SPECIAL VALUES OF L-FUNCTIONS AND THE ARITHMETIC OF DARMON POINTS

MATTEO LONGO, VICTOR ROTGER AND STEFANO VIGNI

Abstract. Building on our previous work on rigid analytic uniformizations, we introduce Darmon points on Jacobians of Shimura curves attached to quaternion algebras over $\mathbb{Q}$ and formulate conjectures about their rationality properties. Moreover, if K is a real quadratic field, E is an elliptic curve over $\mathbb{Q}$ without complex multiplication and χ is a ring class character such that $L_K(E,\chi,1)\neq 0$ we prove a Gross–Zagier type formula relating Darmon points to a suitably defined algebraic part of $L_K(E,\chi,1)$; this generalizes results of Bertolini, Darmon and Dasgupta to the case of division quaternion algebras and arbitrary characters. Finally, as an application of this formula, assuming the rationality conjectures for Darmon points we obtain vanishing results for Selmer groups of E over extensions of K contained in narrow ring class fields when the analytic rank of E is zero, as predicted by the Birch and Swinnerton-Dyer conjecture.

1. Introduction

The purpose of this article is threefold. Firstly, following [10], [12] and [15] and building on our previous work [22] on rigid analytic uniformizations, we introduce a special supply of points on Jacobians of Shimura curves which we call *Darmon points*, after the foundational work [10] of Henri Darmon in his investigation of counterparts in the real setting of the theory of complex multiplication. To be in line with the current language, our points could also be called "Stark–Heegner points" (as in *loc. cit.*), but we feel that the new terminology we adopt here is more representative of the genesis of our constructions. Secondly, we prove an avatar of the Gross–Zagier formula relating Darmon points to the special values of twists by ring class characters of base changes to real quadratic fields K of L-functions of elliptic curves E over $\mathbb{Q}$, provided the analytic rank of E over K is 0. Finally, under this analytic condition we use this formula to prove vanishing results for (twisted) Selmer groups of elliptic curves over narrow ring class fields of real quadratic fields. Let us describe first the motivation and background and then our results more in detail.

Let $A_{/\mathbb{Q}}$ be an elliptic curve of conductor N_A and let K be a real quadratic field of discriminant δ_K with $(N_A,\delta_K)=1$. Assume that there exists a prime ℓ which is inert in K and divides N_A exactly. If one further assumes the *Heegner condition* that all primes dividing N_A/ℓ be split in K then the sign of the functional equation of the L-function $L_K(A,s)$ of A over K is -1 and the Birch and Swinnerton-Dyer conjecture predicts that the rank of the Mordell–Weil group $A(H)$ is at least $[H:K]$ for all (narrow) ring class fields H of K.

Under these conditions, in [10] Darmon introduced a family of *local* points on A over the unramified quadratic extension of $\mathbb{Q}_\ell$ and conjectured that they are in fact *global*. More precisely, he predicted that his points are rational over narrow ring class fields of K and satisfy properties which are analogous to those enjoyed by classical Heegner points over abelian extensions of imaginary quadratic fields (see [4] for results in this direction); these points should account for the expectations of high rank described above. Darmon's points were later lifted from elliptic curves to certain quotients of classical modular Jacobians by Dasgupta in

2000 *Mathematics Subject Classification.* 14G35, 11G40.

Key words and phrases. Darmon points, special values of L-series, Selmer groups.

The research of the second author is financially supported by DGICYT Grant MTM2009-13060-C02-01.

[12]; this was achieved by proving a rigid analytic uniformization result for modular Jacobians which can be phrased as an equality of $\mathcal{L}$-invariants and turns out to be a strong form of a theorem of Greenberg and Stevens ([16]). Both Darmon's and Dasgupta's constructions, relying heavily on the theory of modular symbols, do not lend themselves to straightforward extensions to more general settings in which the sign of the functional equation of $L_K(A,s)$ is still -1 (so that a similar family of points should exist) but the Heegner condition is not verified (cf. [11, Conjecture 3.16] or below for details). To circumvent this problem, in [15] M. Greenberg reinterpreted Darmon's theory in terms of group cohomology; this allowed him to conjecturally define local points on A, generalizing Darmon's original constructions to much broader arithmetic contexts. It must be noted that Greenberg's definitions are conditional on the validity of an unproved statement ([15, Conjecture 2]); this conjecture (over $\mathbb{Q}$) has been proved by the authors of the present paper in [22] and, independently, by Dasgupta and Greenberg in [13]. The two proofs use different methods and, as a by-product, lead to different arithmetic applications: while the present paper is a sequel of [22] and the results obtained here could probably not be tackled by means of [13], the latter can be exploited to show the rationality of Darmon points in some cases, in the spirit of [4] (see forthcoming work of Greenberg and Shahabi).

The main result of [22], of which Greenberg's conjecture is a corollary, provides an explicit rigid analytic uniformization of the maximal toric quotient of the Jacobian of a Shimura curve attached to a division quaternion algebra over $\mathbb{Q}$ at a prime dividing exactly the level, and can be viewed as complementary to the classical theorem of Čerednik and Drinfeld that gives rigid uniformizations at primes dividing the discriminant. Moreover, it extends to arbitrary quaternion algebras the results of Dasgupta for classical modular curves.

In order to describe the content of this article we need to introduce some notation, which will be used throughout our work. As above, let K be a real quadratic field of discriminant δ_K, which we embed into the real numbers by using one of its two archimedean places ∞_1, ∞_2, and let ℓ be a prime number that remains inert in K. Let $\mathcal{O}_K$ be the ring of integers of K and for every integer $c \geq 1$ let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order of K of conductor c. Setting $\widehat{\mathcal{O}}_c := \mathcal{O}_c \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ (with $\widehat{\mathbb{Z}}$ being the profinite completion of $\mathbb{Z}$), let

$$\mathrm{Pic}^+(\mathcal{O}_c) = \widehat{\mathcal{O}}_c^\times K_{\infty,+}^\times \backslash \mathbb{A}_K^\times / K^\times$$

be the narrow (or strict) class group of $\mathcal{O}_c$, where $\mathbb{A}_K$ is the ring of adeles of K and $K_{\infty,+}^\times$ is the connected component of the identity in $K_{\infty_1}^\times \times K_{\infty_2}^\times$. By class field theory, $\mathrm{Pic}^+(\mathcal{O}_c)$ is canonically isomorphic to the Galois group $G_c := \mathrm{Gal}\,(H_c/K)$ where H_c is the narrow ring class field of K of conductor c.

Let $D \geq 1$ be the square-free product of an even number of primes and $M \geq 1$ be a positive integer prime to D such that $\ell \nmid DM$. Let $X_0^D(M)$ and $X_0^D(M\ell)$ denote the Shimura curves attached to the indefinite quaternion algebra B of reduced discriminant D and choices of Eichler orders $R' \subset R$ of levels $M\ell$ and M, respectively (cf. [31], [10, Ch. IV]).

In the first part of this paper we introduce local Darmon points on the ℓ-new quotient $J_0^D(M\ell)^{\ell\text{-new}}$ of the Jacobian of $X_0^D(M\ell)$; if $A_{/\mathbb{Q}}$ is an elliptic curve of conductor $DM\ell$ then we know by modularity and by the Jacquet–Langlands correspondence that A is a quotient of $J_0^D(M\ell)^{\ell\text{-new}}$ and our points lift from A those defined by Greenberg. Following [10], [12] and [15], we formulate global rationality and reciprocity conjectures for them. All definitions and conjectures, together with a quick review of the main results of [22], can be found in Section 3 (see, in particular, §3.2). A crucial role in the definition of Darmon points is played by the group

$$\Gamma_\ell := \big(R \otimes \mathbb{Z}[1/\ell]\big)_1^\times$$

of elements of reduced norm 1 of $R \otimes \mathbb{Z}[1/\ell]$, which can be embedded in $\mathrm{SL}_2(\mathbb{Q}_\ell)$ and we call the *Ihara group* at ℓ (see §2.1). The abelianization $\Gamma_\ell^{\mathrm{ab}}$ of Γ_ℓ is well known to be finite,

and to the study of its support we devote Section 2. In the absence of the counterparts for Shimura curves associated with division quaternion algebras of the results proved by Ribet in [29] (this being due to the lack of a full analogue for general Shimura curves of the so-called Ihara's Lemma for modular curves), we invoke a theorem of Diamond and Taylor ([14]) on the Eisenstein-ness of certain maximal ideals of Hecke algebras to get a bound on the support of $\Gamma_\ell^{\mathrm{ab}}$ which is fine enough for our arithmetic purposes. The reader can find all details in §2.3 (see, in particular, Theorem 2.2), which may be of independent interest.

Let us now describe the main results of this article. Let $E_{/\mathbb{Q}}$ be an elliptic curve without complex multiplication of conductor $N = N_E$ prime to δ_K and denote by $f_0(q) = \sum_{n=1}^{\infty} a_n q^n$ the normalized newform of weight 2 on $\Gamma_0(N)$ associated with E by the Shimura–Taniyama correspondence. Let $L_K(E,s) = L_K(f_0,s)$ be the complex L-function of E over K and assume that

- the sign of the functional equation of $L_K(E,s)$ is $+1$.

This implies that $L_K(E,s)$ vanishes to even order (and is expected to be frequently non-zero) at the critical point $s=1$. This is equivalent to saying that the set of primes

$$\Sigma := \big\{q|N:\ \mathrm{ord}_q(N) \text{ is odd and } q \text{ is inert in } K\big\}$$

has *even* cardinality (and is possibly empty). We shall further assume that $\mathrm{ord}_q(N) = 1$ for all $q \in \Sigma$. Let D be the product of the primes in Σ (with $D := 1$ if $\Sigma = \emptyset$), then set $M := N/D$.

Write $\widehat{G}_c$ for the group of complex-valued characters of G_c, fix $\chi \in \widehat{G}_c$ and let $L_K(E,\chi,s)$ be the twist of $L_K(E,s)$ by χ. For the remainder of this article choose c prime to $\delta_K N$. By [11, Theorem 3.15], it follows from our running assumptions that the sign of the functional equation for $L_K(E,\chi,s)$ is $+1$ as well.

Write $\mathbb{Z}[\chi]$ for the cyclotomic subring of $\mathbb{C}$ generated over $\mathbb{Z}$ by the values of χ. In Section 4 we introduce the algebraic part $\mathcal{L}_K(E,\chi,1) \in \mathbb{Z}[\chi]_S$ of the special value $L_K(E,\chi,1)$, where S is a certain auxiliary finite set of prime numbers. Such an algebraic part is defined in terms of a twisted sum of homology cycles associated with conjugacy classes of oriented optimal embeddings of $\mathcal{O}_c$ into a fixed Eichler order of B of level M. Thanks to previous work of Popa ([27]), it can be shown that $L_K(E,\chi,1) \neq 0$ if and only if $\mathcal{L}_K(E,\chi,1) \neq 0$ (cf. Theorem 4.8).

From now on assume that $L_K(E,\chi,1) \neq 0$. Suppose that p is a prime number fulfilling the conditions listed in Assumption 5.1, which exclude only finitely many primes. In particular, p is a prime of good reduction for E such that $\mathcal{L}_K(E,\chi,1)$ is not zero modulo p. Corresponding to any such p, in §5.2 we introduce the notion of p-admissible primes (usually simply called "admissible"), which are certain primes not dividing Np and inert in K. For a sign $\epsilon \in \{\pm\}$ and a suitable p-admissible prime ℓ we introduce a map

$$\partial_\ell : J_\epsilon^{(\ell)}(K_\ell) \otimes \mathbb{Z}[\chi]_S \longrightarrow \mathbb{Z}[\chi]/p\mathbb{Z}[\chi]_S$$

(denoted by $\partial'_\ell \otimes \mathrm{id}$ in §7.2) and a twisted sum of Darmon points $P_\chi^\epsilon \in J_\epsilon^{(\ell)}(K_\ell) \otimes \mathbb{Z}[\chi]_S$. Here $J_\epsilon^{(\ell)}$ is an abelian variety over $\mathbb{Q}$ whose existence is a conjectural consequence of our work in [22] and which is predicted to be isogenous to $J_0^D(M\ell)^{\ell\text{-new}}$ (see §3.1 and §3.2 for details). If $D = 1$ (i.e., $B \simeq \mathrm{M}_2(\mathbb{Q})$) then our Darmon points need to be replaced by the points on modular Jacobians defined by Dasgupta in [12, §3.3] (see also [5, §1.2]).

Letting $[\star]$ denote the class of the element $\star$ in a quotient group and writing t_ℓ for the exponent of $\Gamma_\ell^{\mathrm{ab}}$, our Gross–Zagier type formula for the special value of $L_K(E,\chi,s)$ can then be stated as follows.

Theorem 1.1. *The equality* $\partial_\ell(P_\chi^\epsilon) = t_\ell \cdot [\mathcal{L}_K(E,\chi,1)]$ *holds in* $\mathbb{Z}[\chi]_S/p\mathbb{Z}[\chi]_S$.

This result extends the main theorem of [5], where a similar formula was proved for $D = 1$ and χ trivial. The extension of [5, Theorem 3.9] to the case of $D = 1$ and arbitrary characters is relatively straightforward, the only ingredient that needs to be added being a version of

Popa's classical formula in the twisted setting. However, note that the methods of [5] are heavily based on modular symbol constructions, while our proof for arbitrary $D > 1$ relies on the techniques introduced in [22]. A proof of Theorem 1.1, which can also be viewed as a "reciprocity law" in the sense of [3], is given in Theorem 7.4. As in [5], a key ingredient is a level raising result (Theorem 6.3) at the admissible prime ℓ; more precisely, since ℓ is inert in K, the construction of Darmon points is available "at level $M\ell$", and the proof of the above theorem boils down to suitably relating Darmon points on $J_\epsilon^{(\ell)}$ to the class modulo p of the algebraic part $\mathcal{L}_K(E,\chi,1)$. We devote Sections 6 and 7 to a careful analysis of these issues.

What makes the formula of Theorem 1.1 interesting, and especially useful for the arithmetic applications we are going to describe, is the fact that p does not divide the integer t_ℓ. The possibility of requiring such a non-divisibility for a p-admissible prime ℓ is non-trivial and rests on the results on the support of $\Gamma_\ell^{\mathrm{ab}}$ that, as already mentioned, we obtain in Section 2.

We conclude this introduction by stating the main arithmetic consequences of Theorem 1.1. Let K' be an extension of K contained in H_c for some $c \geq 1$ as before and let $L_{K'}(E,s)$ be the L-function of E over K'. For any prime number p let $\mathrm{Sel}_p(E/K')$ be the p-Selmer group of E over K'. While Theorem 1.1 is of a genuinely local nature (that is, to obtain it we do not need to use any conjectural global property of Darmon points), to prove the following vanishing result (Theorem 8.15) we have to assume the validity of Conjecture 3.6, which predicts that the Darmon points are rational over suitable (narrow) ring class fields of K.

Theorem 1.2. *Assume Conjecture 3.6. If $L_{K'}(E,1) \neq 0$ then*

$$\mathrm{Sel}_p(E/K') = 0$$

for all but finitely many primes p. In particular, $E(K')$ is finite.

Theorem 1.2 is a consequence of a vanishing result for p-Selmer groups of E twisted by anticyclotomic characters (Theorem 8.11), and the set of primes for which it is valid contains those satisfying Assumption 5.1. Observe that this result, which is predicted by the conjecture of Birch and Swinnerton-Dyer, is (a strengthening of) the counterpart in the real quadratic setting of the main result of [23], which was obtained (unconditionally) in the more classical context of imaginary quadratic fields and Heegner points. When $D = 1$ the above theorem represents an explicit instance of the "potential arithmetic applications" of Theorem 1.1 which are alluded to by Bertolini, Darmon and Dasgupta in the introduction to [5]. We refer the reader to §8.6 for other arithmetic consequences of Theorem 1.1 (e.g., twisted versions of the Birch and Swinnerton-Dyer conjecture for E over K' in analytic rank 0).

Notation and conventions. Throughout our work we fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and view all number fields as subfields of $\bar{\mathbb{Q}}$. If F is a number field we write $\mathcal{O}_F$ and G_F for the ring of integers and the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/F)$ of F, respectively, and denote by F_v the completion of F at a place v.

For all prime numbers ℓ we fix an algebraic closure $\bar{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ and an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$. Moreover, $\mathbb{C}_\ell$ denotes the completion of $\bar{\mathbb{Q}}_\ell$.

If ℓ is a prime then $\mathbb{F}_\ell$ is the finite field with ℓ elements. We sometimes write $\mathbb{F}_p$ in place of $\mathbb{Z}/p\mathbb{Z}$ when we want to emphasize the field structure of $\mathbb{Z}/p\mathbb{Z}$.

If G is a profinite group and M is a continuous G-module we let $H^1(G,M)$ be the first group of continuous cohomology of G with coefficients in M. In particular, if G is the absolute Galois group of a (local or global) field F then we denote $H^1(G,M)$ also by $H^1(F,M)$.

Let F be a number field, p a prime number and $A_{/F}$ an abelian variety. We write $A[p^n]$ for the p^n-torsion subgroup of $A(\bar{\mathbb{Q}})$. As customary, we let $\mathrm{Sel}_{p^n}(A/F)$ be the p^n-Selmer group of A over F, i.e. the subgroup of $H^1(F,A[p^n])$ consisting of those classes which locally at every place of F belong to the image of the local Kummer map. If A has good reduction at a prime

ideal $\mathfrak{q} \subset \mathcal{O}_F$ such that $\mathfrak{q} \nmid p$ we let $H^1_{\mathrm{sing}}(F_\mathfrak{q}, A[p])$ and $H^1_{\mathrm{fin}}(F_\mathfrak{q}, A[p])$ denote the singular and finite parts of $H^1(F_\mathfrak{q}, A[p])$ as defined in [23, §3].

Finally, for any ring R and any pair of maps $f : M \to N$, $g : P \to Q$ of R-modules we write $f \otimes g : M \otimes_R P \to N \otimes_R Q$ for the R-linear map obtained by extending additively the rule $m \otimes p \mapsto f(m) \otimes g(p)$.

Acknowledgements. It is a pleasure to thank Kevin Buzzard, Henri Darmon, Benedict Gross, Yasutaka Ihara and Alexei Skorobogatov for enlightening discussions and correspondence which helped improve some of the results of this article. Heartfelt gratitude goes to Frank Sullivan for his invaluable help which allowed the first named author to spend March 2010 in Barcelona, at a delicate stage of this project. The three authors also thank the Centre de Recerca Matemàtica (Bellaterra, Spain) for its warm hospitality in Winter 2010, when part of this research was carried out.

2. On Ihara's group

2.1. **Basic definitions.** As in the introduction, let $D \geq 1$ be a square-free product of an *even* number of primes and let $M \geq 1$ be an integer coprime with D. Let B be the (unique, up to isomorphism) indefinite quaternion algebra over $\mathbb{Q}$ of discriminant D. Let $R = R(M)$ be a fixed Eichler order of level M in B and write $\Gamma_0^D(M)$ for the group of norm 1 elements in R. If $\ell \nmid DM$ is a prime number then let $R' = R(M\ell) \subset R$ be an Eichler order of level $M\ell$ contained in R and let $\Gamma_0^D(M\ell)$ be the group of norm 1 elements in R'.

Fix an isomorphism of $\mathbb{Q}_\ell$-algebras

$$\iota_\ell : B \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{Q}_\ell)$$

such that $\iota_\ell(R \otimes \mathbb{Z}_\ell)$ is equal to $\mathrm{M}_2(\mathbb{Z}_\ell)$ and $\iota_\ell(R' \otimes \mathbb{Z}_\ell)$ is equal to the subgroup of $\mathrm{M}_2(\mathbb{Z}_\ell)$ consisting of upper triangular matrices modulo ℓ. Letting the subscript "1" denote elements of norm 1, we define the Ihara group at ℓ to be the subgroup of $\mathrm{SL}_2(\mathbb{Q}_\ell)$ given by

$$\Gamma_\ell := \big(R \otimes \mathbb{Z}[1/\ell]\big)^\times_1 \xhookrightarrow{\iota_\ell} \mathrm{SL}_2(\mathbb{Q}_\ell).$$

It acts on Drinfeld's ℓ-adic half-plane $\mathcal{H}_\ell := \mathbb{C}_\ell - \mathbb{Q}_\ell$ with dense orbits. The study of Γ_ℓ (or, rather, of its abelianization) when ℓ varies over the set of primes not dividing MD will be the goal of the next two subsections.

2.2. **Finiteness of $\Gamma_\ell^{\mathrm{ab}}$.** We begin our discussion with a direct proof of the finiteness of the abelianization $\Gamma_\ell^{\mathrm{ab}}$ of Γ_ℓ for all $\ell \nmid MD$, which is a well-known fact (cf., e.g., [19]). The reader is referred to [25, Ch. VIII and IX] (in particular, to [25, Proposition 5.3, p. 324]) for general results of this type.

Before proving the proposition we are interested in, let us introduce some notation. Let

$$\pi_1, \pi_2 : X_0^D(M\ell) \longrightarrow X_0^D(M), \qquad \Gamma_0^D(M\ell)z \xmapsto{\pi_1} \Gamma_0^D(M)z, \qquad \Gamma_0^D(M\ell)z \xmapsto{\pi_2} \Gamma_0^D(M)\omega_\ell z$$

be the two natural degeneracy maps. Here ω_ℓ is an element in $R(M\ell)$ of reduced norm ℓ that normalizes $\Gamma_0^D(M\ell)$. As a piece of notation, for any element γ in (respectively, subgroup G of) $\Gamma_0^D(M\ell)$ we shall write $\hat{\gamma} := \omega_\ell \gamma \omega_\ell^{-1}$ (respectively, $\hat{G} := \omega_\ell G \omega_\ell^{-1}$). Moreover, let

$$\pi^* := \pi_1^* \oplus \pi_2^* : H_1\big(X_0^D(M), \mathbb{Z}\big)^2 \longrightarrow H_1\big(X_0^D(M\ell), \mathbb{Z}\big)$$

and

$$\pi_* := (\pi_{1,*}, \pi_{2,*}) : H_1\big(X_0^D(M\ell), \mathbb{Z}\big) \longrightarrow H_1\big(X_0^D(M), \mathbb{Z}\big)^2$$

be the maps induced in homology by pull-back and push-forward, respectively. In terms of group homology, they correspond to the maps

$$\pi_* := (\pi_{1,*}, \pi_{2,*}) : H_1\big(\Gamma_0^D(M\ell), \mathbb{Z}\big) \longrightarrow H_1\big(\Gamma_0^D(M), \mathbb{Z}\big)^2$$

induced by corestriction and restriction, respectively.

Proposition 2.1. *The group $\Gamma_\ell^{\mathrm{ab}}$ is finite for all primes $\ell \nmid MD$.*

Proof. As shown in [22, equation (30)], there is a long exact sequence in homology

$$H_1\big(\Gamma_0^D(M\ell),\mathbb{Z}\big) \xrightarrow{\pi_*} H_1\big(\Gamma_0^D(M),\mathbb{Z}\big)^2 \longrightarrow H_1(\Gamma_\ell,\mathbb{Z}) \longrightarrow H_0\big(\Gamma_0^D(M\ell),\mathbb{Z}\big) \longrightarrow H_0\big(\Gamma_0^D(M),\mathbb{Z}\big)^2. \tag{1}$$

Since the actions on $\mathbb{Z}$ are trivial, the last homomorphism can be naturally identified with the diagonal embedding of $\mathbb{Z}$ into $\mathbb{Z}^2$, which is obviously injective. Thus the exactness of (1) implies that $\mathrm{coker}(\pi_*) \simeq H_1(\Gamma_\ell,\mathbb{Z})$, which in turn is isomorphic to $\Gamma_\ell^{\mathrm{ab}}$. But in the proof of [22, Lemma 6.2] it is shown that the endomorphism $\pi_* \circ \pi^*$ is injective with finite cokernel. Since $\mathrm{coker}(\pi_*)$ is a quotient of $\mathrm{coker}(\pi_* \circ \pi^*)$, it follows that $\Gamma_\ell^{\mathrm{ab}}$ is finite. □

2.3. **Results on the support of $\Gamma_\ell^{\mathrm{ab}}$.** In this subsection we study the support (i.e., the set of primes dividing the order) of $\Gamma_\ell^{\mathrm{ab}}$, which is finite by Proposition 2.1, as ℓ varies in the set of primes not dividing MD. Thanks to Ihara's Lemma, in the case of modular curves (i.e., when $D = 1$) the size of $\Gamma_\ell^{\mathrm{ab}}$ is controlled in [29, Theorem 4.3], and an explicit result on the support of $\Gamma_\ell^{\mathrm{ab}}$ has been given by Dasgupta in [12]. Namely, in [12, Proposition 3.7] it is shown that the primes in this set are divisors of $6\phi(M)(\ell^2-1)$ where ϕ is the classical Euler function.

Assume $D > 1$. The extra difficulties in the non-split quaternionic setting arise from the fact that the counterpart of [29] is not yet available. Results of this type would follow, for instance, if Γ_ℓ had the so-called "congruence subgroup property". In this case, it might be possible to show that the support of $\Gamma_\ell^{\mathrm{ab}}$ is contained in the set of primes dividing $\phi(M)$, thus showing that it is in fact independent of ℓ. See [7] for an account of this problem.

We will obtain results on the support of $\Gamma_\ell^{\mathrm{ab}}$ by means of a theorem of Diamond and Taylor ([14, Theorem 2]) which represents a weak analogue of Ihara's Lemma for Shimura curves.

To begin our study, observe that the two coverings π_1 and π_2 of §2.2 give rise by Picard functoriality to a homomorphism of abelian varieties

$$\xi : J_0^D(M) \oplus J_0^D(M) \longrightarrow J_0^D(M\ell)$$

between Jacobians. The kernel of ξ is isomorphic to $\mathrm{Hom}(\Gamma_\ell^{\mathrm{ab}},\mathbf{U})$ where $\mathbf{U}$ is the group of complex numbers of norm 1. Thus we see that if a prime number p is in the support of $\Gamma_\ell^{\mathrm{ab}}$ then the map

$$\xi_p : J_0^D(M)[p] \oplus J_0^D(M)[p] \longrightarrow J_0^D(M\ell)[p]$$

induced by ξ on the p-torsion subgroup is not injective. We study the kernel of ξ_p by means of [14, Theorem 2].

To start with, let us fix some notation. For any prime $q \nmid D$ choose an isomorphism $\varphi_q : B \otimes_{\mathbb{Q}} \mathbb{Q}_q \simeq \mathrm{M}_2(\mathbb{Q}_q)$ of $\mathbb{Q}_q$-algebras in such a way that for all $q|M$ one has

$$\varphi_q(R \otimes \mathbb{Z}_q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_q) \;\middle|\; c \equiv 0 \pmod{q^{n(q)}} \right\}$$

where $q^{n(q)}$ is the exact power of q dividing M. We also require that φ_ℓ satisfies the additional condition

$$\varphi_\ell(R' \otimes \mathbb{Z}_\ell) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell) \;\middle|\; c \equiv 0,\, d \equiv 1 \pmod{\ell} \right\}.$$

For every q as above and every integer $m \geq 0$ write $\Gamma_0^{\mathrm{loc}}(q^m)$ for the subgroup of $\mathrm{GL}_2(\mathbb{Z}_q)$ consisting of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c \equiv 0 \pmod{q^m}$. We further denote by $\Gamma_1^{\mathrm{loc}}(q^m)$ the subgroup of $\Gamma_0^{\mathrm{loc}}(q^m)$ consisting of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $d \equiv 1 \pmod{q^m}$ and $c \equiv 0 \pmod{q^m}$. For primes $q \nmid D$ let

$$i_q : B \hookrightarrow \mathrm{GL}_2(\mathbb{Q}_q)$$

denote the composition of the canonical inclusion $B \hookrightarrow B \otimes \mathbb{Q}_q$ with isomorphism φ_q. Let $\Gamma_1^D(M)$ be the subgroup of $\Gamma_0^D(M)$ consisting of those elements γ such that $i_q(\gamma) \in \Gamma_1^{\mathrm{loc}}(q^{n(q)})$

for all $q|M$. Moreover, let $Q \geq 1$ be the smallest integer such that $MQ \geq 4$ and $\ell \nmid Q$ (so $Q = 1$ if $M \geq 4$) and define $\Gamma_1^D(MQ)$ as the subgroup of $\Gamma_1^D(M)$ consisting of those elements γ such that $i_q(\gamma) \in \Gamma_1^{\mathrm{loc}}(q)$. Finally, consider the subgroup $\Gamma_{1,0}^D(MQ,\ell)$ of $\Gamma_1^D(MQ)$ whose elements are the γ such that $i_\ell(\gamma) \in \Gamma_0^{\mathrm{loc}}(\ell)$. Write $X_1^D(M)$, $X_1^D(MQ)$ and $X_{1,0}^D(MQ,\ell)$ for the compact Shimura curves associated with $\Gamma_1^D(M)$, $\Gamma_1^D(MQ)$ and $\Gamma_{1,0}^D(MQ,\ell)$, respectively, and let $J_1^D(M)$, $J_1^D(MQ)$ and $J_{1,0}^D(MQ,\ell)$ denote their Jacobian varieties. For $i = 1, 2$ the inclusion $\Gamma_{1,0}^D(MQ,\ell) \subset \Gamma_1^D(MQ)$ induces coverings

$$\vartheta_i : X_{1,0}^D(MQ,\ell) \longrightarrow X_1^D(MQ)$$

defined, as above, by $\vartheta_1([z]) = [z]$ and $\vartheta_2([z]) = [\omega_\ell(z)]$. By Picard functoriality, we obtain a homomorphism

$$\vartheta : J_1^D(MQ) \oplus J_1^D(MQ) \longrightarrow J_{1,0}^D(MQ,\ell)$$

between Jacobians. Further, the inclusions

$$\Gamma_1^D(MQ) \subset \Gamma_1^D(M) \subset \Gamma_0^D(M)$$

induce converings of the relevant Riemann surfaces and thus, again by Picard functoriality, homomorphisms $\sigma : J_0^D(M) \to J_1^D(M)$ and $\eta : J_1^D(M) \to J_1^D(MQ)$. Finally, the inclusion $\Gamma_0^D(M\ell) \subset \Gamma_{1,0}^D(MQ,\ell)$ gives a homomorphism $\rho : J_0^D(M\ell) \to J_{1,0}^D(MQ,\ell)$. These maps fit in the commutative diagram

$$\begin{array}{ccccc} J_0^D(M) \oplus J_0^D(M) & \xrightarrow{\sigma\oplus\sigma} & J_1^D(M) \oplus J_1^D(M) & \xrightarrow{\eta\oplus\eta} & J_1^D(MQ) \oplus J_1^D(MQ) \\ \downarrow{\scriptstyle \xi} & & & & \downarrow{\scriptstyle \vartheta} \\ J_0^D(M\ell) & & \xrightarrow{\qquad\qquad\rho\qquad\qquad} & & J_{1,0}^D(MQ,\ell). \end{array} \tag{2}$$

Since σ and η arise by Picard functoriality from coverings of Riemann surfaces, their kernels are finite. Thus the kernels of $\sigma \oplus \sigma$ and $\eta \oplus \eta$ are finite too, and we denote by C_1 and C_2 their orders. Note that C_1 and C_2 do not depend on ℓ (the kernel of σ is, by definition, the *Shimura subgroup* of $J_0^D(M)$ and its size is known to divide $\phi(M)$: see [21]).

Observe that the kernel of ϑ is finite as well. To show this, note that the maps ϑ_1 and ϑ_2 induce, this time by Albanese functoriality, a homomorphism

$$\vartheta' : J_{1,0}^D(MQ,\ell) \longrightarrow J_1^D(MQ) \oplus J_1^D(MQ)$$

on Jacobians, and the composition $\vartheta' \circ \vartheta$ is represented by the matrix $\left(\begin{smallmatrix} \ell+1 & T_\ell \\ T_\ell & \ell+1 \end{smallmatrix}\right)$. Since the eigenvalues of T_ℓ are bounded by $2\sqrt{\ell}$, we see that $\vartheta' \circ \vartheta$ is injective on tangent spaces, and thus its kernel is finite. So the kernel of ϑ is finite; we denote its cardinality by $C(\ell)$. In the following we study the size of $C(\ell)$. We first note that if a prime p divides $C(\ell)$ then the map

$$\vartheta_p : J_1^D(MQ)[p] \oplus J_1^D(MQ)[p] \longrightarrow J_{1,0}^D(MQ,\ell)[p]$$

induced by ϑ on the p-torsion subgroup is not injective.

For any discrete subgroup G of $\mathrm{SL}_2(\mathbb{R})$ denote by $S_2(G,\mathbb{C})$ the $\mathbb{C}$-vector space of cusp forms of weight 2 and level G. Let $\mathcal{F} = \{f_1, \ldots, f_h\}$, where h is the dimension of $J_1^D(MQ)$, be a basis of $S_2\big(\Gamma_1^D(MQ),\mathbb{C}\big)$ consisting of eigenforms for the action of the Hecke algebra and (at the cost of renumbering) assume that $\{f_1, \ldots, f_m\}$ is a set of representatives for the set of orbits of $\mathcal{F}$ under the action of $G_{\mathbb{Q}}$. Denote by $A_1 = A_{f_1}, \ldots, A_m = A_{f_m}$ the abelian varieties associated with these forms via the Eichler–Shimura construction, fix an isogeny

$$J_1^D(MQ) \xrightarrow{\sim} \prod_{i=1}^m A_i$$

and let C_3 be the order of its kernel, which of course does not depend on ℓ. By the Jacquet–Langlands correspondence, each of the abelian varieties A_i is isogenous over $\mathbb{Q}$ to the abelian variety $A_{f_{0,i}}$ associated with a classical modular form $f_{0,i} \in S_2\big(\Gamma_1(MDQ), \mathbb{C}\big)$ for the congruence subgroup $\Gamma_1(MDQ) \subset \mathrm{SL}_2(\mathbb{Z})$.

For every $i = 1, \dots, m$ fix an isogeny $\psi_i : A_i \to A_{f_{0,i}}$ and denote by d_i the size of its kernel. Set $C_4 := \prod_{i=1}^m d_i$ and notice that C_4 is independent of ℓ. Finally, recall that the mod p representation of $G_{\mathbb{Q}}$ associated with a modular form $f \in S_2\big(\Gamma_1^D(MQ), \mathbb{C}\big)$ is irreducible for all but finitely many prime numbers p. For every i let e_i be the product of the primes p such that the $G_{\mathbb{Q}}$-representation $A_{f_{0,i}}[p]$ is reducible, then set $C_5 := \prod_{i=1}^m e_i$.

Now let us recall [14, Theorem 2], which is a (weak) substitute for Ihara's Lemma in the context of Shimura curves attached to non-split quaternion algebras. Let p be a prime number not dividing $6MDQ\ell$. Following [14], denote by $\mathbb{T}$ the image in $\mathrm{End}\big(J_1^D(MQ)\big)$ of the polynomial ring generated over $\mathbb{Z}$ by the Hecke operators T_q and the spherical (i.e., diamond) operators S_q for primes $q \nmid MDQ$. A maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ containing p is said to be *Eisenstein* if for some integer $d \geq 1$ and all but finitely many primes q with $q \equiv 1 \pmod{d}$ we have $T_q - 2 \in \mathfrak{m}$ and $S_q - 1 \in \mathfrak{m}$. By [14, Theorem 2], the maximal ideals of $\mathbb{T}$ in the support of $\ker(\vartheta_p)$ are Eisenstein.

If $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ belonging to the support of $S_2\big(\Gamma_1(MDQ), \mathbb{C}\big)$ with residual characteristic p then $\mathfrak{m}$ is the kernel of the reduction modulo p of the homomorphism $\mathbb{T} \to \mathcal{O}_E$ associated with one of the eigenforms $f_{0,i} \in S_2\big(\Gamma_1(MDQ), \mathbb{C}\big)$, where E is a suitable number field. For simplicity, denote by f the eigenform associated with $\mathfrak{m}$. By [14, Proposition 2], the ideal $\mathfrak{m}$ is Eisenstein if and only if the mod p Galois representation $\rho_{\mathfrak{m}}$ attached to $\mathfrak{m}$ is reducible. With notation as above, this can rephrased by saying that $\mathfrak{m}$ is Eisenstein if and only if the $G_{\mathbb{Q}}$-representation $A_f[p]$ is reducible.

The main result of this subsection is the following

Theorem 2.2. *There exists an integer $C \geq 1$ such that for all but finitely many primes $\ell \nmid MD$ the support of $\Gamma_\ell^{\mathrm{ab}}$ is contained in the set of primes dividing $C\ell$.*

Proof. With notation as before, we show that the integer

$$C := 6C_1C_2C_3C_4C_5MDQ,$$

which only depends on M, D and Q, does the job. More precisely, we show that if $\ell \nmid MDQ$ and the prime p belongs to the support of $\Gamma_\ell^{\mathrm{ab}}$ then p divides $C\ell$. Thus fix a prime $\ell \nmid MDQ$. As remarked earlier if the prime p lies in the support of $\Gamma_\ell^{\mathrm{ab}}$ then $\ker(\xi_p)$ is not zero.

The first step of the proof consists in showing that if $p \nmid C_3C_4MDQ\ell$ but p divides the order of $\ker(\vartheta_p)$ then $p|C_5$. To this aim, fix a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ in the support of $\ker(\vartheta_p)$. Then $\mathfrak{m}$ has residual characteristic p and is Eisenstein because $p \nmid 6MDQ\ell$. Since

$$\ker(\vartheta_p) \subset J_1^D(MQ)[p] \oplus J_1^D(MQ)[p],$$

it follows that $\mathfrak{m}$ belongs to the support of $J_1^D(MQ)[p]$. As $p \nmid C_3$, the ideal $\mathfrak{m}$ belongs to the support of the $\mathbb{T}$-module $A_i[p]$ for some $i \in \{1, \dots, m\}$. Next, since $p \nmid C_4$, the isogeny $\psi_i : A_i \to A_{f_{0,i}}$ induces an isomorphism $A_i[p] \simeq A_{f_{0,i}}[p]$ of $G_{\mathbb{Q}}$-modules where, as before, $f_{0,i}$ is the classical cusp form associated with f_i by the Jacquet–Langlands correspondence. Hence $\mathfrak{m}$ belongs to the support of the $\mathbb{T}$-module $A_{f_{0,i}}[p]$ as well. But, as pointed out before, $\mathfrak{m}$ is Eisenstein, so the $G_{\mathbb{Q}}$-representation $A_{f_{0,i}}[p]$ is reducible, and this proves that $p|C_5$.

The second (and final) step is an easy diagram chasing. Suppose that $p \nmid 6C_3C_4C_5MDQ\ell$. Thanks to the first step, we already know that ϑ_p is injective (note that the order of $\ker(\vartheta_p)$ is *a priori* a power of p). The commutativity of diagram (2) shows that

$$\ker(\xi_p) \subset \ker\big((\eta \oplus \eta) \circ (\sigma \oplus \sigma)\big),$$

so the order of $\ker(\xi_p)$ divides C_1C_2, whence $p|C_1C_2$. □

3. Darmon points on Jacobians of Shimura curves

In this section assume that $D > 1$. Our goal is to define Darmon points on Jacobians of Shimura curves over $\mathbb{Q}$ and on closely related abelian varieties. These points are lifts of the local points on elliptic curves introduced by M. Greenberg in [15]. The constructions we perform and the conjectures we formulate are the counterparts of those proposed by Dasgupta in [12, §3.3] when $D = 1$, later conjecturally refined by Bertolini, Darmon and Dasgupta in [5, §§1.2–1.3]. We keep the notation of Section 2 in force for the rest of the article.

3.1. **Rigid uniformizations of Jacobians of Shimura curves.** In this subsection we recall, and conjecturally refine, the main results of [22].

Denote by H the maximal torsion-free quotient of the cokernel of the map π^* introduced in §2.2, let $J_0^D(M\ell)$ be the Jacobian variety of $X_0^D(M\ell)$ and let $J_0^D(M\ell)^{\ell\text{-new}}$ be its ℓ-new quotient, whose dimension will be denoted by g; the abelian group H is free of rank $2g$. Now consider the torus

$$T := \mathbb{G}_m \otimes_{\mathbb{Z}} H$$

where $\mathbb{G}_m$ denotes the multiplicative group (viewed as a functor on commutative $\mathbb{Q}$-algebras). We will regard H and T as Γ_ℓ-modules with trivial action, where Γ_ℓ is the Ihara group of §2.1. In analogy with what is proved in [12] for modular Jacobians, the abelian variety $J_0^D(M\ell)^{\ell\text{-new}}$ is uniformized by means of a suitable quotient of T. In order to do this, in [22, Sections 4–6] an explicit element $\boldsymbol{\mu}$ in the cohomology group $H^1\big(\Gamma_\ell, \mathrm{Meas}\big(\mathbb{P}^1(\mathbb{Q}_\ell), H\big)\big)$ is introduced as follows.

Denote by $\mathcal{T}$ the Bruhat–Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$, by $\mathcal{V}$ the set of its vertices and by $\mathcal{E}$ the set of its oriented edges. For any edge $e \in \mathcal{E}$ write $s(e), t(e) \in \mathcal{V}$ for its source and its target, respectively, and $\bar{e}$ for the same edge with reversed orientation. Let v_* be the distinguished vertex corresponding to the maximal order $\mathrm{M}_2(\mathbb{Z}_\ell)$ and let e_* be the edge emanating from v_* and corresponding to the Eichler order consisting of the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z}_\ell)$ such that $\ell | c$. Set $\hat{v}_* := t(e_*)$.

For any abelian group M let $\mathcal{F}(\mathcal{V}, M)$ and $\mathcal{F}(\mathcal{E}, M)$ denote the set of maps $m : \mathcal{V} \to M$ (respectively, $m : \mathcal{E} \to M$). Both are natural left Γ_ℓ-modules with action $(\gamma \cdot m)(x) := m(\gamma^{-1}x)$ for any $\gamma \in \Gamma_\ell$ and $x \in \mathcal{V}$ or $\mathcal{E}$. Define also

$$\mathcal{F}_0(\mathcal{E}, M) := \big\{ m \in \mathcal{F}(\mathcal{E}, M) \mid m(\bar{e}) = -m(e) \big\}$$

and

$$\mathcal{F}_{\mathrm{har}}(M) := \left\{ m \in \mathcal{F}_0(\mathcal{E}, M) \;\middle|\; \sum_{s(e)=v} m(e) = 0 \text{ for all } v \in \mathcal{V} \right\},$$

which are Γ_ℓ-submodules of $\mathcal{F}(\mathcal{E}, M)$. The Γ_ℓ-module of H-valued measures on $\mathbb{P}^1(\mathbb{Q}_p)$ with total mass equal to zero can be identified with $\mathcal{F}_{\mathrm{har}}(H)$.

Fix once and for all

- a prime number $r \nmid \ell DM$;
- a system of representatives $\{g_i\}_{i=0}^{\ell}$ for $\Gamma_0^D(M\ell)\backslash\Gamma_0^D(M)$;
- a system of representatives $\mathcal{Y} = \{\gamma_e\}_{e \in \mathcal{E}^+}$ for $\Gamma_0^D(M\ell)\backslash\Gamma_\ell$ such that $\gamma_e(e) = e_*$ and of the form

$$\gamma_e = g_{i_1}\hat{g}_{j_1}g_{i_2}\hat{g}_{j_2}\cdots g_{i_s}\hat{g}_{j_s} \qquad \text{with } i_k, j_k \in \{0, \dots, \ell\}$$

for every *even* oriented edge $e \in \mathcal{E}^+$.

Notice that, with these choices, for every even vertex $v \in \mathcal{V}^+$ there exists an edge e_0 with $s(e_0) = v$ such that, putting $\gamma_v := \gamma_{e_0}$, we have $\{\gamma_e\}_{s(e)=v} = \{g_i\gamma_v\}_{i=0}^{\ell}$. This way, the set $\{\gamma_v\}_{v \in \mathcal{V}^+}$ is also a system of representatives for $\Gamma_0^D(M)\backslash\Gamma_\ell$ satisfying $\gamma_v(v) = v_*$ for every

$v \in \mathcal{V}^+$. Similarly, for any odd vertex $v \in \mathcal{V}^-$ we have $\{\gamma_e\}_{t(e)=v} = \{\hat{g}_i \gamma_v\}_{i=0}^{\ell}$ where $\{\gamma_v\}_{v\in\mathcal{V}^-}$ is a system of representatives for $\hat{\Gamma}_0^D(M)\backslash\Gamma_\ell$ satisfying $\gamma_v(v) = \hat{v}_*$ for every $v \in \mathcal{V}^-$.

The next object made its first appearance in [22, §4], where it is shown that it is indeed well defined.

Definition 3.1. Set

$$\boldsymbol{\mu} := (T_r - r - 1) \cdot \boldsymbol{\mu}^{\mathcal{Y}} \in H^1\big(\Gamma_\ell, \mathcal{F}_{\mathrm{har}}(H)\big) = H^1\big(\Gamma_\ell, \mathrm{Meas}\big(\mathbb{P}^1(\mathbb{Q}_\ell), H\big)\big)$$

where $\boldsymbol{\mu}^{\mathcal{Y}}$ is the class of the cocycle

$$\mu^{\mathcal{Y}} \in Z^1\big(\Gamma_\ell, \mathrm{Meas}\big(\mathbb{P}^1(\mathbb{Q}_\ell), H\big)\big), \qquad \mu_\gamma^{\mathcal{Y}}(U_e) := [g_{\gamma,e}] \quad \text{for all } \gamma \in \Gamma_\ell \text{ and } e \in \mathcal{E}^+.$$

Here $g_{\gamma,e} := \gamma_e \gamma \gamma_{\gamma^{-1}(e)}^{-1} \in \Gamma_0^D(M\ell)$ and for every $g \in \Gamma_0^D(M\ell)$ we write $[g] \in H$ for the class of g in the quotient H of $H_1\big(\Gamma_0^D(M\ell), \mathbb{Z}\big) \simeq \Gamma_0^D(M\ell)^{\mathrm{ab}}$. Finally, $U_e := \gamma_e^{-1}(\mathbb{Z}_\ell)$.

By cup product, the cohomology class $\boldsymbol{\mu}$ defines an integration map on the homology group $H_1(\Gamma_\ell, \mathrm{Div}^0 \mathcal{H}_\ell)$ with values in $T(\mathbb{C}_\ell)$. Composing the boundary homomorphism $H_2(\Gamma_\ell, \mathbb{Z}) \to H_1(\Gamma_\ell, \mathrm{Div}^0 \mathcal{H}_\ell)$ induced by the degree map with the integration map produces a further map $H_2(\Gamma_\ell, \mathbb{Z}) \to T(\mathbb{C}_\ell)$ whose image is denoted by L. It turns out that L is a lattice of rank $2g$ in $T(\mathbb{Q}_\ell)$ which is preserved by the action of a suitable Hecke algebra. Finally, let K_ℓ denote the (unique, up to isomorphism) unramified quadratic extension of $\mathbb{Q}_\ell$.

The following is [22, Theorem 1.1].

Theorem 3.2. *The quotient T/L admits a Hecke-equivariant isogeny over K_ℓ to the rigid analytic space associated with the product of two copies of $J_0^D(M\ell)^{\ell\text{-new}}$.*

In fact, something more precise can be said. Write W_∞ for the Atkin–Lehner involution defined in [22, §2.2], and for any $\mathbb{Z}[W_\infty]$-module M and sign $\epsilon \in \{\pm\}$ set $M_\epsilon := M/(W_\infty - \epsilon 1)$. Define

$$T_\epsilon := \mathbb{G}_m \otimes_{\mathbb{Z}} H_\epsilon.$$

Since the cokernel of the canonical map $H \to H_+ \oplus H_-$ is supported at 2, it follows that there exists an isogeny of 2-power degree

$$T/L \longrightarrow T_+/L_+ \oplus T_-/L_- \tag{3}$$

of rigid analytic tori over $\mathbb{Q}_\ell$. Then Theorem 3.2 is proved in [22] by showing that for all $\epsilon \in \{+,-\}$ the quotient T_ϵ/L_ϵ admits a Hecke-equivariant isogeny over K_ℓ to the rigid analytic space associated with the abelian variety $J_0^D(M\ell)^{\ell\text{-new}}$. In the sequel we shall assume the following variant of [5, Conjecture 1.5].

Conjecture 3.3. *If $\epsilon \in \{+,-\}$ then the quotient T_ϵ/L_ϵ is isomorphic over K_ℓ to the rigid analytic space associated with an abelian variety $J_\epsilon^{(\ell)}$ defined over $\mathbb{Q}$.*

As in *loc. cit.*, we expect that the abelian variety $J_\epsilon^{(\ell)}$ will be endowed with a natural action of the Hecke algebra and that the isomorphism of Conjecture 3.3 will be Hecke equivariant; moreover, we also expect that if one lets the non-trivial element of $\mathrm{Gal}\,(K_\ell/\mathbb{Q}_\ell)$ act on T/L via the Hecke operator U_ℓ then the above isomorphism will be defined over $\mathbb{Q}_\ell$. Granting Conjecture 3.3, fix once and for all isomorphisms

$$T_\pm/L_\pm \xrightarrow{\simeq} J_\pm^{(\ell)} \tag{4}$$

defined over K_ℓ.

3.2. **Darmon points on $J_\pm^{(\ell)}$ and on $J_0^D(M\ell)^{\ell\text{-new}}$.** In this subsection we also assume that ℓ is inert in K, so K_ℓ is nothing other than the completion of K at the prime above ℓ. We freely use the notation of [22], to which we refer for all details. Since ℓ is kept fixed in the discussion to follow, for simplicity we set

$$\Gamma := \Gamma_\ell.$$

In [22, §7.3] a class $\boldsymbol{d} \in H^2\big(\Gamma, T(\mathbb{C}_\ell)\big)$ is introduced whose image in $H^2\big(\Gamma, T(\mathbb{C}_\ell)/L\big)$ is trivial; moreover, the lattice L is the smallest subgroup of $T(\mathbb{Q}_\ell)$ with this property. Let

$$r : \mathcal{H}_\ell \longrightarrow \mathcal{T}$$

denote the $\mathrm{GL}_2(\mathbb{Q}_\ell)$-equivariant reduction map (see, e.g., [11, §5.1]) and fix once and for all a base point $\tau \in K_\ell - \mathbb{Q}_\ell$, i.e., a K_ℓ-rational point on $\mathcal{H}_\ell$, such that $r(\tau) = v_*$. The class $\boldsymbol{d}$ can then be represented by the 2-cocycle $d = d_\tau \in Z^2\big(\Gamma, T(K_\ell)\big)$ given by

$$d_{\gamma_1,\gamma_2} := \fint_{\mathbb{P}^1(\mathbb{Q}_\ell)} \frac{t - \gamma_1^{-1}(\tau)}{t - \tau} d\mu_{\gamma_2}^{\mathcal{Y}}(t). \tag{5}$$

It follows that there exists a map $\beta = \beta_\tau : \Gamma \to T/L$ such that

$$\beta_{\gamma_1\gamma_2} - \beta_{\gamma_1} - \beta_{\gamma_2} \equiv d_{\gamma_1,\gamma_2} \pmod{L} \tag{6}$$

for all $\gamma_1, \gamma_2 \in \Gamma$. Notice that β is well defined only up to elements of $\mathrm{Hom}(\Gamma, T/L)$.

Denote by $\vartheta : K \hookrightarrow \mathbb{R}$ the embedding fixed at the beginning of this paper and choose also an embedding $K \hookrightarrow \mathbb{C}_\ell$. If $\mathcal{O}$ is an order of K then an embedding $\psi : K \hookrightarrow B$ is said to be an *optimal embedding of $\mathcal{O}$ into R* if $\psi^{-1}(R) = \mathcal{O}$. Denote by $\mathrm{Emb}(\mathcal{O}, R)$ the set of such embeddings. For every $\psi \in \mathrm{Emb}(\mathcal{O}, R)$ there is a unique $z_\psi \in \mathcal{H}_\ell \cap K$ such that

$$\psi(\alpha)\begin{pmatrix} z_\psi \\ 1 \end{pmatrix} = \alpha \begin{pmatrix} z_\psi \\ 1 \end{pmatrix} \qquad \text{for all } \alpha \in K.$$

Define

$$\mathcal{H}_\ell^{\mathcal{O}} := \big\{ z_\psi \;\big|\; \psi \in \mathrm{Emb}(\mathcal{O}, R) \big\} \subset \mathcal{H}_\ell \cap K.$$

Let $z_\psi \in \mathcal{H}_\ell^{\mathcal{O}}$ and let z'_ψ be its conjugate over $\mathbb{Q}$. By Dirichlet's unit theorem, the abelian group of units in $\mathcal{O}^\times$ of norm 1 is free of rank 1; let γ_ψ be the generator of this group such that $\vartheta(\gamma_\psi) > 1$ if $\vartheta(z_\psi) > \vartheta(z'_\psi)$ and such that $\vartheta(\gamma_\psi) < 1$ if $\vartheta(z_\psi) < \vartheta(z'_\psi)$.

Let $t = t_\ell$ denote the exponent of Γ^{ab}. Set

$$\Phi(z_\psi) := t \cdot \beta\big(\psi(\gamma_\psi)\big) \in T(K_\ell)/L.$$

Multiplication by t ensures that $\Phi(z_\psi)$ does not depend on the choice of a map β as above. Actually, the point $\Phi(z_\psi)$ depends only on the Γ-orbit of z_ψ, so we can consider

$$\Phi([z_\psi]) := \Phi(z_\psi) \in T(K_\ell)/L$$

where $[z_\psi]$ is the class of z_ψ in $\Gamma\backslash(\mathcal{H}_\ell \cap K)$.

Let $\nu_\pm : T/L \to J_\pm^{(\ell)}$ be the two maps obtained by composing isogeny (3) with the canonical projections onto the factors and then with isomorphisms (4).

Definition 3.4. The *Darmon points on $J_\pm^{(\ell)}$ attached to $\mathcal{O}$* are the points

$$P_\psi^\pm := \nu_\pm\big(\Phi([z_\psi])\big) \in J_\pm^{(\ell)}(K_\ell)$$

for $z_\psi \in \mathcal{H}_\ell^{\mathcal{O}}$.

When a choice of sign $\epsilon \in \{\pm\}$ has been made the point P_ψ^ϵ will be denoted simply by P_ψ (or even by P_d where d is the conductor of $\mathcal{O}$, if the embedding ψ is understood). Although in this article we shall ultimately work with points on $J_\epsilon^{(\ell)}$ for a fixed choice of sign ϵ, it is worthwhile to explicitly introduce Darmon points on Jacobians of Shimura curves. To do this, choose isogenies

$$T_\pm/L_\pm \longrightarrow J_0^D(M\ell)^{\ell\text{-new}} \tag{7}$$

over K_ℓ and write $\lambda_\pm : T/L \to J_0^D(M\ell)^{\ell\text{-new}}$ for the two maps obtained by composing isogeny (3) with the canonical projections onto the factors and then with isogenies (7).

Definition 3.5. The *Darmon points on* $J_0^D(M\ell)^{\ell\text{-new}}$ *attached to* $\mathcal{O}$ are the points

$$\lambda_\pm\big(\Phi([z_\psi])\big) \in J_0^D(M\ell)^{\ell\text{-new}}(K_\ell)$$

for $z_\psi \in \mathcal{H}_\ell^{\mathcal{O}}$.

If A is an elliptic curve over $\mathbb{Q}$ of conductor $N = DM$ then the points introduced in Definition 3.5 map to the local points on A defined by M. Greenberg in [15] under the modular projection $J_0^D(M\ell)^{\ell\text{-new}} \to A$.

We conclude this subsection by stating the algebraicity properties conjecturally satisfied by our Darmon points. Write H for the narrow ring class field of K attached to $\mathcal{O}$ and denote by

$$(\mathfrak{a}, \psi) \longmapsto \psi^{\mathfrak{a}}$$

the action of $\mathfrak{a} \in \mathrm{Pic}^+(\mathcal{O})$ on $\psi \in \mathcal{E}(\mathcal{O}, R)$ as described, e.g., in [32, Ch. III, §5C] (see also Proposition 4.2). Finally, let $\mathrm{Pic}^+(\mathcal{O})$ be the narrow class group of $\mathcal{O}$ and let

$$\mathrm{rec} : \mathrm{Pic}^+(\mathcal{O}) \xrightarrow{\simeq} \mathrm{Gal}\,(H/K)$$

be the isomorphism induced by the reciprocity map of global class field theory.

For the purposes of the present paper, we formulate our rationality conjecture only for Darmon points on $J_\pm^{(\ell)}$, but completely analogous statements could be given for points on $J_0^D(M\ell)^{\ell\text{-new}}$ as well.

Conjecture 3.6. *If* $z_\psi \in \mathcal{H}_\ell^{\mathcal{O}}$ *then* $P_\psi^\pm \in J_\pm^{(\ell)}(H)$ *and*

$$P_{\psi^{\mathfrak{a}}}^\pm = \mathrm{rec}(\mathfrak{a})^{-1}\big(P_\psi^\pm\big)$$

for all $\mathfrak{a} \in \mathrm{Pic}^+(\mathcal{O})$.

This is the analogue of [5, Conjecture 1.7] and is a refinement of [12, Conjecture 3.9], which in turn is the counterpart of [10, Conjectures 5.6 and 5.9]. From here on we shall assume the validity of Conjecture 3.6.

4. Algebraic parts of special values and a theorem of Popa

Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N and let K be a real quadratic field as in the introduction; moreover, again with the notation of the introduction, set

$$D := \prod_{q \in \Sigma} q \geq 1, \qquad M := N/D.$$

Let f denote the modular form on $\Gamma_0^D(M)$ (well defined up to scalars) associated with f_0 by the Jacquet–Langlands correspondence; in particular, if $D = 1$ then $f = f_0$. In this section we introduce the algebraic part of the special value at $s = 1$ of the L-function

$$L_K(E, \chi, s) = L_K(f_0, \chi, s) = L_K(f, \chi, s)$$

and describe some consequences of a formula proved by Popa in [27].

4.1. **Review of the group structure of** $\mathrm{Pic}^+(\mathcal{O}_c)$**.** Recall the notation of the introduction; in particular, let $c \geq 1$ be an integer prime to $\delta_K N$. As before, the reciprocity map of global class field theory provides a canonical isomorphism

$$\mathrm{rec} : \mathrm{Pic}^+(\mathcal{O}_c) \xrightarrow{\simeq} G_c$$

where G_c is the Galois group over K of the narrow ring class field of K of conductor c. Let now $\mathrm{Pic}(\mathcal{O}_c)$ be the Picard group of $\mathcal{O}_c$, that is the group of homothety classes of proper $\mathcal{O}_c$-ideals of K; class field theory then identifies $\mathrm{Pic}(\mathcal{O}_c)$ with the Galois group over K of the (weak) ring class field K_c of K of conductor c. It turns out that if $h(c)$ is the order of $\mathrm{Pic}(\mathcal{O}_c)$ and $h^+(c)$ is the order of $\mathrm{Pic}^+(\mathcal{O}_c)$ then $h^+(c)/h(c) = 1$ or 2, so H_c is an extension of K_c of degree at most 2 (see, e.g., [8, Ch. 15, §I]).

Since $(c, \delta_K) = 1$ by assumption, the principal ideal $(\sqrt{\delta_K})$ is a proper $\mathcal{O}_c$-ideal of K, so we can consider its class $\mathfrak{D}_K$ in $\mathrm{Pic}^+(\mathcal{O}_c)$. Of course, $\mathfrak{D}_K^2 = 1$, hence $\mathfrak{D}_K$ is either trivial or of order 2. Furthermore, there is a short exact sequence

$$0 \longrightarrow \{1, \mathfrak{D}_K\} \longrightarrow \mathrm{Pic}^+(\mathcal{O}_c) \longrightarrow \mathrm{Pic}(\mathcal{O}_c) \longrightarrow 0, \tag{8}$$

so the natural surjection $\mathrm{Pic}^+(\mathcal{O}_c) \twoheadrightarrow \mathrm{Pic}(\mathcal{O}_c)$ is an isomorphism (i.e., $h^+(c) = h(c)$) precisely when $\mathfrak{D}_K$ is trivial. Equivalently, $\mathrm{Pic}^+(\mathcal{O}_c) = \mathrm{Pic}(\mathcal{O}_c)$ if and only if the order $\mathcal{O}_c$ has a unit of norm -1. In general, sequence (8) does not split; in fact, it splits if and only if the integer δ_K is not a sum of two squares (see [8, Ch. 14, §B]).

Now define the Galois element

$$\sigma_K := \mathrm{rec}(\mathfrak{D}_K) \in G_c.$$

It follows that σ_K is trivial when $h^+(c) = h(c)$ and has order 2 otherwise.

The automorphism σ_K plays a special role in our considerations because it allows us to introduce, as in [2], a natural notion of parity for characters of G_c. As before, write $\widehat{G}_c$ for the group of complex-valued characters of G_c.

Definition 4.1. A character $\chi \in \widehat{G}_c$ is said to be *even* (respectively, *odd*) if $\chi(\sigma_K) = 1$ (respectively, $\chi(\sigma_K) = -1$).

Equivalently, a character is even if it factors through $\mathrm{Gal}\,(K_c/K)$, and is odd otherwise. In particular, if $h^+(c) = h(c)$ then $\sigma_K = 1$ and all characters of G_c are even.

4.2. **Oriented optimal embeddings.** Equip R and $\mathcal{O}_c$ with local orientations at prime numbers dividing $N = DM$, i.e., ring homomorphisms

$$\mathfrak{O}_q : R \longrightarrow k_q, \qquad \mathfrak{o}_q : \mathcal{O}_c \longrightarrow k_q$$

for every prime $q|N$ where k_q stands for the finite field with q (respectively, q^2) elements if $q|M$ (respectively, $q|D$).

Write $\mathrm{Emb}(K, B)$ for the set of embeddings of K into B, which is non-empty because all the primes at which B is ramified are inert in K. The group $B^\times$ acts on $\mathrm{Emb}(K, B)$ by conjugation on B and the stabilizer of $\psi \in \mathrm{Emb}(K, B)$ is the (non-split) torus $\psi(K^\times)$. We say that $\psi \in \mathrm{Emb}(K, B)$ is an *oriented optimal embedding of* $\mathcal{O}_c$ *into* R if $\psi \in \mathrm{Emb}(\mathcal{O}_c, R)$ and

$$\mathfrak{O}_q \circ \psi|_{\mathcal{O}_c} = \mathfrak{o}_q$$

for every prime $q|N$. The set of all such embeddings will be denoted by $\mathcal{E}(\mathcal{O}_c, R)$, and the cardinality of the set of $\Gamma_0^D(M)$-conjugacy classes of elements of $\mathcal{E}(\mathcal{O}_c, R)$ is $h^+(c)$.

Let $\omega_\infty \in R^\times$ be an element of reduced norm -1. Note that ω_∞ normalizes $\Gamma_0^D(M)$; in fact, all such elements lie in a single orbit for the action of $\Gamma_0^D(M)$. For any $\gamma \in B^\times$ set

$$\gamma^* := \omega_\infty \gamma \omega_\infty^{-1}. \tag{9}$$

In particular, $\gamma^* \in R$ when $\gamma \in R$. Moreover, if $\psi \in \mathcal{E}(\mathcal{O}_c, R)$ then it is immediate to check that

$$\psi^* := \omega_\infty \psi \omega_\infty^{-1}$$

is in $\mathcal{E}(\mathcal{O}_c, R)$ too. By definition, if $\psi(\sqrt{\delta_K}) = \gamma$ then $\psi^*(\sqrt{\delta_K}) = \gamma^*$.

Proposition 4.2. *There exists a bijection*

$$F : \mathcal{E}(\mathcal{O}_c, R)/\Gamma_0^D(M) \longrightarrow \mathrm{Pic}^+(\mathcal{O}_c)$$

such that $F([\psi^*]) = \mathfrak{D}_K \cdot F([\psi])$ *for all* $\psi \in \mathcal{E}(\mathcal{O}_c, R)$.

Proof. To begin with, the claimed correspondence is not canonical, as $\mathcal{E}(\mathcal{O}_c, R)/\Gamma_0^D(M)$ is naturally a torsor under the action of $\mathrm{Pic}^+(\mathcal{O}_c)$. In order to describe it, we are thus led to fix an auxiliary optimal embedding $\psi_0 \in \mathcal{E}(\mathcal{O}_c, R)$. We can now provide an explicit bijection

$$\mathrm{Pic}^+(\mathcal{O}_c) \longrightarrow \mathcal{E}(\mathcal{O}_c, R)/\Gamma_0^D(M) \tag{10}$$

as follows. Given the class $[\mathfrak{a}] \in \mathrm{Pic}^+(\mathcal{O}_c)$ of an ideal $\mathfrak{a}$, the set $R\psi_0(\mathfrak{a})$ is a left ideal, which is known to be principal because B is indefinite. Since $n(R^\times) = \{\pm 1\}$, we may find an element $a \in R$ with reduced norm $n(a) > 0$ such that $R\psi_0(\mathfrak{a}) = Ra$, this a being well defined up to elements in $\Gamma_0^D(M)$. Set

$$\psi_{[\mathfrak{a}]} := a\psi_0 a^{-1} \in \mathcal{E}(\mathcal{O}_c, R).$$

It is easy to check that the rule $[\mathfrak{a}] \mapsto \left[\psi_{[\mathfrak{a}]}\right]$ induces a well-defined bijection as in (10). The inverse of (10) can then be taken to be the searched-for F in the statement of the proposition.

Finally, notice that if $\mathfrak{a} = \mathfrak{b} \cdot (\sqrt{\delta_K})$ then we can take

$$a = \omega_\infty \cdot b \cdot \psi_0(\sqrt{d_K})$$

where $b \in R$ is such that $n(b) > 0$ and $R\psi_0(\mathfrak{b}) = Rb$. Hence

$$\psi_{\mathfrak{a}} = \big(\omega_\infty \cdot b \cdot \psi_0(\sqrt{d_K})\big)\psi_0\big(\psi_0(\sqrt{d_K})^{-1} \cdot b^{-1} \cdot \omega_\infty^{-1}\big).$$

Since $\psi_0(\sqrt{d_K})\psi_0\psi_0(\sqrt{d_K})^{-1} = \psi_0$ because $\mathcal{O}_c$ is a commutative ring, we conclude that

$$\psi_{[\mathfrak{b}]\mathfrak{D}_K} = \psi_{[\mathfrak{b}]}^*.$$

Thus

$$F([\psi^*]) = \mathfrak{D}_K \cdot F([\psi])$$

for all $\psi \in \mathcal{E}(\mathcal{O}_c, R)$, as was to be shown. □

We choose once and for all an optimal embedding $\psi_0 \in \mathcal{E}(\mathcal{O}_c, R)$ and regard the bijection F of Proposition 4.2, built out of ψ_0, as fixed. Notice that, by this proposition, $[\psi^*] = [\psi]$ if and only if $h^+(c) = h(c)$. Observe also that this is the case precisely when ω_∞ can be taken to lie in $\mathcal{O}_c$. Consider the composition

$$G := \mathrm{rec} \circ F : \mathcal{E}(\mathcal{O}_c, R)/\Gamma_0^D(M) \longrightarrow G_c,$$

which is a bijection satisfying

$$G([\psi^*]) = \sigma_K \cdot G([\psi]) \tag{11}$$

for all $\psi \in \mathcal{E}(\mathcal{O}_c, R)$. Now for every $\sigma \in G_c$ choose an embedding

$$\psi_\sigma \in G^{-1}(\sigma),$$

so that the family $\{\psi_\sigma\}_{\sigma \in G_c}$ is a set of representatives of the $\Gamma_0^D(M)$-conjugacy classes of oriented optimal embeddings of $\mathcal{O}_c$ into R. If $\gamma, \gamma' \in R$ write $\gamma \sim \gamma'$ to indicate that γ and γ' are in the same $\Gamma_0^D(M)$-conjugacy class, and adopt a similar notation for (oriented) optimal embeddings of $\mathcal{O}_c$ into R. Since

$$G([\psi_\sigma^*]) = \sigma_K \cdot G([\psi_\sigma]) = \sigma_K \sigma$$

by equality (11), we deduce that

$$\psi_\sigma^* \sim \psi_{\sigma_K\sigma} \tag{12}$$

for all $\sigma \in G_c$.

After choosing a (fundamental) unit ε_c of $\mathcal{O}_c$ of norm 1, normalized so that $\varepsilon_c > 1$ with respect to the fixed real embedding of K, define

$$\gamma_\sigma := \psi_\sigma(\varepsilon_c) \in \Gamma_0^D(M) \tag{13}$$

for all $\sigma \in G_c$. As an immediate consequence of (12) and (13), one has

$$\gamma_\sigma^* = \psi_\sigma^*(\varepsilon_c) \sim \psi_{\sigma_K\sigma}(\varepsilon_c) = \gamma_{\sigma_K\sigma} \tag{14}$$

for all $\sigma \in G_c$. This seemingly innocuous conjugacy relation will play a crucial role in the proof of Proposition 4.4.

4.3. **Homology of Shimura curves and complex conjugation.** Let $\mathbb{T}_M = \mathbb{T}_M^D$ be the algebra of Hecke operators acting on cusp forms of weight 2 on $\Gamma_0^D(M)$, which is generated over $\mathbb{Z}$ by the Hecke operators T_ℓ for primes $\ell \nmid DM$ and U_q for primes $q|M$. The algebra $\mathbb{T}_M$ acts naturally on the (singular) homology group $H_1\big(X_0^D(M), \mathbb{Z}\big)$. As before, let $a_\ell \in \mathbb{Z}$ be the eigenvalue of f for the action of the Hecke operator T_ℓ (respectively, U_ℓ) if $\ell \nmid M$ (respectively, if $\ell|M$). Set

$$I_f := \big\langle T_\ell - a_\ell,\ \ell \nmid DM;\ U_q - a_q,\ q|M \big\rangle \subset \mathbb{T}_M,$$

so that I_f is the kernel of the algebra homomorphism

$$\varphi_f : \mathbb{T}_M \longrightarrow \mathbb{Z}, \qquad T_\ell \longmapsto a_\ell, \qquad U_q \longmapsto a_q \tag{15}$$

determined by f. As a piece of notation, for any $\mathbb{T}_M$-module A write $A_f := A/I_fA$ for the maximal quotient of A on which $\mathbb{T}_M$ acts via φ_f.

We want to embed $X_0^D(M)$ into its Jacobian. If $D = 1$ then let

$$\zeta : X_0(M) \longrightarrow J_0(M) \tag{16}$$

be the usual map sending the cusp ∞ on $X_0(M)$ to the origin of $J_0(M)$.

If $D > 1$ then, following [33], let the *Hodge class* be the unique $\xi \in \mathrm{Pic}(X_0^D(M)) \otimes \mathbb{Q}$ of degree 1 on which the Hecke operators at primes not dividing M act as multiplication by their degree (see [33, p. 30] for an explicit expression of ξ and [9, §3.5] for a detailed exposition). Writing $J_0^D(M)$ for the Jacobian variety of $X_0^D(M)$, one can define a map

$$X_0^D(M) \longrightarrow J_0^D(M) \otimes \mathbb{Q}$$

by sending a point $x \in X_0^D(M)$ to the class $[x] - \xi$. Multiplying this map by a suitable integer $m \gg 0$ gives a finite embedding

$$\zeta : X_0^D(M) \longrightarrow J_0^D(M) \tag{17}$$

defined over $\mathbb{Q}$ (cf. [9, §3.5]), which we fix once and for all.

Choose a parametrization

$$J_0^D(M) \longrightarrow E$$

defined over $\mathbb{Q}$, whose existence is guaranteed by the modularity of E and (when $D > 1$) the Jacquet–Langlands correspondence. Denote by

$$\pi_E : X_0^D(M) \longrightarrow E,$$

the surjective morphism over $\mathbb{Q}$ obtained by pre-composing the parametrization above with the map ζ defined either in (16) or in (17). Let now d_E be the degree of π_E, and if T is a finite set of prime numbers write $\mathbb{Z}_T$ for the localization of $\mathbb{Z}$ in which the primes in T are inverted. Throughout this article we fix a (minimal) finite set of primes S such that

- all prime divisors of $6d_E$ belong to S;

- the $\mathbb{Z}_S$-module $H_1\big(X_0^D(M),\mathbb{Z}_S\big)_f$ is torsion-free.

The universal coefficient theorem for homology ensures that this can actually be done. Then push-forward gives an isomorphism

$$\pi_{E,*} : H_1\big(X_0^D(M),\mathbb{Z}_S\big)_f \xrightarrow{\simeq} H_1(E,\mathbb{Z}_S). \tag{18}$$

Remark 4.3. Although – in order to make our choice somewhat more canonical – the set S is taken to be minimal, enlarging S does not affect the above two properties, and so all statements proved remain valid when S is replaced by any set containing it. This freedom of modifying the size of S will be exploited in the proof of Theorem 6.3.

Let $\mathcal{H}$ be the complex upper half-plane and let $\Pi : \mathcal{H} \to X_0^D(M)$ be the canonical surjection. For every point $z_0 \in \mathcal{H}$ there is a group homomorphism

$$\Gamma_0^D(M) \longrightarrow \pi_1\big(X_0^D(M), \Pi(z_0)\big) \tag{19}$$

defined by the following recipe: if $\gamma \in \Gamma_0^D(M)$ and $\alpha : [0,1] \to \mathcal{H}$ is a path from z_0 to $\gamma(z_0)$ then the map (19) sends γ to the (strict) homotopy class of the loop $\Pi \circ \alpha$ around $\Pi(z_0)$. Since $\mathcal{H}$ is simply connected, this class does not depend on the choice of α.

By Hurewicz's theorem, the abelianization of $\pi_1\big(X_0^D(M),\Pi(z_0)\big)$ is canonically isomorphic to $H_1\big(X_0^D(M),\mathbb{Z}\big)$, hence there is a group homomorphism

$$[\,\cdot\,] : \Gamma_0^D(M) \longrightarrow H_1\big(X_0^D(M),\mathbb{Z}_S\big)$$

which is independent of the choice of the base point z_0 in $\mathcal{H}$.

Recall the elements $\gamma_\sigma \in \Gamma_0^D(M)$ with $\sigma \in G_c$ that were introduced in §4.2. Since the group $H_1\big(X_0^D(M),\mathbb{Z}_S\big)$ is abelian, for each $\sigma \in G_c$ the homology class $[\gamma_\sigma]$ does not depend on the representative ψ_σ of the $\Gamma_0^D(M)$-conjugacy class of (oriented) optimal embeddings in terms of which γ_σ was defined (cf. equation (13)).

Let now $\varepsilon \in R^\times$ be a unit of norm -1 and let τ denote the involution on $\mathcal{H}$ given by $z \mapsto \varepsilon(\bar z)$ where $\bar z$ is the conjugate of the complex number z. Since $\Gamma_0^D(M)$ is a normal subgroup of $R^\times$, the map τ descends to an involution on $X_0^D(M)$ by the formula

$$\Pi(z)^\tau = \Pi\big(\varepsilon(\bar z)\big) \tag{20}$$

for all $z \in \mathcal{H}$; according to Shimura, this action does not depend on the choice of an ε as above and coincides with the natural action of complex conjugation on the Riemann surface $X_0^D(M)$ (see, e.g., [31] for details).

The rule (20) induces an action of τ on the homology of $X_0^D(M)$. With notation as in (9), by definition of the homomorphism $[\,\cdot\,]$, for all $\gamma \in \Gamma_0^D(M)$ one has

$$[\gamma]^\tau = [\gamma^*] \tag{21}$$

in $H_1\big(X_0^D(M),\mathbb{Z}_S\big)$. The involution τ restricts to a permutation of the subset $\big\{[\gamma_\sigma]\big\}_{\sigma\in G_c}$; the understanding of this permutation provided by equation (14) will be crucial for our definition of the algebraic part of $L_K(E,\chi,1)$.

4.4. **The algebraic part.** Here we introduce the algebraic part of the special value of $L_K(E,\chi,s)$ at the critical point $s=1$. Set

$$I_\chi := \sum_{\sigma\in G_c} \chi^{-1}(\sigma)[\gamma_\sigma] \in H_1\big(X_0^D(M),\mathbb{Z}[\chi]_S\big).$$

Since the $[\gamma_\sigma]$ do not depend on z_0 in $\mathcal{H}$, the cycle I_χ is independent of z_0. Consider the push-forward

$$I_{\chi,E} := \pi_{E,*}(I_\chi) \in H_1(E,\mathbb{Z}[\chi]_S),$$

write $H_1\big(X_0^D(M),\mathbb{Z}[\chi]_S\big)^{\pm}$ for the eigenspace of $H_1\big(X_0^D(M),\mathbb{Z}[\chi]_S\big)$ on which the involution τ acts as multiplication by ± 1, and adopt a similar convention for $H_1(E,\mathbb{Z}[\chi]_S)$. Since the morphism π_E is defined over $\mathbb{Q}$, one has

$$I_\chi \in H_1\big(X_0^D(M),\mathbb{Z}[\chi]_S\big)^{\epsilon} \implies I_{\chi,E} \in H_1(E,\mathbb{Z}[\chi]_S)^{\epsilon}$$

for $\epsilon \in \{+,-\}$. The reader is suggested to compare our homology cycle $I_{\chi,E}$ with the twisted sum of period integrals $I(f,\chi)$ introduced in [2, p. 191].

The next result says that τ acts either as $+1$ or as -1 on I_χ according to the parity of χ that was introduced in Definition 4.1.

Proposition 4.4. *The cycle I_χ lies in the $+1$-eigenspace (respectively, -1-eigenspace) for τ if χ is even (respectively, odd).*

Proof. Thanks to equality (21) and the conjugacy relation of equation (14), one has

$$\begin{aligned} I_\chi^\tau &= \sum_{\sigma\in G_c} \chi^{-1}(\sigma)[\gamma_\sigma]^\tau = \sum_{\sigma\in G_c} \chi^{-1}(\sigma)[\gamma_\sigma^*] = \sum_{\sigma\in G_c} \chi^{-1}(\sigma)[\gamma_{\sigma_K\sigma}] \\ &= \chi^{-1}(\sigma_K)\cdot\Big(\sum_{\sigma\in G_c}\chi^{-1}(\sigma_K\sigma)[\gamma_{\sigma_K\sigma}]\Big) = \chi(\sigma_K)\cdot\Big(\sum_{\varsigma\in G_c}\chi^{-1}(\varsigma)[\gamma_\varsigma]\Big) \\ &= \chi(\sigma_K) I_\chi, \end{aligned}$$

whence the claim. □

Keeping in mind that $H_1(E,\mathbb{Z})$ identifies with the lattice of periods associated with a Weierstrass equation for E, it can be checked that both $H_1(E,\mathbb{Z}[\chi]_S)^+$ and $H_1(E,\mathbb{Z}[\chi]_S)^-$ are free of rank one over $\mathbb{Z}[\chi]_S$; here we fix canonical generators α_E^+ and α_E^- of these two eigenspaces over $\mathbb{Z}[\chi]_S$ as described in [26, §2.2].

Now suppose that $I_\chi \in H_1\big(X_0^D(M),\mathbb{Z}[\chi]_S\big)^{\epsilon}$ with $\epsilon\in\{+,-\}$: by Proposition 4.4, the nature of ϵ depends on the parity of χ. Let $\mathcal{L}_K(E,\chi,1)_S$ be the unique element of $\mathbb{Z}[\chi]_S$ such that the equality

$$I_{\chi,E} = \mathcal{L}_K(E,\chi,1)_S\cdot\alpha_E^{\epsilon} \tag{22}$$

holds in $H_1(E,\mathbb{Z}[\chi]_S)$.

Definition 4.5. The element $\mathcal{L}_K(E,\chi,1)_S\in\mathbb{Z}[\chi]_S$ appearing in (22) is the *algebraic part* of $L_K(E,\chi,1)$.

Since the finite set S has been fixed once and for all, from here on we drop the dependence of the algebraic part of $L_K(E,\chi,1)$ on S from the notation and simply write $\mathcal{L}_K(E,\chi,1)$ in place of $\mathcal{L}_K(E,\chi,1)_S$.

Before we proceed to crucial considerations on the vanishing of $L_K(E,\chi,1)$, a few comments are in order.

Remark 4.6. By construction, I_χ naturally belongs to the submodule $H_1\big(X_0^D(M),\mathbb{Z}[\chi]\big)$. In fact, as in [5], the need to localize at S will become evident only later, but for clarity of exposition we decided to introduce the required formalism at the outset of our work.

Remark 4.7. The definition of the algebraic part of the special value $L_K(E,\chi,1)$ given by Bertolini, Darmon and Dasgupta in [5] is slightly different. In fact, $\mathcal{L}_K(E,\chi,1)$ is defined in [5, Section 2] to be the natural image of I_χ in $H_1\big(X_0^D(M),\mathbb{Z}[\chi]_S\big)_f$ (note, however, that the authors of *loc. cit.* only consider the classical case of modular curves, with $c=1$ and trivial χ). On the other hand, tensoring the isomorphism in (18) with $\mathbb{Z}[\chi]_S$ over $\mathbb{Z}_S$ shows that the two definitions of $\mathcal{L}_K(E,\chi,1)$ are essentially equivalent.

4.5. **Vanishing of the special value.** The goal of this subsection is to prove that the special value of $L_K(E,\chi,s)$ vanishes exactly when its algebraic part does. This is a consequence of a result proved by Popa in [27, Section 5] and reformulated in more classical terms in [27, Section 6] when $D=1$ and χ is unramified. In this special case, Popa's computations are based on a very explicit description of a bijection between suitable ideal classes and conjugacy classes of optimal embeddings. While it seems difficult to exhibit such an explicit correspondence when $D>1$, Proposition 4.2 provides sufficient information to allow for a "classical" formulation of Popa's theorem in the general setting as well.

The result we are interested in is the following

Theorem 4.8 (Popa)**.** *The special value $L_K(E,\chi,1)$ is non-zero if and only if $\mathcal{L}_K(E,\chi,1)$ is non-zero.*

Proof. As already remarked, this is a consequence of the formula for $L_K(E,\chi,1)$ proved by Popa in [27]. Since the results of Popa are expressed in the adelic language of automorphic representations, we explain how to deduce the theorem in the formulation that is convenient for our purposes. In fact, in equality (27) we give an explicit formula for $L_K(E,\chi,1)$ when the character χ is not necessarily trivial; in doing this, we freely use the notation of [27].

First of all, observe that, due to the normalization commonly adopted in automorphic-theoretic contexts (cf. [20, §5.14]), the special value of $L_K(E,\chi,s)$ at $s=1$ corresponds to $L(1/2,\pi_f\times\pi_\chi)$ in [27]. As recalled in §4.2, the $\Gamma_0^D(M)$-conjugacy classes of oriented optimal embeddings of $\mathcal{O}_c$ into R are in bijection with the elements of the Galois group G_c. With arguments analogous to those exposed in [27, Section 6], if $\omega_f := 2\pi i f(z)dz$ is the differential on $X_0^D(M)$ associated with f one then obtains an equality

$$|l(\phi_f)|^2 = \left|\sum_{\sigma\in G_c}\chi^{-1}(\sigma)\int_{z_0}^{\gamma_\sigma(z_0)} f(z)dz\right|^2 = \left|\int_{I_\chi}\omega_f\right|^2 \tag{23}$$

where l is a certain linear form on a suitable space of automorphic forms (see [27, p. 852]) and ϕ_f is the automorphic form on $\mathrm{GL}_2(\mathbb{A})$ which can be attached to f as in [27, p. 857]. Equality (23) is the analogue (with $k=1$) of the formula given, in the split case, in [27, p. 862] for an unramified χ (in this setting, see also [27, Theorem 6.3.1], which provides a formulation of Popa's results suitable for the arithmetic applications of [5]). Now [27, Theorem 5.3.9] with $k=1$ asserts that there is a non-zero constant Ω (denoted by C in *loc. cit.*) such that

$$L_K(E,\chi,1) = \frac{\Omega N c^2}{\sqrt{\delta_K}}\prod_{\ell\mid Nc}\Big(1+\frac{1}{\ell}\Big)|l(\phi_f)|^2; \tag{24}$$

the explicit expression of Ω in the case where $c=1$ can be found in [27, §5.4].

Combining equations (23) and (24) yields immediately the formula

$$L_K(E,\chi,1) = \frac{\Omega M c^2}{\sqrt{\delta_K}}\prod_{\ell\mid Mc}\Big(1+\frac{1}{\ell}\Big)\left|\int_{I_\chi}\omega_f\right|^2, \tag{25}$$

and the claim of the theorem follows from (25) by passing to the push-forward

$$I_{\chi,E} = \pi_{E,*}(I_\chi)\in H_1(E,\mathbb{Z}[\chi]_S).$$

Namely, let ω_E be a Néron differential on the Néron model of E over $\mathbb{Z}$; by [34, Theorem 5.6], there is an equality

$$\pi_E^*(\omega_E) = c(\pi_E)\omega_f$$

with $c(\pi_E)\in\mathbb{C}^\times$; then one has

$$c(\pi_E)\int_{I_\chi}\omega_f = \int_{I_{\chi,E}}\omega_E = \mathcal{L}_K(E,\chi,1)\int_{\alpha_E^\epsilon}\omega_E \tag{26}$$

where $\epsilon \in \{+,-\}$ and $I_\chi \in H_1\big(X_0^D(M),\mathbb{Z}[\chi]_S\big)^\epsilon$. Finally, combining (25) and (26) gives the equality

$$L_K(E,\chi,1) = \big|\mathcal{L}_K(E,\chi,1)\big|^2 \cdot \frac{\Omega M c^2}{c(\pi_E)^2\sqrt{\delta_K}} \prod_{\ell \mid Mc}\Big(1+\frac{1}{\ell}\Big)\Big|\int_{\alpha_E^\epsilon}\omega_E\Big|^2, \tag{27}$$

and the theorem is proved. □

5. Admissible primes relative to f and p

For any prime number q fix an isomorphism $E[q] \simeq (\mathbb{Z}/q\mathbb{Z})^2$ by choosing a basis of $E[q]$ over $\mathbb{Z}/q\mathbb{Z}$ and let

$$\rho_{E,q} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$$

be the representation of $G_{\mathbb{Q}}$ acting on $E[q]$.

5.1. **Choice of p.** Here we introduce the restrictions on the prime numbers p under which we will prove our main results; they are analogous to those made in [23, Assumption 4.1]. Before doing this, recall the finite set of primes S of §4.3, the algebraic part $\mathcal{L}_K(E,\chi,1) \in \mathbb{Z}[\chi]_S$ introduced in §4.4 and the prime r appearing in Definition 3.1. Finally, fix an integer C as in Theorem 2.2.

Assumption 5.1. Suppose that $L_K(E,\chi,1) \neq 0$. Then

(1) $p \notin S$;
(2) $p \nmid 2cNC\delta_K h^+(c)(r+1-a_r)$;
(3) the Galois representation $\rho_{E,p}$ is surjective;
(4) the image of $\mathcal{L}_K(E,\chi,1)$ in the quotient $\mathbb{Z}[\chi]_S/p\mathbb{Z}[\chi]_S$ is not zero;
(5) $p \nmid |E(H_{c,\mathfrak{q}})_{\mathrm{tors}}|$ where $H_{c,\mathfrak{q}}$ is the completion of H_c at a prime $\mathfrak{q}$ dividing DM.

The "open image theorem" of Serre ([30]) ensures that condition 3 is satisfied for all but finitely many primes p, while the torsion subgroup of $E(H_{c,\mathfrak{q}})$ is finite by a well-known theorem of Lutz ([24]); moreover, condition 4 excludes only a finite number of primes p since $\mathcal{L}_K(E,\chi,1) \neq 0$ by Theorem 4.8. As a consequence, Assumption 5.1 is fulfilled by almost all prime numbers p. Observe that, in order to avoid ambiguities, the condition $L_K(E,\chi,1) \neq 0$ will always explicitly appear in the statements of our results.

Remark 5.2. Condition 5 in Assumption 5.1 is introduced in order to "trivialize" the image of the local Kummer map at primes of bad reduction for E. The reader is referred to, e.g., [18] to see how one could relax Assumption 5.1 by imposing suitable local conditions at these primes too.

5.2. **Admissible primes.** Let p be the prime number chosen in §5.1 and recall the quaternionic modular form f of weight 2 on $\Gamma_0^D(M)$ associated with E by the Jacquet–Langlands correspondence. Following [5, §3.3] (see also [3, §2] and [23, §4.2] for an analogous definition in the imaginary quadratic setting), we say that a prime number ℓ is *admissible relative to f and p* (or *p-admissible*, or even simply *admissible*) if it satisfies the following conditions:

(1) $\ell \nmid Npc$;
(2) the support of $\Gamma_\ell^{\mathrm{ab}}$ is contained in the set of prime divisors of $C\ell$;
(3) ℓ is inert in K;
(4) $p \nmid \ell^2-1$;
(5) $p|(\ell+1)^2 - a_\ell^2$.

Note that, thanks to Theorem 2.2, the first two conditions exclude only a finite number of primes ℓ. Moreover, as a consequence of condition 2 in Assumption 5.1, the prime p does not divide the exponent t_ℓ of $\Gamma_\ell^{\mathrm{ab}}$ for all admissible primes ℓ.

For every admissible prime ℓ choose once and for all a prime λ_0 of H_c above ℓ (we will never deal with more than one admissible prime at the same time, so ignoring the dependence of λ_0 on ℓ should cause no confusion). Since admissible primes are inert in K and do not divide c, if ℓ is such a prime then $\ell\mathcal{O}_K$ splits completely in H_c, hence there are exactly $h^+(c)$ primes of H_c above ℓ. The choice of λ_0 allows us to fix an explicit bijection between G_c and the set of these primes via the rule

$$\sigma \in G_c \longmapsto \sigma(\lambda_0). \tag{28}$$

The inverse to this bijection will be denoted

$$\lambda \longmapsto \sigma_\lambda \in G_c,$$

so that $\sigma_\lambda(\lambda_0) = \lambda$. Finally, an element $\sigma \in G_c$ acts on the group rings $\mathbb{Z}[G_c]$ and $\mathbb{Z}/p\mathbb{Z}[G_c]$ in the natural way by multiplication on group-like elements (that is, $\gamma \mapsto \sigma\gamma$ for all $\gamma \in G_c$).

Lemma 5.3. *Let ℓ be an admissible prime relative to f and p. The local cohomology groups $H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])$ and $H^1_{\mathrm{sing}}(H_{c,\ell}, E[p])$ are both isomorphic to $\mathbb{Z}/p\mathbb{Z}[G_c]$ as $\mathbb{Z}[G_c]$-modules.*

Proof. Since $p \nmid \ell^2 - 1$, one can mimic the proof of [3, Lemma 2.6] and show that the groups $H^1_{\mathrm{fin}}(K_\ell, E[p])$ and $H^1_{\mathrm{sing}}(K_\ell, E[p])$ are both isomorphic to $\mathbb{Z}/p\mathbb{Z}$. But the prime ideal $\ell\mathcal{O}_K$ of $\mathcal{O}_K$ splits completely in H_c, hence $H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])$ and $H^1_{\mathrm{sing}}(H_{c,\ell}, E[p])$ are both isomorphic to $\mathbb{Z}/p\mathbb{Z}[G_c]$ as $\mathbb{F}_p$-vector spaces. Finally, bijection (28) establishes isomorphisms which are obviously G_c-equivariant. □

For $\star \in \{\mathrm{fin}, \mathrm{sing}\}$ we fix once and for all isomorphisms

$$H^1_\star(K_\ell, E[p]) \simeq \mathbb{Z}/p\mathbb{Z}$$

which will often be viewed as identifications according to convenience.

The next result is the counterpart of [23, Proposition 4.5]. In fact, since the group $\mathrm{Gal}\,(H_c/\mathbb{Q})$ is generalized dihedral, with the non-trivial element ρ of $\mathrm{Gal}\,(K/\mathbb{Q})$ acting on the abelian normal subgroup G_c by

$$\sigma \longmapsto \rho\sigma\rho^{-1} = \sigma^{-1},$$

the proof of [23, Proposition 4.5] is valid *mutatis mutandis* in our present context as well.

Proposition 5.4. *Let s be a non-zero element of $H^1(H_c, E[p])$. For every $\delta \in \{\pm 1\}$ there are infinitely many admissible primes ℓ such that p divides $a_\ell + \delta(\ell+1)$ and $\mathrm{res}_\ell(s) \neq 0$.*

The existence result of Proposition 5.4 will be crucially exploited in §8.5 to show the vanishing of Selmer groups which is one of the goals of this paper.

6. Level raising and Galois representations

In this section we prove a level raising result modulo p at admissible primes (Theorem 6.3) and an isomorphism between certain Galois representations over $\mathbb{F}_p$ attached to $J_\epsilon^{(\ell)}$ and E (Theorem 6.4).

6.1. **Raising the level in one admissible prime.** As in Section 3, fix a prime $\ell \nmid DM$ and a character $\chi \in \widehat{G}_c$ whose parity is denoted by ϵ. Recall the modular eigenform f for $\Gamma_0^D(M)$ introduced in Section 4 and the homomorphism $\varphi_f : \mathbb{T}_M \to \mathbb{Z}$ of (15). Write

$$\bar{\varphi}_f : \mathbb{T}_M \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

for the composition of φ_f with the projection $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ and denote by $\mathfrak{m}_f$ its kernel, so that $\mathfrak{m}_f = I_f + (p)$ where $I_f = \ker(\varphi_f)$.

As is well known, π^* is injective and this allows us to identify $H_1\big(X_0^D(M), \mathbb{Z}_S\big)^2$ with the submodule $\mathrm{im}(\pi^*)$ of $H_1\big(X_0^D(M\ell), \mathbb{Z}_S\big)$, which is stable under the action of $\mathbb{T}_{M\ell}$; this provides

$H_1\big(X_0^D(M),\mathbb{Z}_S\big)^2$ with a natural structure of $\mathbb{T}_{\ell M}$-module. More precisely, π^* is equivariant for the actions of T_q, t_q for primes $q\nmid M\ell$ and of U_q, u_q for primes $q|M$, while it intertwines the actions of $\left(\begin{smallmatrix} T_\ell & -1 \\ \ell & 0\end{smallmatrix}\right)$ on the domain and of u_ℓ on the codomain.

Thanks to [22, Lemma 6.2], the natural inclusion $\ker(\pi_*)\subset H_1\big(X_0^D(M),\mathbb{Z}\big)^2_\epsilon$ induces an injection $\ker(\pi_*)\hookrightarrow\mathrm{coker}(\pi^*)$, so we may consider the $\mathbb{Z}$- and $\mathbb{Z}_S$-modules

$$\Phi_\ell := \mathrm{coker}(\pi^*)/\ker(\pi_*), \qquad \Phi_{\ell,S} := \Phi_\ell\otimes\mathbb{Z}_S,$$

respectively, which are endowed with canonical structures of $\mathbb{T}_{M\ell}$-modules and, again by [22, Lemma 6.2], have finite cardinality.

For any abelian group M endowed with an action of the involution τ, let $M_\pm$ denote the maximal quotient of M on which τ acts as ±1. Since the maps π_1 and π_2 of Section 3 are defined over $\mathbb{Q}$, if $\epsilon\in\{+,-\}$ then there are morphisms

$$\pi_\epsilon^*: H_1\big(X_0^D(M),\mathbb{Z}\big)^2_\epsilon\to H_1\big(X_0^D(M\ell),\mathbb{Z}\big)_\epsilon, \quad \pi_{*,\epsilon}: H_1\big(X_0^D(M\ell),\mathbb{Z}\big)_\epsilon\to H_1\big(X_0^D(M),\mathbb{Z}\big)^2_\epsilon$$

and an equality $\Phi_{\ell,\epsilon}=\mathrm{coker}(\pi_\epsilon^*)/\ker(\pi_{*,\epsilon})$.

By a slight abuse of notation, from here on we will use the symbols π_* and π^* to denote also the analogues with $\mathbb{Z}_S$-coefficients of the maps of Section 3. For any congruence subgroup G let $S_2(G)$ denote the $\mathbb{C}$-vector space of weight 2 cusp forms on G. Write $\mathbb{T}_{M\ell}^{\ell\text{-old}}$ and $\mathbb{T}_{M\ell}^{\ell\text{-new}}$ for the quotients of $\mathbb{T}_{M\ell}$ acting faithfully, respectively, on the image $S_2^{\ell\text{-old}}\big(\Gamma_0^D(M\ell)\big)$ of the degeneracy map

$$S_2\big(\Gamma_0^D(M)\big)\oplus S_2\big(\Gamma_0^D(M)\big)\longrightarrow S_2\big(\Gamma_0^D(M\ell)\big)$$

and on its orthogonal complement with respect to the Petersson scalar product. We keep the notations T_q and U_q to denote Hecke operators in $\mathbb{T}_M$, while t_q and u_q will be used for those in $\mathbb{T}_{M\ell}$.

Let $\mathfrak{m}_f'$ denote the ideal of $\mathbb{T}_{M\ell}$ generated by t_q-a_q for primes $q\nmid M\ell$, u_q-a_q for primes $q|M$, $u_\ell-\delta$ and the prime p. Tensoring π_* and π^* with $\mathbb{T}_{M\ell}/\mathfrak{m}_f'$ over $\mathbb{T}_{M\ell}$ we obtain maps

$$\bar\pi^*: H_1\big(X_0^D(M),\mathbb{Z}_S\big)^2/\mathfrak{m}_f'\longrightarrow H_1\big(X_0^D(M\ell),\mathbb{Z}_S\big)/\mathfrak{m}_f'$$

and

$$\bar\pi_*: H_1\big(X_0^D(M\ell),\mathbb{Z}_S\big)/\mathfrak{m}_f'\longrightarrow H_1\big(X_0^D(M),\mathbb{Z}_S\big)^2/\mathfrak{m}_f'.$$

Lemma 6.1. *The map $\bar\pi_*$ is surjective.*

Proof. As in the proof of Proposition 2.1, there is an exact sequence

$$0\longrightarrow\ker(\pi_*)\longrightarrow H_1\big(X_0^D(M\ell),\mathbb{Z}_S\big)\xrightarrow{\pi_*}H_1\big(X_0^D(M),\mathbb{Z}_S\big)^2\longrightarrow\Gamma_\ell^{\mathrm{ab}}\otimes\mathbb{Z}_S\longrightarrow0.$$

Since the image of π_* is stable under $\mathbb{T}_{M\ell}$, the group $\Gamma_\ell^{\mathrm{ab}}\otimes\mathbb{Z}_S$ inherits an action of $\mathbb{T}_{M\ell}$. Since p does not divide the cardinality of $\Gamma_\ell^{\mathrm{ab}}$ and the residual characteristic of $\mathfrak{m}_f'$ is p, we have $\Gamma_\ell^{\mathrm{ab}}/\mathfrak{m}_f'=0$, and the result follows. □

Proposition 6.2. *There is a canonical isomorphism*

$$\mathrm{coker}(\bar\pi_*\circ\bar\pi^*)\simeq\Phi_\ell/\mathfrak{m}_f'.$$

Proof. The module $\Phi_{\ell,S}$ is the quotient of $\mathrm{coker}(\pi^*)$ by $\ker(\pi_*)$, so it is isomorphic to the quotient of $H_1(X_0^D(M\ell),\mathbb{Z}_S)$ by the $\mathbb{Z}_S$-submodule generated by $\ker(\pi_*)$ and $\mathrm{im}(\pi^*)$. Hence there is an exact sequence

$$\langle\ker(\pi_*),\mathrm{im}(\pi^*)\rangle/\mathfrak{m}_f'\longrightarrow H_1\big(X_0^D(M\ell),\mathbb{Z}_S\big)/\mathfrak{m}_f'\longrightarrow\Phi_{\ell,S}/\mathfrak{m}_f'\longrightarrow0 \tag{29}$$

Thanks to Lemma 6.1, there is also an exact sequence

$$\ker(\pi_*)/\mathfrak{m}_f'\longrightarrow H_1\big(X_0^D(M\ell),\mathbb{Z}_S\big)/\mathfrak{m}_f'\xrightarrow{\bar\pi_*}H_1\big(X_0^D(M),\mathbb{Z}_S\big)^2/\mathfrak{m}_f'\longrightarrow0.$$

We conclude that $\bar\pi_*$ induces an isomorphism

$$\bar\pi_* : \big(H_1(X_0^D(M\ell),\mathbb{Z}_S)/\mathfrak{m}_f'\big)/\langle\ker(\bar\pi_*),\mathrm{im}(\bar\pi^*)\rangle \xrightarrow{\simeq} \mathrm{coker}(\bar\pi_*\circ\bar\pi^*). \tag{30}$$

Since $\langle\ker(\bar\pi_*),\mathrm{im}(\bar\pi^*)\rangle$ is equal to the image of $\langle\ker(\pi_*),\mathrm{im}(\pi^*)\rangle/\mathfrak{m}_f'$ in $H_1\big(X_0^D(M\ell),\mathbb{Z}_S\big)/\mathfrak{m}_f'$ via the first map in (29), this shows that $\mathrm{coker}(\bar\pi_*\circ\bar\pi^*)$ is isomorphic to $\Phi_{\ell,S}/\mathfrak{m}_f'$. Finally, since $p\notin S$ the groups $\Phi_{\ell,S}/\mathfrak{m}_f'$ and $\Phi_\ell/\mathfrak{m}_f'$ are canonically identified, whence the claim. □

Now we can prove the main result of this subsection.

Theorem 6.3. *Suppose that ℓ is an admissible prime such that $p|a_\ell-\delta(\ell+1)$ for a suitable $\delta\in\{+1,-1\}$. There exists a morphism*

$$f_\ell : \mathbb{T}_{M\ell}^{\ell\text{-}new} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

such that

- *$f_\ell(t_q)=a_q \pmod p$ for all primes $q\nmid M\ell$;*
- *$f_\ell(u_q)=a_q \pmod p$ for all primes $q|M$;*
- *$f_\ell(u_\ell)=\delta \pmod p$.*

If $\mathfrak{m}_{f_\ell}$ denotes the kernel of f_ℓ then there is a group isomorphism

$$\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \xrightarrow{\simeq} H_1(E,\mathbb{Z})_\epsilon/pH_1(E,\mathbb{Z})_\epsilon \simeq \mathbb{Z}/p\mathbb{Z}. \tag{31}$$

Proof. At the cost of enlarging S, in this proof we assume that $\ell+1$ is invertible in $\mathbb{Z}_S$ (cf. Remark 4.3). Then, since $\pi_*\circ\pi^*=\left(\begin{smallmatrix}\ell+1 & T_\ell\\ T_\ell & \ell+1\end{smallmatrix}\right)$, the assignment $(m,n)\mapsto(\ell+1)m-T_\ell(n)$ induces an isomorphism of groups

$$H_1\big(X_0^D(M),\mathbb{Z}_S\big)^2/\mathrm{im}(\pi_*\circ\pi^*) \xrightarrow{\simeq} H_1\big(X_0^D(M),\mathbb{Z}_S\big)/\big(T_\ell^2-(\ell+1)^2\big) \tag{32}$$

which is equivariant for the action of the Hecke operators t_q (respectively, T_q) for $q\nmid N\ell$ and u_q (respectively, U_q) for $q|M$ on the left-hand (respectively, right-hand) side. Since u_ℓ acts as $\left(\begin{smallmatrix}T_\ell & -1\\ \ell & 0\end{smallmatrix}\right)$ on $H_1(X_0^D(M),\mathbb{Z}_S)^2$, we see that $x\in H_1\big(X_0^D(M),\mathbb{Z}_S\big)/pH_1\big(X_0^D(M),\mathbb{Z}_S\big)$ is an eigenvector for T_ℓ with eigenvalue $a_\ell\equiv\delta(\ell+1) \pmod p$ if and only if $(x,\delta\ell x)$ is an eigenvector for u_ℓ with eigenvalue δ. Thanks to this and (32), we find an isomorphism of groups

$$\mathrm{coker}(\pi_*\circ\pi^*)/\mathfrak{m}_f' \xrightarrow{\simeq} H_1\big(X_0^D(M),\mathbb{Z}_S\big)/\mathfrak{m}_f. \tag{33}$$

Since $\mathrm{coker}(\pi_*\circ\pi^*)/\mathfrak{m}_f'$ and $\mathrm{coker}(\bar\pi_*\circ\bar\pi^*)$ are canonically isomorphic, Proposition 6.2 yields an isomorphism of groups

$$\Phi_\ell/\mathfrak{m}_f' \xrightarrow{\simeq} H_1\big(X_0^D(M),\mathbb{Z}_S\big)/\mathfrak{m}_f. \tag{34}$$

It is now immediate to check that there is a canonical isomorphism

$$H_1\big(X_0^D(M),\mathbb{Z}_S\big)/\mathfrak{m}_f \simeq H_1\big(X_0^D(M),\mathbb{Z}_S\big)_f/pH_1\big(X_0^D(M),\mathbb{Z}_S\big)_f.$$

By (18), the group $H_1\big(X_0^D(M),\mathbb{Z}_S\big)_f$ is isomorphic to $H_1(E,\mathbb{Z}_S)$. Since $p\notin S$, isomorphism (34) induces an isomorphism of groups

$$\Phi_\ell/\mathfrak{m}_f' \xrightarrow{\simeq} H_1(E,\mathbb{Z})/pH_1(E,\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^2.$$

All the maps involved are equivariant for the action of τ, so we get yet another isomorphism

$$\Phi_{\ell,\epsilon}/\mathfrak{m}_f' \xrightarrow{\simeq} H_1(E,\mathbb{Z})_\epsilon/pH_1(E,\mathbb{Z})_\epsilon \simeq \mathbb{Z}/p\mathbb{Z}.$$

The action of $\mathbb{T}_{M\ell}$ on Φ_ℓ is through its ℓ-new quotient, so $\mathfrak{m}_f'$ is fact belongs to $\mathbb{T}_{M\ell}^{\ell\text{-new}}$. Since $\Phi_\ell/\mathfrak{m}_f'$ is a one-dimensional $\mathbb{F}_p$-vector space, the action of $\mathbb{T}_{M\ell}^{\ell\text{-new}}$ is given by a character $f_\ell:\mathbb{T}_{M\ell}^{\ell\text{-new}}\to\mathbb{Z}/p\mathbb{Z}$ whose kernel is $\mathfrak{m}_{f_\ell}$, as was to be proved. □

6.2. **Galois representations.** In this subsection we show the existence of an isomorphism of $G_{\mathbb{Q}}$-modules $J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell} \simeq E[p]$ and of an isomorphism of groups $\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \simeq H^1_{\mathrm{sing}}(K_\ell, E[p])$. Our arguments are inspired by those in [3, §5.6]. We fix an admissible prime ℓ and we suppose that $p \mid a_\ell - \delta(\ell+1)$.

Write $G_{K_\ell} := \mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/K_\ell)$ for the absolute Galois group of the local field K_ℓ. Since we are assuming Conjecture 3.3, there is a short exact sequence of left $\mathbb{T}_{M\ell}[G_{K_\ell}]$-modules

$$0 \longrightarrow L_\epsilon \longrightarrow T_\epsilon(\bar{\mathbb{Q}}_\ell) \longrightarrow J_\epsilon^{(\ell)}(\bar{\mathbb{Q}}_\ell) \longrightarrow 0.$$

Since L is a free abelian group and $T_\epsilon(\bar{\mathbb{Q}}_\ell)$ is divisible, the snake lemma implies that there is a short exact sequence of $\mathbb{T}_{M\ell}[G_{K_\ell}]$-modules

$$0 \longrightarrow T_\epsilon[p] \longrightarrow J_\epsilon^{(\ell)}[p] \longrightarrow L_\epsilon/p \longrightarrow 0 \tag{35}$$

where $T_\epsilon[p]$ and $J_\epsilon^{(\ell)}[p]$ are the p-torsion subgroups of $T_\epsilon(\bar{\mathbb{Q}}_\ell)$ and $J_\epsilon^{(\ell)}(\bar{\mathbb{Q}}_\ell)$, respectively. By tensoring the above exact sequence with $\mathbb{T}_{M\ell}/\mathfrak{m}_{f_\ell}$ over $\mathbb{T}_{M\ell}$, and recalling that $p \in \mathfrak{m}_{f_\ell}$, we find an exact sequence of $\mathbb{T}_{M\ell}/\mathfrak{m}_{f_\ell}[G_{K_\ell}]$-modules

$$0 \longrightarrow \big(T_\epsilon[p]/\mathfrak{m}_{f_\ell}\big)/M \longrightarrow J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell} \longrightarrow L_\epsilon/\mathfrak{m}_{f_\ell} \longrightarrow 0$$

for a certain $\mathbb{T}_{M\ell}/\mathfrak{m}_{f_\ell}[G_{K_\ell}]$-submodule M of $T_\epsilon[p]/\mathfrak{m}_{f_\ell}$. Taking G_{K_ℓ}-cohomology of the above exact sequence yields an exact sequence of $\mathbb{T}_{M\ell}/\mathfrak{m}_{f_\ell}$-modules

$$L_\epsilon/\mathfrak{m}_{f_\ell} \longrightarrow H^1\big(K_\ell, (T_\epsilon[p]/\mathfrak{m}_{f_\ell})/M\big) \longrightarrow H^1\big(K_\ell, J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell}\big) \longrightarrow H^1(K_\ell, L_\epsilon/\mathfrak{m}_{f_\ell}). \tag{36}$$

We first study the last term in (36). Let $\mathbb{Q}_\ell^{\mathrm{ab}}$ be the maximal abelian extension of $\mathbb{Q}_\ell$; since $L_\epsilon/\mathfrak{m}_{f_\ell}$ is abelian and defined over K_ℓ, the cohomology group $H^1(K_\ell, L_\epsilon/\mathfrak{m}_{f_\ell})$ is equal to the group of continuous homomorphisms $\mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}\,(\mathbb{Q}_\ell^{\mathrm{ab}}/K_\ell), L_\epsilon/\mathfrak{m}_{f_\ell}\big)$. By local class field theory, there is an isomorphism

$$\mathrm{Gal}\,(\mathbb{Q}_\ell^{\mathrm{ab}}/K_\ell) \simeq \hat{\mathbb{Z}} \times \mathcal{O}_{K_\ell}^\times,$$

where $\mathcal{O}_{K_\ell}^\times$ is the group of units in the ring of integers $\mathcal{O}_{K_\ell}$ of K_ℓ and $\hat{\mathbb{Z}} \simeq \mathrm{Gal}\,(\mathbb{Q}_\ell^{\mathrm{unr}}/K_\ell)$ is (isomorphic to) the Galois group of the maximal unramified extension K_ℓ^{unr} of K_ℓ, which is equal to $\mathbb{Q}_\ell^{\mathrm{unr}}$ because the extension $K_\ell/\mathbb{Q}_\ell$ is unramified. Now recall the short exact sequence

$$0 \longrightarrow \mathcal{O}_{K_\ell,1}^\times \longrightarrow \mathcal{O}_{K_\ell}^\times \longrightarrow (\mathcal{O}_{K_\ell}/\ell\mathcal{O}_{K_\ell})^\times \longrightarrow 0$$

where $\mathcal{O}_{K_\ell,1}^\times$ is the group of the elements of $\mathcal{O}_{K_\ell}^\times$ of norm 1. Since $\mathcal{O}_{K_\ell,1}^\times$ is a pro-ℓ-group and $L_\epsilon/\mathfrak{m}_{f_\ell}$ is p-torsion, the group $\mathrm{Hom}_{\mathrm{cont}}(\mathcal{O}_{K_\ell,1}^\times, L_\epsilon/\mathfrak{m}_{f_\ell})$ is trivial, hence

$$\mathrm{Hom}_{\mathrm{cont}}(\mathcal{O}_{K_\ell}^\times, L_\epsilon/\mathfrak{m}_{f_\ell}) = \mathrm{Hom}_{\mathrm{cont}}\big((\mathcal{O}_{K_\ell}/\ell\mathcal{O}_{K_\ell})^\times, L_\epsilon/\mathfrak{m}_{f_\ell}\big) = 0,$$

the second equality being due to the fact that $p \nmid \ell^2 - 1 = |(\mathcal{O}_{K_\ell}/\ell\mathcal{O}_{K_\ell})^\times|$. It follows that there are canonical isomorphisms of groups

$$\begin{aligned}\mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}\,(\mathbb{Q}_\ell^{\mathrm{ab}}/K_\ell), L_\epsilon/\mathfrak{m}_{f_\ell}\big) &\simeq \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}\,(\mathbb{Q}_\ell^{\mathrm{unr}}/K_\ell), L_\epsilon/\mathfrak{m}_{f_\ell}\big)\\ &\simeq \mathrm{Hom}\big(\mathbb{Z}/p\mathbb{Z}, L_\epsilon/\mathfrak{m}_{f_\ell}\big).\end{aligned}$$

Let $\boldsymbol{\mu}_p$ be the group of p-th roots of unity in $\bar{\mathbb{Q}}_\ell$. To study the term $H^1\big(K_\ell, (T_\epsilon[p]/\mathfrak{m}_{f_\ell})/M\big)$ in sequence (36), first recall that T_ϵ is isomorphic to $\mathbb{G}_m \otimes H_\epsilon$, so $T_\epsilon[p]$ is isomorphic to $\boldsymbol{\mu}_p \otimes H_\epsilon$ as a G_{K_ℓ}-module. Since the structure of $\mathbb{T}_{M\ell}$-module on T_ϵ is given by the Hecke action on H_ϵ, there is an isomorphism

$$T_\epsilon[p]/\mathfrak{m}_{f_\ell} \simeq \boldsymbol{\mu}_p \otimes (H_\epsilon/\mathfrak{m}_{f_\ell}).$$

Furthermore, it can be easily seen that there exists a submodule N of $H_\epsilon/\mathfrak{m}_{f_\ell}$ such that the $\mathbb{T}_{M\ell}/\mathfrak{m}_{f_\ell}$-module $(T_\epsilon[p]/\mathfrak{m}_{f_\ell})/M$ is isomorphic to $\boldsymbol{\mu}_p \otimes \big((H_\epsilon/\mathfrak{m}_{f_\ell})/N\big)$. Now, the group G_{K_ℓ} acts trivially on H_ϵ and, as a consequence of Hilbert's Theorem 90, the group $H^1(K_\ell, \boldsymbol{\mu}_p)$ is

isomorphic to $K_\ell^\times/(K_\ell^\times)^p$. Since $p \nmid \ell^2-1$, the quotient $K_\ell^\times/(K_\ell^\times)^p$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. We conclude that there are group isomorphisms

$$H^1\big(K_\ell, (T_\epsilon[p]/\mathfrak{m}_{f_\ell})/M\big) \simeq (H_\epsilon/\mathfrak{m}_{f_\ell})/N \otimes \mathbb{Z}/p\mathbb{Z} \simeq (H_\epsilon/\mathfrak{m}_{f_\ell})/N,$$

the second one being a consequence of the fact that $p \in \mathfrak{m}_{f_\ell}$.

The connecting map in (36), which under the above identifications can be rewritten as $L_\epsilon/\mathfrak{m}_{f_\ell} \to (H_\epsilon/\mathfrak{m}_{f_\ell})/N$, can be explicitly computed as follows. Let $\overline{\ker}(\pi_{*,\epsilon})$ be the projection of $\ker(\pi_{*,\epsilon})$ to H_ϵ. As above, one has

$$H^1(K_\ell, T_\epsilon[p]) \simeq H^1(K_\ell, \boldsymbol{\mu}_p) \otimes H_\epsilon \simeq K_\ell^\times/(K_\ell^\times)^p \otimes H_\epsilon \simeq \mathbb{Z}/p\mathbb{Z} \otimes H_\epsilon \simeq H_\epsilon/p,$$

and the connecting homomorphism $L_\epsilon/p \to H^1(K_\ell, T_\epsilon[p])$ which arises by taking the G_{K_ℓ}-cohomology of sequence (35) can be rewritten as $L_\epsilon/p \to H_\epsilon/p$ and is induced by composing the natural inclusion $L_\epsilon \hookrightarrow T_\epsilon(\mathbb{Q}_\ell)$ with the valuation map

$$\mathrm{ord}_\ell : T_\epsilon(\mathbb{Q}_\ell) = \mathbb{Q}_\ell^\times \otimes H_\epsilon \xrightarrow{\mathrm{ord}_\ell \otimes \mathrm{id}} \mathbb{Z} \otimes H_\epsilon = H_\epsilon.$$

Thanks to [22, Proposition 6.3] and the fact that all the maps involved are equivariant for the action of τ, we have $\mathrm{ord}_\ell(L_\epsilon) = t_r\big(\overline{\ker}(\pi_{*,\epsilon})\big)$ where $t_r := T_r - r - 1$.

Since the Galois action commutes with the Hecke action, it follows that the image of the connecting homomorphism $L_\epsilon/\mathfrak{m}_{f_\ell} \to (H_\epsilon/\mathfrak{m}_{f_\ell})/N$ is $t_r\big(\overline{\ker}(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}\big)$. The endomorphism t_r of $\overline{\ker}(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}$ is just multiplication by the reduction modulo p of $a_r - (r+1)$, which is an isomorphism because $p \nmid a_r - (r+1)$ by Assumption 5.1. Hence t_r takes $\overline{\ker}(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}$ isomorphically onto its image and induces an isomorphism

$$(H_\epsilon/\mathfrak{m}_{f_\ell})\big/\big(\overline{\ker}(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}\big) \xrightarrow{\simeq} (H_\epsilon/\mathfrak{m}_{f_\ell})/t_r\big(\overline{\ker}(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}\big).$$

Now recall that, by definition, $\Phi_{\ell,\epsilon} := \mathrm{coker}(f_\epsilon^*)/\ker(\pi_{*,\epsilon})$, so $\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell}$ is isomorphic to the quotient of $\mathrm{coker}(f_\epsilon^*)/\mathfrak{m}_{f_\ell}$ by the image of $\ker(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}$. This last quotient maps surjectively onto $(H_\epsilon/\mathfrak{m}_{f_\ell})\big/\big(\overline{\ker}(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}\big)$ and thus there exists a canonical surjective homomorphism

$$\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \twoheadrightarrow (H_\epsilon/\mathfrak{m}_{f_\ell})/t_r\big(\overline{\ker}(\pi_{*,\epsilon})/\mathfrak{m}_{f_\ell}\big).$$

The exact sequence of $\mathbb{T}_{M\ell}/\mathfrak{m}_{f_\ell}$-modules (36) can therefore be rewritten as

$$0 \longrightarrow \Psi \longrightarrow H^1\big(K_\ell, J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell}\big) \longrightarrow \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}\,(\mathbb{Q}_\ell^{\mathrm{unr}}/K_\ell), L_\epsilon/\mathfrak{m}_{f_\ell}\big) \tag{37}$$

where Ψ is a suitable quotient of $\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell}$.

Theorem 6.4. (1) *The $G_\mathbb{Q}$-modules $J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell}$ and $E[p]$ are isomorphic.*
(2) *The groups $\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell}$ and $H^1_{\mathrm{sing}}(K_\ell, E[p])$ are isomorphic.*
(3) *Exact sequence* (37) *can be rewritten as*

$$0 \longrightarrow \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \longrightarrow H^1(K_\ell, E[p]) \longrightarrow \mathrm{Hom}_{\mathrm{cont}}\big(\mathrm{Gal}\,(\mathbb{Q}_\ell^{\mathrm{unr}}/K_\ell), L_\epsilon/\mathfrak{m}_{f_\ell}\big).$$

Proof. By [6] and the Eichler–Shimura relations, the quotient $J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell}$ is isomorphic as a $G_\mathbb{Q}$-module to the direct sum of $h \geq 1$ copies of $E[p]$. By [3, Lemma 2.6], the $\mathbb{F}_p$-vector space $H^1(K_\ell, E[p])$ has dimension 2 and can be (non-canonically) decomposed into a sum

$$H^1(K_\ell, E[p]) = H^1_{\mathrm{fin}}(K_\ell, E[p]) \oplus H^1_{\mathrm{sing}}(K_\ell, E[p])$$

of one-dimensional subspaces. The image of $H^1_{\mathrm{sing}}(K_\ell, E[p])$ in the group of continuous homomorphisms in exact sequence (37) is trivial. Since $\dim_{\mathbb{F}_p}(\Psi) \leq \dim_{\mathbb{F}_p}(\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell})$ and $\dim_{\mathbb{F}_p}(\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell}) = 1$ by the last claim of Theorem 6.3, we conclude that $h = 1$ and

$$\Psi \simeq \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \simeq H^1_{\mathrm{sing}}(K_\ell, E[p]),$$

from which all the statements follow. □

In light of Theorem 6.4, from here on we fix an isomorphism

$$J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell} \simeq E[p] \tag{38}$$

of $G_{\mathbb{Q}}$-modules and an isomorphism

$$\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \simeq H^1_{\mathrm{sing}}(K_\ell, E[p]) \tag{39}$$

of $\mathbb{F}_p$-vector spaces.

7. Gross–Zagier type formula and Darmon points

In this section assume that $D > 1$. Fix throughout an admissible prime ℓ, set

$$\Gamma := \Gamma_\ell$$

for the Ihara group at ℓ and denote by t the exponent t_ℓ of Γ^{ab}. Building on the arguments and constructions of [22], in this section we prove our Gross–Zagier type formula (Theorem 7.4) relating the class modulo p of $\mathcal{L}_K(E,\chi,1)$ to a certain twisted sum of Darmon points. This is a generalization to the case of division quaternion algebras and arbitrary characters of the formula proved in [5, Theorem 3.9]. In fact, a suitable extension of the arguments with modular symbols and specializations of Stark–Heegner points described in [5, §3.3] yields the analogue of Theorem 7.4 in the $D = 1$ setting.

7.1. **Auxiliary results.** Recall from §6.2 and the proof of Theorem 6.4 that the cokernel of the map arising from the composition of the inclusion $L_\epsilon \subset T_\epsilon(\mathbb{Q}_\ell)$, the valuation map $\mathrm{ord}_\ell : T_\epsilon(\mathbb{Q}_\ell) \to H_\epsilon$ and the projection $H_\epsilon \twoheadrightarrow H_\epsilon/\mathfrak{m}_{f_\ell}$, which is denoted by Ψ in (37), is a non-trivial $\mathbb{F}_p$-vector space isomorphic to $\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell}$. For any unramified extension W/K_ℓ denote by

$$\partial_\ell : J_\epsilon^{(\ell)}(W) \longrightarrow \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \tag{40}$$

the map that is obtained by composing the inverse of isomorphism (4) with the valuation map $\mathrm{ord}_\ell : T_\epsilon(W)/L_\epsilon \to H_\epsilon/\mathrm{ord}_\ell(L_\epsilon)$, the canonical projection to Ψ and the isomorphism of this $\mathbb{F}_p$-vector space with $\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell}$.

Recall the $\mathrm{GL}_2(\mathbb{Q}_\ell)$-equivariant reduction map

$$r : \mathcal{H}_\ell \longrightarrow \mathcal{T}$$

and the base point τ such that $r(\tau) = v_*$ which was fixed in §3.2. Let $\gamma_1 \in \Gamma$ and let $\{e_0, \dots, e_n\}$ be a set of edges $e_i \in \mathcal{E}^+$ such that

- $s(e_1) = v_*$, $s(e_n) = \gamma_1(v_*) =: v_n$;
- $t(e_i) = t(e_{i+1}) =: v_i$ for *odd* indices in $\{1, \dots, n-1\}$;
- $s(e_i) = s(e_{i+1}) =: v_i$ for *even* indices in $\{2, \dots, n-2\}$.

Notice that, in the above, the integer n is always even. If $\gamma_2 \in \Gamma$ then, by [22, Proposition 5.2], there is an equality

$$\mathrm{ord}_\ell\left(\int\!\!\!\!\!\!\diagup_{\mathbb{P}^1(\mathbb{Q}_\ell)} \frac{t - \gamma_1^{-1}(\tau)}{t - \tau} d\mu_{\gamma_2}^{\mathcal{Y}}(t) \right) = \sum_{i=0}^{n} (-1)^i \mu_{\gamma_2}^{\mathcal{Y}}(e_i) \tag{41}$$

of elements in H, where $\mu^{\mathcal{Y}}$ is the cocycle introduced in Definition 3.1.

Remark 7.1. In the following we adopt the identification $H_1\big(\Gamma_0^D(M), \mathbb{Z}_S\big) = \Gamma_0^D(M)^{\mathrm{ab}} \otimes \mathbb{Z}_S$ and write $[\gamma]$ for the natural image in $H_1\big(\Gamma_0^D(M), \mathbb{Z}_S\big)$ of an element $\gamma \in \Gamma_0^D(M)$.

Now we introduce the 1-cocycle

$$\tilde{m}^{\mathcal{Y}} \in Z^1\Big(\Gamma, \mathcal{F}\big(\mathcal{V}, H_1\big(\Gamma_0^D(M), \mathbb{Z}_S\big)\big)\Big)$$

defined by the rule

$$\tilde{m}_\gamma^{\mathcal{Y}}(v) := [g_{\gamma,v}]$$

where $g_{\gamma,v} \in \Gamma_0^D(M)$ is given by the formula

$$g_{\gamma,v} := \begin{cases} \gamma_v \gamma \gamma_{\gamma^{-1}(v)}^{-1} & \text{if } v \in \mathcal{V}^+ \\ \omega_\ell^{-1} \gamma_v \gamma \gamma_{\gamma^{-1}(v)}^{-1} \omega_\ell & \text{if } v \in \mathcal{V}^-. \end{cases}$$

Note that $\gamma_v \gamma \gamma_{\gamma^{-1}(v)}^{-1}$ stabilizes v_* (respectively, $\hat{v}_*$), and thus lies in $\Gamma_0^D(M)$ (respectively, in $\hat{\Gamma}_0^D(M)$), if $v \in \mathcal{V}^+$ (respectively, $v \in \mathcal{V}^-$). Hence $g_{\gamma,v}$ always lies in $\Gamma_0^D(M)$. We leave it to the reader to check that $\tilde{m}^{\mathcal{Y}}$ is a well-defined cocycle; see Definition 3.1 and [22, §4] for a similar construction.

Consider the composition

$$\mathrm{pr}_1 : H_1\big(X_0^D(M), \mathbb{Z}_S\big)^2 \twoheadrightarrow H_1\big(X_0^D(M), \mathbb{Z}_S\big)^2 \big/ \mathfrak{m}_f' \twoheadrightarrow \mathrm{coker}(\bar{\pi}_* \circ \bar{\pi}^*) \twoheadrightarrow \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}$$

where the first two maps are the canonical projections, the third is induced by Proposition 6.2 and the isomorphism is that of (31). If $e \in \mathcal{E}$ then set

$$\tilde{\mu}_\gamma^{\mathcal{Y}}(e) := \mathrm{pr}_1\big(\tilde{m}_\gamma^{\mathcal{Y}}(s(e)), \tilde{m}_\gamma^{\mathcal{Y}}(t(e))\big). \tag{42}$$

Similarly, define also the composition

$$\mathrm{pr}_2 : H_1\big(X_0^D(M), \mathbb{Z}_S\big) \twoheadrightarrow H_1\big(X_0^D(M), \mathbb{Z}_S\big)\big/\mathfrak{m}_f \simeq \mathrm{coker}(\bar{\pi}_* \circ \bar{\pi}^*) \twoheadrightarrow \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}$$

where the first isomorphism is (33). Recall from condition 5 in Assumption 5.1 that there exists $\delta \in \{\pm 1\}$ such that $p | a_\ell + \delta(\ell+1)$. The isomorphism in (32) is induced by the map $(x,y) \mapsto (\ell+1)x - T_\ell(y)$; since $p | a_\ell - \delta(\ell+1)$, this map is just $(x,y) \mapsto (\ell+1)(x - \delta y)$ from $H_1\big(X_0^D(M), \mathbb{Z}_S\big)^2/\mathfrak{m}_f'$ to $H_1\big(X_0^D(M), \mathbb{Z}_S\big)/\mathfrak{m}_f$. It follows that

$$\tilde{\mu}_\gamma^{\mathcal{Y}}(e) = (\ell+1)\mathrm{pr}_2\big(\tilde{m}_\gamma^{\mathcal{Y}}(t(e)) - \delta \tilde{m}_\gamma^{\mathcal{Y}}(s(e))\big). \tag{43}$$

We thus obtain that $\tilde{\mu}^{\mathcal{Y}}$ is also well defined with values in $\mathcal{F}_0(\mathcal{E}, \mathbb{Z}/p\mathbb{Z})$.

Finally, introduce the map

$$\mathrm{pr}_3 : H_1\big(X_0^D(M\ell), \mathbb{Z}_S\big) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{coker}(\bar{\pi}_* \circ \bar{\pi}^*) \longrightarrow\!\!\!\!\!\rightarrow \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \simeq \mathbb{Z}/p\mathbb{Z}$$

where the first arrow is the composition of the canonical projection

$$H_1\big(X_0^D(M\ell), \mathbb{Z}_S\big) \longrightarrow\!\!\!\!\!\rightarrow \big(H_1(X_0^D(M\ell), \mathbb{Z}_S)/\mathfrak{m}_f'\big)\big/\langle \ker(\bar{\pi}_*), \mathrm{im}(\bar{\pi}^*)\rangle$$

with isomorphism (30), and define

$$\bar{\mu}^{\mathcal{Y}} := \mathrm{pr}_3(\mu^{\mathcal{Y}}).$$

Lemma 7.2. $\bar{\mu}^{\mathcal{Y}} = \tilde{\mu}^{\mathcal{Y}}$.

Proof. Fix $\gamma \in \Gamma$ and $e \in \mathcal{E}^+$ and let $g_{\gamma,e} \in \Gamma_0^D(M\ell)$ be such that $\gamma_e \gamma = g_{\gamma,e} \gamma_{e'}$ for some $e' \in \mathcal{E}^+$. By Definition 3.1, one has

$$\bar{\mu}_\gamma^{\mathcal{Y}}(e) = \mathrm{pr}_3\big([g_{\gamma,e}]\big),$$

while by (42) there is an equality

$$\tilde{\mu}_\gamma^{\mathcal{Y}}(e) = \mathrm{pr}_1\big([g_{\gamma,e}], [\omega_\ell^{-1} g_{\gamma,e} \omega_\ell]\big).$$

By construction, there is a commutative triangle

$$\begin{array}{ccc} H_1\big(X_0^D(M\ell), \mathbb{Z}_S\big) & \twoheadrightarrow & \mathrm{coker}(\bar{\pi}_* \circ \bar{\pi}^*) \\ \downarrow & \nearrow & \\ H_1\big(X_0^D(M), \mathbb{Z}_S\big)^2 & & \end{array}$$

where the vertical arrow is induced by the map $\Gamma_0^D(M\ell) \to \Gamma_0^D(M)^2$ taking γ to $(\gamma, \omega_\ell^{-1}\gamma\omega_\ell)$ via the canonical projections and the other two maps are the surjections already appearing in the definitions of pr_1 and pr_3. This shows the required equality for even edges, and the analogous equality for odd edges follows similarly. □

Let us denote by ∂'_ℓ the composition of the map ∂_ℓ in (40) with the isomorphism (31) between $\Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell}$ and $\mathbb{Z}/p\mathbb{Z}$. Let us also write d_ϵ for the composition of the 2-cocycle d introduced in (5) with the map $T(K_\ell) \to J_\epsilon^{(\ell)}(K_\ell)$ defined in the obvious way. Similarly, if β is as in (6) then let $\beta_\epsilon : \Gamma \to J_\epsilon^{(\ell)}(K_\ell)$ be the induced map. Observe that, with this notation in force, Definition 3.4 reads

$$P_\psi^\epsilon := t \cdot \beta_\epsilon\big(\psi(\gamma_\psi)\big) \in J_\epsilon^{(\ell)}(K_\ell). \tag{44}$$

It is worthwhile to explicitly remark that in this section we view the Darmon points P_ψ^ϵ as rational over the local field K_ℓ. In fact, the Gross–Zagier type results we are about to prove are of a genuinely local nature, so we do not need to assume that the points we work with are global, as predicted by Conjecture 3.6.

From (41) and Lemma 7.2 we obtain equalities

$$\partial'_\ell\big(d_\epsilon(\gamma_1,\gamma_2)\big) = \sum_{i=0}^{n}(-1)^i\bar{\mu}_{\gamma_2}^{\mathcal{Y}}(e_i) = \sum_{i=0}^{n}(-1)^i\tilde{\mu}_{\gamma_2}^{\mathcal{Y}}(e_i), \tag{45}$$

with the edges e_i being defined as for equality (41); namely, the $e_i \in \mathcal{E}^+$ satisfy

- $s(e_1) = v_*$, $s(e_n) = \gamma_1^{-1}(v_*) =: v_n$;
- $t(e_i) = t(e_{i+1}) =: v_i$ for *odd* indices in $\{1,\dots,n-1\}$;
- $s(e_i) = s(e_{i+1}) =: v_i$ for *even* indices in $\{2,\dots,n-2\}$.

Define a function $\alpha_\tau : \Gamma \to \mathbb{Z}/p\mathbb{Z}$ by setting

$$\alpha_\tau(\gamma) := -(\ell+1)\mathrm{pr}_2\big(\tilde{m}_\gamma^{\mathcal{Y}}(v_*)\big).$$

Observe that, by definition, $\alpha_\tau = \alpha_{\tau'}$ for all τ' with $r(\tau') = v_*$. Fix now $z_\psi \in \mathcal{H}_\ell^{\mathcal{O}}$ and recall the element $\gamma_\psi \in \mathcal{O}^\times$ attached to z_ψ as in §3.2.

Lemma 7.3. *Suppose $\delta = -1$. The equality*

$$\partial'_\ell(P_\psi^\epsilon) = t \cdot \alpha_\tau\big(\psi(\gamma_\psi)\big)$$

holds in $\mathbb{Z}/p\mathbb{Z}$.

Proof. Fix $\gamma_1, \gamma_2 \in \Gamma$ and $e \in \mathcal{E}$. Choose a sequence $\{e_0,\dots,e_n\}$ of even edges joining the vertices v_* and $\gamma_1^{-1}(v_*)$ as in (45). Since $\delta = -1$, by (43) there is an equality

$$\sum_{i=0}^{n}(-1)^i\tilde{\mu}_{\gamma_2}^{\mathcal{Y}}(e_i) = (\ell+1)\sum_{i=0}^{n}(-1)^i\mathrm{pr}_2\big(\tilde{m}_\gamma^{\mathcal{Y}}(t(e)) + \tilde{m}_\gamma^{\mathcal{Y}}(s(e))\big).$$

The terms in the right-hand sum cancel out telescopically and we find that

$$\sum_{i=0}^{n}(-1)^i\tilde{\mu}_{\gamma_2}^{\mathcal{Y}}(e_i) = -(\ell+1)\mathrm{pr}_2\big(\tilde{m}_\gamma^{\mathcal{Y}}(t(e_n)) - \tilde{m}_\gamma^{\mathcal{Y}}(s(e_0))\big). \tag{46}$$

Observe that

$$\begin{aligned}\tilde{m}_{\gamma_1\gamma_2}^{\mathcal{Y}}(v_*) - \tilde{m}_{\gamma_1}^{\mathcal{Y}}(v_*) &= \big[\gamma_1\gamma_2\gamma_{\gamma_2^{-1}\gamma_1^{-1}(v_*)}^{-1}\big] - \big[\gamma_1\gamma_{\gamma_1^{-1}(v_*)}^{-1}\big] \\ &= \big[\gamma_{\gamma_1^{-1}(v_*)}\gamma_2\gamma_{\gamma_2^{-1}\gamma_1^{-1}(v_*)}^{-1}\big] = \tilde{m}_{\gamma_2}^{\mathcal{Y}}\big(\gamma_1^{-1}(v_*)\big).\end{aligned} \tag{47}$$

Combining (45), (46) and (47) we obtain

$$\partial'_\ell\big(d_\epsilon(\gamma_1,\gamma_2)\big) = \alpha_\tau(\gamma_1\gamma_2) - \alpha_\tau(\gamma_1) - \alpha_\tau(\gamma_2). \tag{48}$$

It is then a consequence of equations (6) and (48) that both $\partial'_\ell \circ \beta_\epsilon$ and α_τ split the 2-cocycle $\partial'_\ell \circ d_\epsilon \in Z^2(\Gamma, \mathbb{Z}/p\mathbb{Z})$, whence

$$\partial'_\ell\big(t \cdot \beta_\epsilon(\gamma)\big) = t \cdot \alpha_\tau(\gamma) \tag{49}$$

for all $\gamma \in \Gamma$ because ∂'_ℓ is a group homomorphism. In light of (44), the claim of the lemma follows upon taking $\gamma = \psi(\gamma_\psi)$ in equality (49). □

7.2. **A Gross–Zagier formula.** If $\psi : K \hookrightarrow B$ is an embedding then, as in §3.2, let $z_\psi \in \mathcal{H}_\ell \cap K$ be the (unique) point such that $\psi(\alpha)\binom{z_\psi}{1} = \alpha\binom{z_\psi}{1}$ for all $\alpha \in K$.

Recall the set $\{\psi_\sigma \mid \sigma \in G_c\}$ of representatives for the $\Gamma_0^D(M)$-equivalence classes of optimal embeddings of $\mathcal{O}_c$ into R fixed in §4.2. For simplicity, set $\tau_\sigma := z_{\psi_\sigma}$ and $v_\sigma := r(\tau_\sigma)$ for all $\sigma \in G_c$. Since the reduction map is Γ-equivariant and ℓ is prime to c, the stabilizer of v_σ in $\mathrm{GL}_2(\mathbb{Q}_\ell)$ coincides with $\mathrm{GL}_2(\mathbb{Z}_\ell)$, hence $v_\sigma = v_*$ for all $\sigma \in G_c$. Define

$$P_\chi^\epsilon := \sum_{\sigma \in G_c} P_{\psi_\sigma}^\epsilon \otimes \chi^{-1}(\sigma) \in J_\epsilon^{(\ell)}(K_\ell) \otimes \mathbb{Z}[\chi]_S \tag{50}$$

and, again to ease the writing, set $\gamma_\sigma := \gamma_{\psi_\sigma} \in \mathcal{O}_c^\times$ for all $\sigma \in G_c$.

Let $[\star]$ be the class of the element $\star$ in a quotient group. Now we can prove our Gross–Zagier type formula for the (algebraic part of the) special value $L_K(E, \chi, 1)$, which can also be regarded as an explicit reciprocity law in the sense of [3].

Theorem 7.4. *Suppose $\delta = -1$. Then*

$$(\partial'_\ell \otimes \mathrm{id})(P_\chi^\epsilon) = t \cdot \big[\mathcal{L}_K(E, \chi, 1)\big]$$

in $\mathbb{Z}[\chi]_S/p\mathbb{Z}[\chi]_S$.

Proof. Combining Lemma 7.3 with the fact that $r(\tau_\sigma) = v_*$ for all $\sigma \in G_c$ gives

$$(\partial'_\ell \otimes \mathrm{id})(P_\chi^\epsilon) = t \cdot \sum_{\sigma \in G_c} \alpha_{\tau_\sigma}\big(\psi_\sigma(\gamma_\sigma)\big) \otimes \chi^{-1}(\sigma) \tag{51}$$

in $\mathbb{Z}[\chi]_S/p\mathbb{Z}[\chi]_S$. Since $\alpha_{\tau_\sigma}\big(\psi_\sigma(\gamma_\sigma)\big) = \mathrm{pr}_2\big([\gamma_\sigma]\big)$, by definition of $\mathcal{L}_K(E, \chi, 1)$ one has

$$\sum_{\sigma \in G_c} \alpha_{\tau_\sigma}\big(\psi_\sigma(\gamma_\sigma)\big) \otimes \chi^{-1}(\sigma) = \big[\mathcal{L}_K(E, \chi, 1)\big]$$

in $\mathbb{Z}[\chi]_S/p\mathbb{Z}[\chi]_S$. The result then follows from equality (51). □

8. Arithmetic results and consequences

With our special value formula (Theorem 7.4) at hand, in this section we prove the results on the vanishing of the Selmer groups and on the Birch and Swinnerton-Dyer conjecture for E in the case of analytic rank 0 that were anticipated in the introduction.

8.1. **A result on local Kummer maps.** Quite generally, let F be a number field and let

$$\kappa : J_\epsilon^{(\ell)}(F) \longrightarrow H^1\big(F, J_\epsilon^{(\ell)}[p]\big)$$

be the Kummer map relative to $J_\epsilon^{(\ell)}$. Composing κ with the maps induced by the canonical projection $J_\epsilon^{(\ell)}[p] \to J_\epsilon^{(\ell)}[p]/\mathfrak{m}_{f_\ell}$ and by isomorphism (38) yields a map

$$\bar\kappa : J_\epsilon^{(\ell)}(F) \longrightarrow H^1(F, E[p]). \tag{52}$$

By a slight abuse of notation, we adopt the symbol $\bar\kappa$ also for the map

$$\bar\kappa : J_\epsilon^{(\ell)}(K_\ell) \longrightarrow H^1(K_\ell, E[p])$$

which is obtained by considering the local counterpart of the Kummer map κ and viewing (38) as an isomorphism of $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/K_\ell)$-modules via the inclusion $\mathrm{Gal}\,(\bar{\mathbb{Q}}_\ell/K_\ell) \hookrightarrow G_{\mathbb{Q}}$ induced by the injection $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ fixed at the outset.

If q is a prime number let $\mathrm{res}_q : H^1(F, E[p]) \to H^1(F_q, E[p])$ be the restriction map and let

$$\delta_q : E(F_q) \longrightarrow H^1(F_q, E[p]), \qquad \kappa_q : J_\epsilon^{(\ell)}(F_q) \longrightarrow H^1\big(F_q, J_\epsilon^{(\ell)}[p]\big)$$

be the local Kummer maps at q relative to E and $J_\epsilon^{(\ell)}$, respectively. Finally, for any prime $\mathfrak{p}$ of F above p let $\nu_\mathfrak{p}$ be the (normalized) valuation of $F_\mathfrak{p}$ and let $e_\mathfrak{p} := \nu_\mathfrak{p}(p)$ be the absolute ramification index of $F_\mathfrak{p}$ (in particular, $e_\mathfrak{p} = 1$ if p is unramified in F).

Proposition 8.1. *Assume that $e_\mathfrak{p} < p-1$ for all $\mathfrak{p}|p$. If $P \in J_\epsilon^{(\ell)}(F)$ then*

$$\mathrm{res}_q\big(\bar{\kappa}(P)\big) \in \mathrm{Im}(\delta_q)$$

for all primes $q \nmid M\ell$.

A proof of this proposition, obtained by combining the description of the image of the local Kummer maps above p in terms of flat cohomology given in [23, §3.3] with classical results of Raynaud on p-torsion group schemes ([28]), can be found in [23, Proposition 5.2].

8.2. **Linear algebra preliminaries.** The goal of this subsection is to recall the arguments in [23, §8] and introduce the technical tools (Propositions 8.4 and 8.6) that will be needed to prove the main arithmetic theorems of this paper.

Let $\chi \in \widehat{G}_c$ be our complex-valued character of G_c. Since $p \notin S$ by condition 1 in Assumption 5.1, every prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\chi]$ above p determines a prime ideal $\mathfrak{p}_S := \mathfrak{p}\mathbb{Z}[\chi]_S$ of $\mathbb{Z}[\chi]_S$.

Lemma 8.2. *Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\chi]$ above p. The completion of $\mathbb{Z}[\chi]$ at $\mathfrak{p}$ is canonically isomorphic to the completion of $\mathbb{Z}[\chi]_S$ at $\mathfrak{p}_S$.*

Proof. For all integers $n \geq 1$ write $\bar{S}_n$ for the multiplicative system of $\mathbb{Z}[\chi]/\mathfrak{p}^n$ which is the image of S under the natural projection. For every $n \geq 1$ there is a canonical ring isomorphism

$$\big(\mathbb{Z}[\chi]/\mathfrak{p}^n\big)_{\bar{S}_n} \simeq \mathbb{Z}[\chi]_S/\mathfrak{p}_S^n. \tag{53}$$

But the elements of $\bar{S}_n$ are invertible in $\mathbb{Z}[\chi]/\mathfrak{p}^n$ since p does not belong to S, hence the localization $\big(\mathbb{Z}[\chi]/\mathfrak{p}^n\big)_{\bar{S}_n}$ canonically identifies with $\mathbb{Z}[\chi]/\mathfrak{p}^n$. In light of (53), the lemma is proved by passing to the inverse limit. □

Choose a prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\chi]$ above p such that

$$\text{the image of } \mathcal{L}_K(E, \chi, 1) \text{ in } \mathbb{Z}[\chi]_S/\mathfrak{p}_S \text{ is not zero.} \tag{54}$$

This can be done thanks to condition 4 in Assumption 5.1. Denote by $\mathcal{W}$ the $\mathfrak{p}$-adic completion of $\mathbb{Z}[\chi]$. The prime p is unramified in $\mathbb{Z}[\chi]$ since it does not divide $h^+(c)$ by condition 2 in Assumption 5.1, hence the ideal $p\mathcal{W}$ is the maximal ideal of $\mathcal{W}$; in particular, we conclude from Lemma 8.2 that

$$\mathbb{Z}[\chi]_S/\mathfrak{p}_S = \mathcal{W}/p\mathcal{W}.$$

For any $\mathbb{Z}[G_c]$-module M write $M \otimes_\chi \mathbb{C}$ (respectively, $M \otimes_\chi \mathcal{W}$) for the tensor product of the $\mathbb{Z}[G_c]$-modules M and $\mathbb{C}$ (respectively, M and $\mathcal{W}$), where the structure of $\mathbb{Z}[G_c]$-module on $\mathbb{C}$ (respectively, $\mathcal{W}$) is induced by χ. As in the introduction, if M is a $\mathbb{Z}[G_c]$-module define also

$$M^\chi := \big\{x \in M \otimes_{\mathbb{Z}} \mathbb{C} \mid \sigma(x) = \chi(\sigma)x \text{ for all } \sigma \in G_c\big\},$$

so that there is a canonical identification

$$M^\chi = M \otimes_\chi \mathbb{C}$$

of $\mathbb{C}[G_c]$-modules (for a proof of this fact see, e.g., [23, Proposition 8.1]).

Choose once and for all an (algebraic) isomorphism $\mathbb{C}_p \simeq \mathbb{C}$ which is the identity on $\mathbb{Z}[\chi]$. Henceforth we shall view $\mathbb{C}$ as a $\mathcal{W}$-module via this isomorphism, obtaining an isomorphism

$$\big(E(H_c) \otimes_\chi \mathcal{W}\big) \otimes_{\mathcal{W}} \mathbb{C} \simeq E(H_c) \otimes_\chi \mathbb{C}.$$

The following flatness result will be frequently used in the sequel.

Lemma 8.3. *The module $\mathcal{W}$ is flat over $\mathbb{Z}[G_c]$, and every $\mathbb{F}_p[G_c]$-module is flat.*

Proof. First of all, $\mathcal{W}$ is flat over $\mathbb{Z}$. Moreover, if ℓ is a prime number dividing $h^+(c)$ then $\ell \neq p$, hence $\mathcal{W}/\ell\mathcal{W} = 0$. The flatness of $\mathcal{W}$ follows from [1, Theorem 1.6]. The second assertion can be shown in the same way. □

The next statement is proved exactly as [23, Proposition 8.3].

Proposition 8.4. *If $\mathrm{Sel}_p(E/H_c) \otimes_\chi \mathcal{W} = 0$ then $E(H_c)^\chi = 0$.*

Thus the triviality of $E(H_c)^\chi$ is guaranteed by that of $\mathrm{Sel}_p(E/H_c) \otimes_\chi \mathcal{W}$.

The rest of this subsection is devoted to a couple of further algebraic lemmas which are needed to prove the vanishing of the twisted p-Selmer groups; this part follows [23, §8.2] closely, so we will merely sketch the arguments and refer to *loc. cit.* for complete proofs.

In the following, use the symbol χ also to denote the $\mathbb{Z}$-linear extension

$$\mathbb{Z}[G_c] \xrightarrow{\chi} \mathbb{Z}[\chi] \subset \mathcal{W}$$

of the character χ. Composing χ with the projection onto $\mathcal{W}/p\mathcal{W}$ yields a homomorphism which factors through $\mathbb{F}_p[G_c] = \mathbb{Z}[G_c]/p\mathbb{Z}[G_c]$, and we define $\chi_p : \mathbb{F}_p[G_c] \to \mathcal{W}/p\mathcal{W}$ to be the resulting map. In particular, the homomorphism χ_p gives $\mathcal{W}/p\mathcal{W}$ a structure of $\mathbb{F}_p[G_c]$-module (which is nothing other than the structure induced naturally by that of $\mathbb{Z}[G_c]$-module on $\mathcal{W}$), and for an $\mathbb{F}_p[G_c]$-module M the notation $M \otimes_{\chi_p} (\mathcal{W}/p\mathcal{W})$ will indicate that the tensor product is taken over $\mathbb{F}_p[G_c]$ with respect to χ_p.

Set $I_{\chi_p} := \ker(\chi_p)$ and for any $\mathbb{F}_p[G_c]$-module M let $M[I_{\chi_p}]$ be the I_{χ_p}-torsion submodule of M, i.e. the submodule of M which is annihilated by all the elements of I_{χ_p}. Finally, adopt similar notations and conventions for the map $\chi_p^{-1} : \mathbb{F}_p[G_c] \to \mathcal{W}/p\mathcal{W}$ which is induced by the inverse character to χ.

The flatness result of Lemma 8.3 yields the following important facts:

- for every $\mathbb{F}_p[G_c]$-module M there are canonical identifications
$$M \otimes_\chi \mathcal{W} = M \otimes_{\chi_p} (\mathcal{W}/p\mathcal{W}) = M[I_{\chi_p}] \otimes_{\chi_p} (\mathcal{W}/p\mathcal{W}) = M[I_{\chi_p}] \otimes_\chi \mathcal{W}$$
of $\mathcal{W}$-modules ([23, Lemma 8.4]);
- if M is an $\mathbb{F}_p[G_c]$-module then $M[I_{\chi_p}]$ injects into $M \otimes_\chi \mathcal{W}$ amd $M\big[I_{\chi_p^{-1}}\big]$ injects into $M\big[I_{\chi_p^{-1}}\big] \otimes_\chi \mathcal{W}$ ([23, Lemma 8.5]).

As a consequence, the linear algebra results in [23, §8.2] carry over *verbatim* to our real quadratic setting; here we content ourselves with recalling the proof of a crucial statement about the non-triviality of (the dual of) a certain restriction map in Galois cohomology.

To begin with, for any $\mathbb{F}_p$-vector space V denote the $\mathbb{F}_p$-dual of V by

$$V^\vee := \mathrm{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p).$$

The dual of an $\mathbb{F}_p[G_c]$-module inherits a natural structure of $\mathbb{F}_p[G_c]$-module: a Galois element σ acts on a homomorphism φ by $\sigma(\varphi) := \varphi \circ \sigma^{-1}$. Furthermore, if f is a map of $\mathbb{F}_p[G_c]$-modules then its dual $f^\vee$ is again G_c-equivariant. It can be immediately checked that if an $\mathbb{F}_p[G_c]$-module is of I_{χ_p}-torsion then its dual is of $I_{\chi_p^{-1}}$-torsion.

Let ℓ be an admissible prime and let

$$\mathrm{res}_\ell : \mathrm{Sel}_p(E/H_c) \longrightarrow H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])$$

be the natural restriction map; with a slight abuse of notation, we will adopt the same symbol also for the map

$$\mathrm{res}_\ell : \mathrm{Sel}_p(E/H_c)[I_{\chi_p}] \longrightarrow H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])[I_{\chi_p}]$$

between the I_{χ_p}-torsion submodules which is induced by the previous one.

Lemma 8.5. *If there exists* $s \in \mathrm{Sel}_p(E/H_c)[I_{\chi_p}]$ *such that* $\mathrm{res}_\ell(s) \neq 0$ *then the map*

$$\mathrm{res}_\ell^\vee \otimes \mathrm{id} : H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])[I_{\chi_p}]^\vee \otimes_\chi \mathcal{W} \longrightarrow \mathrm{Sel}_p(E/H_c)[I_{\chi_p}]^\vee \otimes_\chi \mathcal{W}$$

is injective and non-zero.

Proof. Keeping in mind the two consequences of Lemma 8.3 recalled above, proceed as in the proof of [23, Lemma 8.8]. □

With this auxiliary result at hand, we can prove

Proposition 8.6. *If there exists* $s \in \mathrm{Sel}_p(E/H_c)[I_{\chi_p}]$ *such that* $\mathrm{res}_\ell(s) \neq 0$ *then the map*

$$\mathrm{res}_\ell^\vee \otimes \mathrm{id} : H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])^\vee \otimes_\chi \mathcal{W} \longrightarrow \mathrm{Sel}_p(E/H_c)^\vee \otimes_\chi \mathcal{W}$$

is non-zero.

Proof. In the commutative square

$$\begin{array}{ccc} H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])^\vee \otimes_\chi \mathcal{W} & \xrightarrow{\mathrm{res}_\ell^\vee \otimes \mathrm{id}} & \mathrm{Sel}_p(E/H_c)^\vee \otimes_\chi \mathcal{W} \\ \downarrow & & \downarrow \\ H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])[I_{\chi_p}]^\vee \otimes_\chi \mathcal{W} & \hookrightarrow & \mathrm{Sel}_p(E/H_c)[I_{\chi_p}]^\vee \otimes_\chi \mathcal{W} \end{array}$$

the vertical maps are surjective and the bottom horizontal arrow is (injective and) non-zero by Lemma 8.5. Hence the upper horizontal arrow must be non-zero. □

8.3. **Construction of an Euler system.** As before, let $\mathcal{O}_c$ be the order of K of conductor c and let H_c be the narrow ring class field of K of conductor c. Let ℓ be an admissible prime such that $p|\ell+1+a_\ell$ (so $\delta=-1$ in Theorem 6.3) and choose $z_\psi \in \mathcal{H}_\ell^{\mathcal{O}_c}$. Now recall the prime λ_0 of H_c above ℓ fixed in §5.2; there is a canonical isomorphism

$$i_{\lambda_0} : H_{c,\lambda_0} \xrightarrow{\simeq} K_\ell,$$

with H_{c,λ_0} being the completion of H_c at λ_0. Since we are assuming Conjecture 3.6, we can consider the Darmon point

$$P_c = P_\psi^\epsilon \in J_\epsilon^{(\ell)}(H_c) \hookrightarrow J_\epsilon^{(\ell)}(K_\ell),$$

where the injection is induced by i_{λ_0}. With $\bar\kappa$ as in (52) for $F = H_c$, define a cohomology class

$$\kappa(\ell) := \bar\kappa(P_c) \in H^1(H_c, E[p]).$$

The collection of classes $\{\kappa(\ell)\}$ indexed by the set of admissible primes is an *Euler system* relative to $E_{/K}$ and, as in [23], will be used in the sequel to bound the p-Selmer groups. In the following we will deduce the main properties of $\kappa(\ell)$.

Recall the choice of the prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\chi]$ above p made in (54); the ring $\mathcal{W}$ is the completion of $\mathbb{Z}[\chi]$ at $\mathfrak{p}$. Let us introduce the map

$$d_\ell^\chi : H^1(H_c, E[p]) \longrightarrow H^1_{\mathrm{sing}}(H_{c,\ell}, E[p]) \otimes_\chi \mathcal{W} \tag{55}$$

obtained by composing the restriction from $H^1(H_c, E[p])$ to $H^1(H_{c,\ell}, E[p])$ with the map $H^1(H_{c,\ell}, E[p]) \to H^1(H_{c,\ell}, E[p]) \otimes_\chi \mathcal{W}$ which takes x to $x \otimes 1$ and finally with the canonical projection to the singular part of the cohomology.

As explained in [23, §9.3] (to which we refer for details), the choice of a prime λ_0 of H_c above ℓ made in §5.2 induces natural isomorphisms

$$H^1_\star(H_{c,\ell}, E[p]) \xrightarrow{\simeq} H^1_\star(K_\ell, E[p]) \otimes_{\mathbb{Z}} \mathbb{Z}[G_c]$$

for $\star \in \{\mathrm{fin}, \mathrm{sing}\}$, so that we can (and do) view d_ℓ^χ as taking values in the $\mathcal{W}$-module $H^1_{\mathrm{sing}}(K_\ell, E[p]) \otimes_{\mathbb{Z}} \mathcal{W}$.

Proposition 8.7. *If $L_K(E,\chi,1) \neq 0$ then $d_\ell^\chi\big(\kappa(\ell)\big) \neq 0$.*

Proof. Let $\iota : \mathbb{Z}[\chi]_S \hookrightarrow \mathcal{W}$ be the natural inclusion (cf. Lemma 8.2). There is a commutative square

$$\begin{array}{ccc} J_\epsilon^{(\ell)}(K_\ell) & \xrightarrow{\bar\kappa} & H^1(K_\ell, E[p]) \\ \big\downarrow{\scriptstyle \partial_\ell} & & \big\downarrow{\scriptstyle \delta_\ell} \\ \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} & \xrightarrow[\simeq]{\vartheta_\ell} & H^1_{\mathrm{sing}}(K_\ell, E[p]) \end{array}$$

in which δ_ℓ is the projection and ϑ_ℓ is isomorphism (39). Tensoring with $\mathbb{Z}[\chi]_S$ over $\mathbb{Z}$ and then composing with the relevant maps $\mathrm{id} \otimes \iota$ yields a commutative diagram

$$\begin{array}{ccccc} J_\epsilon^{(\ell)}(K_\ell) \otimes \mathbb{Z}[\chi]_S & \xrightarrow{\bar\kappa\otimes\mathrm{id}} & H^1(K_\ell, E[p]) \otimes \mathbb{Z}[\chi]_S & \xrightarrow{\mathrm{id}\otimes\iota} & H^1(K_\ell, E[p]) \otimes \mathcal{W} \\ \big\downarrow{\scriptstyle \partial_\ell\otimes\mathrm{id}} & & \big\downarrow{\scriptstyle \delta_\ell\otimes\mathrm{id}} & & \big\downarrow{\scriptstyle \delta_\ell\otimes\mathrm{id}} \\ \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \otimes \mathbb{Z}[\chi]_S & \xrightarrow[\simeq]{\vartheta_\ell\otimes\mathrm{id}} & H^1_{\mathrm{sing}}(K_\ell, E[p]) \otimes \mathbb{Z}[\chi]_S & \xrightarrow{\mathrm{id}\otimes\iota} & H^1_{\mathrm{sing}}(K_\ell, E[p]) \otimes \mathcal{W} \\ \big\downarrow{\scriptstyle \mathrm{id}\otimes\iota} & & & \nearrow{\scriptstyle \simeq}\ {\scriptstyle \vartheta_\ell\otimes\mathrm{id}} & \\ \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \otimes \mathcal{W} & & & & \end{array} \tag{56}$$

The arguments described in [23, §§9.1–9.3] show that

$$d_\ell^\chi\big(\kappa(\ell)\big) = \big((\vartheta_\ell \circ \partial_\ell) \otimes \iota\big)(P_\chi^\epsilon)$$

where P_χ^ϵ is defined in (50). Since $\vartheta_\ell \otimes \mathrm{id}$ is an isomorphism, showing that $d_\ell^\chi\big(\kappa(\ell)\big) \neq 0$ is equivalent to showing that

$$(\partial_\ell \otimes \iota)(P_\chi^\epsilon) \neq 0 \qquad \text{in } \Phi_{\ell,\epsilon}/\mathfrak{m}_{f_\ell} \otimes \mathcal{W} \simeq \mathcal{W}/p\mathcal{W} \tag{57}$$

(here the map $\partial_\ell \otimes \iota$ is equal to the composition of the left vertical arrows in (56)).

In order to prove (57) consider the map

$$\mathbb{Z}[\chi]_S/p\mathbb{Z}[\chi]_S \xrightarrow{\iota} \mathcal{W}/p\mathcal{W}$$

induced by ι. The non-vanishing of $L_K(E,\chi,1)$ is equivalent, by Theorem 4.8, to the non-vanishing of $\mathcal{L}_K(E,\chi,1)$. On the other hand, $\iota\big(\big[\mathcal{L}_K(E,\chi,1)\big]\big) \neq 0$ by (54) and $p \nmid t_\ell$ because ℓ is admissible, hence claim (57) follows from Theorem 7.4. □

8.4. **Local Tate pairings and global duality.** For every place v of $\mathbb{Q}$, including the archimedean one, denote by

$$\langle\,,\rangle_v : H^1(H_{c,v}, E[p]) \times H^1(H_{c,v}, E[p]) \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

the local Tate pairing at v. Global Tate duality, which is a consequence of the reciprocity law of class field theory (specifically, of the global reciprocity law for elements in the Brauer group of H_c), asserts that

$$\sum_v \langle \mathrm{res}_v(k), \mathrm{res}_v(s)\rangle_v = 0 \tag{58}$$

for all $k, s \in H^1(H_c, E[p])$. Actually, since the Brauer group of $\mathbb{R}$ has order 2 and p is odd by condition 2 in Assumption 5.1, for all $k, s \in H^1(H_c, E[p])$ one has

$$\sum_q \langle \mathrm{res}_q(k), \mathrm{res}_q(s) \rangle_q = 0 \tag{59}$$

with q running over the set of prime numbers (in other words, in (58) we can restrict the sum to the *finite* places of $\mathbb{Q}$).

Let now ℓ be an admissible prime. As explained in [23, §9.4], the local Tate pairing $\langle\,,\rangle_\ell$ gives rise to isomorphisms of one-dimensional $\mathcal{W}/p\mathcal{W}$-vector spaces

$$H^1_\star(H_{c,\ell}, E[p]) \otimes_\chi \mathcal{W} \xrightarrow{\simeq} H^1_\bullet(H_{c,\ell}, E[p])^\vee \otimes_\chi \mathcal{W} \tag{60}$$

for $\{\star, \bullet\} = \{\mathrm{fin}, \mathrm{sing}\}$. Moreover, the restriction

$$\mathrm{res}_\ell : \mathrm{Sel}_p(E/H_c) \longrightarrow H^1_{\mathrm{fin}}(H_{c,\ell}, E[p])$$

induces a $\mathcal{W}$-linear map

$$\eta_\ell : H^1_{\mathrm{sing}}(H_{c,\ell}, E[p]) \otimes_\chi \mathcal{W} \longrightarrow \mathrm{Sel}_p(E/H_c)^\vee \otimes_\chi \mathcal{W}.$$

Lemma 8.8. *If there exists $s \in \mathrm{Sel}_p(E/H_c)[I_{\chi_p}]$ such that $\mathrm{res}_\ell(s) \neq 0$ then η_ℓ is non-zero.*

Proof. Immediate from (60) and Proposition 8.6. □

In the next lemma the symbol δ_q stands for the local Kummer map at q.

Lemma 8.9. *If q is a prime dividing N then $\mathrm{Im}(\delta_q) = 0$.*

Proof. Since δ_q factors through $E(H_{c,q})/pE(H_{c,q})$, the statement follows from condition 5 in Assumption 5.1. □

Now recall the map d^χ_ℓ defined in (55).

Proposition 8.10. *The element $d^\chi_\ell\big(\kappa(\ell)\big)$ belongs to the kernel of η_ℓ.*

Proof. Keeping Lemma 8.9 and formula (59) in mind, proceed exactly as in the proof of [23, Proposition 9.6]. □

8.5. **Proof of the first vanishing result.** As a first arithmetic consequence of Theorem 7.4, we prove a vanishing result for twisted Selmer groups: all other results will follow from this one. Recall that we are assuming Conjecture 3.6 throughout.

Theorem 8.11. *If $L_K(E, \chi, 1) \neq 0$ then $\mathrm{Sel}_p(E/H_c) \otimes_\chi \mathcal{W} = 0$.*

Proof. By what was said in §8.2, it is enough to show that $\mathrm{Sel}_p(E/H_c)[I_{\chi_p}] = 0$. Assume that $s \in \mathrm{Sel}_p(E/H_c)[I_{\chi_p}]$ is not zero and choose an admissible prime ℓ such that $p | a_\ell + \ell + 1$ and $\mathrm{res}_\ell(s) \neq 0$, which exists by Proposition 5.4. Since $L_K(E, \chi, 1) \neq 0$, Proposition 8.7 ensures that $d^\chi_\ell\big(\kappa(\ell)\big) \neq 0$; then $d^\chi_\ell\big(\kappa(\ell)\big)$ generates $H^1_{\mathrm{sing}}(H_{c,\ell}, E[p]) \otimes_\chi \mathcal{W}$ over $\mathcal{W}$. On the other hand, Proposition 8.10 says that $d^\chi_\ell\big(\kappa(\ell)\big)$ belongs to the kernel of the $\mathcal{W}$-linear map η_ℓ, and this contradicts the non-triviality of η_ℓ that was shown in Lemma 8.8. □

By exploiting the surjectivity of the representation $\rho_{E,p}$ (condition 3 in Assumption 5.1) and the flatness of $\mathcal{W}$ over $\mathbb{Z}[G_c]$ (Lemma 8.3), formal algebraic considerations yield also the following reformulation of Theorem 8.11.

Theorem 8.12. *If $L_K(E, \chi, 1) \neq 0$ then*

$$\mathrm{Sel}_{p^n}(E/H_c) \otimes_\chi \mathcal{W} = 0$$

for all integers $n \geq 1$.

The reader is referred to [23, Theorem 9.8] for details.

8.6. **Applications.** In this subsection let K' be an extension of K contained in H_c and let

$$\lambda : \mathrm{Gal}\,(K'/K) \longrightarrow \mathbb{C}^\times$$

be a character. Adopting the usual notation for twisted L-functions and eigenspaces, the first consequence of Theorem 8.11 is the following

Theorem 8.13. *If $L_K(E,\lambda,1) \neq 0$ then $E(K')^\lambda = 0$.*

Proof. Let $\chi \in \widehat{G}_c$ be the character induced by λ in the obvious way, so that there is an equality of twisted L-functions

$$L_K(E,\chi,s) = L_K(E,\lambda,s)$$

up to finitely many Euler factors (cf., e.g., [34, §7]). Therefore $L_K(E,\chi,1) \neq 0$, whence $E(H_c)^\chi = 0$ by a combination of Proposition 8.4 and Theorem 8.11. But there is a natural inclusion $E(K')^\lambda \subset E(H_c)^\chi$, and the theorem is proved. □

Theorem 8.13 is the λ-twisted conjecture of Birch and Swinnerton-Dyer for E over K' in the case of analytic rank 0. In fact, under this analytic condition Theorem 8.11 also yields a vanishing result for the groups $\mathrm{Sel}_p(E/K')$ for all prime numbers p satisfying Assumption 5.1 (recall that this excludes only finitely many primes). As will be clear, to obtain this it is crucial that we were able to prove Theorem 8.11 for *all* complex-valued characters χ of G_c.

To begin with, we need some further notation and an auxiliary result. Let $\mathbb{Q}_p^{\mathrm{nr}}$ be the maximal unramified extension of $\mathbb{Q}_p$, let $\mathcal{O}_{\mathbb{Q}_p^{\mathrm{nr}}}$ be its ring of integers and let κ_p be its residue field (which is an algebraic closure of $\mathbb{F}_p$). In order to avoid confusion, for every $\chi \in \widehat{G}_c$ denote by $\mathcal{W}_\chi$ the ring $\mathcal{W}$ associated with χ as in §8.2. Finally, since every $\mathcal{W}_\chi$ is a finite unramified extension of $\mathbb{Z}_p$, for all χ we can (and do) fix embeddings $\mathcal{W}_\chi \hookrightarrow \mathcal{O}_{\mathbb{Q}_p^{\mathrm{nr}}}$, which endow κ_p with a structure of $\mathcal{W}_\chi$-module. Then define

$$\mathrm{Sel}_p(E/K')^\lambda := \big\{ x \in \mathrm{Sel}_p(E/K') \otimes_{\mathbb{Z}} \kappa_p \mid \sigma(x) = \lambda(\sigma)x \text{ for all } \sigma \in \mathrm{Gal}\,(K'/K) \big\}.$$

From here on let p be a prime satisfying Assumption 5.1.

Lemma 8.14. *If $L_K(E,\lambda,1) \neq 0$ then $\mathrm{Sel}_p(E/K')^\lambda = 0$.*

Proof. Let $\chi \in \widehat{G}_c$ be the character induced by λ. Then, as in the proof of Theorem 8.13, $L_K(E,\chi,1) \neq 0$, whence $\mathrm{Sel}_p(E/H_c) \otimes_\chi \mathcal{W}_\chi = 0$ by Theorem 8.11. Since $p \nmid h^+(c)$, one can apply Maschke's theorem to the G_c-representation $\mathrm{Sel}_p(E/H_c) \otimes_{\mathbb{Z}} \kappa_p$ and mimic the proof of [23, Proposition 8.1] to obtain an identification

$$\mathrm{Sel}_p(E/H_c)^\chi = \mathrm{Sel}_p(E/H_c) \otimes_\chi \kappa_p$$

of $\kappa_p[G_c]$-modules. Thus we get that

$$\mathrm{Sel}_p(E/H_c)^\chi = \big(\mathrm{Sel}_p(E/H_c) \otimes_\chi \mathcal{W}_\chi\big) \otimes_{\mathcal{W}_\chi} \kappa_p = 0. \tag{61}$$

On the other hand, as explained in [17, Lemma 4.3], the surjectivity of $\rho_{E,p}$ ensures that E has no non-trivial p-torsion rational over H_c, and then the inflation-restriction exact sequence in Galois cohomology gives an injection $\mathrm{Sel}_p(E/K') \hookrightarrow \mathrm{Sel}_p(E/H_c)$, which in turn induces an injection

$$\mathrm{Sel}_p(E/K')^\lambda \longhookrightarrow \mathrm{Sel}_p(E/H_c)^\chi \tag{62}$$

of eigenspaces. The lemma follows by combining (61) and (62). □

Let now $L_{K'}(E,s)$ be the L-function of E over K'.

Theorem 8.15. *If $L_{K'}(E,1) \neq 0$ then*

$$\mathrm{Sel}_{p^n}(E/K') = 0$$

for all integers $n \geq 1$.

Proof. Routine algebraic considerations show that it is enough to prove the result for $n = 1$. For simplicity, set $G' := \mathrm{Gal}\,(K'/K)$. There is a factorization

$$L_{K'}(E, s) = \prod_{\lambda} L_K(E, \lambda, s) \tag{63}$$

where λ varies over the complex-valued characters of G'. Now observe that the embeddings $\mathcal{W}_\chi \hookrightarrow \mathcal{O}_{\mathbb{Q}_p^{\mathrm{nr}}}$ fixed before induce a bijection between the κ_p-valued and the $\mathbb{C}$-valued characters of G'. Therefore, since $p \nmid [K' : K]$, Maschke's theorem ensures that there is a decomposition

$$\mathrm{Sel}_p(E/K') \otimes_{\mathbb{Z}} \kappa_p = \bigoplus_{\lambda} \mathrm{Sel}_p(E/K')^\lambda \tag{64}$$

as a direct sum of eigenspaces. Since $L_{K'}(E, 1) \neq 0$, equality (63) implies that $L_K(E, \lambda, 1) \neq 0$ for all λ, hence $\mathrm{Sel}_p(E/K')^\lambda = 0$ for all λ by Lemma 8.14. Since $\mathrm{Sel}_p(E/K')$ is a finite-dimensional $\mathbb{F}_p$-vector space, the theorem is an immediate consequence of (64). □

As a piece of notation, for every integer $n \geq 1$ let $Ш_{p^n}(E/K')$ be the p^n-Shafarevich–Tate group of E over K'. Theorem 8.15 immediately yields

Corollary 8.16. *If $L_{K'}(E, 1) \neq 0$ then $Ш_{p^n}(E/K') = 0$ for all $n \geq 1$ and $E(K')$ is finite.*

This is the conjecture of Birch and Swinnerton-Dyer for E over K' in analytic rank 0.

Remark 8.17. 1) The Birch and Swinnerton-Dyer conjecture for E over K' in analytic rank 0 can also be obtained directly from Theorem 8.13 via a decomposition argument analogous to the one used in the proof of Theorem 8.15.

2) If $K' = K$ then Theorem 8.15 is part of a result due to Kolyvagin (a sketch of proof of which can be found in [23, Theorem 9.11]) establishing (unconditionally) the finiteness of $E(K)$ and $Ш(E/K)$ for all quadratic fields K such that $L_K(E, 1) \neq 0$. The key ingredients in Kolyvagin's proof of this theorem are non-vanishing results for the special values of the first derivatives of base changes of $L(E, s)$ to suitable auxiliary *imaginary* quadratic fields and Kolyvagin's results in rank one. In light of this, even in the particular case where $K' = K$ our proof of Theorem 8.15, albeit conditional, is genuinely new, since it takes place entirely "in rank zero" and in the *real* quadratic setting, without invoking any result over imaginary quadratic fields.

3) It should be possible, with some extra effort, to extend the techniques of this article and obtain the finiteness of the full Shafarevich–Tate groups $Ш(E/K')$.

References

[1] D. J. Benson, K. R. Goodearl, Periodic flat modules, and flat modules for finite groups, *Pacific J. Math.* **196** (2000), no. 1, 45–67.

[2] M. Bertolini, H. Darmon, A Birch and Swinnerton-Dyer conjecture for the Mazur–Tate circle pairing, *Duke Math. J.* **122** (2004), no. 1, 181–204.

[3] M. Bertolini, 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.

[4] M. Bertolini, H. Darmon, The rationality of Stark–Heegner points over genus fields of real quadratic fields, *Ann. of Math. (2)* **170** (2009), no. 1, 343–369.

[5] M. Bertolini, H. Darmon, S. Dasgupta, Stark–Heegner points and special values of L-series, in *L-functions and Galois representations*, D. Burns, K. Buzzard and J. Nekovář (eds.), London Mathematical Society Lecture Note Series **320**, Cambridge University Press, Cambridge, 2007, 1–23.

[6] N. Boston, H. Lenstra, K. Ribet, Quotients of group rings arising from two-dimensional representations, *C. R. Acad. Sci. Paris Sér. I Math.* **312** (1991), no. 4, 323–328.

[7] M. Ciavarella, L. Terracini, Towards an analogue of Ihara's lemma for Shimura curves, arXiv:0802.0596.

[8] H. Cohn, *A classical invitation to algebraic numbers and class fields*, Universitext **9**, Springer-Verlag, New York, 1978.

[9] C. Cornut, V. Vatsal, Nontriviality of Rankin–Selberg L-functions and CM points, in *L-functions and Galois representations*, D. Burns, K. Buzzard and J. Nekovář (eds.), London Mathematical Society Lecture Note Series **320**, Cambridge University Press, Cambridge, 2007, 121–186.
[10] H. Darmon, Integration on $\mathcal{H}_p \times \mathcal{H}$ and arithmetic applications, *Ann. of Math. (2)* **154** (2001), no. 3, 589–639.
[11] H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics **101**, American Mathematical Society, Providence, RI, 2004.
[12] S. Dasgupta, Stark–Heegner points on modular Jacobians, *Ann. Sci. École Norm. Sup. (4)* **38** (2005), no. 3, 427–469.
[13] S. Dasgupta, M. Greenberg, $\mathscr{L}$-invariants and Shimura curves, submitted (2009).
[14] F. Diamond, R. Taylor, Nonoptimal levels of mod l modular representations, *Invent. Math.* **115** (1994), no. 3, 435–462.
[15] M. Greenberg, Stark–Heegner points and the cohomology of quaternionic Shimura varieties, *Duke Math. J.* **147** (2009), no. 3, 541–575.
[16] R. Greenberg, G. Stevens, p-adic L-functions and p-adic periods of modular forms, *Invent. Math.* **111** (1993), no. 2, 407–447.
[17] B. H. Gross, Kolyvagin's work on modular elliptic curves, in *L-functions and arithmetic*, J. Coates and M. J. Taylor (eds.), London Mathematical Society Lecture Note Series **153**, Cambridge University Press, Cambridge, 1991, 235–256.
[18] B. H. Gross, J. A. Parson, On the local divisibility of Heegner points, preprint (2006).
[19] Y. Ihara, Shimura curves over finite fields and their rational points, in *Curves over finite fields*, M. D. Fried (ed.), Contemp. Math. **245** (1999), 15–23.
[20] H. Iwaniec, E. Kowalski, *Analytic number theory*, AMS Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004.
[21] S. Ling, Shimura subgroups of Jacobians of Shimura curves, *Proc. Amer. Math. Soc.* **118** (1993), no. 2, 385–390.
[22] M. Longo, V. Rotger, S. Vigni, On rigid analytic uniformizations of Jacobians of Shimura curves, arXiv:0910.3391, submitted.
[23] M. Longo, S. Vigni, On the vanishing of Selmer groups for elliptic curves over ring class fields, *J. Number Theory* **150** (2010), no. 1, 128–163.
[24] E. Lutz, Sur l'équation $y^2 = x^3 - Ax - B$ dans les corps $\mathfrak{p}$-adiques, *J. Reine Angew. Math.* **177** (1937), 238–247.
[25] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **17**, Springer-Verlag, Berlin, 1991.
[26] B. Mazur, H. P. F. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.* **25** (1974), no. 1, 1–61.
[27] A. Popa, Central values of Rankin L-series over real quadratic fields, *Comp. Math.* **142** (2006), no. 4, 811–866.
[28] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.
[29] K. Ribet, Congruence relations between modular forms, in *Proceedings of the International Congress of Mathematicians, vol. 1, 2*, Warsaw (1983), 503–514.
[30] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), no. 4, 259–331.
[31] G. Shimura, Construction of class fields and zeta functions of algebraic curves, *Ann. of Math. (2)* **85** (1967), no. 1, 58–159.
[32] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics **800**, Springer-Verlag, Berlin, 1980.
[33] S.-W. Zhang, Heights of Heegner points on Shimura curves, *Ann. of Math. (2)* **153** (2001), no. 1, 27–147.
[34] S.-W. Zhang, Elliptic curves, L-functions, and CM-points, in *Current Developments in Mathematics* **6**, G. Lusztig, B. Mazur, D. Jerison, A. J. de Jong, W. Schmid and S.-T. Yau (eds.), International Press, Somerville, MA, 2001, 179–219.

M. L.: Dipartimento di Matematica Pura e Applicata, Università di Padova, Via Trieste 63, 35121 Padova, Italy
E-mail address: mlongo@math.unipd.it

V. R., S. V.: Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, C. Jordi Girona 1-3, 08034 Barcelona, Spain
E-mail address: victor.rotger@upc.edu
E-mail address: stefano.vigni@upc.edu