p^m, and we are done.

Finally, we show that one can choose infinitely many primes ℓ as in (38) such that (2) is true. Fix a prime ℓ' satisfying (38) but not (2), so that $\ell'+1 \equiv \epsilon a_{\ell'} \pmod{\mathfrak{p}^{m+1}}$ for a suitable $\epsilon \in \{\pm 1\}$. It is known that $\mathrm{tr}(F_{\ell'} \mid A_\mathfrak{p}) = a_{\ell'}/\ell'^{k/2-1}$ and $\det(F_{\ell'} \mid A_\mathfrak{p}) = \ell'$. Take any $\alpha \in \mathbb{Z}_p^\times$ such that $\alpha \equiv 1 \pmod{p^m}$ and set $M := \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right)$. By [10, Lemma 6.2], the matrix M lies in the image of the representation $\vartheta_\mathfrak{p}$ of $G_\mathbb{Q}$ on $A_\mathfrak{p}$; hence there is $\sigma_\alpha \in G_\mathbb{Q}$ having M as its image. Then

$$\mathrm{tr}(F_{\ell'}\sigma_\alpha \mid A_\mathfrak{p}) = \alpha a_{\ell'}/\ell'^{k/2-1}, \qquad \det(F_{\ell'}\sigma_\alpha \mid A_\mathfrak{p}) = \alpha^2\ell'.$$

Let ℓ be a prime number such that $\ell \nmid NDSp$ and $\mathrm{Frob}_\ell = \mathrm{Frob}_{\ell'}\sigma_\alpha|_{\tilde{L}_{S,m+1}}$ in $\mathrm{Gal}(\tilde{L}_{S,m+1}/\mathbb{Q})$, where we denote by $\mathrm{Frob}_{\ell'}\sigma_\alpha|_{\tilde{L}_{S,m+1}}$ the conjugacy class of $f \cdot \sigma_\alpha|_{\tilde{L}_{S,m+1}}$ for any choice of $f \in \mathrm{Frob}_{\ell'}$. Again, Čebotarev's density theorem guarantees that there exist infinitely many such ℓ. Then

$$a_\ell/\ell^{k/2-1} \equiv \alpha a_{\ell'}/\ell'^{k/2-1} \pmod{\mathfrak{p}^{m+1}}, \qquad \ell \equiv \alpha^2\ell' \pmod{\mathfrak{p}^{m+1}},$$

and one deduces that there exists an α as above such that $\ell+1 \pm a_\ell \not\equiv 0 \pmod{\mathfrak{p}^{m+1}}$. This shows that ℓ satisfies (2). But the image of Frob_ℓ in $\mathrm{Gal}(\tilde{L}_{S,m}/\mathbb{Q})$ is equal to that of $\mathrm{Frob}_{\ell'}$, and so ℓ satisfies (38) too. □

3.11. **Divisibility properties of Heegner cycles.** The arguments in this subsection follow those in [18, §5.1]. As before, ℓ belongs to $\mathcal{S}_{p^m}$ and λ is the unique prime of K above ℓ. Moreover, recall the shorthand $\mathbb{F}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}/p\mathcal{O}_\mathfrak{p}$ and for any $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-module M set

$$r_\mathfrak{p}(M) := \dim_{\mathbb{F}_\mathfrak{p}}\big(M \otimes_{\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}} \mathbb{F}_\mathfrak{p}\big).$$

To use uniform notation, also put $r_\mathfrak{p} := r_{\mathfrak{p},1}$.

Lemma 3.28. $r_\mathfrak{p}\big(H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^\pm\big) \le 1$.

Proof. To ease notation, in this proof we use the symbol $\otimes$ to denote tensorization over $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$. With this convention in mind, note that for any $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-module M equipped with an action of $\mathrm{Gal}(K/\mathbb{Q})$ there are injections

$$M^\pm \otimes \mathbb{F}_\mathfrak{p} \hookrightarrow (M \otimes \mathbb{F}_\mathfrak{p})^\pm. \tag{40}$$

If $\widehat{\mathbb{Z}}$ is the profinite completion of $\mathbb{Z}$, then $\mathrm{Gal}(K_\lambda^{\mathrm{ur}}/K_\lambda) \simeq \widehat{\mathbb{Z}}$; hence well-known results in group cohomology (see, e.g., [54, Ch. XIII, Proposition 1]) show that there is a short exact sequence

$$0 \longrightarrow (\mathrm{Frob}_\lambda - 1)W_\mathfrak{p}[p^m] \longrightarrow W_\mathfrak{p}[p^m] \longrightarrow H^1_f(K_\lambda, W_\mathfrak{p}[p^m]) \longrightarrow 0. \tag{41}$$

Tensoring (41) with $\mathbb{F}_\mathfrak{p}$ produces an exact sequence

$$(\mathrm{Frob}_\lambda - 1)W_\mathfrak{p}[p^m] \otimes \mathbb{F}_\mathfrak{p} \xrightarrow{\iota} W_\mathfrak{p}[p^m] \otimes \mathbb{F}_\mathfrak{p} \longrightarrow H^1_f(K_\lambda, W_\mathfrak{p}[p^m]) \otimes \mathbb{F}_\mathfrak{p} \longrightarrow 0. \tag{42}$$

By [10, Proposition 6.3, (4)], $W_\mathfrak{p}[p^m]^\pm$ is free of rank 1 over $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$, and then (40) with $M = W_\mathfrak{p}[p^m]$ gives

$$\dim_{\mathbb{F}_\mathfrak{p}}\big((W_\mathfrak{p}[p^m] \otimes \mathbb{F}_\mathfrak{p})^\pm\big) = 1. \tag{43}$$

If $\mathrm{im}(\iota) = 0$, then (42) induces isomorphisms

$$\big(W_\mathfrak{p}[p^m] \otimes \mathbb{F}_\mathfrak{p}\big)^\pm \simeq \big(H^1_f(K_\lambda, W_\mathfrak{p}[p^m]) \otimes \mathbb{F}_\mathfrak{p}\big)^\pm, \tag{44}$$

and the inequalities $r_\mathfrak{p}\big(H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^\pm\big) \le 1$ follow by combining (43), (44) and (40) with $M = H^1_f(K_\lambda, W_\mathfrak{p}[p^m])$. Finally, $W_\mathfrak{p}[p^m] \otimes \mathbb{F}_\mathfrak{p}$ has dimension 2 over $\mathbb{F}_\mathfrak{p}$, so if $\mathrm{im}(\iota) \neq 0$, then (42) implies that $r_{\mathfrak{p}}\big(H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])\big) \leq 1$ and, *a fortiori*, $r_{\mathfrak{p}}\big(H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])^{\pm}\big) \leq 1$. □

Remark 3.29. If $\ell \in \tilde{\mathcal{S}}_{p^m}$, then Lemma 3.18 shows that equality holds in Lemma 3.28.

To simplify our notation, for every integer $S' > 1$ define

$$A(S') := \bigoplus_{\lambda | S'} H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m]). \tag{45}$$

Of course, the module $A(S')$ depends on m, but no confusion is likely to arise.

Lemma 3.30. *If $\ell \in \tilde{\mathcal{S}}_{p^m}$, then*

$$\begin{aligned} r_{\mathfrak{p},m}\big(H^1_{f,S'}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) \leq\, & r_{\mathfrak{p},m}\big(H^1_{f,S'\ell}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) \\ & + r_{\mathfrak{p}}\big(A(S'\ell)^{\pm}\big) - r_{\mathfrak{p}}\big(A(S')^{\pm}\big). \end{aligned}$$

Proof. There is an exact sequence

$$0 \longrightarrow H^1_{f,S'\ell}(K, W_{\mathfrak{p}}[p^m])^{\pm} \longrightarrow H^1_{f,S'}(K, W_{\mathfrak{p}}[p^m])^{\pm} \longrightarrow H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])^{\pm}$$

where λ is the prime of K above ℓ. Combining part (3) of Lemma 3.4 and the obvious inequality

$$r_{\mathfrak{p},m}\big(H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])^{\pm}\big) \leq r_{\mathfrak{p}}\big(H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])^{\pm}\big)$$

we find

$$r_{\mathfrak{p},m}\big(H^1_{f,S'}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) \leq r_{\mathfrak{p},m}\big(H^1_{f,S'\ell}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) + r_{\mathfrak{p}}\big(H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])^{\pm}\big).$$

Applying Lemma 3.28 to the inequality above yields

$$r_{\mathfrak{p},m}\big(H^1_{f,S'}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) \leq r_{\mathfrak{p},m}\big(H^1_{f,S'\ell}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) + 1. \tag{46}$$

Now ℓ belongs to $\tilde{\mathcal{S}}_{p^m}$, so by Lemma 3.18 one has

$$r_{\mathfrak{p}}\big(H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])^{\pm}\big) = 1,$$

and we deduce that

$$r_{\mathfrak{p}}\big(A(S'\ell)^{\pm}\big) = r_{\mathfrak{p}}\big(A(S')^{\pm}\big) + 1.$$

Hence inequality (46) becomes

$$\begin{aligned} r_{\mathfrak{p},m}\big(H^1_{f,S'}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) \leq\, & r_{\mathfrak{p},m}\big(H^1_{f,S'\ell}(K, W_{\mathfrak{p}}[p^m])^{\pm}\big) \\ & + r_{\mathfrak{p}}\big(A(S'\ell)^{\pm}\big) - r_{\mathfrak{p}}\big(A(S')^{\pm}\big), \end{aligned}$$

as was to be shown. □

Proposition 3.31. *Let $\mathbf{D}_\kappa$ be a derivative of support S and conductor S'. If either*

(1) $m = 1$ *and* $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p}}\big(H^1_{f,S'}(K, W_{\mathfrak{p}}[p])^{\epsilon_\kappa}\big) + r_{\mathfrak{p}}\big(A(S')^{\epsilon_\kappa}\big)$

or

(2) $m \geq 1$ *and* $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p},m}\big(H^1_f(K, W_{\mathfrak{p}}[p^m])^{\epsilon_\kappa}\big)$,

then $\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \equiv 0 \pmod{p^m}$.

Proof. Define the *weight* of $\mathbf{D}_\kappa$ to be

$$\mathrm{wt}(\mathbf{D}_\kappa) := \mathrm{ord}(\mathbf{D}_\kappa) - \#\big\{\ell \text{ prime number } \big| \; \ell \,|\, S \text{ and } \ell \in \tilde{\mathcal{S}}_{p^m}\big\}.$$

To prove the proposition we proceed by induction on $\mathrm{wt}(\mathbf{D}_\kappa)$.

First of all, observe that if $\mathrm{wt}(\mathbf{D}_\kappa) < 0$, then the result is true. Indeed, in this case $\mathbf{D}_\kappa$ contains at least one factor of the form $\mathbf{D}^0_\ell$ for some prime $\ell \in \tilde{\mathcal{S}}_{p^m}$. By part (1) of Proposition 3.1 and the relation (1) between restriction, corestriction and Galois trace, we have

$$\mathbf{D}^0_\ell(y_{T\ell,\mathfrak{p}}) = \mathrm{res}_{K_{T\ell}/K_T}(y_{T,\mathfrak{p}}) \cdot (a_\ell/\ell^{k/2-1}) \equiv 0 \pmod{p^m},$$

where the congruence holds because $\ell \in \tilde{\mathcal{S}}_{\mathfrak{p}^m}$ (here $\mathrm{res}_{K_{T\ell}/K_T}$ denotes the restriction map in cohomology from $H^1(K_T, A_\mathfrak{p})$ to $H^1(K_{T\ell}, A_\mathfrak{p})$). Then the result follows (without assuming any condition on the order of $\mathbf{D}_\kappa$).

Now set $k := \mathrm{wt}(\mathbf{D}_\kappa)$ and assume by induction that the theorem is true for all derivatives $\mathbf{D}_{\kappa'}$ such that $\mathrm{wt}(\mathbf{D}_{\kappa'}) < k$. We argue by contradiction, supposing that

$$\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \not\equiv 0 \pmod{p^m}. \tag{47}$$

We first show that the inequality in the statement of the proposition plus (47) implies that

$$r_{\mathfrak{p},m}\big(H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}\big) \geq 1. \tag{48}$$

In fact, if this were not the case, then there would be an inequality

$$\mathrm{ord}(\mathbf{D}_\kappa) < r_\mathfrak{p}\big(A(S')\big). \tag{49}$$

In case (1), this inequality is obvious, while in case (2) our assumption implies that

$$\begin{aligned}\mathrm{ord}(\mathbf{D}_\kappa) &< r_{\mathfrak{p},m}\big(H^1_f(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}\big)\\ &\leq r_{\mathfrak{p},m}\big(H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}\big) + r_\mathfrak{p}\big(A(S')^{\epsilon_\kappa}\big) \leq r_\mathfrak{p}\big(A(S')\big).\end{aligned}$$

By Lemma 3.28, the right hand side of (49) is less than or equal to the number of primes dividing S'. But each of these primes contributes at least 1 unity in the sum defining $\mathrm{ord}(\mathbf{D}_\kappa)$, so the inequality above does not occur and we conclude that (48) holds.

Equations (47) and (48) show that the assumptions in Proposition 3.27 are fulfilled, and therefore, with the usual notation, one can find a prime number ℓ such that

- $\ell \nmid pNDS$ and $\mathrm{Frob}_\ell = \mathrm{Frob}_\infty$ in $\mathrm{Gal}(L_{S,m}/\mathbb{Q})$;
- $\mathfrak{p}^{m+1} \nmid (\ell+1) \pm a_\ell$;
- the image of $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$ in $H^1_f(K_\lambda, W_\mathfrak{p}[p^m])$ is not zero;
- the map of $\mathcal{O}_\mathfrak{p}/p^m\mathcal{O}_\mathfrak{p}$-modules

$$H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa} \longrightarrow H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa} \tag{50}$$

  is surjective.

Dualizing the map in (50) and using (33) and (34), we see that the map

$$\phi_\lambda : H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa} \longrightarrow \big(H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^*\big)^{\epsilon_\kappa} \tag{51}$$

is injective.

Now we want to show that the derivative $\mathbf{D}_\kappa \mathbf{D}^1_\ell$ satisfies Assumption 3.12. Fix $\mathbf{D}_{\kappa'}$ strictly less than $\mathbf{D}_\kappa \mathbf{D}^1_\ell$. Then

$$\mathrm{ord}(\mathbf{D}_{\kappa'}) < \mathrm{ord}(\mathbf{D}_\kappa \mathbf{D}^1_\ell) = \mathrm{ord}(\mathbf{D}_\kappa) + 1,$$

hence

$$\mathrm{ord}(\mathbf{D}_{\kappa'}) \leq \mathrm{ord}(\mathbf{D}_\kappa). \tag{52}$$

Since the support of $\mathbf{D}_{\kappa'}$ is divisible by an extra prime $\ell \in \tilde{\mathcal{S}}_{p^m}$, we see that

$$\mathrm{wt}(\mathbf{D}_{\kappa'}) < \mathrm{wt}(\mathbf{D}_\kappa). \tag{53}$$

In case (2), since $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p},m}\big(H^1_f(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}\big)$ by assumption, this is enough to check that $\mathbf{D}_{\kappa'}$ satisfies the inductive hypothesis, hence $\mathbf{D}_{\kappa'}(y_{S\ell,\mathfrak{p}}) \equiv 0 \pmod{p^m}$. Suppose we are in case (1). By Lemma 3.30, one has

$$r_\mathfrak{p}\big(H^1_{f,S'}(K, W_\mathfrak{p}[p])^{\epsilon_\kappa}\big) \leq r_\mathfrak{p}\big(H^1_{f,S'\ell}(K, W_\mathfrak{p}[p])^{\epsilon_\kappa}\big) + r_\mathfrak{p}\big(A(S'\ell)^{\epsilon_\kappa}\big) - r_\mathfrak{p}\big(A(S')^{\epsilon_\kappa}\big).$$

Combining this inequality with the one in the statement of the proposition, we find that

$$\mathrm{ord}(\mathbf{D}_\kappa) < r_\mathfrak{p}\big(H^1_{f,S'\ell}(K, W_\mathfrak{p}[p])^{\epsilon_\kappa}\big) + r_\mathfrak{p}\big(A(S'\ell)^{\epsilon_\kappa}\big),$$

and therefore, applying (52), we get

$$\mathrm{ord}(\mathbf{D}_{\kappa'}) < r_\mathfrak{p}\big(H^1_{f,S'\ell}(K, W_\mathfrak{p}[p])^{\epsilon_\kappa}\big) + r_\mathfrak{p}\big(A(S'\ell)^{\epsilon_\kappa}\big). \tag{54}$$

Equations (54) and (53) show that $\mathbf{D}_{\kappa'}$ satisfies the inductive hypothesis when $\mathrm{cond}(\mathbf{D}_{\kappa'}) = \mathbf{S}'\ell$, and we conclude that $\mathbf{D}_{\kappa'}(y_{S\ell,\mathfrak{p}}) \equiv 0 \pmod{p}$ in this case. Now suppose that $\mathrm{cond}(\mathbf{D}_{\kappa'}) = S''$ with $S'' \mid S'\ell$ and let $Q := S'\ell/S''$. Then every prime t dividing Q gives a derivative of the form $\mathbf{D}^0_t$ in $\mathbf{D}_{\kappa'}$. If there exists a prime t dividing Q with $t \in \tilde{\mathcal{S}}_p$, then $\mathbf{D}_{\kappa'}(y_{S\ell,\mathfrak{p}}) \equiv 0 \pmod{p}$ (to check this, use the norm relation and the divisibility $p \mid a_t$). If no such prime t appears, then $p \nmid a_t$ for all $t \mid Q$, which implies that $r_\mathfrak{p}\big(H^1_f(K_\lambda, W_\mathfrak{p}[p^m])^{\pm}\big) = 0$ at $\lambda \mid t$. Therefore $A(S'') = A(S'\ell)$. On the other hand, one clearly has

$$r_\mathfrak{p}\big(H^1_{f,S'\ell}(K, W_\mathfrak{p}[p])^{\epsilon_\kappa}\big) \leq r_\mathfrak{p}\big(H^1_{f,S''}(K, W_\mathfrak{p}[p])^{\epsilon_\kappa}\big),$$

and we conclude using (54) that

$$\mathrm{ord}(\mathbf{D}_{\kappa'}) < r_\mathfrak{p}\big(H^1_{f,S''}(K, W_\mathfrak{p}[p])^{\epsilon_\kappa}\big) + r_\mathfrak{p}\big(A(S'')^{\epsilon_\kappa}\big). \tag{55}$$

Equations (53) and (55) show that the inductive hypothesis holds, and so we may again conclude that $\mathbf{D}_{\kappa'}(y_{S\ell,\mathfrak{p}}) \equiv 0 \pmod{p}$. This shows that Assumption 3.12 is satisfied in our setting.

Since Assumption 3.12 holds, we may apply the construction of §3.6 and obtain a class $d(\ell) \in H^1(K, W_\mathfrak{p}[p^m])$. The image of $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$ in $H^1_f(K_\lambda, W_\mathfrak{p}[p^m])$ being non-zero, it follows from Proposition 3.20 (which we can apply because $\mathfrak{p}^{m+1} \nmid \ell+1\pm a_\ell$) that the image of $d(\ell)_\lambda$ in $H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])$ is non-zero as well. Therefore, since $d(\ell)$ belongs to the ϵ_κ-eigenspace for c thanks to Proposition 3.14, Proposition 3.21 ensures that the map

$$\phi_\lambda : H^1_{sin}(K_\lambda, W_\mathfrak{p}[p^m])^{\epsilon_\kappa} \longrightarrow \big(H^1_{f,S'}(K, W_\mathfrak{p}[p^m])^*\big)^{\epsilon_\kappa}$$

is not injective. But this contradicts (51), and the proposition is proved. □

Now we keep notation and assumptions as in Proposition 3.31 and prove two corollaries.

Corollary 3.32. *If* $\mathrm{ord}(\mathbf{D}_\kappa) < p$ *and either*

(1) $m = 1$ *and* $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p}}\big(H^1_{f,S'}(K, W_{\mathfrak{p}}[p])^{-\epsilon_\kappa}\big) + r_{\mathfrak{p}}\big(A(S')^{-\epsilon_\kappa}\big) - 1$

or

(2) $m \geq 1$ *and* $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p},m}\big(H^1_f(K, W_{\mathfrak{p}}[p^m])^{-\epsilon_\kappa}\big) - 1$,

then $\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \equiv 0 \pmod{p^m}$.

Proof. Suppose $\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \not\equiv 0 \pmod{p^m}$ and pick a prime ℓ such that $\mathrm{Frob}_\ell = \mathrm{Frob}_\infty$ in $\mathrm{Gal}(L_{S,m}/\mathbb{Q})$ and the image of $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$ in $H^1_f(K_\lambda, W_{\mathfrak{p}}[p^m])$ is not zero (that such a choice is possible can be checked along the same lines as in the proof of Proposition 3.27, and the arguments are actually simpler).

Now we show that

$$\mathbf{D}_\kappa\mathbf{D}^1_\ell(y_{S\ell,\mathfrak{p}}) \text{ is not zero in } H^1(K, W_{\mathfrak{p}}[p^m]). \tag{56}$$

If there is a derivative $\mathbf{D}_{\kappa'}$ strictly less than $\mathbf{D}_\kappa\mathbf{D}^1_\ell$ such that $\mathbf{D}_{\kappa'}(y_{S\ell,\mathfrak{p}})$ is not zero in $H^1(K, W_{\mathfrak{p}}[p^m])$, using formula (24) recursively one easily shows that (56) holds (use here the fact that $\mathrm{ord}(\mathbf{D}_\kappa) < p$). On the contrary, if for all derivatives $\mathbf{D}_{\kappa'}$ strictly less than $\mathbf{D}_\kappa\mathbf{D}^1_\ell$ we have $\mathbf{D}_{\kappa'}(y_{S\ell,\mathfrak{p}}) = 0$ in $H^1(K, W_{\mathfrak{p}}[p^m])$ then one can construct the class $d(\ell)$ which, by Proposition 3.20, is not locally trivial at λ. Hence, *a fortiori*, $d(\ell)$ is not globally trivial, and therefore also $P(\ell) = \mathbf{D}_\kappa\mathbf{D}^1_\ell(y_{S\ell,\mathfrak{p}})$ is not trivial.

In case (1), since

$$\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell) = \mathrm{ord}(\mathbf{D}_\kappa) + 1, \tag{57}$$

we obtain that

$$\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell) < r_{\mathfrak{p}}\big(H^1_{f,S'}(K, W_{\mathfrak{p}}[p])^{-\epsilon_\kappa}\big) + r_{\mathfrak{p}}\big(A(S')^{-\epsilon_\kappa}\big).$$

By Lemma 3.30, the right hand side of the inequality above is less than or equal to

$$r_{\mathfrak{p}}\big(H^1_{f,S'\ell}(K, W_{\mathfrak{p}}[p])^{-\epsilon_\kappa}\big) + r_{\mathfrak{p}}\big(A(S'\ell)^{-\epsilon_\kappa}\big),$$

so we obtain the inequality

$$\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell) < r_{\mathfrak{p}}\big(H^1_{f,S'\ell}(K, W_{\mathfrak{p}}[p])^{-\epsilon_\kappa}\big) + r_{\mathfrak{p}}\big(A(S'\ell)^{-\epsilon_\kappa}\big).$$

In case (2), again using (57), we get the inequality

$$\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell) < r_{\mathfrak{p},m}\big(H^1_f(K, W_{\mathfrak{p}}[p^m])^{-\epsilon_\kappa}\big).$$

By (57), we have $(-1)^{\mathrm{ord}(\mathbf{D}_\kappa\mathbf{D}^1_\ell)} = -\epsilon_\kappa$. Therefore in both cases we can apply Proposition 3.31, which shows that $\mathbf{D}_\kappa\mathbf{D}^1_\ell(y_{S\ell,\mathfrak{p}}) \equiv 0 \pmod{p}$. In light of (56), this is a contradiction. □

Corollary 3.33. *If either*

(1) $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p},m}\big(H^1_f(K, W_{\mathfrak{p}}[p^m])^{\epsilon_\kappa}\big)$

or

(2) $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p},m}\big(H^1_f(K, W_{\mathfrak{p}}[p^m])^{-\epsilon_\kappa}\big) - 1$ *and* $\mathrm{ord}(\mathbf{D}_\kappa) < p$,

then $\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \equiv 0 \pmod{p^m}$.

Proof. Use Proposition 3.31 if (1) holds and Corollary 3.32 if (2) holds. □

We are now in a position to state and prove the main result of this section.

Theorem 3.34. *Let* S *be a square-free product of primes in* $\mathcal{S}_{p^m}$. *If* $\mathrm{ord}(\mathbf{D}_\kappa) < \min\{r_{\mathfrak{p},m}, p\}$, *then* $\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \equiv 0 \pmod{p^m}$.

Proof. Since $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p},m}$ and

$$r_{\mathfrak{p},m} = r_{\mathfrak{p},m}\big(H^1_f(K, W_{\mathfrak{p}}[p^m])^{\epsilon_\kappa}\big) + r_{\mathfrak{p},m}\big(H^1_f(K, W_{\mathfrak{p}}[p^m])^{-\epsilon_\kappa}\big),$$

at least one of the conditions in Corollary 3.33 is satisfied (in (2) we also need the condition $\mathrm{ord}(\mathbf{D}_\kappa) < p$, which is not needed for (1)), and we are done. □

4. Theta elements and refined Beilinson–Bloch conjecture

In this section we prove our main result on the order of vanishing of certain combinations of Heegner cycles.

4.1. Theta elements and arithmetic L-functions.

For any square-free product T of prime numbers belonging to the set $\mathcal{S}$ defined in (17) consider the resolvent element

$$\theta_{T,\mathfrak{p}} := \sum_{\sigma \in G_T} \sigma(y_{T,\mathfrak{p}}) \otimes \sigma \in \Lambda_{\mathfrak{p}}(K_T) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}[G_T].$$

Our main result relates these elements to the dimension of $X_{\mathfrak{p}}(K)$ over $F_{\mathfrak{p}}$.

We also need to introduce suitable variants and combinations of the elements above. To begin with, we trace them down to K as follows. As in §3.6, fix any lift $\mathbf{N}_T \in \mathbb{Z}[\Gamma_T]$ of the norm $\mathbf{N} = \sum_{\sigma \in \Gamma_1} \sigma$; in other words, for every $\sigma \in \Gamma_1$ choose $\sigma' \in \Gamma_T$ such that $\sigma'|_{K_1} = \sigma$. Define

$$\zeta_{T,\mathfrak{p}} := \mathbf{N}_T(\theta_{T,\mathfrak{p}}) = \sum_{\sigma \in G_T} \sigma \mathbf{N}_T(y_{T,\mathfrak{p}}) \otimes \sigma \in \Lambda_{\mathfrak{p}}(K_T) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}[G_T]. \tag{58}$$

Note that these elements depend on the choice of $\mathbf{N}_T$, but for simplicity we shall drop this dependence from the notation.

Let $x \mapsto x^*$ denote the involution of $\mathcal{O}_{\mathfrak{p}}[G_T]$ induced by the map $\sigma \mapsto \sigma^{-1}$ on G_T and denote by $\zeta^*_{T,\mathfrak{p}}$ the element obtained by applying to $\zeta_{T,\mathfrak{p}}$ the map induced by this involution.

Fix a square-free product S of primes belonging to $\mathcal{S}$. As before, fix a lift $\mathbf{N}_S$ of $\mathbf{N}$ to $\mathbb{Z}[\Gamma_S]$. By projection, this gives lifts $\mathbf{N}_T$ for all $T \mid S$ that may be used to define $\zeta_{T,\mathfrak{p}}$ and $\zeta^*_{T,\mathfrak{p}}$ as in (58). Since the extension $K_S/\mathbb{Q}$ is generalized dihedral and hence solvable, part (1) of Lemma 3.10 ensures that $A_{\mathfrak{p}}(K_S) = 0$, so for every $T \mid S$ the inflation-restriction exact sequence yields an injection $\Lambda_{\mathfrak{p}}(K_T) \hookrightarrow \Lambda_{\mathfrak{p}}(K_S)$. On the other hand, the natural inclusion $G_T \subset G_S$ (see §3.1) induces an injection $\mathcal{O}_{\mathfrak{p}}[G_T] \hookrightarrow \mathcal{O}_{\mathfrak{p}}[G_S]$ of (free) $\mathcal{O}_{\mathfrak{p}}$-modules, and therefore we obtain an injection

$$\Lambda_{\mathfrak{p}}(K_T) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}[G_T] \longrightarrow \Lambda_{\mathfrak{p}}(K_S) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}[G_S] \tag{59}$$

of $\mathcal{O}_{\mathfrak{p}}$-modules. Furthermore, the canonical inclusion $G_S \subset \Gamma_S$ induces an injection

$$\Lambda_{\mathfrak{p}}(K_S) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}[G_S] \longrightarrow \Lambda_{\mathfrak{p}}(K_S) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}[\Gamma_S] \tag{60}$$

of $\mathcal{O}_{\mathfrak{p}}$-modules. The composition of (59) and (60) allows us to view $\zeta_{T,\mathfrak{p}}$ and $\zeta^*_{T,\mathfrak{p}}$ as elements of $\Lambda_{\mathfrak{p}}(K_S) \otimes_{\mathcal{O}_{\mathfrak{p}}} \mathcal{O}_{\mathfrak{p}}[\Gamma_S]$, which from here on we shall do without any further warning.

For S fixed as above and every $T \mid S$ set

$$a_T := \mu(T) \sum_{\sigma \in \mathrm{Gal}(K_S/K_T)} \sigma, \qquad a^*_T := \chi_K(T) a_T \tag{61}$$

where μ is the Möbius function and χ_K is the quadratic character attached to K. Define the *arithmetic L-function* attached to S and $\mathfrak{p}$ as

$$\mathcal{L}_{S,\mathfrak{p}} := \Big(\sum_{T|S} a_T\zeta_{T,\mathfrak{p}}\Big)\otimes\Big(\sum_{T|S} a_T^*\zeta_{T,\mathfrak{p}}^*\Big) \in \Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_S]. \tag{62}$$

Here we are using the canonical identification

$$\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_S] = \big(\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_S]\big)\otimes_{\mathcal{O}_{\mathfrak{p}}[\Gamma_S]}\big(\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_S]\big),$$

the superscript "$\otimes 2$" denoting tensorization over $\mathcal{O}_{\mathfrak{p}}$. Note that if $T \mid S$ and

$$\mu_{S,T} : \Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_S] \longrightarrow \Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[\Gamma_T]$$

is the map induced by the canonical projection $\Gamma_S \twoheadrightarrow \Gamma_T$, then

$$\mu_{S,T}(\mathcal{L}_{S,\mathfrak{p}}) = \mathcal{L}_{T,\mathfrak{p}}\cdot\prod_{\ell|(S/T)}(1+\ell-a_\ell/\ell^{k/2-1})\cdot(1+\ell+a_\ell/\ell^{k/2-1}). \tag{63}$$

Remark 4.1. One could define an element $\mathcal{L}_{S,\mathfrak{p}}$ as in (62) by replacing the coefficients a_T and a_T^* with any choice of b_T and b'_T in $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$, obtaining compatibility relations similar to (63). Our preference is motivated by the existence of a regulator of Mazur–Tate type, called *Nekovář regulator* and denoted by $\mathscr{R}^{\mathrm{Nek}}(S)$ in Section 5, that enjoys properties analogous to those of the regulator defined in [36] and [37] and used in [18]. The regulator $\mathscr{R}^{\mathrm{Nek}}(S)$ is predicted to appear in the expression of the leading coefficient of $\mathcal{L}_{S,\mathfrak{p}}$ for this specific choice of a_T and a_T^*. However, it is reasonable to expect alternative choices of coefficients b_T and b'_T to be related to other types of regulators having formal properties different from those of Mazur–Tate regulators. Finally, observe that the results for $\mathcal{L}_{S,\mathfrak{p}}$ proved in this paper still hold for any choice of b_T and b'_T; see Remarks 4.8 and 4.17 below.

4.2. **Results on the order of vanishing.** Recall that I_{G_S} and I_{Γ_S} are the augmentation ideals of $\mathcal{O}_{\mathfrak{p}}[G_S]$ and $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$, respectively. The powers of I_{G_S} define a decreasing filtration

$$\mathcal{O}_{\mathfrak{p}}[G_S] = I_{G_S}^0 \supset I_{G_S}^1 \supset I_{G_S}^2 \supset\cdots\supset I_{G_s}^n \supset\cdots \tag{64}$$

on $\mathcal{O}_{\mathfrak{p}}[G_S]$. On the other hand, since the $\mathcal{O}_{\mathfrak{p}}$-module $\Lambda_{\mathfrak{p}}(K_S)$ is not in general torsion-free, we cannot expect tensorization of the sequence (64) by $\Lambda_{\mathfrak{p}}(K_S)$ over $\mathcal{O}_{\mathfrak{p}}$ to yield a filtration on $\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[G_S]$. In light of this, when we write that an element θ of $\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[G_S]$ belongs to $\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}I_{G_S}^r$ we really mean that θ belongs to the natural image of the $\mathcal{O}_{\mathfrak{p}}$-module $\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}I_{G_S}^r$ inside $\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[G_S]$.

Definition 4.2. Let $r\in\mathbb{N}$.

(1) An element $\theta\in\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[G_S]$ is said to *vanish to order at least* r if $\theta\in\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}I_{G_S}^r$.
(2) An element $\theta\in\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}\mathcal{O}_{\mathfrak{p}}[G_S]$ is said to *vanish to order (exactly)* r if $\theta\in\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}I_{G_S}^r$ but $\theta\notin\Lambda_{\mathfrak{p}}(K_S)\otimes_{\mathcal{O}_{\mathfrak{p}}}I_{G_S}^{r+1}$.

Analogous definitions and conventions apply to $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$ and I_{Γ_S} and, below, with $\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}$ in place of $\Lambda_{\mathfrak{p}}(K_S)$.

The first conjecture we formulate is

Conjecture 4.3 ("Weak vanishing")**.** *The element $\mathcal{L}_{S,\mathfrak{p}}$ vanishes to order at least $\tilde\rho_{\mathfrak{p}}-1$ and vanishes to order exactly $\tilde\rho_{\mathfrak{p}}-1$ if and only if $|\rho_{\mathfrak{p}}^+-\rho_{\mathfrak{p}}^-|=1$.*

A similar statement in the context of p-adic analogues of the Birch–Swinnerton-Dyer conjecture for elliptic curves can be found in [4, Conjecture 4.2].

Remark 4.4. We explicitly observe that Conjecture 4.3 involves $\tilde{\rho}_{\mathfrak{p}} - 1$, and not $\tilde{\rho}_{\mathfrak{p}}$, because, as in [18], the element $\mathcal{L}_{S,\mathfrak{p}}$ should mirror the behaviour of the first derivative $L'(f \otimes K, s)$ at $s = k/2$ (in fact, to be somewhat more in line with the notation adopted in [18] we should write $\mathcal{L}'_{S,\mathfrak{p}}$ in place of $\mathcal{L}_{S,\mathfrak{p}}$).

Corollary 4.7, which is a consequence of the next result, will provide a proof of part of Conjecture 4.3.

Theorem 4.5. *If $\rho_{\mathfrak{p}} \leq p$, then $\theta_{S,\mathfrak{p}} \in \Lambda_{\mathfrak{p}}(K_S) \otimes_{\mathcal{O}_{\mathfrak{p}}} I_{G_S}^{\rho_{\mathfrak{p}}}$.*

Proof. Let $\mathbf{D}_\kappa$ be a derivative with $\mathrm{ord}(\mathbf{D}_\kappa) < \rho_{\mathfrak{p}}$, $\mathrm{supp}(\mathbf{D}_\kappa) = S$ and $\mathrm{cond}(\mathbf{D}_\kappa) \mid S$. Set $S' := \mathrm{cond}(\mathbf{D}_\kappa)$ and write $\mathbf{D}_\kappa = \mathbf{D}_{\kappa'} \cdot \mathbf{D}_{\kappa''}$ where the derivative $\mathbf{D}_{\kappa'}$ satisfies $\mathrm{supp}(\mathbf{D}_{\kappa'}) = \mathrm{cond}(\mathbf{D}_{\kappa'}) = S'$ and the derivative $\mathbf{D}_{\kappa''}$ has order 0 and support in S/S' (so $\mathbf{D}_{\kappa''}$ is nothing other than the norm operator from G_S to $G_{S'}$). Part (1) of Proposition 3.1 combined with the relation (1) between Galois trace, restriction and corestriction maps shows that

$$\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) = \mathrm{res}_{K_{S'}/K_S}\big(\mathbf{D}_{\kappa'}(y_{S',\mathfrak{p}})\big) \cdot \prod_{\ell \mid (S/S')} a_\ell/\ell^{k/2-1} \tag{65}$$

where $\mathrm{res}_{K_{S'}/K_S}$ is the restriction from $H^1(K_{S'}, A_{\mathfrak{p}})$ to $H^1(K_S, A_{\mathfrak{p}})$. Let $m = \eta(\kappa)$ denote the smallest power of p dividing the orders of the groups G_ℓ with $\ell \mid S$. By definition, all primes dividing S belong to $\mathcal{S}_{p^m}$. Since $\rho_{\mathfrak{p}} \leq r_{\mathfrak{p},m}$ by Lemma 3.7, we have $\mathrm{ord}(\mathbf{D}_\kappa) < r_{\mathfrak{p},m}$. Therefore the assumptions of Theorem 3.34 are satisfied, and then

$$\mathbf{D}_{\kappa'}(y_{S',\mathfrak{p}}) \equiv 0 \pmod{p^m}. \tag{66}$$

Combining (65) and (66), we see that if $\mathrm{ord}(\mathbf{D}_\kappa) < \rho_{\mathfrak{p}}$, then $p^m \mid \mathbf{D}_\kappa(y_{S,\mathfrak{p}})$. The result follows from the divisibility criterion in §3.4.2, which we can apply thanks to the condition $\rho_{\mathfrak{p}} \leq p$. □

Corollary 4.6. $\zeta_{S,\mathfrak{p}}, \zeta^*_{S,\mathfrak{p}} \in \Lambda_{\mathfrak{p}}(K_S) \otimes_{\mathcal{O}_{\mathfrak{p}}} I_{G_S}^{\rho_{\mathfrak{p}}}$.

Proof. The element $\zeta_{S,\mathfrak{p}}$ is the image of $\theta_{S,\mathfrak{p}}$ via the endomorphism of $\Lambda_{\mathfrak{p}}(K_S) \otimes I_{G_S}^{\rho_{\mathfrak{p}}}$ defined by $x \otimes i \mapsto \big(\mathbf{N}_S(x)\big) \otimes i$. Since the Abel–Jacobi map commutes with Galois actions, it follows from Theorem 4.5 that $\zeta_{S,\mathfrak{p}}$ belongs to $\Lambda_{\mathfrak{p}}(K_S) \otimes I_{G_S}^{\rho_{\mathfrak{p}}}$. Applying the main involution, one obtains that $\zeta^*_{S,\mathfrak{p}}$ belongs to $\Lambda_{\mathfrak{p}}(K_S) \otimes I_{G_S}^{\rho_{\mathfrak{p}}}$ as well. □

Corollary 4.7. $\mathcal{L}_{S,\mathfrak{p}} \in \Lambda_{\mathfrak{p}}(K_S)^{\otimes 2} \otimes_{\mathcal{O}_{\mathfrak{p}}} I_{\Gamma_S}^{2\rho_{\mathfrak{p}}}$.

Proof. Since $\mathcal{L}_{S,\mathfrak{p}}$ is a linear combination with coefficients in $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$ of the elements $\zeta_{T,\mathfrak{p}}$ and $\zeta^*_{T,\mathfrak{p}}$ for $T \mid S$, the result is a consequence of Corollary 4.6 applied to these elements. □

In light of Lemma 3.5, Corollary 4.7 implies the first part of Conjecture 4.3 and is, in fact, equivalent to it when $|\rho_{\mathfrak{p}}^+ - \rho_{\mathfrak{p}}^-| = 1$. On the other hand, if $|\rho_{\mathfrak{p}}^+ - \rho_{\mathfrak{p}}^-| > 1$, then $2\rho_{\mathfrak{p}} > \tilde{\rho}_{\mathfrak{p}} - 1$, and Corollary 4.7 shows more than what is predicted by the first part of Conjecture 4.3. In other words, if $|\rho_{\mathfrak{p}}^+ - \rho_{\mathfrak{p}}^-| > 1$, then there is *extra vanishing* of $\mathcal{L}_{S,\mathfrak{p}}$.

Remark 4.8. More generally, the result of Corollary 4.7 is valid (with the same proof) for any linear combination with coefficients in $\mathcal{O}_\mathfrak{p}[\Gamma_S]$ of the elements $\zeta_{T,\mathfrak{p}}$ and $\zeta^*_{T,\mathfrak{p}}$ with $T \mid S$. See Remark 4.1 for a detailed discussion of our specific choice of coefficients for $\mathcal{L}_{S,\mathfrak{p}}$.

4.3. **Results on the leading terms.** We study, in some particular cases, the reductions modulo p of the leading terms of $\zeta_{S,\mathfrak{p}}$ and $\mathcal{L}_{S,\mathfrak{p}}$. Here S is a square-free product of primes in $\mathcal{S}_p$ and $\rho_\mathfrak{p} < p$.

We first consider the *leading coefficient* (or *leading term*) $\tilde{\theta}_{S,\mathfrak{p}}$ of $\theta_{S,\mathfrak{p}}$, which is defined to be the image of $\theta_{S,\mathfrak{p}}$ in $\Lambda_\mathfrak{p}(K_S) \otimes_{\mathcal{O}_\mathfrak{p}} \big(I_{G_S}^{\rho_\mathfrak{p}}/I_{G_S}^{\rho_\mathfrak{p}+1}\big)$. Analogous definitions can be given for $\zeta_{S,\mathfrak{p}}$ and $\mathcal{L}_{S,\mathfrak{p}}$.

Remark 4.9. A more accurate choice would be to call $\tilde{\theta}_{S,\mathfrak{p}}$ the $\rho_\mathfrak{p}$*-th coefficient* of $\theta_{S,\mathfrak{p}}$, as Theorem 4.5 only shows that $\theta_{S,\mathfrak{p}}$ vanishes to order at least $\rho_\mathfrak{p}$. However, we find this slight abuse to be convenient and the resulting terminology to be more suggestive of the global underlying philosophy, and we are confident that this convention will cause no confusion.

Together with Conjecture 5.1, the following conjecture takes care of the leading coefficient of $\mathcal{L}_{S,\mathfrak{p}}$, which is the image $\tilde{\mathcal{L}}_{S,\mathfrak{p}}$ of $\mathcal{L}_{S,\mathfrak{p}}$ in $\Lambda(K_S)^{\otimes 2} \otimes \big(I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}-1}/I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}}\big)$; the reader is reminded to keep Conjecture 4.3 in mind.

Conjecture 4.10 ("Rationality of the leading coefficient")**.** *The element $\tilde{\mathcal{L}}_{S,\mathfrak{p}}$ belongs to the image of the natural map*

$$\Lambda(K)^{\otimes 2} \otimes \big(I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}-1}/I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}}\big) \longrightarrow \Lambda(K_S)^{\otimes 2} \otimes \big(I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}-1}/I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}}\big). \tag{67}$$

When $|\rho_\mathfrak{p}^+ - \rho_\mathfrak{p}^-| = 1$ and all the prime factors of S belong to $\mathcal{S}_p$, a weaker, mod p version of Conjecture 4.10 will be proved in part (2) of Corollary 4.16.

By Theorem 4.5, there is a congruence

$$\tilde{\theta}_{S,\mathfrak{p}} \equiv \sum_{\kappa} \mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \otimes (\sigma_1 - 1)^{k_1} \dots (\sigma_t - 1)^{k_s} \pmod{p} \tag{68}$$

where the sum is over all the κ with $\mathrm{ord}(\kappa) = \rho_\mathfrak{p}$. Denote by

$$\mathbf{D}_\kappa^{(p)}(y_{S,\mathfrak{p}}) \in \Lambda_\mathfrak{p}(K_S)/p\Lambda_\mathfrak{p}(K_S)$$

the reduction modulo p of $\mathbf{D}_\kappa(y_{S,\mathfrak{p}})$ for $\mathrm{ord}(\kappa) = \rho_\mathfrak{p}$.

Lemma 4.11. $\mathbf{D}_\kappa^{(p)}(y_{S,\mathfrak{p}}) \in \big(\Lambda_\mathfrak{p}(K_S)/p\Lambda_\mathfrak{p}(K_S)\big)^{G_S}$.

Proof. Combine Theorem 4.5 and formula (24), for which the condition $\rho_\mathfrak{p} < p$ is needed. ☐

Recall that $\mathbf{N}_S \in \mathbb{Z}[\Gamma_S]$ is a lift of the norm operator in $\mathbb{Z}[\Gamma_1]$.

Lemma 4.12. $\mathbf{D}_\kappa^{(p)}\big(\mathbf{N}_S(y_{S,\mathfrak{p}})\big) \in \big(\Lambda_\mathfrak{p}(K_S)/p\Lambda_\mathfrak{p}(K_S)\big)^{\Gamma_S}$.

Proof. Immediate from Lemma 4.11. ☐

By (15), for all $m \geq 1$ there is an injection $\Lambda_\mathfrak{p}(K)/p^m\Lambda_\mathfrak{p}(K) \hookrightarrow H^1_f(K, W_\mathfrak{p}[p^m])$. Define the p^m-part $Ш_{p^m}(K, W_\mathfrak{p})$ of the Shafarevich–Tate group of $W_\mathfrak{p}$ over K as the cokernel of this map, so that there is a short exact sequence

$$0 \longrightarrow \Lambda_\mathfrak{p}(K)/p^m\Lambda_\mathfrak{p}(K) \longrightarrow H^1_f(K, W_\mathfrak{p}[p^m]) \longrightarrow Ш_{p^m}(K, W_\mathfrak{p}) \longrightarrow 0. \tag{69}$$

Since $H^1_f(K, W_\mathfrak{p}[p^m])$ is finite, the abelian group $\text{Ш}_{p^m}(K, W_\mathfrak{p})$ is finite as well. By passing to the direct limit over m in (69), we obtain the p^∞-part $\text{Ш}_{p^\infty}(K, W_\mathfrak{p})$ of the Shafarevich–Tate group of $W_\mathfrak{p}$ over K, which sits in the short exact sequence

$$0 \longrightarrow \Lambda_\mathfrak{p}(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1_f(K, W_\mathfrak{p}) \longrightarrow \text{Ш}_{p^\infty}(K, W_\mathfrak{p}) \longrightarrow 0.$$

Proposition 4.13. *Suppose that* $|\rho_\mathfrak{p}^+ - \rho_\mathfrak{p}^-| = 1$ *and let* $\mathbf{D}_\kappa$ *have order* $\rho_\mathfrak{p}$ *and support* S. *If* $\mathbf{D}_\kappa(y_{S,\mathfrak{p}}) \not\equiv 0 \pmod{p}$, *then*

(1) $\text{Ш}_p(K, W_\mathfrak{p}) = 0$;
(2) *with* $A(S)$ *defined as in* (45), *the natural map*
$$H^1_f(K, W_\mathfrak{p}[p]) \longrightarrow A(S)$$
is surjective.

Proof. We first observe that, by definition, one has

$$2\rho_\mathfrak{p} = \dim_{F_\mathfrak{p}}\big(X_\mathfrak{p}(K)\big) - 1. \tag{70}$$

Proposition 3.31 shows that

$$\rho_\mathfrak{p} \geq r_\mathfrak{p}\big(H^1_{f,S}(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}\big) + r_\mathfrak{p}\big(A(S)^{\epsilon_\kappa}\big) \geq r_\mathfrak{p}\big(H^1_f(K, W_\mathfrak{p}[p^m])^{\epsilon_\kappa}\big), \tag{71}$$

while Corollary 3.32 implies that

$$\rho_\mathfrak{p} \geq r_\mathfrak{p}\big(H^1_{f,S}(K, W_\mathfrak{p}[p^m])^{-\epsilon_\kappa}\big) + r_\mathfrak{p}\big(A(S)^{-\epsilon_\kappa}\big) - 1 \geq r_\mathfrak{p}\big(H^1_f(K, W_\mathfrak{p}[p^m])^{-\epsilon_\kappa}\big) - 1 \tag{72}$$

(for the last inequalities in the chains above, see the proof of Lemma 3.30). Since

$$r_\mathfrak{p}\big(H^1_f(K, W_\mathfrak{p}[p^m])^{\pm}\big) \geq r_\mathfrak{p}\Big(\big(\Lambda_\mathfrak{p}(K)/p\Lambda_\mathfrak{p}(K)\big)^{\pm}\Big) \geq \rho_\mathfrak{p}^{\pm}, \tag{73}$$

we obtain the inequalities $\rho_\mathfrak{p} \geq \rho_\mathfrak{p}^{\epsilon_\kappa}$ and $\rho_\mathfrak{p} \geq \rho_\mathfrak{p}^{-\epsilon_\kappa} - 1$. Therefore we have the inequality

$$2\rho_\mathfrak{p} \geq \dim_{F_\mathfrak{p}}\big(X_\mathfrak{p}(K)\big) - 1. \tag{74}$$

Comparing (70) and (74), we conclude that all the inequalities above are, in fact, equalities; in particular, the first inequality in (73) is an equality, from which (1) follows immediately by definition of $\text{Ш}_\mathfrak{p}(f/K)$. Furthermore, the second inequalities in (71) and (72) are equalities, and then

$$r_\mathfrak{p}\big(H^1_f(K, W_\mathfrak{p}[p^m])\big) = r_\mathfrak{p}\big(H^1_{f,S}(K, W_\mathfrak{p}[p^m])\big) + r_\mathfrak{p}\big(A(S)\big).$$

Comparing this equality with the definition of $H^1_{f,S}(K, W_\mathfrak{p}[p^m])$ in (35) proves (2). □

Proposition 4.14. *If* $|\rho_\mathfrak{p}^+ - \rho_\mathfrak{p}^-| = 1$ *and* $\mathrm{ord}(\kappa) = \rho_\mathfrak{p}$, *then* $\mathbf{D}_\kappa^{(p)}\big(\mathbf{N}_S(y_{S,\mathfrak{p}})\big)$ *lies in the image of* $\Lambda_\mathfrak{p}(K)/p\Lambda_\mathfrak{p}(K)$.

Proof. By (15), there is an injective map

$$\Lambda_\mathfrak{p}(K_S)/p\Lambda_\mathfrak{p}(K_S) \hookrightarrow H^1_f(K_S, W_\mathfrak{p}[p]) \subset H^1(K_S, W_\mathfrak{p}[p]). \tag{75}$$

Recall that restriction gives an isomorphism $H^1(K, W_\mathfrak{p}[p]) \simeq H^1(K_S, W_\mathfrak{p}[p])^{\Gamma_S}$ and that $\mathbf{D}_\kappa^{(p)}(\mathbf{N}_S y_{S,\mathfrak{p}})$ belongs to $(\Lambda_\mathfrak{p}(K_S)/p\Lambda_\mathfrak{p}(K_S))^{\Gamma_S}$ by Lemma 4.12. In light of these facts and the Γ_S-equivariance of the injection (75), write d for the image of $\mathbf{D}_\kappa^{(p)}(\mathbf{N}_S y_{S,\mathfrak{p}})$ in $H^1(K, W_\mathfrak{p}[p])$.

We first show that $d \in H^1_f(K, W_{\mathfrak{p}}[p])$. By an argument similar to those in Propositions 3.16 and 3.17, one can check that the restriction of d at all places $v \nmid S$ is finite. There is a map

$$\bigoplus_{v|S} H^1_{sin}(K_v, W_{\mathfrak{p}}[p]) \longrightarrow H^1_f(K, W_{\mathfrak{p}}[p])^* \tag{76}$$

taking $x = (x_v)_{v|S}$ to the linear function

$$s \longmapsto \sum_{v \in S} \langle x, \mathrm{res}_v(s) \rangle_v$$

on $H^1_f(K, W_{\mathfrak{p}}[p])$ (recall that all the primes dividing S are inert in K). Since d is a global class, Tate duality ensures that the image of d in $\bigoplus_{v|S} H^1_{sin}(K_v, W_{\mathfrak{p}}[p])$ belongs to the kernel of (76). With $A(S)$ as in (45), part (2) of Proposition 4.13 shows that the map

$$H^1_f(K, W_{\mathfrak{p}}[p]) \longrightarrow A(S)$$

is surjective and hence, dually, that the map in (76) is injective (here we are implicitly using isomorphism (34)). It follows that d is locally finite everywhere and belongs to $H^1_f(K, W_{\mathfrak{p}}[p])$.

Since $Ш_p(K, W_{\mathfrak{p}}) = 0$ by part (1) of Proposition 4.13, we conclude that d comes from a class in $\Lambda_{\mathfrak{p}}(K)/p\Lambda_{\mathfrak{p}}(K)$. But there is a commutative diagram

$$\begin{tikzcd}
\Lambda_{\mathfrak{p}}(K)/p\Lambda_{\mathfrak{p}}(K) \arrow[r, "\simeq"] \arrow[d] & H^1_f(K, W_{\mathfrak{p}}[p]) \arrow[r, hook] \arrow[d] & H^1(K, W_{\mathfrak{p}}[p]) \arrow[d, "\simeq"] \\
\big(\Lambda_{\mathfrak{p}}(K_S)/p\Lambda_{\mathfrak{p}}(K_S)\big)^{\Gamma_S} \arrow[r, hook] & H^1_f(K_S, W_{\mathfrak{p}}[p])^{\Gamma_S} \arrow[r, hook] & H^1(K_S, W_{\mathfrak{p}}[p])^{\Gamma_S}
\end{tikzcd}$$

in which all the horizontal arrows are injective, and the proposition follows. $\square$

The information collected above on $\mathbf{D}^{(p)}_\kappa\big(\mathbf{N}_S(y_{S,\mathfrak{p}})\big)$ when $\mathrm{ord}(\kappa) = \rho_{\mathfrak{p}}$ yields a result on the reduction modulo p of the leading term $\tilde{\zeta}_{S,\mathfrak{p}}$ of $\zeta_{S,\mathfrak{p}}$. More precisely, define $\tilde{\zeta}_{S,\mathfrak{p}}$ as the image of $\zeta_{S,\mathfrak{p}}$ in $\Lambda_{\mathfrak{p}}(K_S) \otimes_{\mathcal{O}_{\mathfrak{p}}} \big(I^{\rho_{\mathfrak{p}}}_{\Gamma_S}/I^{\rho_{\mathfrak{p}}+1}_{\Gamma_S}\big)$ and consider its mod p reduction

$$\tilde{\zeta}^{(p)}_{S,\mathfrak{p}} \in \big(\Lambda_{\mathfrak{p}}(K_S)/p\Lambda_{\mathfrak{p}}(K_S)\big) \otimes_{\mathcal{O}_{\mathfrak{p}}} \big(I^{\rho_{\mathfrak{p}}}_{\Gamma_S}/I^{\rho_{\mathfrak{p}}+1}_{\Gamma_S}\big).$$

Finally, let $J(S)$ denote the cokernel of the map $H^1_f(K, W_{\mathfrak{p}}[p]) \to A(S)$; see (45) with $S' = S$ and $m = 1$ for the definition of $A(S)$.

Theorem 4.15. *Fix a square-free product S of primes in $\mathcal{S}_p$.*

(1) $\tilde{\zeta}^{(p)}_{S,\mathfrak{p}} \in \big(\Lambda_{\mathfrak{p}}(K_S)/p\Lambda_{\mathfrak{p}}(K_S)\big)^{\Gamma_S} \otimes_{\mathcal{O}_{\mathfrak{p}}} \big(I^{\rho_{\mathfrak{p}}}_{G_S}/I^{\rho_{\mathfrak{p}}+1}_{S,\mathfrak{p}}\big)$.

(2) *If $|\rho^+_{\mathfrak{p}} - \rho^-_{\mathfrak{p}}| = 1$, then $\tilde{\zeta}^{(p)}_{S,\mathfrak{p}}$ belongs to the image of the map*

$$\big(\Lambda_{\mathfrak{p}}(K)/p\Lambda_{\mathfrak{p}}(K)\big) \otimes_{\mathcal{O}_{\mathfrak{p}}} \big(I^{\rho_{\mathfrak{p}}}_{G_S}/I^{\rho_{\mathfrak{p}}+1}_{G_S}\big) \longrightarrow \big(\Lambda_{\mathfrak{p}}(K_S)/p\Lambda_{\mathfrak{p}}(K_S)\big)^{\Gamma_S} \otimes_{\mathcal{O}_{\mathfrak{p}}} \big(I^{\rho_{\mathfrak{p}}}_{G_S}/I^{\rho_{\mathfrak{p}}+1}_{G_S}\big).$$

(3) *If $|\rho^+_{\mathfrak{p}} - \rho^-_{\mathfrak{p}}| = 1$ and p divides $|Ш_p(K, W_{\mathfrak{p}})| \cdot |J(S)|$, then $\tilde{\zeta}^{(p)}_{S,\mathfrak{p}} = 0$.*

Proof. Part (1) follows from (68) and Lemma 4.12, while part (2) follows from (68) and Proposition 4.14. As for part (3), if $\tilde{\zeta}^{(p)}_{S,\mathfrak{p}} \neq 0$ then *a fortiori* $\mathbf{D}^{(p)}_\kappa(\mathbf{N}_S y_{S,\mathfrak{p}}) \not\equiv 0$ for all κ with $\mathrm{ord}(\kappa) = \rho_{\mathfrak{p}}$, and so Proposition 4.13 gives the triviality of both $Ш_p(K, W_{\mathfrak{p}})$ and $J(S)$. $\square$

Corollary 4.16. *Fix a square-free product S of primes in $\mathcal{S}_p$.*

(1) *The image $\tilde{\mathcal{L}}_{S,\mathfrak{p}}^{(p)}$ of $\mathcal{L}_{S,\mathfrak{p}}$ in*

$$\big(\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}/p\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\big)\otimes_{\mathcal{O}_{\mathfrak{p}}}\big(I_{\Gamma_S}^{2\rho_{\mathfrak{p}}}/I_{\Gamma_S}^{2\rho_{\mathfrak{p}}+1}\big)$$

belongs to the image of

$$\big(\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}/p\Lambda_{\mathfrak{p}}(K_S)^{\otimes 2}\big)^{\Gamma_S}\otimes_{\mathcal{O}_{\mathfrak{p}}}\big(I_{\Gamma_S}^{2\rho_{\mathfrak{p}}}/I_{\Gamma_S}^{2\rho_{\mathfrak{p}}+1}\big).$$

(2) *If $|\rho_{\mathfrak{p}}^{+}-\rho_{\mathfrak{p}}^{-}|=1$, then $\tilde{\mathcal{L}}_{S,\mathfrak{p}}^{(p)}$ belongs to the image of*

$$\big(\Lambda_{\mathfrak{p}}(K)^{\otimes 2}/p\Lambda_{\mathfrak{p}}(K)^{\otimes 2}\big)\otimes_{\mathcal{O}_{\mathfrak{p}}}\big(I_{\Gamma_S}^{2\rho_{\mathfrak{p}}}/I_{\Gamma_S}^{2\rho_{\mathfrak{p}}+1}\big).$$

(3) *If $|\rho_{\mathfrak{p}}^{+}-\rho_{\mathfrak{p}}^{-}|=1$ and p divides $|Ш_p(K,W_{\mathfrak{p}})|\cdot|J(S)|$, then $\tilde{\mathcal{L}}_{S,\mathfrak{p}}^{(p)}=0$.*

Proof. The term $\mathcal{L}_{S,\mathfrak{p}}$ is an $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$-linear combination of the elements $\zeta_{T,\mathfrak{p}}$ and $\zeta_{T,\mathfrak{p}}^{*}$ for $T\,|\,S$, and the result is obtained by applying Theorem 4.15 to each of them. □

Remark 4.17. In parallel with Remark 4.8, we observe that the results of Corollary 4.16 hold more generally for any $\mathcal{O}_{\mathfrak{p}}[\Gamma_S]$-linear combination of the elements $\zeta_{T,\mathfrak{p}}$ and $\zeta_{T,\mathfrak{p}}^{*}$ for $T\,|\,S$.

4.4. **Galois module structure of Heegner cycles.** Fix a prime number $\ell\in\mathcal{S}_p$. Define $\mathcal{H}(K_\ell)$ to be the $\mathcal{O}_{\mathfrak{p}}[G_\ell]$-module generated by $y_{\ell,\mathfrak{p}}$ inside $\Lambda_{\mathfrak{p}}(K_\ell)$ and denote by $\mathcal{H}_p(K_\ell)$ the $\mathbb{F}_{\mathfrak{p}}$-subspace $\mathcal{H}(K_\ell)/p\mathcal{H}(K_\ell)$ of $\Lambda_{\mathfrak{p}}(K_\ell)/p\,\Lambda_{\mathfrak{p}}(K_\ell)$. Finally, recall from §3.11 that $r_{\mathfrak{p}}=r_{\mathfrak{p},1}$.

Theorem 4.18. $\dim_{\mathbb{F}_{\mathfrak{p}}}\big(\mathcal{H}_p(K_\ell)\big)\le \ell+1-r_{\mathfrak{p}}$.

Proof. By §3.4.5, an $\mathcal{O}_{\mathfrak{p}}$-basis of $\mathcal{H}(K_\ell)$ is given by $\big\{\mathbf{D}_\ell^i(y_{\ell,\mathfrak{p}})\mid i=0,\dots,\ell\big\}$. Theorem 3.34 shows then that $\mathbf{D}_\ell^k(y_{\ell,\mathfrak{p}})\equiv 0\pmod{p}$ if $k<r_{\mathfrak{p}}$, and hence at most $\ell+1-r_{\mathfrak{p}}$ elements of the $\mathcal{O}_{\mathfrak{p}}$-basis of $\mathcal{H}(K_\ell)$ under consideration are non-zero. □

5. Regulators and leading coefficients

In this final section we propose a construction of regulators that are defined in terms of Nekovář's p-adic height pairings and generalize those introduced by Mazur and Tate in [36] and [37] and used in Darmon's work [18].

5.1. **Nekovář's regulator.** Let K be an imaginary quadratic field of discriminant coprime to Np and let $S>1$ be a square-free product of primes that are inert in K. Then define

$$\Lambda_{\mathfrak{p},S}(K):=\ker\left(\Lambda_{\mathfrak{p}}(K)\longrightarrow\bigoplus_{\lambda|S}H_f^1(K_\lambda,A_{\mathfrak{p}})\right)\tag{77}$$

where the map is induced by (14) via localizations. Finally, recall the maps $\mu_{S,T}$ introduced in §4.1, which are defined for integers $T\,|\,S$. We expect that Nekovář's theory of p-adic height pairings ([43, Ch. 11]; see also [40]) will yield a bilinear pairing

$$\langle\cdot,\cdot\rangle_S^{\mathrm{Nek}}:\Lambda_{\mathfrak{p}}(K)\times\Lambda_{\mathfrak{p},S}(K)\longrightarrow I_{\Gamma_S}/I_{\Gamma_S}^2\tag{78}$$

satisfying the compatibility condition

$$\mu_{S,T}\circ\langle\cdot,\cdot\rangle_S^{\mathrm{Nek}}=\langle\cdot,\cdot\rangle_T^{\mathrm{Nek}}\tag{79}$$

for all $T \mid S$ and the equivariance

$$\big\langle c(x), c(y)\big\rangle_S^{\mathrm{Nek}} = c \cdot \langle x, y\rangle_S^{\mathrm{Nek}} = -\langle x, y\rangle_S^{\mathrm{Nek}} \tag{80}$$

for all $x \in \Lambda_{\mathfrak{p}}(K)$, $y \in \Lambda_{\mathfrak{p},S}(K)$ under the action of $c \in \mathrm{Gal}(K/\mathbb{Q})$. Details on the explicit definition of pairing (78) will be provided in a future project; for now, we content ourselves with assuming its existence and the validity of properties (79) and (80).

As in [18], we use this pairing to construct a regulator term. Let ℓ be a prime divisor of S and, as before, let λ be the unique prime of K above ℓ; then write F_λ for the arithmetic Frobenius in $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{nr}}/K_\lambda)$. Recall from §2.4 that $V_{\mathfrak{p}} = A_{\mathfrak{p}} \otimes_{\mathcal{O}_{\mathfrak{p}}} F_{\mathfrak{p}}$. We have

$$\det(F_\ell \pm 1 \mid V_{\mathfrak{p}}) = \ell + 1 \mp \frac{a_\ell}{\ell^{\frac{k}{2}-1}},$$

which are non-zero thanks to the Weil bounds, hence

$$\begin{aligned}\det(F_\lambda - 1 \mid V_{\mathfrak{p}}) &= \det(F_\ell + 1 \mid V_{\mathfrak{p}}) \cdot \det(F_\ell - 1 \mid V_{\mathfrak{p}}) \\ &= (\ell+1)^2 - \frac{a_\ell^2}{\ell^{k-2}} \neq 0.\end{aligned}$$

Then [12, Theorem 4.1, (i)] implies that $H^1_f(K_\lambda, A_{\mathfrak{p}})$ is finite, so the codomain of the map in (77) is finite and the ranks of $\Lambda_{\mathfrak{p},S}(K)$ and $\Lambda_{\mathfrak{p}}(K)$ over $\mathcal{O}_{\mathfrak{p}}$ are equal. As in (21), this common rank will be denoted by $\tilde{\rho}_{\mathfrak{p}}$. Fix finite index subgroups $A \subset \Lambda_{\mathfrak{p}}(K)$ and $B \subset \Lambda_{\mathfrak{p},S}(K)$ that are $\mathcal{O}_{\mathfrak{p}}$-free and choose $\mathcal{O}_{\mathfrak{p}}$-bases $\{P_1, \dots, P_{\tilde{\rho}_{\mathfrak{p}}}\}$ and $\{Q_1, \dots, Q_{\tilde{\rho}_{\mathfrak{p}}}\}$ of A and B, respectively. Form the matrix

$$R(A,B) := \big(\langle P_i, Q_j\rangle_S^{\mathrm{Nek}}\big)_{i,j=1,\dots,\tilde{\rho}_{\mathfrak{p}}}$$

with entries in $I_{\Gamma_S}/I_{\Gamma_S}^2$ and let $R_{i,j}(A,B)$ be the (i,j)-minor of $R(A,B)$. Consider the element

$$\mathrm{Reg}(A,B) := \sum_{i,j=1}^{\tilde{\rho}_{\mathfrak{p}}} (-1)^{i+j} (P_i \otimes Q_j) \otimes \det\big(R_{i,j}(A,B)\big) \in \Lambda_{\mathfrak{p}}(K)^{\otimes 2} \otimes \big(I_{\Gamma_S}^{\tilde{\rho}_{\mathfrak{p}}-1}/I_{\Gamma_S}^{\tilde{\rho}_{\mathfrak{p}}}\big),$$

set $j := [\Lambda_{\mathfrak{p}}(K) : A] \cdot [\Lambda_{\mathfrak{p},S}(K) : B]$ and suppose that the multiplication-by-j map is invertible on $\Lambda_{\mathfrak{p}}(K)^{\otimes 2} \otimes \big(I_{\Gamma_S}^{\tilde{\rho}_{\mathfrak{p}}-1}/I_{\Gamma_S}^{\tilde{\rho}_{\mathfrak{p}}}\big)$. Then define the *Nekovář regulator* $\mathscr{R}^{\mathrm{Nek}}(S)$ as

$$\mathscr{R}^{\mathrm{Nek}}(S) := \mathrm{Reg}(A,B)/([\Lambda_{\mathfrak{p}}(K) : A] \cdot [\Lambda_{\mathfrak{p},S}(K) : B]).$$

This is independent of the choice of A and B. In fact, one can impose conditions on S that ensure the existence of suitable A and B as above for which j is invertible (see [18, p. 127], [37, p. 735]); for simplicity, here we shall just assume that this is the case.

5.2. **A refined conjecture for the leading coefficient.** Let $B(S)$ denote the cokernel of the map in (77) so that there is an exact sequence

$$0 \longrightarrow \Lambda_{\mathfrak{p},S}(K) \longrightarrow \Lambda_{\mathfrak{p}}(K) \longrightarrow \bigoplus_{\lambda \mid S} H^1_f(K_\lambda, A_{\mathfrak{p}}) \longrightarrow B(S) \longrightarrow 0.$$

The analogue of part 3 of [18, Conjecture 2.3] in the present context is

Conjecture 5.1 ("Refined formula for the leading coefficient")**.** *Assume that* $\text{Ш}_{p^\infty}(K, W_\mathfrak{p})$ *is finite. The equality*

$$\tilde{\mathcal{L}}_{S,\mathfrak{p}} = \left|\text{Ш}_{p^\infty}(K, W_\mathfrak{p})\right| \cdot |B(S)| \cdot \mathscr{R}^{\mathrm{Nek}}(S) \tag{81}$$

holds in $\Lambda(K_S)^{\otimes 2} \otimes \left(I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}-1}/I_{\Gamma_S}^{\tilde{\rho}_\mathfrak{p}}\right)$*. Here* $\mathscr{R}^{\mathrm{Nek}}(S)$ *denotes also the image of the regulator* $\mathscr{R}^{\mathrm{Nek}}(S)$ *via the map in* (67).

Remark 5.2. Since the definition of $\langle\cdot\,,\cdot\rangle_S^{\mathrm{Nek}}$ has not been given, the recipe of Conjecture 5.1 is still somewhat unsatisfactory. One may interpret it as predicting the existence of a suitable regulator $\mathscr{R}^{\mathrm{Nek}}(S)$ that can be explicitly described in terms of a height pairing *à la* Nekovář such that equality (81) holds.

Thanks to the compatibility condition (79), one can show that

$$\begin{aligned}\mu_{S,T}\big(|B(T)| \cdot \mathscr{R}^{\mathrm{Nek}}(T)\big) = {} & |B(S)| \cdot \mathscr{R}^{\mathrm{Nek}}(S) \\ & \times \prod_{\ell \mid (S/T)} \left(1 + \ell - a_\ell/\ell^{k/2-1}\right) \cdot \left(1 + \ell + a_\ell/\ell^{k/2-1}\right)\end{aligned}$$

whenever $T \mid S$. Comparing with (63), one sees that Conjectures 4.3, 4.10 and 5.1 are all compatible with the map $\mu_{S,T}$ when $T \mid S$. Actually, as in [18], it is this compatibility relation that suggests the definition of $\mathcal{L}_{S,\mathfrak{p}}$ given above. However, different regulators might be attached to different choices of the coefficients b_T and b'_T, as discussed in Remark 4.1. The choice of *correct* regulators and $\mathcal{L}$-elements is an open problem, although we believe that, in light of (63) and the properties of Nekovář's regulator, our definition of $\mathcal{L}_{S,\mathfrak{p}}$ is in some sense the "standard" one.

Let us finally observe that, by Lemma 3.5, if $|\rho_\mathfrak{p}^+ - \rho_\mathfrak{p}^-| > 1$, then $2\rho_\mathfrak{p} \geq \tilde{\rho}_\mathfrak{p}$; hence the leading coefficient $\tilde{\mathcal{L}}_{S,\mathfrak{p}}$, as defined in §4.3, vanishes. In order to obtain something non-trivial, in this situation the leading coefficient $\tilde{\mathcal{L}}_{S,\mathfrak{p}}$ should be defined instead as the image of $\mathcal{L}_{S,\mathfrak{p}}$ in the quotient $\Lambda(K_S)^{\otimes 2} \otimes \left(I_{\Gamma_S}^{2\rho_\mathfrak{p}}/I_{\Gamma_S}^{2\rho_\mathfrak{p}+1}\right)$. Unfortunately, when $|\rho_\mathfrak{p}^+ - \rho_\mathfrak{p}^-| > 1$ we cannot offer any prediction about the exact value of $\tilde{\mathcal{L}}_{S,\mathfrak{p}}$, but we expect that the study of $\tilde{\mathcal{L}}_{S,\mathfrak{p}}$ might be approached, at least in some special cases, via a suitable theory of generalized Mazur–Tate regulators as developed in [2] and [3].

Acknowledgements

It is a pleasure to thank Jan Nekovář for enlightening conversations on some of the topics of this paper. The authors would also like to thank Masataka Chida for helpful comments on Abel–Jacobi maps and Kazuto Ota for pointing out a flaw in the proof of a previous version of Proposition 3.31 and for suggesting how to fix it. Finally, the authors would like to thank the anonymous referee for carefully reading the paper and for useful remarks.

References

[1] A. A. Beĭlinson, *Higher regulators and values of L-functions* (Russian), Current problems in mathematics, Vol. 24, Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1984, pp. 181–238. MR760999

[2] Massimo Bertolini and Henri Darmon, *Derived heights and generalized Mazur-Tate regulators*, Duke Math. J. **76** (1994), no. 1, 75–111, DOI 10.1215/S0012-7094-94-07604-7. MR1301187

[3] Massimo Bertolini and Henri Darmon, *Derived p-adic heights*, Amer. J. Math. **117** (1995), no. 6, 1517–1554, DOI 10.2307/2375029. MR1363078

[4] M. Bertolini and H. Darmon, *Heegner points on Mumford-Tate curves*, Invent. Math. **126** (1996), no. 3, 413–456, DOI 10.1007/s002220050105. MR1419003

[5] Massimo Bertolini and Henri Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization*, Invent. Math. **131** (1998), no. 3, 453–491, DOI 10.1007/s002220050211. MR1614543

[6] Massimo Bertolini and Henri Darmon, *p-adic periods, p-adic L-functions, and the p-adic uniformization of Shimura curves*, Duke Math. J. **98** (1999), no. 2, 305–334, DOI 10.1215/S0012-7094-99-09809-5. MR1695201

[7] Massimo Bertolini and Henri Darmon, *The p-adic L-functions of modular elliptic curves*, Mathematics unlimited—2001 and beyond, Springer, Berlin, 2001, pp. 109–170. MR1852156

[8] M. Bertolini and H. Darmon, *Iwasawa's main conjecture for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*, Ann. of Math. (2) **162** (2005), no. 1, 1–64, DOI 10.4007/annals.2005.162.1. MR2178960

[9] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *Generalized Heegner cycles and p-adic Rankin L-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148, DOI 10.1215/00127094-2142056. With an appendix by Brian Conrad. MR3053566

[10] Amnon Besser, *On the finiteness of* Ш *for motives associated to modular forms*, Doc. Math. **2** (1997), 31–46 (electronic). MR1443065

[11] Spencer Bloch, *Algebraic cycles and values of L-functions*, J. Reine Angew. Math. **350** (1984), 94–108, DOI 10.1515/crll.1984.350.94. MR743535

[12] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400. MR1086888

[13] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), no. 3, 543–618, DOI 10.1007/BF01233440. MR1074487

[14] David Burns, *Congruences between derivatives of abelian L-functions at $s = 0$*, Invent. Math. **169** (2007), no. 3, 451–499, DOI 10.1007/s00222-007-0052-3. MR2336038

[15] D. Burns and M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001), 501–570 (electronic). MR1884523

[16] Francesc Castella, *Heegner cycles and higher weight specializations of big Heegner points*, Math. Ann. **356** (2013), no. 4, 1247–1282, DOI 10.1007/s00208-012-0871-4. MR3072800

[17] Masataka Chida and Ming-Lun Hsieh, *On the anticyclotomic Iwasawa main conjecture for modular forms*, Compos. Math. **151** (2015), no. 5, 863–897, DOI 10.1112/S0010437X14007787. MR3347993

[18] Henri Darmon, *A refined conjecture of Mazur-Tate type for Heegner points*, Invent. Math. **110** (1992), no. 1, 123–146, DOI 10.1007/BF01231327. MR1181819

[19] Henri Darmon, *Thaine's method for circular units and a conjecture of Gross*, Canad. J. Math. **47** (1995), no. 2, 302–317, DOI 10.4153/CJM-1995-016-6. MR1335080

[20] Pierre Deligne, *Formes modulaires et représentations l-adiques* (French), Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Math., vol. 175, Springer, Berlin, 1971, Exp. No. 355, pp. 139–172. MR3077124

[21] Fred Diamond, Matthias Flach, and Li Guo, *The Tamagawa number conjecture of adjoint motives of modular forms* (English, with English and French summaries), Ann. Sci. École Norm. Sup. (4) **37** (2004), no. 5, 663–727, DOI 10.1016/j.ansens.2004.09.001. MR2103471

[22] Olivier Fouquet, *Dihedral Iwasawa theory of nearly ordinary quaternionic automorphic forms*, Compos. Math. **149** (2013), no. 3, 356–416, DOI 10.1112/S0010437X12000619. MR3040744

[23] Benedict H. Gross, *On the values of abelian L-functions at $s = 0$*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **35** (1988), no. 1, 177–197. MR931448

[24] Benjamin Howard, *Variation of Heegner points in Hida families*, Invent. Math. **167** (2007), no. 1, 91–128, DOI 10.1007/s00222-006-0007-0. MR2264805

[25] Uwe Jannsen, *Mixed motives and algebraic K-theory*, Lecture Notes in Mathematics, vol. 1400, Springer-Verlag, Berlin, 1990. MR1043451

[26] Matteo Longo, *On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves over totally real fields* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **56** (2006), no. 3, 689–733. MR2244227

[27] Matteo Longo, *Euler systems obtained from congruences between Hilbert modular forms*, Rend. Semin. Mat. Univ. Padova **118** (2007), 1–34. MR2378387

[28] Matteo Longo, *Anticyclotomic Iwasawa's main conjecture for Hilbert modular forms*, Comment. Math. Helv. **87** (2012), no. 2, 303–353, DOI 10.4171/CMH/255. MR2914851

[29] Matteo Longo, Victor Rotger, and Stefano Vigni, *Special values of L-functions and the arithmetic of Darmon points*, J. Reine Angew. Math. **684** (2013), 199–244. MR3181561

[30] Matteo Longo and Stefano Vigni, *On the vanishing of Selmer groups for elliptic curves over ring class fields*, J. Number Theory **130** (2010), no. 1, 128–163, DOI 10.1016/j.jnt.2009.07.004. MR2569846

[31] Matteo Longo and Stefano Vigni, *An irreducibility criterion for group representations, with arithmetic applications*, Proc. Amer. Math. Soc. **138** (2010), no. 10, 3437–3447, DOI 10.1090/S0002-9939-2010-10485-9. MR2661544

[32] Matteo Longo and Stefano Vigni, *Quaternion algebras, Heegner points and the arithmetic of Hida families*, Manuscripta Math. **135** (2011), no. 3-4, 273–328, DOI 10.1007/s00229-010-0409-6. MR2813438

[33] Matteo Longo and Stefano Vigni, *Vanishing of special values and central derivatives in Hida families*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **13** (2014), no. 3, 859–888. MR3331531

[34] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96, DOI 10.1090/memo/0799. MR2031496

[35] Barry Mazur and Karl Rubin, *Refined class number formulas and Kolyvagin systems*, Compos. Math. **147** (2011), no. 1, 56–74, DOI 10.1112/S0010437X1000494X. MR2771126

[36] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237. MR717595

[37] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. **54** (1987), no. 2, 711–750, DOI 10.1215/S0012-7094-87-05431-7. MR899413

[38] J. S. Milne, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press, Inc., Boston, MA, 1986. MR881804

[39] Jan Nekovář, *Kolyvagin's method for Chow groups of Kuga-Sato varieties*, Invent. Math. **107** (1992), no. 1, 99–125, DOI 10.1007/BF01231883. MR1135466

[40] Jan Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202, DOI 10.1007/s10107-005-0696-y. MR1263527

[41] Jan Nekovář, *On the p-adic height of Heegner cycles*, Math. Ann. **302** (1995), no. 4, 609–686, DOI 10.1007/BF01444511. MR1343644

[42] Jan Nekovář, *p-adic Abel-Jacobi maps and p-adic heights*, The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), CRM Proc. Lecture Notes, vol. 24, Amer. Math. Soc., Providence, RI, 2000, pp. 367–379. MR1738867

[43] Jan Nekovář, *Selmer complexes* (English, with English and French summaries), Astérisque **310** (2006), viii+559. MR2333680

[44] Jan Nekovář, *The Euler system method for CM points on Shimura curves*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 471–547, DOI 10.1017/CBO9780511721267.014. MR2392363

[45] Jan Nekovář, *Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two*, Canad. J. Math. **64** (2012), no. 3, 588–668, DOI 10.4153/CJM-2011-077-6. MR2962318

[46] Wieslawa Niziol, *On the image of p-adic regulators*, Invent. Math. **127** (1997), no. 2, 375–400, DOI 10.1007/s002220050125. MR1427624

[47] K. Ota, *Kato's Euler system and the Mazur–Tate refined conjecture of BSD type*, to appear in Amer. J. Math., arXiv:1509.00682.

[48] Kenneth A. Ribet, *On l-adic representations attached to modular forms. II*, Glasgow Math. J. **27** (1985), 185–194, DOI 10.1017/S0017089500006170. MR819838

[49] Karl Rubin, *A Stark conjecture "over $\mathbf{Z}$" for abelian L-functions with multiple zeros* (English, with English and French summaries), Ann. Inst. Fourier (Grenoble) **46** (1996), no. 1, 33–62. MR1385509

[50] Takeshi Saito, *Modular forms and p-adic Hodge theory*, Invent. Math. **129** (1997), no. 3, 607–620, DOI 10.1007/s002220050175. MR1465337

[51] Takeshi Saito, *Weight-monodromy conjecture for l-adic representations associated to modular forms. A supplement to: "Modular forms and p-adic Hodge theory" [Invent. Math.* **129** *(1997), no. 3, 607–620; MR1465337 (98g:11060)]*, The arithmetic and geometry of algebraic cycles (Banff, AB, 1998), NATO Sci. Ser. C Math. Phys. Sci., vol. 548, Kluwer Acad. Publ., Dordrecht, 2000, pp. 427–431. MR1744955

[52] Peter Schneider, *Introduction to the Beĭlinson conjectures*, Beĭlinson's conjectures on special values of L-functions, Perspect. Math., vol. 4, Academic Press, Boston, MA, 1988, pp. 1–35. MR944989

[53] A. J. Scholl, *Motives for modular forms*, Invent. Math. **100** (1990), no. 2, 419–430, DOI 10.1007/BF01231194. MR1047142

[54] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg. MR554237

[55] Shouwu Zhang, *Heights of Heegner cycles and derivatives of L-series*, Invent. Math. **130** (1997), no. 1, 99–152, DOI 10.1007/s002220050179. MR1471887

[56] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253, DOI 10.4310/CJM.2014.v2.n2.a2. MR3295917

Dipartimento di Matematica, Università di Padova, Via Trieste 63, 35121 Padova, Italy

E-mail address: `mlongo@math.unipd.it`

Dipartimento di Matematica, Università di Genova, Via Dodecaneso 35, 16146 Genova, Italy

E-mail address: `vigni@dima.unige.it`