Kolyvagin systems and Iwasawa theory of generalized Heegner cycles

Matteo Longo and Stefano Vigni

Abstract Iwasawa theory of Heegner points on abelian varieties of GL_2 type has been studied by, among others, Mazur, Perrin-Riou, Bertolini, and Howard. The purpose of this ~~paper~~ article is to describe extensions of some of their results in which abelian varieties are replaced by the Galois cohomology of Deligne's p-adic representation attached to a modular form of even weight ~~> 2~~greater than 2. In this setting, the role of Heegner points is played by higher-dimensional Heegner-type cycles that have been recently defined by Bertolini, Darmon, and Prasanna. Our results should be compared with those obtained, via deformation-theoretic techniques, by Fouquet in the context of Hida families of modular forms.

1. Introduction

Initiated by Mazur's paper [20], Iwasawa theory of Heegner points on abelian varieties of GL_2 type (most notably, elliptic curves) has been investigated by, among others, Perrin-Riou (see [29]), Bertolini (see [2], [3]), and Howard (see [13], [14]). A recurrent theme in all these works is the study of pro-p-Selmer groups, where p is a prime number, in terms of Iwasawa modules built out of compatible families of Heegner points over the anticyclotomic $\mathbb{Z}_p$-extension of an imaginary quadratic field. In particular, several results on the structure of Selmer groups obtained by Kolyvagin by using his theory of Euler systems (see

DOI 10.1215/21562261-2019-0005
Received May 11 2016. Revised May 13 2017. Accepted May 18 2017.
2010 Mathematics Subject Classification: Primary 11R23; Secondary 11F11.
Key words and phrases. Iwasawa theory, modular forms, generalized Heegner cycles.
Longo's work was supported in part by PRIN 2010–11 "Arithmetic Algebraic Geometry and Number Theory" and by PRAT 2013 "Arithmetic of Varieties over Number Fields." **Q1**
Vigni's work was supported in part by PRIN 2010–11 "Arithmetic Algebraic Geometry and Number Theory" and by PRA 2013 "Geometria Algebrica e Teoria dei Numeri."

[17]) have been generalized to an Iwasawa-theoretic setting.

The goal of the present ~~paper~~ article is to address similar questions in which abelian varieties are replaced by the Galois cohomology of Deligne's p-adic representation attached to a modular form of even weight ~~>2~~greater than 2. In this context, the role of Heegner points is played by generalized Heegner cycles defined by Bertolini, Darmon, and Prasanna in [5] or, rather, by a variant of them considered by Castella and Hsieh in [8]. As their name suggests, these cycles are a generalization of the Heegner cycles that were introduced by Nekovář in [24] in order to extend Kolyvagin's theory to Chow groups of Kuga–Sato varieties.

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

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

We always assume that f is not a CM form. Let p be a prime number not dividing **Q2**
N, and fix an imaginary quadratic field K of discriminant coprime to Np in which all the prime factors of N split. Fix embeddings $K \hookrightarrow \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, where $\bar{\mathbb{Q}}$ and $\bar{\mathbb{Q}}_p$ denote algebraic closures of $\mathbb{Q}$ and $\mathbb{Q}_p$, respectively. Write F for the totally real number field generated over $\mathbb{Q}$ by the Fourier coefficients a_n of f, let $\mathcal{O}_F$ be the ring of integers of F, and fix an embedding $F \hookrightarrow \bar{\mathbb{Q}}$. The induced embedding $F \hookrightarrow \bar{\mathbb{Q}}_p$ determines a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ above p, and we denote by $V_{f,\mathfrak{p}}$ the p-adic representation of $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ attached to f and $\mathfrak{p}$ by Deligne (see [11]). If $F_{\mathfrak{p}}$ is the completion of F at $\mathfrak{p}$, then $V_{f,\mathfrak{p}}$ is an $F_{\mathfrak{p}}$-vector space of dimension 2 that is equipped with a continuous action of $G_{\mathbb{Q}}$. Let $\mathcal{O}_{\mathfrak{p}}$ be the valuation ring of $F_{\mathfrak{p}}$. In ~~§~~Section 2.2 we introduce the notion of an *admissible triple*: throughout this ~~paper~~ article we assume that $(f, K, \mathfrak{p})$ is such a triple. Here we content ourselves with pointing out that, in addition to the requirement that the primes dividing N split in K, we insist that p be unramified in F and split

in K and that $V_{f,\mathfrak{p}}$ have large Galois image. Moreover, we require that $a_p \in \mathcal{O}_\mathfrak{p}^\times$, which is an ordinariness condition on f at p.

Now let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K (i.e., the unique $\mathbb{Z}_p$-extension of K that is Galois and dihedral over $\mathbb{Q}$), set $\Gamma_\infty := \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$, and form the Iwasawa algebra $\Lambda := \mathcal{O}_\mathfrak{p}[\![\Gamma_\infty]\!] \simeq \mathcal{O}_\mathfrak{p}[\![X]\!]$. Let $V := V_{f,\mathfrak{p}}(k/2)$ be the $k/2$-twist of $V_{f,\mathfrak{p}}$ in the sense of Tate, let T be the $G_\mathbb{Q}$-invariant lattice inside $V_{f,\mathfrak{p}}$ that is defined in [24], and set $A := V/T$. Finally, denote by $H^1_f(K_\infty, A)$ the Bloch–Kato Selmer group of A over K_∞ and by $\mathcal{X}_\infty$ the Pontryagin dual of $H^1_f(K_\infty, A)$, which is finitely generated over Λ (Proposition 2.5). Our main result describes, in particular, the Λ-module structure (up to ~~pseudo-isomorphism~~pseudoisomorphism) of $\mathcal{X}_\infty$.

The key tool in our arguments is a certain Λ-submodule $\mathcal{H}_\infty$ of the pro-p Bloch–Kato Selmer group $\hat{H}^1_f(K_\infty, T)$ of f over K_∞. We introduce this Λ-module, which is built in terms of the generalized Heegner cycles of Bertolini–Darmon–Prasanna as slightly modified by Castella–Hsieh, in Definition 4.16. Two features of the collection of cycles studied by Castella and Hsieh in [8] that we crucially exploit are ~~trace-compatibility and non-triviality~~ trace compatibility and nontriviality along the $\mathbb{Z}_p$-extension K_∞/K, the latter result representing a higher weight analogue of a well-known theorem of Cornut for Heegner points on rational elliptic curves (see [10]). The relation between generalized Heegner cycles and classical Heegner cycles is explained in ~~[5, §2.4]~~[5, Section 2.4]; in particular, it is remarked in ~~*loc. cit.*~~ [5, Section 2.4] that these cycles generate the same $\mathbb{Q}$-vector subspace of the appropriate Chow group. However, the normalization adopted by Castella–Hsieh is crucial for applications to the Kolyvagin system arguments that we describe in our ~~paper~~article.

Let $\iota : \Lambda \to \Lambda$ denote the involution induced by inversion in Γ_∞, and if X is a finitely generated torsion Λ-module, then write $\mathrm{char}(X) \subset \Lambda$ for the characteristic ideal of X. Our main result, which is proved in ~~§~~Section 5.1, is the following.

THEOREM 1.1

Suppose that $(f, K, \mathfrak{p})$ is an admissible triple (in particular, the primes dividing Np split in K). There exist a finitely generated torsion Λ-module M such that $\mathrm{char}(M) = \mathrm{char}(M)^\iota$ *and a ~~pseudo-isomorphism~~ pseudoisomorphism*

$$\mathcal{X}_\infty \sim \Lambda \oplus M \oplus M.$$

Moreover, $\mathrm{char}(M)$ *divides* $\mathrm{char}\Big(\hat{H}^1_f(K_\infty, T)/\mathcal{H}_\infty\Big)$ *as ideals of* Λ.

More generally, we expect Theorem 1.1 to hold when p is unramified in K and $a_p \in \mathcal{O}_\mathfrak{p}^\times$. Under these weaker conditions, we elaborate on the last part of Theorem 1.1 and propose in Conjecture 5.1 the following.

MAIN CONJECTURE

There is an equality $\mathrm{char}(M) = \mathrm{char}\Big(\hat{H}^1_f(K_\infty, T)/\mathcal{H}_\infty\Big)$ of ideals of $\Lambda \otimes_{\mathcal{O}_\mathfrak{p}} F_\mathfrak{p}$.

Our strategy for proving Theorem 1.1 is an extension to higher weights of arguments of Howard for abelian varieties of GL_2 type, ~~i.e.~~that is, for weight 2 eigenforms (see [13], [14]). In turn, Howard's work builds on and refines the theory of Kolyvagin systems developed by Mazur and Rubin (see [21]). More precisely, the main contribution of our ~~paper~~ article is the construction of a Kolyvagin system of generalized Heegner cycles and its application to the study of Iwasawa-theoretic questions for modular forms of even weight ~~≥ 4~~at least 4.

Finally, we remark that, by adopting a deformation-theoretic point of view and using (a generalization of) Howard's big Heegner points (see [16]), essentially the same results have been obtained by Fouquet in the context of Hida families of modular forms (see [12]).

2. Bloch–Kato Selmer groups in $\mathbb{Z}_p$-extensions

Our goal in this section is to introduce the Selmer groups we shall be interested in and state some of their basic properties.

2.1. Bloch–Kato Selmer groups

We begin with a general discussion of Selmer groups of p-adic representations.

For a number field E and a p-adic representation V of the absolute Galois group G_E of E we introduce local conditions as follows. For primes $v \nmid p$ of E we let $H^1_f(E_v, V)$ be the group of unramified cohomology classes, while for primes $v \mid p$ we define $H^1_f(E_v, V)$ to be the kernel of the map induced on cohomology by the natural map $V \to V \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}}$, where B_{cris} is Fontaine's ring of crystalline periods. Moreover, for every place v of E we set

$$H^1_s(E_v, V) := H^1(E_v, V)/H^1_f(E_v, V)$$

and write

$$\partial_v : H^1(E, V) \longrightarrow H^1_s(E_v, V)$$

for the composition of the restriction $H^1(E, V) \to H^1(E_v, V)$ with the canonical projection.

The *Bloch–Kato Selmer group* of V over E ([6, Sections 3 and 5]) is the group $H^1_f(E, V)$ that makes the sequence

$$0 \longrightarrow H^1_f(E, V) \longrightarrow H^1(E, V) \xrightarrow{\prod_v \partial_v} \prod_v H^1_s(E_v, V)$$

exact. If T is a G_E-stable lattice in V, then we set $A := V/T$ and, for all integers $n \geq 1$, let A_{p^n} denote the p^n-torsion of A. There is a canonical isomorphism $A_{p^n} \simeq T/p^nT$.

The projection $p : V \twoheadrightarrow A$ and the inclusion $i : T \hookrightarrow V$ induce maps

$$p : H^1(E, V) \longrightarrow H^1(E, A), \qquad i : H^1(E, T) \longrightarrow H^1(E, V);$$

let us define $H^1_f(E, A) := p\big(H^1_f(E, V)\big)$ and $H^1_f(E, T) := i^{-1}\big(H^1_f(E, V)\big)$. Furthermore, the inclusion $i_n : A_{p^n} \hookrightarrow A$ and the projection $p_n : T \twoheadrightarrow T/p^nT$ induce maps

$$i_n : H^1(E, A_{p^n}) \longrightarrow H^1(E, A), \qquad p_n : H^1(E, T) \longrightarrow H^1(E, T/p^nT);$$

we set $H^1_f(E, T/p^nT) := p_n\big(H^1_f(E, T)\big)$ and $H^1_f(E, A_{p^n}) := i_n^{-1}\big(H^1_f(E, A)\big)$. It can be checked that the isomorphisms $A_{p^n} \simeq T/p^nT$ induce isomorphisms $H^1_f(E, A_{p^n}) \simeq H^1_f(E, T/p^nT)$ between Selmer groups.

Now let $M \in \big\{V, T, A, A_{p^n}, T/p^nT\big\}$. If L/E is a finite extension of number fields, then restriction and corestriction induce maps

$$\mathrm{res}_{L/E} : H^1_f(E, M) \longrightarrow H^1_f(L, M), \qquad \mathrm{cores}_{L/E} : H^1_f(L, M) \longrightarrow H^1_f(E, M).$$

Finally, if E is a number field and ℓ is a prime number, then we set

$$H^i_f(E_\ell, M) := \bigoplus_{\lambda|\ell} H^i_f(E_\lambda, M), \quad H^i_s(E_\ell, M) := \bigoplus_{\lambda|\ell} H^i_s(E_\lambda, M), \quad \partial_\ell := \bigoplus_{\lambda|\ell} \partial_\lambda,$$

the direct sums being taken over the primes λ of E above ℓ.

2.2. Admissible triples

As in the ~~introduction~~Introduction, let f be a normalized newform of weight k for $\Gamma_0(N)$, and write $\mathcal{O}_F$ (~~respectively~~resp., $\mathcal{O}_f$) for the ring of integers (~~respectively~~resp., the order) of the number field F generated by the Fourier coefficients of f. Moreover, let $c_f := [\mathcal{O}_F : \mathcal{O}_f]$ be the conductor of $\mathcal{O}_f$. From now on we assume that

- the form f is not CM in the sense of [30, p. 34, Definition].

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

- $p \,|\, 6N(k-2)!\phi(N)c_f$ where ϕ is Euler's function;
- the image of the p-adic representation

$$\rho_{f,p} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathcal{O}_F \otimes \mathbb{Z}_p)$$

attached to f by Deligne does not contain the set

$$\left\{g \in \mathrm{GL}_2(\mathcal{O}_F \otimes \mathbb{Z}_p) \mid \det(g) \in (\mathbb{Z}_p^\times)^{k-1}\right\}.$$

By [19, Lemma 3.8], which is a consequence of [31, Theorem 3.1], the set Ξ is finite. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}_F$ above p, and let $\mathcal{O}_\mathfrak{p}$ be the completion of $\mathcal{O}_F$ at $\mathfrak{p}$, whose field of fractions will be denoted by $F_\mathfrak{p}$. One recovers, up to isomorphism, $V_{f,\mathfrak{p}}$ from $\rho_{f,p}$ by extending scalars to $\mathbb{Q}_p$ and projecting onto $\mathrm{GL}_2(F_\mathfrak{p})$. Finally, let K be an imaginary quadratic field, and write h_K for its class number.

DEFINITION 2.1

The triple $(f, K, \mathfrak{p})$ is *admissible* if

(1) $p \notin \Xi \cup \{\ell \text{ prime} : \ell \mid h_K\}$;

(2) p does not ramify in F;

(3) the primes dividing Np split in K;

(4) $a_p \in \mathcal{O}_\mathfrak{p}^\times$.

REMARK 2.2

Since Ξ is finite, if f (and hence F) and K are given, then conditions (1) and (2) in Definition 2.1 exclude only finitely many primes. On the other hand, the set of primes satisfying condition (3) has density $\frac{1}{2}$. Finally, in light of results of Serre on eigenvalues of Hecke operators (~~[32, §7.2]~~see [32, Section 7.2]), it seems reasonable to expect that condition (4), which is an ordinariness property of f at p, holds for infinitely many p. In fact, questions of this sort appear to lie in the circle of ideas of the conjectures of Lang and Trotter on the distribution of traces of Frobenius automorphisms acting on elliptic curves (see [18]) and of their extensions to higher weight modular forms (see, e.g., [22], [23]).

Throughout this article we shall always work under the following.

ASSUMPTION 2.3

The triple $(f, K, \mathfrak{p})$ is admissible.

Finally, we also assume, for simplicity, that $\mathcal{O}_K^\times = \{\pm 1\}$, ~~i.e.~~that is, that $K \neq \mathbb{Q}(\sqrt{-1})$ and $K \neq \mathbb{Q}(\sqrt{-3})$.

2.3. The anticyclotomic $\mathbb{Z}_p$-extension of K

In general, for every integer $n \geq 1$ we write $K[n]$ for the ring class field of K of conductor n. The triple $(f, K, \mathfrak{p})$ is assumed to be admissible~~, hence~~; hence, $p \nmid h_K$~~; since~~. Since p is unramified in K, we also have $p \nmid |\mathrm{Gal}(K[p]/K[1])|$. Moreover, $\mathrm{Gal}(K[p^{m+1}]/K[p]) \simeq \mathbb{Z}/p^m\mathbb{Z}$ for all $m \geq 1$. It follows that for all m there is a splitting

$$\mathrm{Gal}(K[p^{m+1}]/K) \simeq \Gamma_m \times \Delta$$

with $\Gamma_m \simeq \mathbb{Z}/p^m\mathbb{Z}$ and $\Delta \simeq \mathrm{Gal}(K[p]/K)$ of order prime to p. For every $m \geq 1$ define K_m as the subfield of $K[p^{m+1}]$ that is fixed by Δ, so that

$$\mathrm{Gal}(K_m/K) = \Gamma_m \simeq \mathbb{Z}/p^m\mathbb{Z}.$$

The field ~~$K_\infty := \cup_{m\geq 1} K_m$~~ $K_\infty := \bigcup_{m\geq 1} K_m$ is the *anticyclotomic* $\mathbb{Z}_p$*-extension* of K; equivalently, it is the $\mathbb{Z}_p$-extension of K that is (generalized) dihedral over $\mathbb{Q}$. Set

$$\Gamma_\infty := \varprojlim_m \Gamma_m = \mathrm{Gal}(K_\infty/K) \simeq \mathbb{Z}_p.$$

Furthermore, for every $m \geq 1$ set $\Lambda_m := \mathcal{O}_\mathfrak{p}[\Gamma_m]$~~, then~~. Then define

$$\Lambda := \varprojlim_m \Lambda_m = \mathcal{O}_\mathfrak{p}[\![\Gamma_\infty]\!].$$

Here the inverse limit is taken with respect to the maps induced by the natural projections $\Gamma_{m+1} \to \Gamma_m$. Let γ be a topological generator of Γ_∞; it is well known that the map

$$\Lambda \xrightarrow{\simeq} \mathcal{O}_{\mathfrak{p}}[\![X]\!], \qquad \gamma \longmapsto 1+X$$

is an isomorphism of $\mathcal{O}_{\mathfrak{p}}$-algebras (see, e.g., [27, Proposition 5.3.5]).

For an abelian pro-p group M write $M^\vee := \mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ for its Pontryagin dual, equipped with the compact-open topology~~(here~~. (Here $\mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}$ denotes continuous homomorphisms of $\mathbb{Z}_p$-modules and $\mathbb{Q}_p/\mathbb{Z}_p$ is discrete~~).~~.) In the rest of the ~~paper~~ article, it will be convenient to use also the alternative definition $M^\vee := \mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}_{\mathfrak{p}}}(M, F_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})$, where $\mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}_{\mathfrak{p}}}$ stands for continuous homomorphisms of $\mathcal{O}_{\mathfrak{p}}$-modules and $F_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}$ is given the discrete topology. It turns out that the two definitions are equivalent, as there is a ~~non-canonical~~ noncanonical isomorphism between $\mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}_{\mathfrak{p}}}(M, F_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}})$ and $\mathrm{Hom}^{\mathrm{cont}}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ that depends on the choice of a $\mathbb{Z}_p$-basis of $\mathcal{O}_{\mathfrak{p}}$. See, ~~e.g.~~for example, [7, Lemma 2.4] for details.

2.4. Selmer groups over K_∞

We resume the notation and conventions that we introduced in ~~§~~Section 2.2; in particular, Assumption 2.3 is in force. As in the ~~introduction~~Introduction, let T be the $G_{\mathbb{Q}}$-representation considered by Nekovář in [24, p. 109], where it is denoted by $A_{\mathfrak{p}}$. This is a free $\mathcal{O}_{\mathfrak{p}}$-module of rank 2. The $G_{\mathbb{Q}}$-representation $V := T \otimes_{\mathcal{O}_{\mathfrak{p}}} F_{\mathfrak{p}}$ is then the $k/2$-twist of the representation $V_{f,\mathfrak{p}}$. Finally, define $A := V/T$. As above, we shall write A_{p^n} for the p^n-torsion submodule of A. Observe that

$$A = \bigcup_{n \geq 1} A_{p^n} = \varinjlim_n A_{p^n}, \tag{1}$$

where the direct limit is taken with respect to the natural inclusions $A_{p^n} \hookrightarrow A_{p^{n+1}}$.

LEMMA 2.4

(1) $H^0(K_m, A) = 0$ *for all* $m \geq 0$.

(2) $H^0(K_\infty, A) = 0$.

(3) $H^0(K_\infty, A_{p^n}) = 0$ *for all* $n \geq 0$.

Proof

Fix an integer $m \geq 0$. The extension $K_m/\mathbb{Q}$ is solvable, so $H^0(K_m, A_{p^n}) = 0$ for all $n \geq 0$ by ~~[19, Lemma 3.10, (2)]~~[19, Lemma 3.10(2)], as $p \notin \Xi$ by Assumption 2.3. It follows from (1) that

$$H^0(K_m, A) = H^0\Big(K_m, \varinjlim_n A_{p^n}\Big) = \varinjlim_n H^0(K_m, A_{p^n}) = 0,$$

which proves part (1). Since $H^0(K_\infty, A) = \varinjlim_m H^0(K_m, A)$, part (2) follows as well. Finally, for all $n \geq 0$ one has $H^0(K_\infty, A_{p^n}) = \varinjlim_m H^0(K_m, A_{p^n})$, which implies part (3). $\square$

Define the discrete Λ-module

$$H^1_f(K_\infty, A) := \varinjlim_m H^1_f(K_m, A),$$

the injective limit being taken with respect to the restriction maps. Let

$$\mathcal{X}_\infty := \mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}_\mathfrak{p}}\big(H^1_f(K_\infty, A), F_\mathfrak{p}/\mathcal{O}_\mathfrak{p}\big)$$

be the Pontryagin dual of $H^1_f(K_\infty, A)$, equipped with its canonical structure of a compact Λ-module. For every $m \geq 0$ let

$$\mathcal{X}_m := \mathrm{Hom}^{\mathrm{cont}}_{\mathcal{O}_\mathfrak{p}}\big(H^1_f(K_m, A), F_\mathfrak{p}/\mathcal{O}_\mathfrak{p}\big)$$

be the Pontryagin dual of $H^1_f(K_m, A)$. Each $\mathcal{X}_m$ has a natural structure of a Λ_m-module, and there is a canonical isomorphism of Λ-modules $\mathcal{X}_\infty \simeq \varprojlim_m \mathcal{X}_m$. Since the Galois representation A is unramified outside Np, the $\mathcal{O}_\mathfrak{p}$-modules $\mathcal{X}_m$ are finitely generated. Using the topological analogue of Nakayama's lemma (see, e.g., [1, p. 226, Corollary], [7, Corollary 1.5] or ~~[27, Corollary 5.2.18, (ii)]~~ [27, Corollary 5.2.18(ii)]), we then obtain the following result.

PROPOSITION 2.5

The Λ-module $\mathcal{X}_\infty$ is finitely generated.

3. The Λ-adic Kolyvagin system argument

In this section we prove a slight generalization of the Λ-adic argument described in [13, §2.2] [13, Section 2.2] that will lead us to Theorem 3.5.

3.1. Selmer triples

Fix a prime number p, a coefficient ring R (i.e., a noetherianNoetherian, complete local ring with finite residue field of characteristic p), an imaginary quadratic field K, and a finitely generated R-module T equipped with a continuous linear action of $G_K := \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ that is unramified outside a finite set Σ of primes of K. Let $\mathfrak{m}$ be the maximal ideal of R, and put $\bar{T} := T/\mathfrak{m}T$. For every prime v of K we write K_v for the completion of K at v and choose a decomposition group $G_{K_v} \subset G_K$, whose inertia subgroup will be denoted by I_{K_v}.

Let $\mathcal{L}_0 = \mathcal{L}_0(T)$ be the set of degree 2 primes of K that do not belong to Σ and do not divide p. We often identify a prime $\lambda \in \mathcal{L}_0$ with its residual characteristic ℓ and write $\lambda \mid \ell$. Consequently, we use indifferently the symbols λ and ℓ to denote the dependence of an object on such a prime; for example, we write either K_λ or K_ℓ for a given $\lambda \in \mathcal{L}_0$. As in [13, Definition 1.2.1], for every $\lambda \in \mathcal{L}_0$ let I_ℓ be the smallest ideal of R containing $\ell + 1$ and such that $\mathrm{Frob}_\lambda \in \mathrm{Gal}(K_v^{\mathrm{unr}}/K_v)$ acts trivially on $T/I_\ell T$. For an integer $k \geq 1$ let $\mathcal{L}_k = \mathcal{L}_k(T)$ be the subset of $\ell \in \mathcal{L}_0$ such that $I_\ell \subset p^k\mathbb{Z}_p$, and for $\lambda \in \mathcal{L}_0$ set $G_\ell := k_\lambda^\times / k_\ell^\times$, where k_λ and k_ℓ are the residue fields at λ and ℓ, respectively. Finally, let $\mathcal{N}_k$ denote the set of square-free products of elements in $\mathcal{L}_k$, and for each $n \in \mathcal{N}_0$ define the ideal $I_n := \sum_{\ell|n} I_\ell$ in R and the group $G_n := \otimes_{\ell|n} G_\ell$ $G_n := \bigotimes_{\ell|n} G_\ell$. By convention, $1 \in \mathcal{N}_k$ for all k, $I_1 = (0)$, and $G_1 = \mathbb{Z}$.

For each prime v of K such that $v \nmid p$ and $v \notin \Sigma$ we write $H^1_{\mathrm{s}}(K_v, T)$ for the *singular* part of $H^1(K_v,T)$, ~~i.e.~~that is, the quotient of $H^1(K_v,T)$ by the *finite* part

$$H^1_{\mathrm{f}}(K_v,T) := H^1_{\mathrm{unr}}(K_v,T) := \ker\Big(H^1(K_v,T) \longrightarrow H^1(K_v^{\mathrm{unr}},T)\Big).$$

For primes v of residual characteristic different from p we also let $K_v^{(p)}$ denote a maximal totally tamely ramified abelian p-extension of K_v and define the *transverse* subgroup as

$$H^1_{\mathrm{tr}}(K_v,T) := \ker\Big(H^1(K_v,T) \longrightarrow H^1(K_v^{(p)},T)\Big).$$

By [13, Proposition 1.1.9], if $|k_v^\times|\cdot T = 0$, then $H^1_{\mathrm{tr}}(K_v,T)$ projects isomorphically onto $H^1_{\mathrm{s}}(K_v,T)$ and there is a canonical splitting

$$H^1(K_v,T) = H^1_{\mathrm{f}}(K_v,T) \oplus H^1_{\mathrm{tr}}(K_v,T).$$

On the other hand, by [13, Proposition 1.1.7] there are canonical isomorphisms

$$H^1_{\mathrm{f}}(K_v,T) \simeq T/(\mathrm{Fr}_v - 1)T, \qquad H^1_{\mathrm{s}}(K_v,T)\otimes k_v^\times \simeq T^{\mathrm{Fr}_v=1},$$

which give a finite-singular comparison isomorphism

$$\phi_v^{\mathrm{fs}} : H^1_{\mathrm{f}}(K_v,T) \simeq T \xrightarrow{\simeq} H^1_{\mathrm{s}}(K_v,T)\otimes k_v^\times$$

when G_{K_v} acts trivially on T.

As in [13, p. 1445], for any $n\ell \in \mathcal{N}_0$ there is a finite-singular isomorphism

$$\phi_\ell^{\mathrm{fs}} : H^1_{\mathrm{f}}(K_\ell, T/I_{n\ell}T) \xrightarrow{\simeq} H^1_{\mathrm{s}}(K_\ell, T/I_{n\ell}T)\otimes G_\ell.$$

Finally, for every prime v of K let

$$\mathrm{loc}_v : H^1(K,T) \longrightarrow H^1(K_v,T)$$

be the localization map.

Now let $(T,\mathcal{F},\mathcal{L})$ be a *Selmer triple*. We refer to [21, Definition 3.1.3] and [13, Definition 1.2.3] for details. In particular, we fix a finite set $\Sigma(\mathcal{F})$ of primes of K containing Σ, all the primes above p, and all the ~~archimedean~~ Archimedean primes. Then $\mathcal{F}$ is a *Selmer structure* on T in the sense of [13, Definition 1.1.10] (cf. also [21, Definition 2.1.1]), so it corresponds to the choice of a local condition (i.e., a subgroup) $H^1_{\mathcal{F}}(K_v,T)\subset H^1(K_v,T)$ at each prime $v\in\Sigma(\mathcal{F})$. Moreover, $\mathcal{L}$ is a subset of $\mathcal{L}_0$ disjoint from $\Sigma(\mathcal{F})$. Let $\mathcal{N}=\mathcal{N}(\mathcal{L})$ be the set of squarefree square-free products of primes in $\mathcal{L}$, with the convention that $1\in\mathcal{N}$.

The *dual* of T is the R-module $T^*:=\mathrm{Hom}_R(T,R(1))$ equipped with the structure of a G_K-module given by $(\sigma\cdot f)(x):=\sigma f(\sigma^{-1}t)$. We define a Selmer structure $\mathcal{F}^*$ on T^* by taking $\Sigma(\mathcal{F}^*)=\Sigma(\mathcal{F})$ and the orthogonal complements with respect to the local Tate pairings as local conditions (see [21, §2.3] [21, Section 2.3] for details). In this way we obtain a Selmer triple $(T^*,\mathcal{F}^*,\mathcal{L})$ such that $\mathcal{F}(n)^*=\mathcal{F}^*(n)$ for all $n\in\mathcal{N}$ (see [21, Example 2.3.2]), where the Selmer structure $\mathcal{F}(n)$ is defined as in [13, Definition 1.2.2].

Denote by $\tau\in G_{\mathbb{Q}}$ the complex conjugation induced by the embedding $\bar{\mathbb{Q}}\hookrightarrow\mathbb{C}$ that we fixed in the introductionIntroduction, so that τ extends the non-trivial nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$. As in [13, §1.3][13, Section 1.3], we require the pair $(T,\mathcal{F})$ to satisfy the following conditions:

(H.0) T is a free R-module of rank 2;

(H.1) $\bar{T}$ is an absolutely irreducible representation of G_K over $R/\mathfrak{m}$;

(H.2) there exists a Galois extension F of $\mathbb{Q}$ containing K such that G_F acts trivially on T and $H^1\big(F(\mu_{p^\infty})/K,\bar{T}\big)=0$;

(H.3) for every $v\in\Sigma(\mathcal{F})$ the local condition $\mathcal{F}$ at v is cartesian Cartesian on the quotient category of T (see [13, Definitions 1.1.2 and 1.1.3] for details);

(H.4) there is a non-degeneratenondegenerate, symmetric, R-bilinear pairing $(\,,\,):T\times T\longrightarrow R(1)$ $(\cdot,\cdot):T\times T\to R(1)$ satisfying $(s^\sigma,t^{\tau\sigma\tau^{-1}})=(s,t)^\sigma$ for every $s,t\in T$ and $\sigma\in G_K$ and such that for every place v of K the local condition $\mathcal{F}$ at v is its own exact orthogonal complement under the induced local pairing

$$\langle\cdot,\cdot\rangle_v:H^1(K_v,T)\times H^1(K_{\bar{v}},T)\longrightarrow R;$$

(H.5) (a) the action of G_K on $\bar{T}$ extends to an action of $G_{\mathbb{Q}}$, and the action of τ splits $\bar{T} = \bar{T}^+ \oplus \bar{T}^-$ into one-dimensional $R/\mathfrak{m}$-subspaces, where $\bar{T}^{\pm}$ is defined as the $\pm$-eigenspace for the action of τ on $\bar{T}$;

(b) the condition $\mathcal{F}$ propagated to $\bar{T}$ (cf. ~~[13, §1.1]~~ [13, Section 1.1] for definitions) is stable under the action of $G_{\mathbb{Q}}$;

(c) if we assume (H.4) to hold, then the residual pairing

$$(\cdot,\cdot) : \bar{T} \times \bar{T} \longrightarrow (R/\mathfrak{m})(1)$$

obtained from ~~(,)~~ $(\cdot,\cdot)$ satisfies $(s^\tau, t^\tau) = (s,t)^\tau$ for all $s, t \in \bar{T}$.

See ~~[13, §1.3]~~ [13, Section 1.3] for a comparison between these conditions and those, similar, in ~~[21, §3.5]~~ [21, Section 3.5]. One then defines the Selmer group attached to the Selmer structure $(T, \mathcal{F})$ as

$$H^1_{\mathcal{F}}(K,T) := \ker\left(H^1(K,T) \longrightarrow \bigoplus_v H^1(K_v,T)/H^1_{\mathcal{F}}(K_v,T) \right). \tag{2}$$

3.2. Kolyvagin systems

Fix a Selmer triple $(T, \mathcal{F}, \mathcal{L})$ such that the pair $(T, \mathcal{F})$ satisfies the assumptions above. Given $c \in \mathcal{N}$, we introduce a new Selmer triple $\big(T, \mathcal{F}(c), \mathcal{L}(c)\big)$ by defining

$$\Sigma\big(\mathcal{F}(c)\big) := \Sigma(\mathcal{F}) \cap \{v : v \mid c\}, \qquad \mathcal{L}(c) := \{v \in \mathcal{L} : v \nmid c\}$$

and taking

$$H^1_{\mathcal{F}(c)}(K_v,T) := \begin{cases} H^1_{\mathcal{F}}(K_v,T) & \text{if } v \nmid c, \\ H^1_{\mathrm{tr}}(K_v,T) & \text{if } v \mid c. \end{cases}$$

For every product $n\ell \in \mathcal{N}_0$ there is a diagram

$$\begin{array}{ccccc} & & & & H^1_{\mathcal{F}(n\ell)}(K, T/I_{n\ell}T) \otimes G_{n\ell} \\ & & & & \downarrow{\scriptstyle \mathrm{loc}_\ell} \\ H^1_{\mathcal{F}(n)}(K, T/I_nT) \otimes G_n & \xrightarrow{\mathrm{loc}_\ell} & H^1_{\mathrm{f}}(K_\ell, T/I_{n\ell}T) \otimes G_n & \xrightarrow{\phi_\ell^{\mathrm{fs}} \otimes 1} & H^1_{\mathrm{s}}(K_\ell, T/I_{n\ell}T) \otimes G_{n\ell} \end{array} \tag{3}$$

whose row is exact. Let $(T, \mathcal{F}, \mathcal{L})$ denote a Selmer triple.

DEFINITION 3.1

A *Kolyvagin system* for $(T, \mathcal{F}, \mathcal{L})$ is a collection $\kappa = \{\kappa_n\}_{n \in \mathcal{N}(\mathcal{L})}$ of classes

$$\kappa_n \in H^1_{\mathcal{F}(n)}(K, T/I_nT) \otimes G_n$$

such that for every $n\ell \in \mathcal{N}(\mathcal{L})$ the images of κ_n and $\kappa_{n\ell}$ under the maps $(\phi_\ell^{\mathrm{fs}} \otimes 1) \circ \mathrm{loc}_\ell$ and loc_ℓ in (3) agree.

The set of all Kolyvagin systems for $(T, \mathcal{F}, \mathcal{L})$ is naturally endowed with an R-module structure. This R-module will be denoted by $\mathbf{KS}(T, \mathcal{F}, \mathcal{L})$; we refer the reader to [13, Remark 1.2.4] and [21, Remark 3.1.4] for the functorial properties enjoyed by it.

3.3. Λ-adic representations

Let $\mathcal{O}$ be the valuation ring of a finite extension $\mathcal{K}$ of $\mathbb{Q}_p$, with maximal ideal $\mathfrak{m} = (\pi)$ and residue field k. Let $\Lambda = \mathcal{O}[\![\Gamma_\infty]\!]$ be the Iwasawa algebra with coefficients in $\mathcal{O}$ of the anticyclotomic $\mathbb{Z}_p$-extension of K. Let T be a free $\mathcal{O}$-module of rank 2 equipped with a continuous linear action of $G_{\mathbb{Q}}$ that is unramified outside a finite set of primes Σ of $\mathbb{Q}$. Set $V := T \otimes_{\mathcal{O}} \mathcal{K}$ and $A := V/T$.

In addition to conditions (H.0)–(H.4) with $R = \mathcal{O}$, we impose on T the following set of assumptions, which are all verified when T, as in the case that concerns us, arises from a modular form.

ASSUMPTION 3.2

(1) The p-adic representation V is crystalline, and for every prime v of K above p its restriction to $G_{\mathbb{Q}_p}$ satisfies the Panchishkin condition, ~~i.e.~~that is, is equipped with a filtration of $G_{\mathbb{Q}_p}$-modules

$$0 \longrightarrow \mathrm{Fil}_v^+(T) \longrightarrow T \longrightarrow \mathrm{Fil}_v^-(T) \longrightarrow 0$$

where $\mathrm{Fil}_v^{\pm}(T)$ are both free of rank 1 over $\mathcal{O}$ and inertia acts on $\mathrm{Fil}_v^-(T)$ by a power of the cyclotomic character.

(2) The pairing in (H.4) gives rise to a pairing

$$(\cdot,\cdot) : T \times A \longrightarrow (\mathcal{K}/\mathcal{O})(1)$$

still denoted by the same symbol, and we require that $\mathrm{Fil}_v^+(T)$ and $\mathrm{Fil}_v^+(A)$ be exact annihilators of each other under $(\ ,\ )$$(\cdot,\cdot)$.

(3) The groups $H^0\big(K_{\infty,v}, \mathrm{Fil}_v^-(A)\big)$ and $H^0\big(K_v, \mathrm{Fil}_v^-(A)\big)$ are finite for all primes $v \mid p$, where $K_{\infty,v}$ denotes the completion of K_∞ at the unique prime v above p.

With notation as in part (1) of Assumption 3.2Assumption 3.2(1), let us define

$$\mathrm{Fil}_v^\pm(V) := \mathrm{Fil}_v^\pm(T) \otimes_{\mathcal{O}} \mathcal{K}, \qquad \mathrm{Fil}_v^\pm(A) := \mathrm{Fil}_v^\pm(V)/\,\mathrm{Fil}_v^\pm(T).$$

For any left G_K-module M and any finite extension L/K we denote by $\mathrm{Ind}_{L/K}(M)$ the induced module from K to L of M, whose elements are functions $f : G_K \to M$ satisfying $f(\sigma x) = \sigma f(x)$ for all $x \in G_K$ and $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/L)$. This is endowed with right and left actions of G_K and $\mathrm{Gal}(L/K)$ defined, respectively, by $(f^\sigma)(x) = f(x\sigma)$ and $(\gamma \cdot f)(x) := \tilde{\gamma} f(\tilde{\gamma}^{-1}x)$ for all $\sigma \in G_K$ and $\gamma \in \mathrm{Gal}(L/K)$, where $\tilde{\gamma} \in G_K$ is any lift of γ. There are corestriction maps

$$\mathrm{Ind}_{K_m/K}(M) \longrightarrow \mathrm{Ind}_{K_{m-1}/K}(M), \qquad f \longmapsto \sum_{\gamma \in \mathrm{Gal}(K_m/K_{m-1})} \gamma \cdot f$$

and restriction maps $\mathrm{Ind}_{K_m/K}(M) \to \mathrm{Ind}_{K_{m+1}/K}(M)$ taking f to itself. Define

$$\mathbf{T} := T \otimes_{\mathcal{O}} \Lambda \simeq \varprojlim_m \mathrm{Ind}_{K_m/K}(T), \qquad \mathbf{A} := \varinjlim_m \mathrm{Ind}_{K_m/K}(A),$$

where the inverse and direct limits are taken with respect to corestrictions and restrictions, respectively. With notation as in Assumption 3.2, we set

$$\mathrm{Fil}_v^\pm(\mathbf{T}) := \mathrm{Fil}_v^\pm(T) \otimes_{\mathcal{O}} \Lambda \simeq \varprojlim_m \mathrm{Ind}_{K_m/K}\big(\mathrm{Fil}_v^\pm(T)\big), \quad \mathrm{Fil}_v^\pm(\mathbf{A}) := \varinjlim_m \mathrm{Ind}_{K_m/K}\big(\mathrm{Fil}_v^\pm(A)\big).$$

We know that for any n prime to p there is an isomorphism

$$H^1(K[n], \mathbf{T}) \simeq \varprojlim_m H^1(K_m[n], T) =: \hat{H}^1(K_\infty[n], T) \tag{4}$$

where the limit on the right is computed with respect to corestrictions. To show this, one can use the arguments in the proof of [9, Proposition II.1.1], as in [21, Lemma 5.3.1].

As in [13, Proposition 2.2.4], one obtains from the pairing ~~$(,) : T \times A \to (\mathcal{K}/\mathcal{O})(1)$~~ $(\cdot,\cdot) : T \times A \to (\mathcal{K}/\mathcal{O})(1)$ in Assumption 3.2 another pairing

$$(\cdot,\cdot)_\infty : \mathbf{T} \times \mathbf{A} \longrightarrow (\mathcal{K}/\mathcal{O})(1) \tag{5}$$

such that $(\lambda x, y)_\infty = (x, \lambda^* y)_\infty$ for all $x \in \mathbf{T}$, $y \in \mathbf{A}$, $\lambda \in \Lambda$, where $\lambda \mapsto \lambda^*$ is the $\mathbb{Z}_p$-linear involution of Λ defined as $\gamma \mapsto \gamma^{-1}$ on ~~group-like~~ grouplike elements. As a consequence of ~~(2) in Assumption 3.2~~Assumption 3.2(2), $\mathrm{Fil}_v^+(\mathbf{T})$ and $\mathrm{Fil}_v^+(\mathbf{A})$ are exact annihilators of each other under ~~$(,)_\infty$~~$(\cdot,\cdot)_\infty$.

For a number field E and a prime $v \mid p$ of E, the *local Greenberg condition* $H^1_{\mathrm{ord}}(E_v, T)$ at v is the kernel of the map from $H^1(E_v, T)$ to $H^1(E_v, \mathrm{Fil}_v^-(T))$; this is also the image of $H^1(E_v, \mathrm{Fil}_v^+(T))$ inside $H^1(E_v, T)$. Then we define *Greenberg's Selmer group* as

$$\mathrm{Sel}_{\mathrm{Gr}}(T/E) := \ker\left(H^1(E,T) \longrightarrow \bigoplus_{v \nmid p} H^1(E_v,T)/H^1_{\mathrm{unr}}(E_v,T) \oplus \bigoplus_{v \mid p} H^1(E_v,T)/H^1_{\mathrm{ord}}(E_v,T)\right).$$

We impose local conditions similar to Greenberg's on the big Galois representation $\mathbf{T}$. More precisely, we define a Selmer structure $\mathcal{F}_\Lambda$ on $\mathbf{T}$ by taking the unramified subgroup of $H^1(K_v, \mathbf{T})$ at primes $v \nmid p$ and

$$H^1_{\mathrm{ord}}(K_v, \mathbf{T}) := \mathrm{im}\Big(H^1\big(K_v, \mathrm{Fil}_v^+(\mathbf{T})\big) \longrightarrow H^1(K_v, \mathbf{T})\Big)$$

at primes $v \mid p$. Then, as in (2), we introduce the corresponding Selmer group $H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$.

3.4. Structure theorems

Fix a height one prime ideal $\mathfrak{P} \neq p\Lambda$ of Λ, write $S_{\mathfrak{P}}$ for the integral closure of $\Lambda/\mathfrak{P}$ in its quotient field $\Phi_{\mathfrak{P}}$, and define $T_{\mathfrak{P}} := T \otimes_{\mathcal{O}} S_{\mathfrak{P}}$. Moreover, set $V_{\mathfrak{P}} := T_{\mathfrak{P}} \otimes_{S_{\mathfrak{P}}} \Phi_{\mathfrak{P}}$. The pairing ~~$(,) : T \times T \to \mathcal{O}(1)$~~ $(\cdot,\cdot) : T \times T \to \mathcal{O}(1)$ gives rise to a pairing $e_{\mathfrak{P}}: T_{\mathfrak{P}} \times T_{\mathfrak{P}} \to S_{\mathfrak{P}}$ satisfying $e_{\mathfrak{P}}(s^\sigma, t^{\tau\sigma\tau^{-1}}) = e_{\mathfrak{P}}(s,t)^\sigma$ for all $s, t \in T_{\mathfrak{P}}$ and all $\sigma \in G_K$ and such that $\mathrm{Fil}^+(T_{\mathfrak{P}})$ is its own exact orthogonal complement.

For any prime v of K above p we define

$$\mathrm{Fil}_v^+(T_{\mathfrak{P}}) := \mathrm{Fil}_v^+(T) \otimes_{\mathcal{O}} S_{\mathfrak{P}}, \qquad \mathrm{Fil}_v^+(V_{\mathfrak{P}}) := \mathrm{Fil}_v^+(T_{\mathfrak{P}}) \otimes_{S_{\mathfrak{P}}} \Phi_{\mathfrak{P}}.$$

As above, the *Greenberg condition* at $v \mid p$ is given by

$$H^1_{\mathrm{ord}}(K_v, V_{\mathfrak{P}}) := \mathrm{im}\Big(H^1\big(K_v, \mathrm{Fil}^+(V_{\mathfrak{P}})\big) \longrightarrow H^1(K_v, V_{\mathfrak{P}})\Big).$$

One then considers the local condition at a prime v of K defined as

$$H^1_{\mathcal{F}_{\mathfrak{P}}}(K_v, V_{\mathfrak{P}}) := \begin{cases} H^1_{\mathrm{ord}}(K_v, V_{\mathfrak{P}}) & \text{if } v \mid p, \\ \\ H^1_{\mathrm{unr}}(K_v, V_{\mathfrak{P}}) & \text{if } v \nmid p. \end{cases}$$

By an abuse of notation, we also denote by $\mathcal{F}_{\mathfrak{P}}$ the local conditions obtained on $T_{\mathfrak{P}}$ and $A_{\mathfrak{P}} := V_{\mathfrak{P}}/T_{\mathfrak{P}}$ by propagation.

PROPOSITION 3.3

Fix an integer $s \geq 1$ and a set of primes $\mathcal{L} \supset \mathcal{L}_s(T_{\mathfrak{P}})$, and suppose that the Selmer triple $(T_{\mathfrak{P}}, \mathcal{F}_{\mathfrak{P}}, \mathcal{L})$ admits a ~~non-trivial~~ nontrivial Kolyvagin system κ.

(1) *$H^1_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}})$ is a free $S_{\mathfrak{P}}$-module of rank 1.*

(2) *$H^1_{\mathcal{F}_{\mathfrak{P}}}(K, A_{\mathfrak{P}}) \simeq \Phi_{\mathfrak{P}}/S_{\mathfrak{P}} \oplus M_{\mathfrak{P}} \oplus M_{\mathfrak{P}}$, where $M_{\mathfrak{P}}$ is a finite $S_{\mathfrak{P}}$-module with*

$$\mathrm{length}(M_{\mathfrak{P}}) \leq \mathrm{length}\Big(H^1_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}})/(S_{\mathfrak{P}} \cdot \kappa_1)\Big).$$

Proof

As in the proof of [13, Proposition 2.1.3], we can apply [13, Theorem 1.6.1] once we show that $T_{\mathfrak{P}}$ satisfies (H.1)–(H.5). The verification of this property goes as in the proof of [13, Proposition 2.1.3]; we just need to replace $E[p]$ and $E(K_\infty)[p]$ in

~~*loc. cit.*~~ [13, Proposition 2.1.3] with A_p and $A_p(K_\infty)$, respectively, and observe that $A_p(K_\infty) = 0$ by ~~part (3) of Lemma 2.4~~Lemma 2.4(3). □

The involution ι of Λ that is induced by $\gamma \mapsto \gamma^{-1}$ on ~~group-like~~ grouplike elements gives a map $S_{\mathfrak{P}} \to S_{\mathfrak{P}^\iota}$ that will be denoted by the same symbol. The map $\psi(t \otimes \alpha) = t^\tau \otimes \alpha^\iota$ induces a bijection $T_{\mathfrak{P}} \to T_{\mathfrak{P}^\iota}$, while the map $(x, y) \mapsto \mathrm{tr} \circ e_{\mathfrak{P}}(\psi^{-1}(x), y)$ (where tr is the trace form) defines a perfect, G_K-equivariant pairing ~~$(,) : T_{\mathfrak{P}^\iota} \times A_{\mathfrak{P}} \to \mu_{p^\infty}$~~ $(\cdot,\cdot) : T_{\mathfrak{P}^\iota} \times A_{\mathfrak{P}} \to \mu_{p^\infty}$ satisfying $(\lambda x, y) = (x, \lambda^\iota y)$. Dualizing $\mathbf{T}/\mathfrak{P}^\iota\mathbf{T} \to T_{\mathfrak{P}^\iota}$ and using the pairing above and the pairing ~~$(,)_\infty$~~ $(\cdot,\cdot)_\infty$ in (5), we obtain a G_K-equivariant map $A_{\mathfrak{P}} \to \mathbf{A}[\mathfrak{P}]$ that gives a map

$$H^1_{\mathcal{F}_{\mathfrak{P}}}(K, A_{\mathfrak{P}}) \longrightarrow H^1_{\mathcal{F}_{\mathfrak{P}}}(K, \mathbf{A})[\mathfrak{P}]. \tag{6}$$

Also, the projection $\mathbf{T} \twoheadrightarrow T_{\mathfrak{P}}$ induces a map

$$H^1_{\mathcal{F}_{\mathfrak{P}}}(K, \mathbf{T})/\mathfrak{P}H^1_{\mathcal{F}_{\mathfrak{P}}}(K, \mathbf{T}) \longrightarrow H^1_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}}). \tag{7}$$

PROPOSITION 3.4

For all but finitely many prime ideals $\mathfrak{P}$ of Λ the maps (6) *and* (7) *have finite kernel and cokernels that are bounded by a constant depending only on* $[S_{\mathfrak{P}} : \Lambda/\mathfrak{P}]$.

Proof

The statement follows from the analogues of [13, Lemma 2.2.7 and Proposition 2.2.8]. The only difference with respect to ~~*loc. cit.*~~ [13, Lemma 2.2.7 and Proposition 2.2.8] is in the case $v \mid p$ of [13, Lemma 2.2.7], for which one has to use ~~condition (3) in Assumption 3.2~~Assumption 3.2(3). □

The next result is the counterpart of [13, Theorem 2.2.10].

THEOREM 3.5

Let $(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L})$ *be a Selmer triple satisfying* (H.1)–(H.5) *and Assumption 3.2. Set* $X := H^1_{\mathcal{F}_\Lambda}(K, \mathbf{A})^\vee$*. Suppose that for some* $s \geq 1$ *the Selmer triple* $(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L}_s)$ *admits a Kolyvagin system* κ *with* $\kappa_1 \neq 0$*. Then*

(1) $H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ *is a torsion-free* Λ*-module of rank* 1*;*

(2) *there exist a torsion* Λ*-module* M *such that* $\mathrm{char}(M) = \mathrm{char}(M)^\iota$ *and a* ~~*pseudo-isomorphism*~~ *pseudoisomorphism*

$$X \sim \Lambda \oplus M \oplus M;$$

(3) $\mathrm{char}(M)$ *divides* $\mathrm{char}\big(H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\Lambda\kappa_1\big)$.

Proof

One first replaces [13, Propositions 2.1.3 and 2.2.8] with Propositions 3.3 and 3.4, respectively, and uses them, together with the vanishing $A_p(K_\infty) = 0$ of ~~part (3) of Lemma 2.4~~Lemma 2.4(3), to show as in [13, Lemma 2.2.9] that $H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ is torsion-free over Λ. Then one proceeds as in the proof of [13, Theorem 2.2.10]. $\square$

4. The Λ-adic Kolyvagin system of generalized Heegner cycles

The goal of this section is to explain how the generalized Heegner cycles of Bertolini, Darmon, and Prasanna (see [5]) can be used to define a Kolyvagin system in the sense of the previous section. Actually, we will use a variant of these cycles introduced by Castella and Hsieh in [8].

From here on, as in ~~§~~Section 2.4, T denotes the $k/2$-twist of the $\mathbb{Z}_p$-representation that is attached to the modular form f satisfying Assumption 2.3. As before, write F for the number field generated over $\mathbb{Q}$ by the Fourier coefficients of f and $\mathcal{O}_F$ for the ring of integers of F. Fix a prime $\mathfrak{p}$ of F above p, and let $F_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ be the completions of F and $\mathcal{O}_F$ at $\mathfrak{p}$, respectively. With the notation of ~~§~~Section 3.3, we take $\mathcal{K} = F_\mathfrak{p}$ and $\mathcal{O} = \mathcal{O}_\mathfrak{p}$. Finally, let K be the imaginary quadratic field that was chosen in the ~~introduction~~Introduction.

4.1. Generalized Heegner cycles

Let $\mathcal{L}_0(\mathbf{T})$ denote the set of degree 2 primes of K that do not divide p and any other prime at which $\mathbf{T}$ is ramified. For any integer $k \geq 0$ define $\mathcal{L}_k(\mathbf{T})$ to be the subset of $\ell \in \mathcal{L}_0(\mathbf{T})$ such that $I_\ell \subset p^k\mathbb{Z}_p$. Let $\mathcal{L} := \mathcal{L}_1(\mathbf{T})$, so that $(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L})$ is a Selmer triple, and let $\mathcal{N} := \mathcal{N}(\mathcal{L})$. Finally, for every $\ell \in \mathcal{N}$ write λ for the unique prime of K above ℓ, and fix a prime $\bar{\lambda}$ of $\bar{\mathbb{Q}}$ above ℓ.

Now let $n \in \mathcal{N}$, and let $K_m[n]$ denote the composite of K_m and $K[n]$. Put $K_0 := K$, and define $K_\infty[n] := \varinjlim_m K_m[n]$. The prime $\bar{\lambda}$ determines a prime $\lambda_{np^m} \in K_m[n]$; we denote by $K_m[n]_{\bar{\lambda}}$ the completion of $K_m[n]$ at λ_{np^m}.

For each $m \geq 0$ let $z_{np^m} \in H^1(K[np^m], T)$ be the class defined in ~~[8, eq. (4.6)]~~ [8, (4.6)] when χ is the trivial character~~(thus~~. (Thus, this is the class denoted by z_{f,χ,np^m} in ~~*loc. cit.*~~ [8, (4.6)] for χ equal to the trivial character~~).~~.) As is explained in [8, Section 4], these classes are built in terms of the generalized Heegner cycles introduced by Bertolini, Darmon, and Prasanna in [5], to which the reader is referred for details. Actually, by [19, Theorem 2.4], for each m the class z_{np^m} belongs to the Selmer group $H^1_f(K[np^m], T)$. Define

$$\alpha_m[n] := \mathrm{cores}_{K[np^{m+1}]/K_m[n]}(z_{np^{m+1}}) \in H^1_f(K_m[n], T). \tag{8}$$

4.2. Iwasawa modules of generalized Heegner cycles

Set $\mathcal{G}(n) := \mathrm{Gal}(K[n]/K)$, and let $\sigma_\wp, \sigma_{\bar{\wp}} \in \mathcal{G}(n)$ be the Frobenius automorphisms at the two primes $\wp$, $\bar{\wp}$ of K above p. We observe, in passing, that $\sigma_{\bar{\wp}} = \sigma_\wp^{-1}$. Now define the following elements of $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$:

$$\begin{aligned} \gamma_1 &:= a_p - p^{(k-2)/2}(\sigma_\wp + \sigma_{\bar{\wp}}), \\ \gamma_2 &:= a_p\gamma_1 - p^{k-2}(p-1) = a_p^2 - p^{(k-2)/2}a_p(\sigma_\wp + \sigma_{\bar{\wp}}) - p^{k-2}(p-1). \end{aligned} \tag{9}$$

~~Notice~~ Note that $p - 1 = \big[K[np^m] : K_{m-1}[n]\big]$ for all m and n. Finally, define

$$\gamma_m := a_p\gamma_{m-1} - p^{k-1}\gamma_{m-2} \tag{10}$$

recursively for all $m \geq 3$. These are higher weight analogues of the elements introduced by Perrin-Riou in [29, §3.3] [29, Section 3.3] in the case of elliptic curves and then considered also by Howard in [13, §2.3][13, Section 2.3].

LEMMA 4.1

For all $n \geq 1$ one has the following relations:

(1) $\mathrm{cores}_{K_{m+1}[n]/K_m[n]}(\alpha_{m+1}[n]) = a_p\alpha_m[n] - p^{k-2}\mathrm{res}_{K_m[n]/K_{m-1}[n]}(\alpha_{m-1}[n])$ $\forall\ m \geq 1$;

(2) $\mathrm{cores}_{K_m[n\ell]/K_m[n]}(\alpha_m[n\ell]) = a_\ell\alpha_m[n]$ *for all primes* $\ell \nmid c$ *inert in* K *and all* $m \geq 0$;

(3) $\mathrm{loc}_\ell(\alpha_m[n\ell]) = \mathrm{res}_{K_m[n\ell]_{\bar\lambda}/K_m[n]_{\bar\lambda}}\left(\mathrm{loc}_\ell(\alpha_m[n])^{\mathrm{Frob}_\ell}\right)$ *for all primes* $\ell \nmid cN$ *inert in* K;

(4) $\mathrm{cores}_{K_m[n]/K[n]}(\alpha_m[n]) = \gamma_{m+1}z_n\ \forall\ m \geq 0$.

Proof

Upon taking corestrictions, parts (1), (2), and (3) follow from the formulas

- $\mathrm{cores}_{K[np^{m+1}]/K[np^m]}(z_{np^{m+1}}) = a_p z_{np^m} - p^{k-2}\mathrm{res}_{K_{np^m}/K_{np^{m-1}}}(z_{np^{m-1}})$,
- $\mathrm{cores}_{K[n\ell p^m]/K[np^m]}(z_{n\ell p^m}) = a_\ell z_{np^m}$,
- $\mathrm{loc}_\ell(z_{n\ell p^m}) = \mathrm{res}_{K[n\ell p^m]_{\bar\lambda}/K[np^m]_{\bar\lambda}}\left(\mathrm{loc}_\ell(z_{np^m})^{\mathrm{Frob}_\ell}\right)$

in [8, Propositions 4.4 and 4.7]. Part (4) follows inductively from (1) and (2), the only step that needs some clarification being for $m = 0$. To deal with this case, one applies the equality

$$a_p z_n = p^{(k-2)/2}(\sigma_\wp + \sigma_{\bar\wp})z_n + \mathrm{cores}_{K[np]/K[n]}(z_{np}), \tag{11}$$

which is the higher weight counterpart of a formula for Heegner points that can be found in [4, §2.5][4, Section 2.5]. While not explicitly stated in the final version of [8], formula (11) can be checked by arguments analogous to those in the proof of [8, Proposition 4.4]. □

Now note that, since p is unramified in F, the maximal ideal of $\mathcal{O}_\mathfrak{p}$ is generated by p.

LEMMA 4.2

If u is an invertible element of $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$, then $u+px$ is invertible in $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$ for all $x \in \mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$.

Proof

Let $x \in \mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$. Setting $y := u^{-1}x$, we can equivalently show that $1+py$ is invertible in $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$. To begin with, note that there is a ring isomorphism

$$\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)] \xrightarrow{\simeq} \varprojlim_r \big((\mathcal{O}_\mathfrak{p}/p^r\mathcal{O}_\mathfrak{p})[\mathcal{G}(n)]\big), \tag{12}$$

the inverse limit being taken with respect to the obvious maps. Moreover, for all $r \geq 1$ write $\pi_r : \mathcal{O}_\mathfrak{p}[\mathcal{G}(n)] \twoheadrightarrow (\mathcal{O}_\mathfrak{p}/p^r\mathcal{O}_\mathfrak{p})[\mathcal{G}(n)]$ for the canonical (surjective) homomorphism. Now define for all $r \geq 1$ the element $\vartheta_r \in \mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$ as

$$\vartheta_r := \begin{cases} 1 & \text{if } r = 1, \\ 1 - py & \text{if } r = 2, \\ (1-py) \cdot \prod_{i=3}^{r}\big(1 + (py)^{2^{i-2}}\big) & \text{if } r \geq 3. \end{cases}$$

A straightforward computation shows that the inverse of $1+py$ is the element of $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$ corresponding to $\big(\pi_r(\vartheta_r)\big)_{r\geq 1}$ under isomorphism (12). □

REMARK 4.3

Of course, Lemma 4.2 remains valid if $\mathcal{G}(n)$ is replaced by any abelian group and $\mathcal{O}_\mathfrak{p}$ is replaced by any p-adically complete ring.

COROLLARY 4.4

The element γ_m *is invertible in* $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$ *for all* $m \geq 1$.

Proof

Since a_p is invertible in $\mathcal{O}_\mathfrak{p}$ and hence, ~~*a fortiori*~~a fortiori, in $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$, definitions (9) and Lemma 4.2 ensure that both γ_1 and γ_2 are invertible in $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$. Finally, the fact that γ_m is invertible for all $m \geq 3$ can be proved inductively by using the recursive formula (10) and, again, Lemma 4.2. □

REMARK 4.5

The invertibility of γ_m for all $m \geq 1$ is peculiar to our higher weight setting. In fact, in the case of weight 2 that is considered, ~~e.g.~~ for example, in [13] the corresponding element γ_1, which is denoted by γ_0 in *loc. cit.*, is not, in general, invertible~~(in~~ . (In particular, Lemma 4.2 does not apply~~).~~ .) It turns out that Corollary 4.4 allows us to simplify some of the arguments used in [13] and extended to higher weights in the present ~~paper~~article. **Q3**

Let

$$\text{aug} : \mathcal{O}_\mathfrak{p}[\mathcal{G}(n)] \longrightarrow \mathcal{O}_\mathfrak{p}, \qquad \sum_{\sigma \in \mathcal{G}(n)} c_\sigma \sigma \longmapsto \sum_{\sigma \in \mathcal{G}(n)} c_\sigma$$

be the augmentation map, which is an $\mathcal{O}_\mathfrak{p}$-algebra homomorphism.

COROLLARY 4.6

The element $\text{aug}(\gamma_m)$ *is invertible in* $\mathcal{O}_\mathfrak{p}$ *for all* $m \geq 1$.

Proof

~~An~~ This is an immediate consequence of Corollary 4.4. □

Recall the classes $\alpha_j[n]$ that we introduced in (8). For every $m \geq 0$ and $n \in \mathcal{N}$ denote by $\mathcal{H}_m[n]$ the $\mathcal{O}_{\mathfrak{p}}[\mathrm{Gal}(K_m[n]/K)]$-submodule of $H^1_f(K_m[n], T)$ generated by the restrictions of the classes z_n and $\alpha_j[n]$ for all $j \leq m$. Now recall the group $\hat{H}^1(K_\infty[n], T)$ of (4), and define the $\Lambda[\mathcal{G}(n)]$-module

$$\hat{H}^1_f(K_\infty[n], T) := \varprojlim_m H^1_f(K_m[n], T) \subset \hat{H}^1(K_\infty[n], T) \simeq H^1(K[n], \mathbf{T}), \qquad (13)$$

where the inverse limit is taken with respect to the corestriction maps and the isomorphism is the one appearing in (4).

DEFINITION 4.7

The *Iwasawa module of generalized Heegner cycles of tame conductor* n is the compact $\Lambda[\mathcal{G}(n)]$-module

$$\mathcal{H}_\infty[n] := \varprojlim_m \mathcal{H}_m[n] \subset \hat{H}^1_f(K_\infty[n], T),$$

the inverse limit being taken with respect to the corestriction maps.

REMARK 4.8

In light of isomorphism (4), according to convenience we shall sometimes view $\mathcal{H}_\infty[n]$ as contained in $H^1(K[n], \mathbf{T})$.

The next proposition is essentially a consequence of Corollary 4.4, and its proof proceeds along the lines of that of [13, Lemma 2.3.3]. However, it is convenient to quickly review the arguments, as this will give us the occasion to introduce some notation that will be used later in the proof of Theorem 4.18.

PROPOSITION 4.9

There exists a family

$$\left\{\beta[n] = (\beta_m[n])_{m\geq 0} \in \mathcal{H}_\infty[n]\right\}_{n\in\mathcal{N}}$$

such that $\beta_0[n] = z_n$ *and*

$$\mathrm{cores}_{K_\infty[n\ell]/K_\infty[n]}\big(\beta[n\ell]\big) = a_\ell \cdot \beta[n]$$

for any $n\ell \in \mathcal{N}$.

Proof

Fix $n \in \mathcal{N}$. For each $m \geq 0$ let $\tilde{\mathcal{H}}_m$ be the quotient of the free $\mathcal{O}_\mathfrak{p}[\mathrm{Gal}(K_m[n]/K)]$-module with a set of generators $\{x, x_j \mid 0 \leq j \leq m\}$ modulo the following relations:

- $\sigma(x) = x$ for all $\sigma \in \mathrm{Gal}(K_m[n]/K[n])$;
- $\sigma(x_j) = x_j$ for all $\sigma \in \mathrm{Gal}(K_m[n]/K_j[n])$ and all $j \leq m$;
- $\mathrm{tr}_{K_j[n]/K_{j-1}[n]}(x_j) = a_p x_{j-1} - p^{k-2} x_{j-2}$ for $j \geq 2$;
- $\mathrm{tr}_{K_1[n]/K[n]}(x_1) = \gamma_2 x$ and $x_0 = \gamma_1 x$.

It follows that

$$\mathrm{tr}_{K_j[n]/K[n]}(x_j) = \gamma_{j+1} x \tag{14}$$

for all $j \leq m$. There are inclusions $\tilde{\mathcal{H}}_m \hookrightarrow \tilde{\mathcal{H}}_{m+1}$ and canonical maps $\mathrm{tr}_{n,m} : \tilde{\mathcal{H}}_n \to \tilde{\mathcal{H}}_m$ induced by the trace for all $m \leq n$~~(in~~. (In particular, $\mathrm{tr}_{s,m} = \mathrm{tr}_{n,m} \circ \mathrm{tr}_{s,n}$ for all $m \leq n \leq s$~~).~~.) By Lemma 4.10 below, $x \in \tilde{\mathcal{H}}_0$ is a trace from every $\tilde{\mathcal{H}}_m$, so we can choose an element

$$y \in \tilde{\mathcal{H}}_\infty := \varprojlim_m \tilde{\mathcal{H}}_m$$

that lifts x. For each divisor t of n we define a map $\phi(t) : \tilde{\mathcal{H}}_\infty \to \mathcal{H}_\infty[t]$ by sending x_m to $\alpha_m[n]$ and x to z_t. Now set $\beta[t] := \phi(t)(y)$. For all $t\ell \mid n$ the square

$$\begin{array}{ccc}
\tilde{\mathcal{H}}_\infty & \xrightarrow{\phi(t\ell)} & \mathcal{H}_\infty[t\ell] \\
\Big\downarrow{\scriptstyle a_\ell} & & \Big\downarrow{\scriptstyle \mathrm{cores}_{K_\infty[t\ell]/K_\infty[t]}} \\
\tilde{\mathcal{H}}_\infty & \xrightarrow{\phi(t)} & \mathcal{H}_\infty[t]
\end{array}$$

is commutative, so we get a family $\{\beta[t]\}_{t|n}$ with the desired properties.

To conclude, it is enough to note that the Λ-module of these families with t running over the divisors of n is compact~~, hence~~; hence, the limit over all $n \in \mathcal{N}$ is ~~non-empty~~nonempty. □

In the next lemma we freely use the notation introduced in the proof of Proposition 4.9.

LEMMA 4.10

The element $x \in \tilde{\mathcal{H}}_0$ is a trace from $\tilde{\mathcal{H}}_m$ for every $m \geq 0$.

Proof

The claim for $m = 0$ being trivial, let $m \geq 1$. By ~~equality~~ (14), we know that

$$\mathrm{tr}_{m,0}(x_m) = \mathrm{tr}_{K_m[n]/K[n]}(x_m) = \gamma_{m+1}x. \tag{15}$$

By Corollary 4.4, the element γ_{m+1} is invertible in $\mathcal{O}_{\mathfrak{p}}[\mathcal{G}(n)]$~~, thus~~; thus, (15) can be written as

$$x = \gamma_{m+1}^{-1}\mathrm{tr}_{m,0}(x_m). \tag{16}$$

On the other hand, for all $\xi \in \mathcal{G}(n)$ and any $\xi_m \in \mathrm{Gal}(K_m[n]/K)$ such that $\xi_m|_{K[n]} = \xi$ one has

$$\xi\mathrm{tr}_{m,0}(x_m) = \mathrm{tr}_{m,0}(\xi_m x_m), \tag{17}$$

with $\xi_m x_m \in \tilde{\mathcal{H}}_m$. In light of (16), by linearity, (17) implies that $x = \mathrm{tr}_{m,0}(w)$ for a suitable $w \in \tilde{\mathcal{H}}_m$, as was to be shown. □

4.3. An alternative description of the elements γ_m

Our goal here is to provide an alternative description of the elements γ_m introduced in (9) and (10). Unlike what is done in the rest of the ~~paper~~article, just for this ~~subsection~~ section we do not assume that a_p is invertible in $\mathcal{O}_{\mathfrak{p}}$ and we take $k \geq 2$, ~~i.e.~~that is, we also deal with the $k = 2$ case that is studied, ~~e.g.~~for example, in [13] and [29]. Albeit not necessary for our subsequent arguments, the result we prove (or, better, its specialization to $k = 2$) is crucially used in [29], and implicitly in [13] as well, where Corollary 4.4 is not available.

With $\sigma_\wp$ and $\sigma_{\bar{\wp}}$ as in ~~§~~Section 4.2, define the following elements of $\mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$:

$$\varrho := p^{k/2} - a_p\sigma_\wp + p^{(k-2)/2}\sigma_\wp^2,$$

$$\bar{\varrho} := p^{k/2} - a_p\sigma_{\bar{\wp}} + p^{(k-2)/2}\sigma_{\bar{\wp}}^2,$$

$$\Phi := \varrho \cdot \bar{\varrho}.$$

The next result is the counterpart of ~~[29, §3.3, Lemme 4]~~ [29, Section 3.3, Lemme 4] for general (even) weight $k \geq 2$.

PROPOSITION 4.11

For all $m \geq 2$ there exist $q_m, r_m \in \mathcal{O}_\mathfrak{p}[\mathcal{G}(n)]$ with $q_{m+1} \equiv a_p q_m \pmod p$, $q_2 = 1$ such that

$$\gamma_m = q_m\Phi + p^{(m-1)k/2} r_m. \tag{18}$$

Proof

One can proceed with an inductive argument as is done in ~~[29, §3.3, Lemme 4]~~ [29, Section 3.3, Lemme 4] for $k = 2$. However, since the proof given in ~~*loc. cit.*~~ [29, Section 3.3, Lemme 4] is quite sketchy, we offer a complete proof in the more complicated case where $k \geq 2$.

To begin with, define the elements r_m recursively by the formulas

- $s_1 := 0$ and $s_{m+1} := \sigma_\wp s_m - \sigma_{\bar{\wp}}^{m-1}$ for all $m \geq 1$,
- $r_m := \varrho s_m + \sigma_{\bar{\wp}}^{m-1}\gamma_0$ for all $m \geq 2$.

As can be easily checked by a direct computation, for $m = 2$ one has $\gamma_2 = \Phi + p^{k/2} r_2$. Next we treat the case $m = 3$. Using the case $m = 2$, we get

$$\gamma_3 = a_p\Phi + p^{k/2}\Big(a_p r_2 - p^{(k-2)/2}\gamma_1\Big). \tag{19}$$

Moreover, there is an equality

$$a_p r_2 - p^{(k-2)/2}\gamma_1 - p^{k/2} r_3 = \Phi(\sigma_\wp + \sigma_{\bar\wp}),$$

which combined with (19) gives the identity

$$\gamma_3 = \Big(a_p + p^{k/2}(\sigma_\wp + \sigma_{\bar\wp})\Big)\Phi + p^k r_3.$$

Putting $q_3 := a_p + p^{k/2}(\sigma_\wp + \sigma_{\bar\wp})$ proves (18) for $m = 3$. Now fix an $m \geq 4$, and assume that the statement of the lemma is true for all integers t with $2 \leq t \leq m-1$. First of all, straightforward calculations show that

$$a_p r_{m-1} - p^{(k-2)/2} r_{m-2} - p^{k/2} r_m = \Phi\Big(s_{m-2}\sigma_\wp^2 + \sigma_{\bar\wp}^{m-2} + \sigma_{\bar\wp}^{m-4}\Big). \tag{20}$$

Using the inductive assumption for γ_{m-1} and γ_{m-2}, we obtain

$$\begin{aligned}
\gamma_m &= a_p\gamma_{m-1} - p^{k-1}\gamma_{m-2}\\
&= a_p\Big(q_{m-1}\Phi + p^{(m-2)k/2} r_{m-1}\Big) - p^{k-1}\Big(q_{m-2}\Phi + p^{(m-3)k/2} r_{m-2}\Big)\\
&= \Phi\Big(a_p q_{m-1} - p^{k-1} q_{m-2}\Big) + p^{(m-2)k/2}\Big(a_p r_{m-1} - p^{(k-2)/2} r_{m-2}\Big)\\
&= \Phi\Big(a_p q_{m-1} - p^{k-1} q_{m-2} + p^{(m-1)k/2}\big(s_{m-2}\sigma_\wp^2 + \sigma_{\bar\wp}^{m-2} + \sigma_{\bar\wp}^{m-4}\big)\Big) + p^{(m-1)k/2} r_m,
\end{aligned}$$

the last equality being a consequence of (20). Finally, setting

$$q_m := a_p q_{m-1} - p^{k-1} q_{m-2} + p^{(m-1)k/2}\Big(s_{m-2}\sigma_\wp^2 + \sigma_{\bar\wp}^{m-2} + \sigma_{\bar\wp}^{m-4}\Big)$$

proves the proposition. □

4.4. Kolyvagin systems

Recall the classes $\beta[n]$ for $n \in \mathcal{N}$ constructed in Proposition 4.9. For each prime $\ell \in \mathcal{N}$ let σ_ℓ be a generator of G_ℓ, and define Kolyvagin's derivative as

$$D_\ell := \sum_{i=1}^{\ell} i\sigma_\ell^i \in \mathbb{Z}[G_\ell].$$

More generally, for every $n \in \mathcal{N}$ set $G(n) := \prod_{\ell|n} G_\ell$ and $D_n := \prod_{\ell|n} D_\ell$, the products being taken over all the primes ℓ dividing n. We also adopt the convention that $G(1)$ is trivial and D_1 is the identity operator. Now fix a set S

of representatives of $G(n)$ in $\mathcal{G}(n)$, and let

$$\tilde{\kappa}_n := \sum_{s\in S} sD_n\beta[n] \in \mathcal{H}_\infty[n] \subset \hat{H}^1(K_\infty[n],T) \simeq H^1(K[n],\mathbf{T}). \tag{21}$$

The image of $\tilde{\kappa}_n$ in $H^1(K[n],\mathbf{T}/I_n\mathbf{T})$ is fixed by $\mathcal{G}(n)$. Define $\kappa_n \in H^1(K,\mathbf{T}/I_n\mathbf{T})$ to be the element mapping to $\tilde{\kappa}_n$ via the isomorphism

$$H^1(K,\mathbf{T}/I_n\mathbf{T}) \xrightarrow{\simeq} H^1(K[n],\mathbf{T}/I_n\mathbf{T})^{\mathcal{G}(n)}$$

induced by restriction. Note that this map is indeed bijective because

- $H^0(K[n],\mathbf{T}/I_n\mathbf{T}) \simeq \varprojlim_m H^0(K_m[n],T/I_nT)$;
- $H^0(K_m[n],T/I_nT) = 0$ since $T/I_nT \simeq A[I_n]$ and A has no ~~non-trivial~~ nontrivial p-torsion over $K_m[n]$ for any m,n.

To check the first assertion one can proceed as in the proof of [9, Proposition II.1.1], while, as $p \notin \Xi$ by Assumption 2.3, the second claim is a consequence, by ~~[19, Lemma 3.10, (2)]~~[19, Lemma 3.10(2)], of the fact that the extension $K_m[n]/\mathbb{Q}$ is solvable.

The following result is the analogue of [13, Lemma 2.3.4]. As we shall see, arguments in ~~*loc. cit.*~~ [13, Lemma 2.3.4] involving reductions of elliptic curves modulo primes above p will be replaced by considerations in p-adic Hodge theory.

LEMMA 4.12

For every $n \in \mathcal{N}$ the class κ_n belongs to $H^1_{\mathcal{F}_\Lambda(n)}(K,\mathbf{T}/I_n\mathbf{T})$.

Proof

To check that the localization of κ_n at a prime $v \mid n$ lies in the transverse subspace one can follow [13, Lemma 2.3.4], which is based on the formal argument described in the proof of [13, Lemma 1.7.3].

The case where $v \nmid Npn$ can also be treated similarly as in [13, Lemma 2.3.4], using the fact that the classes z_{np^m} are unramified.

In the case where $v \mid N$ one needs, as in ~~*loc. cit.*~~[13, Lemma 2.3.4], to check that for all $v' \mid v$ in K_∞, all $w \mid v$ in $K[n]$, and all $w' \mid w$ in $K_\infty[n]$ (note that w and v are finitely decomposed in the respective extensions, since all primes dividing N split in K) the map

$$\bigoplus_{w' \mid w} A\bigl(K_\infty[n]_{w'}\bigr) \longrightarrow \bigoplus_{v' \mid v} A(K_{\infty,v'})$$

induced by the norm is surjective: this is true because the degree of $K_\infty[n]_{w'}/K_{\infty,v'}$ is prime to p.

The case that needs more substantial changes is the one where $v \mid p$, which we describe in greater detail. Let $v \mid p$ be a prime of K, and fix a prime w of $K[n]$ above v. We still denote by v and w the unique primes of K_∞ and $K_\infty[n]$ above v and w, respectively, and similarly for $K_m[n]$. To simplify our notation, we set $\mathcal{K} := K_v$, $\mathcal{K}_\infty := K_{\infty,v}$, $\mathcal{K}[n] := K[n]_w$, and $\mathcal{K}_m[n] := K_m[n]_w$. Moreover, we write $\mathcal{O}$ for the valuation ring of $\mathcal{K}$. Recall the filtrations $\mathrm{Fil}^{\pm}_{\star}(\mathbf{T})$ on $\mathbf{T}$ (and, below, the filtrations $\mathrm{Fil}^{\pm}_{\star}(\mathbf{A})$ on $\mathbf{A}$) that were introduced in ~~§~~Section 3.3. Define

$$H^1_{\mathrm{ord}}(\mathcal{K}[n], \mathbf{T}) := \ker\Bigl(H^1(\mathcal{K}[n], \mathbf{T}) \longrightarrow H^1\bigl(\mathcal{K}[n], \mathrm{Fil}^-_w(\mathbf{T})\bigr)\Bigr).$$

First we note that the image (cf. Remark 4.8) of $\mathcal{H}_\infty[n]$ in $H^1(\mathcal{K}[n], \mathbf{T})$ lies in $H^1_{\mathrm{ord}}(\mathcal{K}[n], \mathbf{T})$. By [25, Theorem 3.1], the image of $\mathcal{H}_m[n]$ is contained in the Bloch–Kato Selmer group $H^1_f(\mathcal{K}_m[n], T)$, which coincides with Greenberg's Selmer group in our setting (cf. ~~[16, §2.4]~~[16, Section 2.4]). Therefore, the composition

$$\mathcal{H}_\infty[n] \longrightarrow H^1(\mathcal{K}_m[n], T) \longrightarrow H^1\bigl(\mathcal{K}_m[n], \mathrm{Fil}^-_w(T)\bigr)$$

is trivial, which implies, by arguments similar to those in the proof of [9, Proposition II.1.1], that the image of $\mathcal{H}_\infty[n]$ in $H^1(\mathcal{K}[n], \mathbf{T})$ lies in $H^1_{\mathrm{ord}}(\mathcal{K}[n], \mathbf{T})$.

To further lighten the notation, we set

$$\mathbf{T}_n := \mathbf{T}/I_n\mathbf{T}, \qquad \mathbf{T}_n^+ := \mathrm{Fil}^+_w(\mathbf{T})/I_n \,\mathrm{Fil}^+_w(\mathbf{T}), \qquad \mathbf{T}_n^- := \mathrm{Fil}^-_w(\mathbf{T})/I_n \,\mathrm{Fil}^-_w(\mathbf{T}).$$

Then we can consider the commutative diagram

$$\begin{array}{ccccc} H^1(\mathcal{K},\mathbf{T}_n^+) & \longrightarrow & H^1(\mathcal{K},\mathbf{T}_n) & \longrightarrow & H^1(\mathcal{K},\mathbf{T}_n^-) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(\mathcal{K}[n],\mathbf{T}_n^+) & \longrightarrow & H^1(\mathcal{K}[n],\mathbf{T}_n) & \longrightarrow & H^1(\mathcal{K}[n],\mathbf{T}_n^-) \end{array} \tag{22}$$

in which the vertical arrows are restrictions and the rows are exact. The argument above concerning $\mathcal{H}_\infty[n]$ shows that the image of the localization of κ_n in $H^1(\mathcal{K}[n],\mathbf{T}_n^-)$ is trivial. By the inflation-restriction sequence, the kernel of the right vertical arrow in (22) is

$$H^1\big(\mathrm{Gal}(\mathcal{K}[n]/\mathcal{K}), H^0(\mathcal{K}[n],\mathbf{T}_n^-)\big).$$

But $H^0(\mathcal{K}[n],\mathbf{T}_n^-) = 0$, as now we prove, hence; hence, the above-mentioned map is injective. In order to justify this vanishing, note that, since the intersection of the cyclotomic and the anticyclotomic $\mathbb{Z}_p$-extensions of $\mathcal{K}[n]$ is a finite extension of $\mathcal{K}$, the invariants of $\mathbf{T}_n^-$ under $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathcal{K}[n])$ are a submodule of the inverse limit with respect to the corestriction (i.e., multiplication-by-p) map $[p]$ of countably many copies of the group $\mathrm{Fil}_w^-(T)/I_n\,\mathrm{Fil}_w^-(T)$. It follows that

$$H^0(\mathcal{K}[n],\mathbf{T}_n^-) \subset \varprojlim_{[p]}\big(\mathrm{Fil}_w^-(T)/I_n\,\mathrm{Fil}_w^-(T)\big).$$

To prove that $H^0(\mathcal{K}[n],\mathbf{T}_n^-)$ is trivial it is therefore enough to show that $\mathrm{Fil}_w^-(T)/I_n\,\mathrm{Fil}_w^-(T)$ is finite. To do this, set $T^- := \mathrm{Fil}_w^-(T)$ and $V^- := \mathrm{Fil}_w^-(T)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$, and let $\varphi \in \mathrm{Gal}(\mathcal{K}^{\mathrm{unr}}/\mathcal{K})$ be the Frobenius automorphism. Write T' and V' for the unramified twists of T^- and V^-, respectively. It is clearly enough to show that T'/I_nT' is finite. As in §Section 2.1, let B_{cris} be Fontaine's ring of crystalline periods, then . Then for any p-adic representation M of $G_{\mathcal{K}}$ set

$$\mathbb{D}_{\mathrm{cris}}(M) := (M \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})^{G_{\mathcal{K}}}.$$

We know that $\mathbb{D}_{\mathrm{cris}}(V')^{\varphi=1} = 0$ (see, e.g., [28, p. 83]), hence; hence, $\varphi - 1$ is an isomorphism on $\mathbb{D}_{\mathrm{cris}}(V')$. Since the functor $\mathbb{D}_{\mathrm{cris}}$ is an equivalence between the category of crystalline representations and the category of filtered admissible φ-modules, and V' is crystalline because V is, it follows that $\varphi - 1$ is an isomorphism on V'. We conclude that $V'/(\varphi-1)V' = 0$, and then $T'/(\varphi-1)T'$ is a finite p-group because $V'/(\varphi-1)V' = \big(T'/(\varphi-1)T'\big) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Now the finiteness of T'/I_nT' is a consequence of the inclusion $(\varphi-1)T' \subset I_nT'$.

Choose a lift $\alpha \in H^1(\mathcal{K}, \mathbf{T}_n^+)$ of κ_n. As $H^0(\mathcal{K}[n], \mathbf{T}_n^-) = 0$, the bottom left horizontal arrow in (22) is injective~~, hence~~; hence, the image of α in $H^1(\mathcal{K}[n], \mathbf{T}_n^+)$ is the unique lift of the image of κ_n in $H^1(\mathcal{K}[n], \mathbf{T}_n)$. Set $\mathbf{T}^+ = \mathrm{Fil}_w^+(\mathbf{T})$. Since κ_n belongs to the image of $H^1(\mathcal{K}[n], \mathbf{T}^+)$ in $H^1(\mathcal{K}[n], \mathbf{T}_n)$ by construction, the class α maps to zero in the right lower entry of

$$\begin{array}{ccccc} H^1(\mathcal{K}, \mathbf{T}^+) & \longrightarrow & H^1(\mathcal{K}, \mathbf{T}_n^+) & \longrightarrow & H^2(\mathcal{K}, \mathbf{T}^+) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(\mathcal{K}[n], \mathbf{T}^+) & \longrightarrow & H^1(\mathcal{K}[n], \mathbf{T}_n^+) & \longrightarrow & H^2(\mathcal{K}[n], \mathbf{T}^+). \end{array}$$

To complete the proof, we only need to show that the right vertical arrow is injective. By duality, it is enough to show that if $\mathbf{A}^- := \mathrm{Fil}_w^-(\mathbf{A})$, then the trace map

$$\mathrm{tr}_{\mathcal{K}[n]/\mathcal{K}} : H^0(\mathcal{K}[n], \mathbf{A}^-) \longrightarrow H^0(\mathcal{K}, \mathbf{A}^-)$$

is surjective. Since the cyclotomic extension of $\mathcal{K}$ is disjoint from $\mathcal{K}[n]$, it is enough to show that the same statement is true for the unramified twist $\mathbf{A}'$ of $\mathbf{A}^-$. Set

$$A^- := \mathrm{Fil}_w^-(A) \simeq \mathrm{Hom}_{\mathbb{Z}_p}\big(T^+, \mathcal{K}/\mathcal{O}(1)\big),$$

and denote by A' the unramified twist of A^-. Using the fact that A' is unramified, we need to check the surjectivity of

$$\mathrm{tr}_{\mathcal{K}[n]/\mathcal{K}} : H^0(\mathcal{K}[n], A') \longrightarrow H^0(\mathcal{K}, A').$$

The first step is to prove that $H^0(\mathcal{K}[n], A')$ is finite. To begin with, if $H^0(\mathbb{Q}_p, A')$ were infinite, then its dual T', which is of rank 1, would be fixed by $G_{\mathbb{Q}_p}$: considering the weight of Frobenius shows that this is impossible. Therefore, $H^0(\mathbb{Q}_p, A')$

is finite, and using the fact that the extension $\mathcal{K}[n]/\mathbb{Q}_p$ is finite we see that $H^0(\mathcal{K}[n], A')$ must be finite as well. Since the Herbrand quotient of a cyclic group acting on a finite module is 1, it suffices to show that $H^1\big(\mathcal{K}[n]/\mathcal{K}, H^0(\mathcal{K}[n], A')\big) = 0$. This group injects into $H^1(\mathcal{K}, A')$~~, hence~~; hence, we are done if we prove that $H^1(\mathcal{K}, A') = 0$. As A' is unramified, the group $H^1(\mathcal{K}, A')$ is isomorphic to $A'/(\varphi - 1)A'$. On the other hand, if V' denotes the unramified twist of V^-, then there is a surjection $V' \twoheadrightarrow A'$~~, therefore~~; therefore, the vanishing of $A'/(\varphi - 1)A'$ follows from the vanishing of $V'/(\varphi - 1)V'$ that we proved above. $\square$

THEOREM 4.13

There exists a Kolyvagin system $\kappa^{\mathrm{Heeg}} \in \mathbf{KS}(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L})$ such that the class $\kappa_1^{\mathrm{Heeg}} \in H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ is ~~non-zero~~nonzero.

Proof

The classes κ_n, $n \in \mathcal{N}$, almost form a Kolyvagin system (cf. Definition 3.1). We only need to slightly modify them in order to gain the compatibility in diagram (3). We proceed as in ~~[13, §1.7]~~[13, Section 1.7]. For every $\ell \in \mathcal{L}$ let u_ℓ be the p-adic unit satisfying the relation

$$\mathrm{loc}_\ell\left(\alpha_m[n\ell]\right) = u_\ell \cdot \phi_\ell^{\mathrm{fs}}\big(\mathrm{loc}_\ell(\alpha_m[n])\big). \tag{23}$$

Such a u_ℓ exists thanks to a combination of ~~[8, §7.2, (K2)]~~ [8, Section 7.2, (K2)] and [24, Proposition 10.2]. If we define

$$\kappa'_n := \left(\prod_{\ell | n} u_\ell^{-1}\right) \cdot \kappa_n \otimes \left(\otimes \bigotimes_{\ell|n} \sigma_\ell\right) \in H^1_{\mathcal{F}(n)}(K, T/I_nT) \otimes G_n,$$

then (23) ensures that $\kappa^{\mathrm{Heeg}} := \{\kappa'_n\}_{n \in \mathcal{N}}$ is a Kolyvagin system. Moreover, $\kappa_1^{\mathrm{Heeg}} = \kappa_1$. The ~~non-triviality~~ nontriviality of κ_1^{Heeg} follows from Theorem 4.18 below. $\square$

Now we introduce the Selmer group where our Iwasawa module of generalized Heegner cycles naturally lives.

DEFINITION 4.14

The *pro-p Bloch–Kato Selmer group of f over K_∞* is the Λ-module

$$\hat{H}^1_f(K_\infty, T) := \varprojlim_m H^1_f(K_m, T),$$

where the inverse limit is taken with respect to the corestriction maps.

REMARK 4.15

It can be shown that $\hat{H}^1_f(K_\infty, T)$ is free of finite rank over Λ.

For every $m \geq 1$ denote by $\mathcal{H}_m$ the Λ_m-submodule of $H^1_f(K_m, T)$ that is generated by $\mathrm{cores}_{K[1]/K}(z_1)$ and $\mathrm{cores}_{K_m[1]/K_m}\big(\mathrm{res}_{K_m[1]/K_j[1]}(\alpha_j[1])\big)$ for all $j \leq m$. In line with Definition 4.7, we give the following.

DEFINITION 4.16

The *Iwasawa module of generalized Heegner cycles* is the compact Λ-module

$$\mathcal{H}_\infty := \varprojlim_m \mathcal{H}_m \subset \hat{H}^1_f(K_\infty, T),$$

where the inverse limit is taken with respect to the corestriction maps.

REMARK 4.17

If we set $K[0] := K$ and allow for $n = 0$ in Definition 4.7, then $\mathcal{H}_\infty$ coincides with $\mathcal{H}_\infty[0]$.

Let $\tilde{\kappa}_1 \in \mathcal{H}_\infty[1]$ be defined as in (21). Since $G(1)$ is trivial and D_1 is the identity operator, we see that $\tilde{\kappa}_1 = \sum_{\sigma \in \mathcal{G}(1)} \sigma\beta[1]$. This shows that we can view $\tilde{\kappa}_1$ as an element of $\mathcal{H}_\infty$.

THEOREM 4.18

The Λ-module $\mathcal{H}_\infty$ is free of rank 1, generated by $\tilde{\kappa}_1$.

Proof

A higher weight analogue due to Castella and Hsieh (see [8, Theorem 6.1]) of a result of Cornut~~(~~ (see [10]) on the ~~non-triviality~~ nontriviality of Heegner points on elliptic curves along anticyclotomic $\mathbb{Z}_p$-extensions ensures that **Q4** $\mathrm{cores}_{K_m[1]/K_m}(\alpha_m[1])$ is ~~non-torsion~~ nontorsion for $m \gg 0$. Using this fact, one can show that $\mathcal{H}_\infty$ is free of rank 1 over Λ by mimicking the proof of ~~[29, §3.4, Proposition 10]~~[29, Section 3.4, Proposition 10], where an analogous result is obtained for Heegner points. Therefore it remains to show that $\mathcal{H}_\infty$ is generated by $\tilde{\kappa}_1$. We follow the proof of [13, Theorem 2.3.7].

Recall that $\Gamma_m = \mathrm{Gal}(K_m/K)$~~, then~~. Then write $\mathrm{Gal}(K_m[1]/K) \simeq \Gamma_m \times \mathcal{G}$ with $\mathcal{G} := \mathcal{G}(1)$. Let $\mathrm{tr}_{\mathcal{G}} := \sum_{g\in\mathcal{G}} g$ be the ~~"trace"~~ trace operator in $\mathcal{O}_{\mathfrak{p}}[\mathcal{G}] \subset \Lambda[\mathcal{G}]$. Recall also the modules $\tilde{\mathcal{H}}_m$ and $\tilde{\mathcal{H}}_\infty$ with $n = 1$ and the elements x, x_j, y that were introduced in the proof of Proposition 4.9. Set, as usual, $\tilde{\mathcal{H}}_\infty^{\mathcal{G}} := H^0(\mathcal{G}, \tilde{\mathcal{H}}_\infty)$~~, then~~. Then define

$$x_j^{\mathcal{G}} := \mathrm{tr}_{\mathcal{G}}(x_j) \in \tilde{\mathcal{H}}_\infty^{\mathcal{G}}, \qquad y^{\mathcal{G}} := \mathrm{tr}_{\mathcal{G}}(y) \in \tilde{\mathcal{H}}_\infty^{\mathcal{G}}.$$

There is a commutative square

$$\begin{array}{ccc} \tilde{\mathcal{H}}_\infty & \twoheadrightarrow & \mathcal{H}_\infty \\ \downarrow{\scriptstyle \mathrm{tr}_{\mathcal{G}}} & & \downarrow{\scriptstyle \mathrm{cores}_{H_1/K}} \\ \tilde{\mathcal{H}}_\infty^{\mathcal{G}} & \twoheadrightarrow & \mathcal{H}_\infty \end{array}$$

in which all maps are surjective, the top horizontal arrow takes x_j to α_j and the bottom horizontal arrow takes $x_j^{\mathcal{G}}$ to $\mathrm{cores}_{H_1/K}(\alpha_j)$ and $y^{\mathcal{G}}$ to $\tilde{\kappa}_1$. Fix a topological generator γ of Γ_∞. By Nakayama's lemma, it is enough to show that

$$\tilde{\mathcal{H}}_\infty^{\mathcal{G}} = \Lambda y^{\mathcal{G}} + (\gamma - 1)\tilde{\mathcal{H}}_\infty^{\mathcal{G}}. \tag{24}$$

This is done in two steps that correspond to [13, Lemmas 2.3.8 and 2.3.9].

For all $m \geq 0$ set $\tilde{\mathcal{H}}_m^{\mathcal{G}} := H^0(\mathcal{G}, \tilde{\mathcal{H}}_m)$. The $\mathcal{O}_{\mathfrak{p}}$-module $\tilde{\mathcal{H}}_0^{\mathcal{G}}$ is free of rank 1, generated by $x^{\mathcal{G}}$, and there is a canonical map

$$\Psi : \tilde{\mathcal{H}}_\infty^{\mathcal{G}} \longrightarrow \tilde{\mathcal{H}}_0^{\mathcal{G}}.$$

CLAIM 4.19

The image of Ψ is a free $\mathcal{O}_{\mathfrak{p}}$-module of rank 1 generated by $\Psi(y^{\mathcal{G}}) = x^{\mathcal{G}}$.

CLAIM 4.20

The map Ψ induces an isomorphism

$$\bar{\Psi} : \tilde{\mathcal{H}}_\infty^{\mathcal{G}}/(\gamma - 1)\tilde{\mathcal{H}}_\infty^{\mathcal{G}} \xrightarrow{\simeq} \tilde{\mathcal{H}}_0^{\mathcal{G}}.$$

Clearly, Claims ~~1 and 2~~ 4.19 and 4.20 imply (24), so it remains to justify these two assertions.

For the first claim one can follow the proof of [13, Lemma 2.3.8]. More precisely, with notation as in ~~§~~Section 4.2, one observes that $\mathrm{tr}_{K_m/K}(x_m^{\mathcal{G}}) = \mathrm{aug}(\gamma_{m+1})x^{\mathcal{G}}$ for all $m \geq 0$. On the other hand, by Corollary 4.6 we know that $\mathrm{aug}(\gamma_{m+1})$ is invertible for all $m \geq 0$, which implies Claim ~~1.~~ 4.19.

The proof of the ~~second claim~~ Claim 4.20 proceeds along the lines of the proof of [13, Lemma 2.3.9], with only a minor variation in one of the recursive relations appearing there. This is due to the fact that the elements γ_m defined in ~~§~~Section 4.2 are slightly different from their namesakes in [13]. However, for the reader's convenience we provide a proof, which largely overlaps with the one given in [13].

First we observe that we only need to show that $\bar{\Psi}$ is injective, since $\bar{\Psi}$ is surjective by Claim ~~1.~~ 4.19. Fix $h = (h_m)_{m\geq 1} \in \ker(\Psi)$. For every $m \geq 1$ the Λ-module $\tilde{\mathcal{H}}_m^{\mathcal{G}}$ is generated by $x_m^{\mathcal{G}}$ and $x_{m-1}^{\mathcal{G}}$, so we can write

$$h_m = a_m x_m^{\mathcal{G}} + b_m x_{m-1}^{\mathcal{G}} + (\gamma - 1)z_m$$

for suitable $a_m, b_m \in \mathcal{O}_{\mathfrak{p}}$. Taking the trace to $\tilde{\mathcal{H}}_0^{\mathcal{G}}$ and using the fact that $x^{\mathcal{G}}$ has infinite order, we obtain

$$a_m \operatorname{aug}(\gamma_{m+1}) + p b_m \operatorname{aug}(\gamma_m) = 0 ~~,~~ ;$$

hence,

$$\operatorname{aug}(\gamma_{m+1}) h_m \in b_m t_m + (\gamma - 1)\tilde{\mathcal{H}}_m^{\mathcal{G}}$$

with

$$t_m := -p \operatorname{aug}(\gamma_m) x_m^{\mathcal{G}} + \operatorname{aug}(\gamma_{m+1}) x_{m-1}^{\mathcal{G}}.$$

Applying the trace operator, we get

$$\begin{aligned}\operatorname{tr}_{K_{m+1}/K_m}(t_{m+1}) &= -p \operatorname{aug}(\gamma_{m+1})(a_p x_m^{\mathcal{G}} - p^{k-2} x_{m-1}^{\mathcal{G}}) + p \operatorname{aug}(a_p \gamma_{m+1} - p^{k-1}\gamma_m) x_m^{\mathcal{G}} \\ &= p^{k-1}\big(\operatorname{aug}(\gamma_{m+1}) x_{m-1}^{\mathcal{G}} - p \operatorname{aug}(\gamma_m) x_m^{\mathcal{G}}\big) \\ &= p^{k-1} t_m.\end{aligned}$$

Since $\operatorname{aug}(\gamma_{m+1})$ is invertible for all $m \geq 0$, if we fix an m, then for every $\ell \geq m$ there exists $u_\ell \in \mathcal{O}_{\mathfrak{p}}^{\times}$ such that

$$h_m = u_\ell \operatorname{aug}(\gamma_{m+1})^{-1} \operatorname{aug}(\gamma_\ell) \operatorname{tr}_{K_\ell/K_m}(h_\ell) \in u_\ell \operatorname{aug}(\gamma_{m+1})^{-1} b_\ell p^{(k-1)(\ell-m)} t_m + (\gamma-1)\tilde{\mathcal{H}}_m^{\mathcal{G}}.$$

Finally, letting $\ell \to \infty$ shows that $h_m \in (\gamma - 1)\tilde{\mathcal{H}}_m^{\mathcal{G}}$ for every $m \geq 0$, and Claim ~~2~~ 4.20 follows. □

REMARK 4.21

The analogue of [8, Theorem 6.1] when $V_{f,\mathfrak{p}}$ is replaced by Deligne's ℓ-adic representation with $\ell \neq p$ was proved by Howard in [15, Theorem A].

REMARK 4.22

For each $n \in \mathcal{N}$ and any integer $m \geq 0$, Castella and Hsieh introduced in ~~[8, §5.2]~~ [8, Section 5.2] certain *α-stabilized Heegner classes*

$$z^{o}_{f,mp^n,\alpha} \in H^1_f(K[np^m], T),$$

where α is the p-adic unit root of the Hecke polynomial $X^2 - a_p X + p^{k-1}$. These classes are defined in terms of the elements z_{mp^n} of ~~§~~Section 4.1 via a regularization process that is analogous to the one used in ~~[4, §2.5]~~ [4, Section 2.5] in the case of Heegner points on elliptic curves. As is shown in [8, Lemma 5.3], for each n one has $\mathrm{cores}_{K[np^m]/K[np^{m-1}]}(z^o_{f,np^m,\alpha}) = \alpha z^o_{f,np^{m-1},\alpha}$, so we get an element

$$\mathbf{z}_{f,n,\alpha} := \varprojlim_m \alpha^{-n} z^o_{f,np^m,\alpha} \in \varprojlim_m H^1_f(K[np^m], T).$$

Using the elements $\mathbf{z}_{f,n,\alpha}$, one might be able to show that the Λ-module $\mathcal{H}_\infty$ is free of rank 1 by adapting the techniques developed by Bertolini in [2].

5. Proof of Theorem 1.1 and Main Conjecture

In this section we prove our main result (Theorem 1.1) and formulate a Main Conjecture ~~*à la*~~ à la Perrin-Riou for generalized Heegner cycles, one divisibility (of a refined form) of which is the content of the last part of Theorem 1.1.

5.1. Proof of Theorem 1.1

We check, as in the proof of [13, Proposition 2.1.3], that hypotheses (H.0)–(H.5) and Assumption 3.2 in ~~§~~Section 3.1 are satisfied in our setting. Then Theorem 1.1 follows by combining Theorems 3.5 and 4.13.

The ordinariness of f that we imposed in ~~part (5) of Assumption 2.3 ensures that condition (1) in Assumption 3.2~~ Assumption 2.3(5) ensures that Assumption 3.2(1) is satisfied. Also, in this case, for any number field E there is a natural identification

$$\mathrm{Sel}_{\mathrm{Gr}}(T/E) = H^1_f(E, T)$$

between Greenberg's and Bloch–Kato's Selmer groups (cf. ~~[16, §2.4]~~[16, Section 2.4]). Moreover, by comparing local conditions, one can prove that there is a canonical isomorphism

$$\hat{H}^1_f(K_\infty, T) \simeq H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T}),$$

where $\mathcal{F}_\Lambda$ is the Selmer structure introduced at the end of §Section 3.3. Recall that we chose the $\mathcal{O}_\mathfrak{p}$-lattice $T \subset V$ as in [24, p. 109]. As a consequence of [24, Proposition 3.1, (2)][24, Proposition 3.1(2)], there is a $G_\mathbb{Q}$-equivariant, skew-symmetric, non-degenerate nondegenerate pairing

$$T \times T \longrightarrow \mathcal{O}_\mathfrak{p}(1); \tag{25}$$

this ensures that (H.4) holds. It is known (see, e.g., [26, §4.3][26, Section 4.3]) that $\mathrm{Fil}_v^+(T)$ and $\mathrm{Fil}^+(A)$ are the exact annihilators of each other under the pairing

$$T \times A \longrightarrow (F_\mathfrak{p}/\mathcal{O}_\mathfrak{p})(1)$$

induced by (25), so condition (2) in Assumption 3.2 Assumption 3.2(2) is satisfied. As for condition (3) in Assumption 3.2Assumption 3.2(3), the finiteness of $H^0\big(K_{\infty,v}, \mathrm{Fil}_v^-(A)\big)$ follows from that of $H^0\big(K_v, \mathrm{Fil}_v^-(A)\big)$, which was checked in the proof of Lemma 4.12, upon noting that a suitable twist of $\mathrm{Fil}_v^-(A)$ is unramified and $K_{\infty,v}/K_v$ is totally ramified. Finally, hypothesis (H.5) holds because for all $\mathfrak{P}$ the residual representation attached to $T_\mathfrak{P}$ is identified with $\bar{T} \otimes_{\mathbb{F}_p} (S_\mathfrak{P}/\mathfrak{m})$, where $\mathbb{F}_p$ is the field with p elements, $\mathfrak{m}$ is the maximal ideal of $S_\mathfrak{P}$, and the Galois action on $S_\mathfrak{P}/\mathfrak{m}$ is trivial, and because condition (H.5) is true for $\bar{T}$.

5.2. Main Conjecture

Theorem 1.1 was proved under the assumption that the triple $(f, K, \mathfrak{p})$ is admissible in the sense of §Section 2.2. More generally, we expect it to hold under the following weaker conditions:

- (M.1) the primes dividing N split in K;
- (M.2) p is unramified in K;
- (M.3) $a_p \in \mathcal{O}_\mathfrak{p}^\times$.

Now recall the finitely generated torsion Λ-module M in part (2) of Theorem

~~1.1~~Theorem 1.1(2). Assuming that $(f, K, \mathfrak{p})$ satisfies (M.1)–(M.3), we propose the following.

CONJECTURE 5.1 (MAIN CONJECTURE)

There is an equality $\mathrm{char}(M) = \mathrm{char}\Big(\hat{H}^1_f(K_\infty, T)/\mathcal{H}_\infty\Big)$ of ideals of $\Lambda \otimes_{\mathcal{O}_\mathfrak{p}} F_\mathfrak{p}$.

Note that the last part of Theorem 1.1 shows that one divisibility in an integral refinement of Conjecture 5.1 is true when $(f, K, \mathfrak{p})$ is admissible.

Conjecture 5.1 should be compared with the "main conjecture" for Heegner points on elliptic curves that was proposed by Perrin-Riou in [29]. Important results ~~towards~~ toward Perrin-Riou's conjecture have been obtained by Bertolini (see [2]) and Howard (see [13], [14]). Recently, a proof of a conjecture of Perrin-Riou type under slightly different ramification conditions has been announced by Wan (see [33]).

Acknowledgments. It is a pleasure to warmly thank the anonymous referee for carefully reading our ~~paper~~article: his or her constructive criticism and extremely valuable remarks led us to rethink some parts of this work and significantly improve the quality of our article. We would also like to thank Antonio Lei for pointing out a flaw in a previous version of this ~~paper~~article.

References

[1] P. N. Balister and S. Howson, *Note on Nakayama's lemma for compact Λ-modules*, Asian J. Math. **1** (1997), no. 2, 224–229. MR1491983. DOI 10.4310/AJM.1997.v1.n2.a2.

[2] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic* $\mathbf{Z}_p$*-extensions*, Compos. Math. **99** (1995), no. 2, 153–182. MR1351834.

[3] ______, *Iwasawa theory for elliptic curves over imaginary quadratic fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 1–25. MR1838067.

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

[5] M. Bertolini, H. Darmon, and K. Prasanna, *Generalized Heegner cycles and p-adic Rankin L-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148. MR3053566. DOI 10.1215/00127094-2142056.

[6] S. Bloch and K. Kato, ~~*L-functions and Tamagawa numbers of motives,*~~ "*L*-functions and Tamagawa numbers of motives" in *The Grothendieck Festschrift, Vol. I*, Progr. Math.~~, vol.~~ **86**, Birkhäuser Boston, Boston, ~~MA,~~ 1990, ~~pp.~~ 333–400. MR1086888.

[7] A. Brumer, *Pseudocompact algebras, profinite groups and class formations*, J. Algebra **4** (1966), no. 3, 442–470. MR0202790. DOI 10.1016/0021-8693(66)90034-2.

[8] F. Castella and M.-L. Hsieh, *Heegner cycles and p-adic L-functions*, Math. Ann. **370** (2018), no. 1–2, ~~to appear.~~ 567–628. MR3747496. **Q5**
DOI 10.1007/s00208-017-1517-3.

[9] P. Colmez, *Théorie d'Iwasawa des représentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1998), no. 2, 485–571. MR1668555. DOI 10.2307/121003.

[10] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523. MR1908058. DOI 10.1007/s002220100199.

[11] P. Deligne, ~~*Formes modulaires et représentations ℓ-adiques,* Séminaire~~ "~~Bourbaki.~~ Formes modulaires et représentations ~~V~~ℓ~~ol. 1968/69:~~ ~~E~~-adiques~~xposés 347–363~~" in *Séminaire Bourbaki. Vol. 1968/69, no.*

355, Lecture Notes in Math. ~~, vol.~~ **175**, Springer, Berlin, 1971, ~~pp.~~ 139–172. MR3077124.

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

[13] B. Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472. MR2098397. DOI 10.1112/S0010437X04000569.

[14] ———, *Iwasawa theory of Heegner points on abelian varieties of* GL_2 *type*, Duke Math. J. **124** (2004), no. 1, 1–45. MR2072210. DOI 10.1215/S0012-7094-04-12411-X.

[15] ———, *Special cohomology classes for modular Galois representations*, J. Number Theory **117** (2006), no. 2, 406–438. MR2213774. DOI 10.1016/j.jnt.2005.07.002.

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

[17] V. A. Kolyvagin, ~~*Euler systems*, The~~ “~~G~~Euler systems~~rothendieck Festschrift, Vol. II,~~” in *The Grothendieck Festschrift, Vol. II,* Progr. Math.~~, vol.~~ **87**, Birkhäuser Boston, Boston, ~~MA,~~ 1990, ~~pp.~~ 435–483. MR1106906.

[18] S. Lang and H. Trotter, *Frobenius ~~distributions~~ Distributions in* GL_2 ~~*-extensions*~~*-Extensions*, Lecture Notes in ~~Mathematics, Vol.~~ Math. **504**~~,~~ ~~**Springer-Verlag, Berlin-New**~~ , Springer, New York, 1976. MR0568299.

[19] M. Longo and S. Vigni, *A refined Beilinson–Bloch conjecture for motives of modular forms*, Trans. Amer. Math. Soc. **369** (2017), no. 10, ~~to appear.~~ 7301–7342. MR3683110. DOI 10.1090/tran/6947. Q6

[20] B. Mazur, ~~*Modular curves and arithmetic*, Proceedings of the~~ “~~I~~Modular curves and arithmetic~~nternational Congress of Mathematicians, Vol. 1,~~

~~2 (Warsaw, 1983), ~~” in *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983),* PWN, Warsaw, 1984, ~~pp.~~ 185–211. MR0804682.

[21] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799. MR2031496. DOI `10.1090/memo/0799`.

[22] M. R. Murty and V. K. Murty, ~~A variant of the~~ “A variant of the Lang–T~~rotter conjecture~~rotter conjecture” in *Number Theory, Analysis and Geometry*, ~~Number theory, analysis and geometry,~~ Springer, New York, 2012, ~~pp.~~ 461–474. MR2867929. DOI `10.1007/978-1-4614-1260-1_21`.

[23] M. R. Murty, V. K. Murty, and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281. MR0935007. DOI `10.2307/2374502`.

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

[25] ~~, *p-adic Abel–Jacobi maps and p-adic heights*, The arithmetic and geometry of algebraic cycles (~~______, “B~~$p$anff, ~~-adic ~~AB~~A~~, 1998),~~ bel–Jacobi maps and p-adic heights” in *The Arithmetic and Geometry of Algebraic Cycles (Banff, AB, 1998),* CRM Proc. Lecture Notes ~~, vol.~~ **24**, Amer. Math. Soc., Providence, ~~RI,~~ 2000, ~~pp.~~ 367–379. MR1738867.

[26] J. Nekovář and A. Plater, *On the parity of ranks of Selmer groups*, Asian J. Math. **4** (2000), no. 2, 437–497. MR1797592. DOI `10.4310/AJM.2000.v4.n2.a11`.

[27] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of ~~number fields~~Number Fields*, Grundlehren ~~der Mathematischen Wissenschaften, vol.~~ Math. Wiss. **323**, Springer, ~~Springer-Verlag,~~ Berlin, 2000. MR1737196.

[28] T. Ochiai, *Control theorem for Bloch–Kato's Selmer groups of p-adic representations*, J. Number Theory **82** (2000), no. 1, 69–90. MR1755154. DOI 10.1006/jnth.1999.2483.

[29] B. Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456. MR0928018.

[30] K. A. Ribet, ~~*Galois representations attached to eigenforms with Nebentypus*, Modular functions of one variable,~~ "~~V(~~Galois representations attached to eigenforms with ~~P~~N~~roc. S~~ebentypus~~econd Internat. Conf., Univ~~" in *Modular Functions of One Variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Math. ~~B~~**601**~~onn, Bonn, 1976), ~~, Springer, Berlin, 1977, ~~pp.~~ 17–51. ~~Lecture Notes in Math., Vol. 601.~~ MR0453647.

[31] ——— *On l-adic representations attached to modular forms*~~.~~, *II*, Glasgow Math. J. **27** (1985), 185–194. MR0819838. DOI 10.1017/S0017089500006170.

[32] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. MR0644559.

[33] X. Wan, *Heegner point Kolyvagin system and Iwasawa Main Conjecture*, preprint~~(~~, 2014~~)~~. **Q7**

Longo: Dipartimento di Matematica, Università di Padova, Padova, Italy;
mlongo@math.unipd.it

Vigni: Dipartimento di Matematica, Università di Genova, Genova, Italy;
vigni@dima.unige.it

Copyeditor's queries:

Q1: Please expand the abbreviations PRIN, PRAT, and PRA in the financial support footnotes. *(1)*

Q2: Please expand the abbreviation CM here. *(2)*

Q3: Please provide the specific citation instead of loc. cit. here. It is not entirely clear what this loc. cit. is referring to. *(24)*

Q4: Please provide a pinpoint cite for this result of Cornut. That is, please provide a theorem number or page number for this result. *(36)*

Q5: We updated [8] to reflect publication. Please verify that this new information is correct. *(42)*

Q6: We updated [19] to reflect publication. Please verify that this new information is correct. *(43)*

Q7: Please provide updated publication information for [33] if available. *(45)*