COMPOSITIO MATHEMATICA

Iwasawa theory for modular forms at supersingular primes

Antonio Lei

Compositio Math. **147** (2011), 803–838.

doi:10.1112/S0010437X10005130

FOUNDATION
COMPOSITIO
MATHEMATICA

*The London
Mathematical
Society*

Compositio Math. 147 (2011) 803–838
doi:10.1112/S0010437X10005130

Iwasawa theory for modular forms at supersingular primes

Antonio Lei

Abstract

We generalise works of Kobayashi to give a formulation of the Iwasawa main conjecture for modular forms at supersingular primes. In particular, we give analogous definitions of the plus and minus Coleman maps for normalised new forms of arbitrary weights and relate Pollack's p-adic L-functions to the plus and minus Selmer groups. In addition, by generalising works of Pollack and Rubin on CM elliptic curves, we prove the 'main conjecture' for CM modular forms.

1. Introduction

The Taniyama–Shimura conjecture, proved by Wiles *et al.*, asserts that elliptic curves over $\mathbb{Q}$ correspond to modular forms of weight two. Therefore, it is natural to ask which results on elliptic curves can be generalised to modular forms of higher weights. In this paper, we discuss how this can be done for some recent results on supersingular primes.

Let p be an odd prime and let G_∞ be the Galois group of the extension k_∞ of $\mathbb{Q}$ by p power roots of unity. We denote by $\Lambda(G_\infty)$ the Iwasawa algebra of G_∞ over $\mathbb{Z}_p$. If Δ denotes the torsion subgroup of G_∞ and γ is a fixed topological generator of the $\mathbb{Z}_p$-part of G_∞, then $\Lambda(G_\infty) \cong \mathbb{Z}_p[\Delta][[\gamma - 1]]$.

Let $f = \sum a_n q^n$ be a normalised eigen-newform of weight $k \geqslant 2$, level N and character ϵ. For notational simplicity, we assume that $a_p \in \mathbb{Z}$ throughout the introduction. We fix p so that $p \nmid N$. Kato [Kat04] has formulated a main conjecture relating an Euler system (which we refer to as a Kato zeta element) to some cohomological group over k_∞ (see § 3.3 for a brief review).

If α is a root of $X^2 - a_p X + \epsilon(p)p^{k-1}$ such that $v_p(\alpha) < k - 1$, where v_p is the p-adic valuation of $\mathbb{C}_p$ with $v_p(p) = 1$, then there exists a p-adic L-function $L_{p,\alpha}$ interpolating complex L-values of f. When f is ordinary at p (i.e. a_p is a p-adic unit) and α is the unique unit root of the quadratic above, $L_{p,\alpha}$ lies inside $\mathbb{Q} \otimes \Lambda(G_\infty)$ and the p-Selmer group $\mathrm{Sel}_p(f/k_\infty)$ of f over k_∞ is $\Lambda(G_\infty)$-torsion, i.e. its Pontryagin dual

$$\mathrm{Sel}_p(f/k_\infty)^\vee = \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Sel}_p(f/k_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

is $\Lambda(G_\infty)$-torsion. If θ is a character on Δ, the θ-isotypical component of $\mathrm{Sel}_p(f/k_\infty)^\vee$ is $\mathbb{Z}_p[[\gamma - 1]]$- torsion. We can associate to it a characteristic ideal. Kato's main conjecture is equivalent to asserting that this ideal is generated by the θ-component of $L_{p,\alpha}$ (written as $L^\theta_{p,\alpha}$),

Received 14 August 2009, accepted in final form 21 July 2010, published online 7 February 2011.
2000 Mathematics Subject Classification 11R23, 11F11 (primary).
Keywords: modular form, supersingular prime, Iwasawa theory, CM form.
The author is supported by Trinity College, Cambridge.

i.e. there is a pseudo-isomorphism (a homomorphism with finite kernel and cokernel)

$$\mathrm{Sel}_p(f/k_\infty)^{\vee,\theta} \to \prod_{i=1}^{r} \mathbb{Z}_p[[\gamma-1]]/(x_i)$$

for some $x_i \in \mathbb{Z}_p[[\gamma-1]]$ such that $x_1 \cdots x_r = L_{p,\alpha}^{\theta}$.

When f is supersingular at p (i.e. $p|a_p$), the p-adic L-functions of f as given above are not in $\mathbb{Q} \otimes \Lambda(G_\infty)$ and $\mathrm{Sel}_p(f/k_\infty)$ is not $\Lambda(G_\infty)$-cotorsion (see § 6.3.1). Therefore, Kato's main conjecture cannot be reformulated in the same way as the ordinary case.

In recent years, much progress has been made on supersingular primes. When $a_p = 0$, Pollack [Pol03] has defined the plus and minus p-adic L-functions $L_p^{\pm}$, which have bounded coefficients. In [Kob03], again assuming that $a_p = 0$, Kobayashi defined the plus and minus Selmer groups $\mathrm{Sel}_p^{\pm}$ for the case when f corresponds to an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ and proved that $\mathrm{Sel}_p^{\pm}(\mathcal{E}/k_\infty)$ are $\Lambda(G_\infty)$-cotorsion. It is then possible to reformulate Kato's main conjecture as follows.

Conjecture 1.1. Let θ be a character on Δ. Under the notation above, the characteristic ideal of $\mathrm{Sel}_p^{\pm}(\mathcal{E}/k_\infty)^{\vee,\theta}$ is generated by $L_p^{\pm,\theta}$.

One inclusion of Conjecture 1.1, namely $L_p^{\pm,\theta}$ does lie inside the said characteristic ideal, follows from that of Kato's main conjecture under some assumptions. For the CM case, the other inclusion has been proved by Pollack and Rubin in [PR04], using the theory of imaginary quadratic fields and elliptic units.

We now explain how $\mathrm{Sel}_p^{\pm}(\mathcal{E}/k_\infty)$ is defined. Let μ_{p^n} be the set of p^nth roots of unity. The idea of Kobayashi is to define subgroups $\mathcal{E}^{\pm}(\mathbb{Q}_p(\mu_{p^n}))$ of $\mathcal{E}(\mathbb{Q}_p(\mu_{p^n}))$ which can be identified with its image in $H^1(\mathbb{Q}_p(\mu_{p^n}), \mathcal{E}[p^\infty])$ under the Kummer map. The $\pm$-Selmer groups over $\mathbb{Q}(\mu_{p^n})$ are defined to be

$$\mathrm{Sel}_p^{\pm}(\mathcal{E}/\mathbb{Q}(\mu_{p^n})) = \ker\left(\mathrm{Sel}_p(\mathcal{E}/\mathbb{Q}(\mu_{p^n})) \to \frac{H^1(\mathbb{Q}_p(\mu_{p^n}), \mathcal{E}[p^\infty])}{\mathcal{E}^{\pm}(\mathbb{Q}_p(\mu_{p^n})) \otimes \mathbb{Q}_p/\mathbb{Z}_p}\right).$$

Then, $\mathrm{Sel}_p^{\pm}(\mathcal{E}/k_\infty)$ is defined to be the direct limit of $\mathrm{Sel}_p^{\pm}(\mathcal{E}/\mathbb{Q}(\mu_{p^n}))$.

On the one hand, $\mathcal{E}[p^\infty]$ gives a p-adic representation of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and one can define analogous representations for arbitrary modular forms (see [Del69] for details). On the other hand, the Kummer image of $\mathcal{E}(\mathbb{Q}_p(\mu_{p^n}))$ can be identified with the so-called finite cohomology subgroup H_f^1 defined in [BK90]. Therefore, we can give a definition of $\mathrm{Sel}^{\pm}(f/k_\infty)$ analogously for any modular forms without much difficulty.

To show that $\mathrm{Sel}_p^{\pm}(\mathcal{E}/k_\infty)$ is $\Lambda(G_\infty)$-cotorsion, Kobayashi constructed the $\pm$-Coleman maps

$$\mathrm{Col}^{\pm} : \varprojlim H^1(\mathbb{Q}_p(\mu_{p^n}), T_p(\mathcal{E})) \to \Lambda(G_\infty),$$

where $T_p(\mathcal{E})$ denotes the Tate module of $\mathcal{E}$ at p. In particular, $\mathrm{Col}^{\pm}$ send the Kato zeta element from [Kat04] to $L_p^{\pm}$, respectively. By applying the Poitou–Tate exact sequence, he then showed that the Pontryagin dual of $\mathrm{Sel}_p^{\pm}(\mathcal{E}/k_\infty)$ is killed by $L_p^{\pm} \neq 0$; hence, $\Lambda(G_\infty)$-cotorsion.

We follow this strategy to show that $\mathrm{Sel}_p^{\pm}(f/k_\infty)$ are $\Lambda(G_\infty)$-cotorsion for f of any weight $k \geqslant 2$. Although the Coleman maps in [Kob03] are defined using formal groups, they can in fact be obtained from Perrin-Riou's exponential map defined in [Per94]. We make use of this and observe that there is a divisibility phenomenon, similar to that used in the construction of $L_p^{\pm}$ in [Pol03]. This enables us to construct analogous $\pm$-Coleman maps for general f. Although we

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

do not need any restrictions on p to define them, we assume that $p+1 \nmid k-1$ in order to describe their kernels, which are related to the local conditions in the definition of $\mathrm{Sel}_p^{\pm}$. We then formulate a main conjecture as follows.

CONJECTURE 1.2. Let f and θ be as above. There exist $n^{\pm} \in \mathbb{Z}$ such that the characteristic ideal of $\mathrm{Sel}_p^{\pm}(f/k_\infty)^{\vee,\theta}$ is generated by $p^{n^{\pm}} L_p^{\pm,\theta}$.

As in the case of elliptic curves, Conjecture 1.2 is equivalent to Kato's main conjecture and one inclusion holds.

It has to be pointed out that we are assuming that $a_p = 0$ as in [Kob03, Pol03]. Since $|a_p| \leqslant 2p^{(k-1)/2}$ (due to Deligne), a_p is always zero when $p > 3$ when f corresponds to an elliptic curve. When $k > 2$, the assumption is much stronger although, if f is a CM modular form, $a_p = 0$ for any supersingular prime p (see § 7). More recently, Sprung [Spr09] has generalised works of Kobayashi to the case $a_p \neq 0$ for elliptic curves over $\mathbb{Q}$. It would be desirable to know whether this can be done for modular forms of higher weights as well.

The layout of this paper is as follows. We fix some notation and review some basic properties in § 2. In § 3, we first review some of the main results which we need from [Per94, Kat04]. We then construct the $\pm$-Coleman maps. The kernels of these maps are worked out explicitly in § 4 and their images are described in § 5. Following [Kob03], we define $\mathrm{Sel}_p^{\pm}$ in § 6. We show that they are $\Lambda(G_\infty)$-cotorsion, which enables us to formulate the 'main conjecture' for which one inclusion of the conjecture is shown. Finally, in § 7, the other inclusion is proved in the case of CM modular forms over $\mathbb{Q}$, following the strategy of [PR04].

2. Background

In this section, we fix some notation which is used throughout the paper. We also state some basic properties of some of the objects which we study.

2.1 Extensions by p power roots of unity

Throughout this paper, p is an odd prime. If K is a field of characteristic 0, either local or global, G_K denotes its absolute Galois group, χ the p-cyclotomic character on G_K and $\mathcal{O}_K$ the ring of integers of K. For an integer $n \geqslant 0$, we write K_n for the extension $K(\mu_{p^n})$, where μ_{p^n} is the set of p^nth roots of unity and K_∞ denotes $\bigcup_{n \geqslant 1} K_n$. The $\mathbb{Z}_p$-cyclotomic extension of K is denoted by K_c and $K^{(n)}$ denotes the p^n-subextension inside K_c.

In particular, we write $\mathbb{Q}_{p,n} = \mathbb{Q}_p(\mu_{p^n})$. For $n \geqslant m$, we write $\mathrm{Tr}_{n/m}$ for the trace map from $\mathbb{Q}_{p,n}$ to $\mathbb{Q}_{p,m}$. For each n, we fix a primitive p^nth root of unity such that $\zeta_{p^n}^p = \zeta_{p^{n-1}}$. Let G_n denote the Galois group $\mathrm{Gal}(\mathbb{Q}_{p,n}/\mathbb{Q}_p)$ for $0 \leqslant n \leqslant \infty$. Then, $G_\infty \cong \Delta \times \Gamma$, where $\Delta = G_1$ is a finite group of order $p-1$ and $\Gamma = \mathrm{Gal}(\mathbb{Q}_{p,\infty}/\mathbb{Q}_{p,1}) \cong \mathbb{Z}_p$. We fix a topological generator γ of Γ and write $u = \chi(\gamma)$. In particular, u is a topological generator of $1 + p\mathbb{Z}_p$.

2.2 Iwasawa algebras and power series

Given a finite extension K of $\mathbb{Q}_p$, $\Lambda_{\mathcal{O}_K}(G_\infty)$ (respectively $\Lambda_{\mathcal{O}_K}(\Gamma)$) denotes the Iwasawa algebra of G_∞ (respectively Γ) over $\mathcal{O}_K$. We write $\Lambda_K(G_\infty) = \Lambda_{\mathcal{O}_K}(G_\infty) \otimes K$ and $\Lambda_K(\Gamma) = \Lambda_{\mathcal{O}_K}(\Gamma) \otimes K$. When $K = \mathbb{Q}_p$ (so $\mathcal{O}_K = \mathbb{Z}_p$), we simply write Λ for $\Lambda_{\mathbb{Z}_p}$. If M is a finitely generated $\Lambda_{\mathcal{O}_K}(\Gamma)$-torsion (respectively $\Lambda_K(\Gamma)$-torsion) module, we write $\mathrm{Char}_{\Lambda_{\mathcal{O}_K}(\Gamma)}(M)$ (respectively $\mathrm{Char}_{\Lambda_K(\Gamma)}(M)$) for its characteristic ideal.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Given a module M over $\Lambda_{\mathcal{O}_K}(G_\infty)$ (respectively $\Lambda_K(G_\infty)$) and a character $\delta:\Delta\to\mathbb{Z}_p^\times$, M^δ denotes the δ-isotypical component of M. For any $m\in M$, we write m^δ for the projection of m into M^δ. The Pontryagin dual of M is written as $M^\vee$.

Let $r\in\mathbb{R}_{\geqslant 0}$. We define

$$\mathcal{H}_r=\left\{\sum_{n\geqslant 0,\sigma\in\Delta} c_{n,\sigma}\cdot\sigma\cdot X^n\in\mathbb{C}_p[\Delta][[X]]:\sup_n\frac{|c_{n,\sigma}|_p}{n^r}<\infty\ \forall\sigma\in\Delta\right\},$$

where $|\cdot|_p$ is the p-adic norm on $\mathbb{C}_p$ such that $|p|_p=p^{-1}$ (the corresponding valuation is written as v_p). We write $\mathcal{H}_\infty=\bigcup_{r\geqslant 0}\mathcal{H}_r$ and $\mathcal{H}_r(G_\infty)=\{f(\gamma-1):f\in\mathcal{H}_r\}$ for $r\in\mathbb{R}_{\geqslant 0}\cup\{\infty\}$. In other words, the elements of $\mathcal{H}_r$ (respectively $\mathcal{H}_r(G_\infty)$) are the power series in X (respectively $\gamma-1$) over $\mathbb{C}_p[\Delta]$ with growth rate $O(\log_p^r)$. If $F,G\in\mathcal{H}_\infty$ or $\mathcal{H}_\infty(G_\infty)$ are such that $F=O(G)$ and $G=O(F)$, we write $F\sim G$.

Given a subfield K of $\mathbb{C}_p$, we write $\mathcal{H}_{r,K}=\mathcal{H}_r\cap K[\Delta][[X]]$ and similarly for $\mathcal{H}_{r,K}(G_\infty)$. In particular, $\mathcal{H}_{0,K}(G_\infty)=\Lambda_K(G_\infty)$. Moreover, we have three operators φ, ∂ and ψ on $\mathcal{H}_{r,K}$ defined by

$$\varphi(f)=f((1+X)^p-1),\quad \partial f=(1+X)\frac{df}{dX}\quad\text{and}\quad \psi(f)=\sum_{\zeta^p=1}f(\zeta(1+X)-1).$$

2.3 Crystalline representations

We write $\mathbb{B}_{\mathrm{cris}}$ and $\mathbb{B}_{\mathrm{dR}}$ for the rings of Fontaine and φ for the Frobenius map acting on these rings. Recall that there exists an element $t\in\mathbb{B}_{\mathrm{dR}}$ such that $\varphi(t)=pt$ and $g\cdot t=\chi(g)t$ for $g\in G_{\mathbb{Q}_p}$.

Let V be a p-adic representation of $G_{\mathbb{Q}_p}$ which is crystalline. We denote the Dieudonné module by $\mathbb{D}(V)=\mathbb{D}_{\mathrm{cris}}(V)=(\mathbb{B}_{\mathrm{cris}}\otimes V)^{G_{\mathbb{Q}_p}}$. If $j\in\mathbb{Z}$, $\mathbb{D}^j(V)$ denotes the jth de Rham filtration of $\mathbb{D}(V)$.

We write $\mathbb{D}_\infty(V)=\mathcal{H}_{0,\mathbb{Q}_p}^{\psi=0}\otimes\mathbb{D}(V)$, which is contained in $\mathcal{H}_{\infty,\mathbb{Q}_p}\otimes\mathbb{D}(V)$. The map $\varphi\otimes\varphi$ on $\mathcal{H}_{\infty,\mathbb{Q}_p}\otimes\mathbb{D}(V)$ is simply written as φ and the map $\partial\otimes 1$ is written as ∂. Note that ∂ acts on $\mathbb{D}_\infty(V)$ bijectively, so ∂^j makes sense for any $j\in\mathbb{Z}$.

Let T be a lattice of V which is stable under $G_{\mathbb{Q}_p}$. For integers $m\geqslant n$, we write $\mathrm{cor}_{m/n}$ for the corestriction map $H^1(\mathbb{Q}_{p,m},A)\to H^1(\mathbb{Q}_{p,n},A)$, where $A=V$ or T. Let $\mathbb{H}^1_{\mathrm{Iw}}(T)$ denote the inverse limit $\varprojlim H^1(\mathbb{Q}_{p,n},T)$ with respect to the corestriction and $\mathbb{H}^1_{\mathrm{Iw}}(V)=\mathbb{Q}\otimes\mathbb{H}^1_{\mathrm{Iw}}(T)$. Moreover, if V arises from the restriction of a p-adic representation of $G_{\mathbb{Q}}$ and T is a lattice stable under $G_{\mathbb{Q}}$, we write

$$\mathbb{H}^1(T)=\varprojlim_n H^1(\mathbb{Z}[\zeta_{p^n},1/p],T),$$
$$\mathbb{H}^1(V)=\mathbb{Q}\otimes\mathbb{H}^1(T).$$

Let $V(j)$ denote the jth Tate twist of V, i.e. $V(j)=V\otimes\mathbb{Q}_pe_j$, where $G_{\mathbb{Q}_p}$ acts on e_j via χ^j. We have $\mathbb{D}(V(j))=t^{-j}\mathbb{D}(V)\otimes e_j$. For any $v\in\mathbb{D}(V)$, $v_j=v\otimes t^{-j}e_j$ denotes its image in $\mathbb{D}(V(j))$. We write $\mathrm{Tw}_{j,V}:\mathbb{H}^1_{\mathrm{Iw}}(V)\to\mathbb{H}^1_{\mathrm{Iw}}(V(j))$ for the isomorphism defined in [Per93, § A.4], which depends on our choice of ζ_{p^n}. For each n and j, we write

$$\exp_{n,j}:\mathbb{Q}_{p,n}\otimes\mathbb{D}(V(j))\to H^1(\mathbb{Q}_{p,n},V(j))$$

for Bloch–Kato's exponential defined in [BK90].

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

2.4 Modular forms

Let $f = \sum a_n q^n$ be a normalised eigen-newform of weight $k \geqslant 2$, level N and character ϵ. Write $F_f = \mathbb{Q}(a_n : n \geqslant 1)$ for its coefficient field. Let $\bar{f} = \sum \bar{a}_n q^n$ be the dual form to f; we have $F_f = F_{\bar{f}}$.

We write $L(f, s)$ for the complex L-function of f. If θ is a finite character of G_∞, we write $L(f_\theta, s)$ for the twisted L-function of f by θ.

We assume that $p \nmid N$ and fix a prime of F_f above p. We denote the completion of F_f at this prime by E and fix a uniformiser ϖ. We write V_f for the two-dimensional E-linear representation of $G_\mathbb{Q}$ associated to f from [Del69]. When restricted to $G_{\mathbb{Q}_p}$, V_f is crystalline and its de Rham filtration is given by

$$\mathbb{D}^i(V_f) = \begin{cases} \mathbb{D}(V_f) & \text{if } i \leqslant 0, \\ E\omega & \text{if } 1 \leqslant i \leqslant k-1, \\ 0 & \text{if } i \geqslant k \end{cases} \tag{1}$$

for some $0 \neq \omega \in \mathbb{D}(V_f)$. Hence, the Hodge–Tate weights of V_f are 0 and $1-k$. The action of φ on $\mathbb{D}(V_f)$ satisfies $\varphi^2 - a_p\varphi + \epsilon(p)p^{k-1} = 0$.

If $v \in V_f$, we write $v^\pm$ for the component of v on which the complex conjugation acts by ± 1.

3. Construction of the Coleman maps

In this section, we define the plus and minus Coleman maps for a modular form f as in § 2.4 under the following condition.

ASSUMPTION 1. $a_p = 0$ and the eigenvalues of φ on $\mathbb{D}(V_f)$ are not integral powers of p.

We first review the definition of Perrin-Riou's exponential from [Per94] for general crystalline representations and results of Kato [Kat04] on general modular forms. We then prove a divisibility property of the image of the Perrin-Riou pairing under Assumption 1 in order to define $\mathrm{Col}^\pm$.

3.1 Perrin-Riou's exponential

Throughout this section, we fix V, a crystalline p-adic representation of $G_{\mathbb{Q}_p}$ such that the action of φ on $\mathbb{D}(V)$ has no eigenvalues which are integral powers of p. Let j be an integer. Since φ acts on t via multiplication by p and $\mathbb{D}(V(j)) = t^{-j}\mathbb{D}(V) \otimes e_j$, the eigenvalues of φ on $\mathbb{D}(V(j))$ are not integral powers of p either.

Since $V(j)^{G_{\mathbb{Q}_{p,\infty}}}$ is also a crystalline representation, it is a sum of characters. But a character is crystalline if and only if it is the product of an unramified character and a power of χ (see for example [Bre01, Example 3.1.4]). Therefore, our assumption on the eigenvalues of φ implies that $V(j)^{G_{\mathbb{Q}_{p,\infty}}} = 0$.

For each $j \in \mathbb{Z}$ and $n \geqslant 0$, under our assumptions on the eigenvalues of φ, the exponential map $\exp_{n,j}$ induces an isomorphism

$$\exp_{n,j} : \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j))/\mathbb{D}^0(V(j)) \to H^1_f(\mathbb{Q}_{p,n}, V(j)).$$

When $n \geqslant 1$, there is a well-defined map

$$\begin{aligned} \Xi_{n,V(j)} : \mathbb{D}_\infty(V(j)) &\to \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j)), \\ g &\mapsto (p \otimes \varphi)^{-n} G(\zeta_{p^n} - 1), \end{aligned}$$

where $G \in \mathcal{H}_{\infty,\mathbb{Q}_p} \otimes \mathbb{D}(V)$ is such that $(1-\varphi)G = g$ (see [Per94, § 3.2.2]). Moreover, $(\exp_{n,j} \circ \Xi_{n,V(j)})_{n \geqslant 1}$ are compatible with the corestriction maps. In other words, the following

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

diagram commutes.

$$\begin{array}{ccc} \mathbb{D}_\infty(V(j)) & \xrightarrow{\exp_{n+1,j}\circ\Xi_{n+1,V(j)}} & H^1(\mathbb{Q}_{p,n+1},V(j)) \\ & \searrow^{\exp_{n,j}\circ\Xi_{n,V(j)}} & \downarrow{\scriptstyle \mathrm{cor}_{n+1/n}} \\ & & H^1(\mathbb{Q}_{p,n},V(j)) \end{array}$$

The definition of the Perrin-Riou exponential is given by the following theorem, which is the main result of [Per94].

Theorem 3.1. *Let h be a positive integer such that $\mathbb{D}^{-h}(V)=\mathbb{D}(V)$. Then, for all integers $j\geqslant 1-h$, there is a unique family of $\Lambda(G_\infty)$-homomorphisms*

$$\Omega_{V(j),h+j}:\mathbb{D}_\infty(V(j))\to\mathcal{H}_\infty(G_\infty)\otimes_{\Lambda(G_\infty)}\mathbb{H}^1_{\mathrm{Iw}}(T(j))$$

such that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{D}_\infty(V(j)) & \xrightarrow{\Omega_{V(j),h+j}} & \mathcal{H}_\infty(G_\infty)\otimes_{\Lambda(G_\infty)}\mathbb{H}^1_{\mathrm{Iw}}(T(j)) \\ {\scriptstyle \Xi_{n,V(j)}}\downarrow & & \downarrow{\scriptstyle \mathrm{pr}} \\ \mathbb{Q}_{p,n}\otimes\mathbb{D}(V(j)) & \xrightarrow{(h+j-1)!\exp_{n,j}} & H^1(\mathbb{Q}_{p,n},V(j)) \end{array}$$

where $n\geqslant 1$ and pr *stands for projection. Moreover, we have*

$$\mathrm{Tw}_{1,V(j)}\circ\Omega_{V(j),h+j}\circ(\partial\otimes te_{-1})=-\Omega_{V(j+1),h+j+1}.$$

Proof. [Per94, § 3.2.3]. □

Remark 3.2. By [Per94, § 3.2.4], if $g\in\mathcal{H}_{0,\mathbb{Q}_p}^{\psi=0}\otimes\mathbb{D}_\alpha(V(j))$, where $\mathbb{D}_\alpha(V(j))$ is the subspace of $\mathbb{D}(V(j))$ in which φ has slope α, then $\Omega_{V(j),h+j}(g)$ is $O(\log_p^{h+\alpha})$, i.e. contained in $\mathcal{H}_{h+\alpha}(G_\infty)\otimes\mathbb{H}^1_{\mathrm{Iw}}(T(j))$.

Remark 3.3. The theorem implies the following congruence for $r\geqslant 0$:

$$\begin{aligned}(-1)^r\,\mathrm{Tw}_{r,V(j)}(\Omega_{V(j),h+j}(g))\equiv{}&(h+j+r-1)!\exp_{n,j+r}\circ\Xi_{n,V(j+r)}\\&\times\circ(\partial^{-r}\otimes t^{-r}e_r)(g)\mod(\gamma^{p^{n-1}}-1).\end{aligned}$$

3.2 Perrin-Riou's pairing

Let M be a finite extension of $\mathbb{Q}_p$ and we further assume that V is a vector space over M and the action of $G_{\mathbb{Q}_p}$ is compatible with the multiplication by M. We fix T, an $\mathcal{O}_M$-lattice of V which is stable under $G_{\mathbb{Q}_p}$. We write V^* for the M-linear dual of V and T^* for the $\mathcal{O}_M$-linear dual of T. Since $H^1(\mathbb{Q}_{p,n},T)$ and $H^1(\mathbb{Q}_{p,n},T^*(1))$ are $\mathcal{O}_M[G_n]$-modules, $\mathbb{H}^1_{\mathrm{Iw}}(T)$ and $\mathbb{H}^1_{\mathrm{Iw}}(T^*(1))$ are $\Lambda_M(G_\infty)$-modules. By [Per94, § 3.6.1], there is a non-degenerate pairing

$$\begin{aligned}\langle\,,\rangle:\mathbb{H}^1_{\mathrm{Iw}}(T)\times\mathbb{H}^1_{\mathrm{Iw}}(T^*(1))&\to\Lambda_{\mathcal{O}_M}(G_\infty),\\((x_n)_n,(y_n)_n)&\mapsto\left(\sum_{\sigma\in G_n}[x_n^\sigma,y_n]_n\cdot\sigma\right)_n,\end{aligned}$$

where $[\,,]_n$ is the natural pairing

$$H^1(\mathbb{Q}_{p,n},T)\times H^1(\mathbb{Q}_{p,n},T^*(1))\to\mathcal{O}_M.$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

The pairing $\langle\,,\rangle$ extends to

$$\left(\mathcal{H}_{\infty,M}(G_\infty)\otimes_{\Lambda_{\mathcal{O}_M}(G_\infty)}\mathbb{H}^1_{\mathrm{Iw}}(T)\right)\times\left(\mathcal{H}_{\infty,M}(G_\infty)\otimes_{\Lambda_{\mathcal{O}_M}(G_\infty)}\mathbb{H}^1_{\mathrm{Iw}}(T^*(1))\right)\to\mathcal{H}_{\infty,M}(G_\infty),$$

which we also denote by $\langle\,,\rangle$. Let j and h be integers satisfying conditions of Theorem 3.1. If $\eta\in\mathbb{D}(V(j))$, then $(1+X)\otimes\eta\in\mathbb{D}_\infty(V(j))$. Using the pairing $\langle\,,\rangle$, we define a map

$$\begin{aligned}\mathcal{L}_\eta^{h,j}:\mathbb{H}^1_{\mathrm{Iw}}(T(j)^*(1))&\to\mathcal{H}_{\infty,M}(G_\infty),\\ \mathbf{z}&\mapsto\langle\Omega_{V(j),h+j}((1+X)\otimes\eta),\mathbf{z}\rangle.\end{aligned}$$

Note that $\mathcal{L}_\eta^{h,j}$ modulo $\gamma^{p^{n-1}}-1$ induces a map into $M[G_n]$, which we denote by $\mathcal{L}_{\eta,n}^{h,j}$. Also, $\mathcal{L}_\eta^{h,j}$ extends naturally to a map on $\mathbb{H}^1_{\mathrm{Iw}}(V(j)^*(1))$, which we write as $\mathcal{L}_\eta^{h,j}$ also.

3.2.1 *Explicit formulae of $\mathcal{L}_{\eta,n}^{h,j}$.* We want to say something about values of the image of $\mathcal{L}_{\eta,n}^{h,j}$ at some special characters on G_∞. To do this, we make use of the following result.

LEMMA 3.4. *Under the notation above, let $\eta\in\mathbb{D}(V(j))$. Then, the projection of*

$$\frac{1}{(h+j-1)!}\Omega_{V(j),h+j}((1+X)\otimes\eta)$$

into $H^1(\mathbb{Q}_{p,n},V(j))$ is given by

$$\begin{cases}p^{-n}\exp_{n,j}\left(\displaystyle\sum_{m=0}^{n-1}\zeta_{p^{n-m}}\otimes\varphi^{m-n}(\eta)+(1-\varphi)^{-1}(\eta)\right) & \text{if } n\geqslant 1,\\ \exp_{0,j}\left(\left(1-\dfrac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(\eta)\right) & \text{if } n=0.\end{cases}$$

Proof. This is a straightforward application of Remark 3.3 to the solution of $(1-\varphi)G=(1+X)\otimes\eta$ as given in [Per94, § 2.2]. □

For $n\geqslant 1$ and $\eta\in\mathbb{D}(V(j))$, we write

$$\gamma_{n,j}(\eta):=p^{-n}\left(\sum_{i=0}^{n-1}\zeta_{p^{n-i}}\otimes\varphi^{i-n}(\eta)+(1-\varphi)^{-1}(\eta)\right).$$

Remark 3.3 and properties of the twist map (see e.g. [Per94, §§ 3.6.1 and 3.6.5]) imply that for $\mathbf{z}\in\mathbb{H}^1_{\mathrm{Iw}}(T(j)^*(1))$ and $r\geqslant 0$,

$$\frac{1}{(h+j+r-1)!}\,\mathrm{Tw}_r(\mathcal{L}_\eta^{h,j}(\mathbf{z}))\equiv\sum_{\sigma\in G_n}[\exp_{n,j+r}(\gamma_{n,j+r}(\eta_r)^\sigma),z_{-r,n}]_n\cdot\sigma\mod(\gamma^{p^{n-1}}-1),\quad(2)$$

where Tw_r acts on $\mathcal{H}_\infty(G_\infty)$ via $\sigma\mapsto\chi(\sigma)^r\sigma$ for $\sigma\in G_\infty$ and $z_{-r,n}$ is the image of $\mathbf{z}$ under the composition

$$\mathbb{H}^1_{\mathrm{Iw}}(T(j)^*(1))\xrightarrow{(-1)^r\,\mathrm{Tw}_{-r}}\mathbb{H}^1_{\mathrm{Iw}}(T(j+r)^*(1))\xrightarrow{\mathrm{pr}}H^1(\mathbb{Q}_{p,n},T(j+r)^*(1)).$$

By [Kat93, ch. II, § 1.4], we also have

$$[\exp_{n,j+r}(\cdot),\cdot]_n=\mathrm{Tr}_{n/0}\otimes\mathrm{id}([\cdot,\exp^*_{n,j+r}(\cdot)]'_n),$$

where $\exp^*_{n,j+r}$ is the dual exponential map

$$\exp^*_{n,j+r}:H^1(\mathbb{Q}_{p,n},V(j+r)^*(1))\to\mathbb{D}^0(V(j+r)^*(1))$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

and the pairing

$$[\,,\,]'_n : \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j+r)) \times \mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j+r)^*(1)) \to \mathbb{Q}_{p,n} \otimes M$$

is induced by the natural pairing

$$\mathbb{D}(V(j+r)) \times \mathbb{D}(V(j+r)^*(1)) \to M.$$

To ease notation, we simply write $[\,,\,]_n$ for $[\,,\,]'_n$ when it does not cause confusion. We can now rewrite (2) as

$$\begin{aligned}
&\frac{1}{(h+j+r-1)!}\,\mathrm{Tw}_r(\mathcal{L}_\eta^h(\mathbf{z})) \\
&\quad\equiv \sum_{\sigma\in G_n} \mathrm{Tr}_{n,0}[\gamma_{n,j+r}(\eta_r)^\sigma, \exp^*_{n,j+r}(z_{-r,n})]_n \cdot \sigma \mod(\gamma^{p^{n-1}}-1) \\
&\quad\equiv \left[\sum_{\sigma\in G_n} \gamma_{n,j+r}(\eta_r)^\sigma \sigma, \sum_{\sigma\in G_n} \exp^*_{n,j+r}(z^\sigma_{-r,n})\sigma^{-1}\right]_n \mod(\gamma^{p^{n-1}}-1). \qquad (3)
\end{aligned}$$

Note that we have recovered the pairing P_n of [Kur02]. We write the quantity in (3) as $P_{n,r}(\eta, z_{-r,n})$. Following the calculations of [Kur02], we can deduce the following special values of $\mathcal{L}_\eta^{h,j}$.

Lemma 3.5. *For an integer $r \geqslant 0$, we have*

$$\frac{1}{(h+j+r-1)!}\chi^r(\mathcal{L}_\eta^{h,j}(\mathbf{z})) = \left[\left(1-\frac{\varphi^{-1}}{p}\right)(1-\varphi^{-1})(\eta_r), \exp^*_{0,r+j}(z_{-r,0})\right]_0.$$

Let θ be a character of G_n which does not factor through G_{n-1} with $n \geqslant 1$; then

$$\frac{1}{(h+j+r-1)!}\chi^r\theta(\mathcal{L}_\eta^{h,j}(\mathbf{z})) = \frac{1}{\tau(\theta^{-1})}\sum_{\sigma\in G_n}\theta^{-1}(\sigma)[\varphi^{-n}(\eta_r), \exp^*_{n,r+j}(z^\sigma_{-r,n})]_n,$$

where τ denotes the Gauss sum.

3.3 Modular forms and Kato zeta elements

The details of the results in this section can be found in [Kat04].

3.3.1 *L-functions and p-adic L-functions.* Let f be as in § 2.4. For any $v \in V_f$ such that $v^\pm \neq 0$, it determines an $\mathcal{O}_E$-lattice T_f of V_f. We choose v such that T_f is stable under $G_\mathbb{Q}$. Note that as a representation of $G_\mathbb{Q}$, $V_f^* \cong V_{\bar{f}}(k-1)$. Hence, T_f determines a lattice $T_{\bar{f}}$ of $V_{\bar{f}}$ naturally.

Let $\mathrm{per} : \mathbb{D}^1(V_f) \to V_f$ be the period map defined in [Kat04]. Fix $0 \neq \omega \in \mathbb{D}^1(V_f)$ and let $\Omega_\pm \in \mathbb{C}^\times$ be such that $\mathrm{per}(\omega) = \Omega_+ v^+ + \Omega_- v^-$. The p-adic L-functions associated to f are given by the following.

Theorem 3.6. *Let α be a root of $X^2 - a_p X + \epsilon(p)p^{k-1}$ such that $v_p(\alpha) < k-1$. Under the notation above, there exists a unique $L_{p,\alpha} \in \mathcal{H}_\infty(G_\infty)$ (depending on the choice of ω and v) such that for any integer $0 \leqslant r \leqslant k-2$ and any character θ of G_n which does not factor through G_{n-1} with $n \geqslant 1$,*

$$\chi^r\theta(L_{p,\alpha}) = \frac{c_{n,r}\alpha^{-n}}{\tau(\theta)\Omega_\pm}L(f,\theta,r),$$

where $c_{n,r}$ is some constant, dependent only on n and r and $\pm = (-1)^{k-r}\theta(-1)$.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Proof. [AV75, MTT86] or [Kat04, Theorem 16.2]. □

If f corresponds to an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$, there is a canonical choice of ω and T_f, namely, the Néron differential and $T_p(\mathcal{E})(-1)$ (see [Kur02, § 2.2.2]), where $T_p(\mathcal{E})$ denotes the Tate module of $\mathcal{E}$ at p.

3.3.2 *Kato's main conjecture.* In order to state Kato's main conjecture, we have to review two important results from [Kat04] first.

THEOREM 3.7. *Under the notation above, we have:*

(a) $\mathbb{H}^2(T_f)$ *is a torsion* $\Lambda_{\mathcal{O}_E}(G_\infty)$*-module;*

(b) $\mathbb{H}^1(T_f)$ *is a torsion-free* $\Lambda_{\mathcal{O}_E(G_\infty)}$*-module and* $\mathbb{H}^1(V_f)$ *is a free* $\Lambda_E(G_\infty)$*-module of rank one.*

Proof. [Kat04, Theorem 12.4]. □

THEOREM 3.8. *Fix a character* $\delta : \Delta \to \mathbb{Z}/(p-1)\mathbb{Z}$.

(a) *Let* θ *be a character of* G_n *and* $\pm = (-1)^{k-r}\theta(-1)$*, where* r *is an integer such that* $1 \leqslant r \leqslant k-1$*. Write*

$$\kappa_\theta : \mathbb{Q}_{p,n} \otimes \mathbb{D}^0(V_f(k-r)) \to V_f,$$
$$x \otimes y \mapsto \sum_{\sigma \in G_n} \theta(\sigma)\sigma(x)\mathrm{per}(y)^{\pm}.$$

There exists a unique E-linear map (independent of θ *and* r*)* $V_f \to \mathbb{H}^1(V_f)$*;* $v \mapsto \mathbf{z}_v$ *such that* κ_θ *sends the image of* $\mathbf{z}_v$ *in* $\mathbb{Q}_{p,n} \otimes \mathbb{D}^0(V_f(k-r))$ *(under the composition of the localisation, the twist map and the dual exponential) to* $d_r \cdot L(\bar{f}, \theta, r) \cdot v^{\pm}$ *and* d_r *is a constant which depends only on* r*.*

(b) *Let* $\mathbb{Z}(T_f) \subset \mathbb{H}^1(V_f)$ *denote the* $\Lambda_{\mathcal{O}_E}(G_\infty)$*-module generated by* $\mathbf{z}_{v^\pm} \in T_f$ *and write* $\mathbb{Z}(V_f) = \mathbb{Z}(T_f) \otimes \mathbb{Q}$*. Then, the quotient* $\mathbb{H}^1(V_f)/\mathbb{Z}(V_f)$ *is a torsion* $\Lambda_E(G_\infty)$*-module and*

$$\mathrm{Char}_{\Lambda_E(\Gamma)}(\mathbb{H}^1(V_f)^\delta/\mathbb{Z}(V_f)^\delta) \subset \mathrm{Char}_{\Lambda_E(\Gamma)}(\mathbb{H}^2(V_f)^\delta).$$

(c) *If the homomorphism* $G_\mathbb{Q} \to \mathrm{GL}_{\mathcal{O}_E}(T_f)$ *is surjective, then* $\mathbb{Z}(T_f) \subset \mathbb{H}^1(T_f)$*. Moreover,* $\mathbb{H}^1(T_f)$ *is a free* $\Lambda_{\mathcal{O}_E}$*-module of rank one and*

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^1(T_f)^\delta/\mathbb{Z}(T_f)^\delta) \subset \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^2(T_f)^\delta).$$

Proof. [Kat04, Theorem 12.5]. □

Kato's main conjecture states the following.

CONJECTURE 3.9. The inclusion $\mathbb{Z}(T_f) \subset \mathbb{H}^1(T_f)$ holds. Moreover, if $\delta : \Delta \to \mathbb{Z}/(p-1)\mathbb{Z}$ is a character, then

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^1(T_f)^\delta/\mathbb{Z}(T_f)^\delta) = \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^2(T_f)^\delta).$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

We call elements of $\mathbb{Z}(V_f)$ Kato zeta elements. In particular, we write $\mathbf{z}_f^{\mathrm{Kato}}$ for the one corresponding to our choice of $v \in V_f$ fixed in § 3.3.1 and call it *the* Kato zeta element associated to f.

We fix $\bar{v} \in V_{\bar{f}}$ and $\bar{\omega} \in \mathbb{D}^{-1}(V_{\bar{f}}(k))$ for the dual form $\bar{f}$ similarly. Below, we relate the Kato zeta element $\mathbf{z}_{\bar{f}}^{\mathrm{Kato}}$ associated to $\bar{f}$ to the p-adic L-functions of f defined by Theorem 3.6 via the map $\mathcal{L}_\eta^{h,j}$. For simplicity, we write $\mathbf{z}^{\mathrm{Kato}} = \mathbf{z}_{\bar{f}}^{\mathrm{Kato}}$ from now on.

Let $V = V_f(1)$; then we can take $h = 1$ and $j \geqslant 0$ in Theorem 3.1 by (1). For $\eta \in \mathbb{D}(V_f)$, we simply write

$$\mathcal{L}_\eta = \mathcal{L}_{\eta_1}^{1,0} : \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1)) \to \mathcal{H}_\infty(G_\infty)$$

for the map we defined in § 3.2, with $M = E$.

Theorem 3.10. *For α as in Theorem 3.6, there exists η_α, an eigenvector of φ on $\mathbb{D}(V_f)$ with eigenvalue α such that $[\eta_\alpha, \bar{\omega}] = 1$. Moreover, the image of $\mathbf{z}^{\mathrm{Kato}}$ under the composition*

$$\mathbb{H}^1(V_{\bar{f}}) \to \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}) \xrightarrow{\mathrm{Tw}_{k-1}} \mathbb{H}^1_{\mathrm{Iw}}(V_{\bar{f}}(k-1)) \xrightarrow{\mathcal{L}_{\eta_\alpha}} \mathcal{H}_\infty(G_\infty)$$

is the p-adic L-function $L_{p,\alpha}$, where the first map is just the localisation and Tw_{k-1} denotes $\mathrm{Tw}_{k-1,V_{\bar{f}}}$.

Proof. [Kat04, Theorem 16.6]. □

We sometimes abuse notation and write the above composition as $\mathcal{L}_{\eta_\alpha}$ also.

Remark 3.11. Let α_1 and α_2 be the roots of $X^2 - a_p X + \epsilon(p)p^{k-1}$. Then, the slope of φ on $\mathbb{D}(V_f)$ is equal to $t = \max(v_p(\alpha_1), v_p(\alpha_2))$. Since $h = 1$ and the slope of φ on $\mathbb{D}(V_f(1))$ is $t - 1$, all elements of $\mathrm{Im}(\mathcal{L}_\eta)$ are $O(\log_p^t)$ by Remark 3.2.

It follows immediately from Lemma 3.5 that, with the same notation as in the lemma, we have

$$\begin{aligned} \chi^r(\mathcal{L}_\eta(\mathbf{z})) &= r!\left[\left(1 - \frac{\varphi^{-1}}{p}\right)(1-\varphi)^{-1}(\eta_{r+1}), \exp^*_{0,r+1}(z_{-r,0})\right]_0, \\ \chi^r\theta(\mathcal{L}_\eta(\mathbf{z})) &= \frac{r!}{\tau(\theta^{-1})}\sum_{\sigma\in G_n}\theta^{-1}(\sigma)[\varphi^{-n}(\eta_{r+1}), \exp^*_{n,r+1}(z^\sigma_{-r,n})]_n. \end{aligned} \tag{4}$$

3.4 The ±-Coleman maps

3.4.1 *±-logarithms.* Let f be as above such that Assumption 1 holds. If α_1 and α_2 are the roots of $X^2 - a_p X + \epsilon(p)p^{k-1}$, then $\alpha_1 = -\alpha_2$. Moreover, $v_p(\alpha_1) = v_p(\alpha_2) = (k-1)/2$, so Remark 3.11 implies that $\mathrm{Im}(\mathcal{L}_\eta) \subset \mathcal{H}_{(k-1)/2}(G_\infty)$ for any $\eta \in \mathbb{D}(V_f)$.

In [Pol03], Pollack defines

$$\log^+_{p,k} = \prod_{j=0}^{k-2}\frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n}(u^{-j}\gamma)}{p},$$

$$\log^-_{p,k} = \prod_{j=0}^{k-2}\frac{1}{p}\prod_{n=1}^{\infty}\frac{\Phi_{2n-1}(u^{-j}\gamma)}{p},$$

where Φ_m denotes the p^mth cyclotomic polynomial.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

By considering the special values of L_{p,α_1} and L_{p,α_2} as given by Theorem 3.6, Pollack showed that we have the following divisibility properties:

$$\log_{p,k}^{+} | \alpha_2 L_{p,\alpha_1} - \alpha_1 L_{p,\alpha_2},$$
$$\log_{p,k}^{-} | L_{p,\alpha_2} - L_{p,\alpha_1}.$$

This enabled him to define

$$L_{p,f}^{+} = \frac{\alpha_2 L_{p,\alpha_1} - \alpha_1 L_{p,\alpha_2}}{(\alpha_2 - \alpha_1)\log_{p,k}^{+}}, \tag{5}$$

$$L_{p,f}^{-} = \frac{L_{p,\alpha_2} - L_{p,\alpha_1}}{(\alpha_2 - \alpha_1)\log_{p,k}^{-}}. \tag{6}$$

To ease notation, we suppress the subscript f and write $L_p^{\pm}$ for $L_{p,f}^{\pm}$. The growth rates of these elements are given by the following theorem.

THEOREM 3.12. *$\log_{p,k}^{+} \sim \log_{p,k}^{-} \sim \log_p^{(k-1)/2}$ and $L_p^{\pm} = O(1)$.*

Proof. [Pol03, Lemma 4.5 and Theorem 5.1]. □

3.4.2 *Definition of the Coleman maps.* Let us first introduce a shorthand. For $0 \leqslant r \leqslant k-2$ and $x \in \mathbb{D}(V_f(r+1))$, we write $x \bmod \omega$ for the image of x in the quotient $\mathbb{D}(V_f(r+1))/E \cdot \omega_{r+1}$. If two elements x and y of $\mathbb{D}(V_f(r+1))$ have the same image, we simply write $x \equiv y \bmod \omega$.

LEMMA 3.13. *Let $0 \leqslant r \leqslant k-2$ be an integer. If θ is a finite character as in Lemma 3.5 and $\eta \in \mathbb{D}(V_f)$, then $\varphi^{-n}(\eta_{r+1}) \equiv 0 \bmod \omega$ implies that $\chi^r\theta(\mathcal{L}_\eta(\mathbf{z})) = 0$ for any $\mathbf{z}$.*

Proof. We have

$$\mathrm{Im}(\exp_{n,r+1}^{*}) = \mathbb{Q}_{p,n} \otimes E \cdot \bar{\omega}_{-r-1} = \mathbb{Q}_{p,n} \otimes \mathbb{D}^0(V_{\bar{f}}(k-1-r)) \quad \text{and} \quad \mathbb{D}^0(V_f(r+1)) = E \cdot \omega_{r+1}.$$

Hence, the fact that $\mathbb{D}^0(V_f(r+1))$ and $\mathbb{D}^0(V_{\bar{f}}(k-1-r))$ are orthogonal complements of each other under $[\,,\,]$ and (4) imply that $\chi^r\theta(\mathcal{L}_\eta(\mathbf{z})) = 0$ if $\varphi^{-n}(\eta_{r+1})$ is a multiple of ω_{r+1}. □

Recall that $\mathcal{L}_{\eta_{\alpha_i}}(\mathbf{z}^{\mathrm{Kato}}) = L_{p,\alpha_i}$ for $i = 1, 2$ by Theorem 3.10. Hence, if we write

$$\eta^{+} = \frac{\alpha_2\eta_{\alpha_1} - \alpha_1\eta_{\alpha_2}}{\alpha_2 - \alpha_1} \quad \text{and} \quad \eta^{-} = \frac{\eta_{\alpha_2} - \eta_{\alpha_1}}{\alpha_2 - \alpha_1},$$

then $\mathcal{L}_{\eta^{\pm}}(\mathbf{z}^{\mathrm{Kato}}) = \log_{p,k}^{\pm} L_p^{\pm}$ by (5), (6) and the linearity of $\mathcal{L}$. In fact, more is true.

PROPOSITION 3.14. *If $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}})$, then $\log_{p,k}^{\pm} | \mathcal{L}_{\eta^{\pm}}(\mathbf{z})$ over $\mathcal{H}_{\infty,E}(G_\infty)$.*

Proof. Recall that $[\omega, \bar{\omega}] = 0$, $[\eta_{\alpha_i}, \bar{\omega}] = 1$ and $\varphi^2 = \alpha_i^2$ on $\mathbb{D}(V_f)$. Therefore, explicit calculation shows that $\eta_{\alpha_i} = (\varphi(\omega) + \alpha_i\omega)/[\varphi(\omega), \bar{\omega}]$ for $i \in \{1, 2\}$. Hence,

$$\eta^{+} = \frac{\varphi(\omega)}{[\varphi(\omega), \bar{\omega}]} \quad \text{and} \quad \eta^{-} = \frac{\omega}{[\varphi(\omega), \bar{\omega}]}.$$

Let r be an integer. Since $\varphi^2 = -\epsilon(p)p^{k-2r-3}$ on $\mathbb{D}(V_f(r+1))$, we have

$$\varphi^{-n}(\eta_{r+1}^{+}) \equiv 0 \mod \omega \text{ if } n \text{ is odd},$$
$$\varphi^{-n}(\eta_{r+1}^{-}) \equiv 0 \mod \omega \text{ if } n \text{ is even}.$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Therefore, by Lemma 3.13 and (4), we have

$$\chi^r\theta(\mathcal{L}_{\eta^+}(\mathbf{z}))=0 \quad \text{if } n \text{ is odd},$$
$$\chi^r\theta(\mathcal{L}_{\eta^-}(\mathbf{z}))=0 \quad \text{if } n \text{ is even},$$

where θ and n are as defined in Lemma 3.5. Recall that $\chi(\gamma)=u$, so we have equivalences $\chi^r\theta(\Phi_m(u^{-r}\gamma))=\Phi_m(\theta(\gamma))=0$ if and only if $\theta(\gamma)$ is a primitive p^mth root of unity if and only if θ factors through G_{m+1} but not G_m. Hence, all the zeros of $\log^{\pm}_{p,k}$, which are all simple, are also zeros of $\mathcal{L}_{\eta^\pm}(\mathbf{z})$, so we are done. □

Remark 3.15. An alternative proof for this proposition is given in § 5.1.

Recall that $\mathcal{L}_{\eta^\pm}(\mathbf{z})=O(\log_p^{(k-1)/2})$ and Theorem 3.12 says that $\log^{\pm}_{p,k}\sim\log_p^{(k-1)/2}$, so we have $\mathcal{L}_{\eta^\pm}(\mathbf{z})/\log^{\pm}_{p,k}=O(1)$, i.e. an element of $\mathcal{H}_{0,E}(G_\infty)=\Lambda_E(G_\infty)$. We define

$$\mathrm{Col}^{\pm}:\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar f}(k-1))\to\Lambda_E(G_\infty),$$
$$\mathbf{z}\mapsto\frac{\mathcal{L}_{\eta^\pm}(\mathbf{z})}{\log^{\pm}_{p,k}}.$$

We call these two maps the plus and minus Coleman maps. Note that we sometimes abuse notation and write $\mathrm{Col}^{\pm}$ for the composition

$$\mathbb{H}^1(T_{\bar f})\to\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar f})\xrightarrow{\mathrm{Tw}_{k-1}}\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar f}(k-1))\xrightarrow{\mathrm{Col}^{\pm}}\Lambda_E(G_\infty)$$

and its natural extension to $\mathbb{H}^1(V_{\bar f})$. In particular, we have

$$\mathrm{Col}^{\pm}(\mathbf{z}^{\mathrm{Kato}})=L_p^{\pm}. \tag{7}$$

Similar to $\mathcal{L}_{\eta^\pm,n}$, we write $\mathrm{Col}^{\pm}_n$ for the map $\mathrm{Col}^{\pm}$ modulo $\gamma^{p^{n-1}}-1$.

Remark 3.16. The Coleman maps in [Kob03] are defined using a pairing with points coming from the formal group associated to an elliptic curve, instead of images of the Perrin-Riou exponential. It is not hard to see that the definition given above agrees with the one given by Kobayashi on comparing [Kob03, Proposition 8.25] and (3).

4. Kernels of the Coleman maps

In addition to Assumption 1, we assume that the following holds.

Assumption 2. Either $p+1\nmid k-1$ or $\epsilon(p)\neq-1$.

Under these two conditions, we give an explicit description of the kernels of the plus and minus Coleman maps defined in § 3. In particular, we generalise [Kob03, Proposition 8.18], which describes the kernels of $\mathrm{Col}^{\pm}$ in the case of elliptic curves defined over $\mathbb{Q}$.

4.1 Some linear algebra

Let us first study some basic properties of $\mathbb{Q}_{p,n}$. Define

$$\pi_n=\begin{cases}\zeta_{p^n} & \text{if } n>1,\\ \zeta_p+\dfrac{1}{p-1} & \text{if } n=1,\\ 1 & \text{if } n=0\end{cases}$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

and $\mathbb{Q}_p^{(n)}$ denotes the $\mathbb{Q}_p$-vector space generated by $\{\pi_n^\sigma : \sigma \in G_n\}$. Then, $\mathrm{Tr}_{n/n-1}\,\pi_n = 0$ for $n \geqslant 1$ and

$$\mathbb{Q}_{p,n} = \bigoplus_{i=0}^{n} \mathbb{Q}_p^{(i)}. \tag{8}$$

PROPOSITION 4.1. *Let $n \geqslant 0$ be an integer and $\alpha = \sum_{i=0}^{n} x_i\pi_i$ for some $x_i \in \mathbb{Q}_p$. Then, the $\mathbb{Q}_p$-vector space generated by $\{\alpha^\sigma : \sigma \in G_n\}$ is given by $\bigoplus_{i\in S} \mathbb{Q}_p^{(i)}$, where $S = \{i : x_i \neq 0\}$.*

Proof. We proceed by induction on $|S|$. The case $|S| = 1$ is immediate, so we assume that $|S| > 1$. Write V for the $\mathbb{Q}_p$-vector space generated by $\{\alpha^\sigma : \sigma \in G_n\}$. Clearly, $V \subset \bigoplus_{i:x_i\neq 0} \mathbb{Q}_p^{(i)}$. Without loss of generality, we assume that $x_n \neq 0$. Let $\beta = \sum_{i=0}^{n-1} x_i\pi_i$. Then, by induction, $\{\beta^\tau : \tau \in G_{n-1}\}$ generates $\bigoplus_{i\in S\setminus\{n\}} \mathbb{Q}_p^{(i)}$ over $\mathbb{Q}_p$. Fix $\tau \in G_{n-1}$; then

$$\sum_{\sigma\in G_n, \sigma|_{\mathbb{Q}_{p,n-1}}=\tau} \alpha^\sigma = r\beta^\tau + (\mathrm{Tr}_{n/n-1}\,\pi_n)^\tau = r\beta^\tau \in V,$$

where $r = [\mathbb{Q}_{p,n} : \mathbb{Q}_{p,n-1}]$. Therefore, for any $\tau \in G_{n-1}$, $\beta^\tau \in V$ and $\pi_n^\sigma \in V$ for any $\sigma \in G_n$. Hence, we are done. □

COROLLARY 4.2. *Let $\eta = a_0 + \sum_{i=1}^{n} a_i\zeta_{p^i}$, where $a_i \in \mathbb{Q}_p$ with $a_1 \neq (p-1)a_0$; then the $\mathbb{Q}_p$-vector space generated by $\{\eta^\sigma : \sigma \in G_n\}$ is given by $\mathbb{Q}_p + \sum_{r\in S}\sum_{\sigma\in G_n} \mathbb{Q}_p \cdot \zeta_{p^r}^\sigma$, where $S = \{r \in [1, n] : a_r \neq 0\}$.*

Proof. The result is immediate if $a_1 = 0$ by Proposition 4.1. If $a_1 \neq 0$, then

$$\eta = \left(a_0 - \frac{a_1}{p-1}\right) + a_1\pi_1 + \sum_{i>1} a_i\pi_i.$$

Hence, we can again apply Proposition 4.1. □

COROLLARY 4.3. *Let $\eta = 1 + \zeta_p + \zeta_{p^2} + \cdots + \zeta_{p^n}$; then η is a normal basis of $\mathbb{Q}_{p,n}$ over $\mathbb{Q}_p$.*

4.2 Properties of H^1

Recall that when f corresponds to an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ and $T_f(1)$ is the Tate module of $\mathcal{E}$, we have $\mathcal{E}[p^\infty] \cong V_f/T_f(1)$ as $G_\mathbb{Q}$-modules. Therefore, the following lemma generalises [Kob03, Proposition 8.7], which says that $\mathcal{E}$ has no p-torsion defined over k_∞.

LEMMA 4.4. *For all $j \in \mathbb{Z}$ and $n \geqslant 0$, $(V_f/T_f)(j)^{G_{\mathbb{Q}_{p,n}}} = 0$.*

Proof. It is enough to show that $(V_f/T_f)^{G_{\mathbb{Q}_{p,\infty}}} = 0$. Since $V_f/T_f = \varprojlim_{\times\varpi} T_f/\varpi^n T_f$, it in fact suffices to show that $(T_f/\varpi T_f)^{G_{\mathbb{Q}_{p,\infty}}} = 0$. We make use of the description of the representation $\rho_f : G_{\mathbb{Q}_{p,n}} \to \mathrm{GL}(T_f/\varpi T_f)$ given by [BLZ04, Proposition 4.1.4] and consider two different cases.

Case 1: $p + 1 \nmid k - 1$. In this case,

$$\rho_f|I = \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix},$$

where I is the inertia group of $G_{\mathbb{Q}_p}$ and ψ and ψ' are fundamental characters of level 2, i.e.

$$\ker\psi = \ker\psi' = G_{\mathbb{Q}_p^{\mathrm{ur}}(\sqrt[p^2-1]{p})}.$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Hence, 1 is not an eigenvalue of $\rho_f(\sigma)$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ur}}(\sqrt[p^2-1]{p})/\mathbb{Q}_p^{\mathrm{ur}}(\sqrt[p-1]{p}))$, as $p+1 \nmid k-1$. Therefore, there exists an element in the above Galois group which lifts to $G_{\mathbb{Q}_{p,\infty}}$ and $(T_f/\varpi T_f)^{G_{\mathbb{Q}_{p,\infty}}} = 0$, as required.

Case 2: $p+1 | k-1$. In this case, $\rho_f|_{G_{\mathbb{Q}_{p,\infty}}}$ factors through $\mathrm{Gal}(\mathbb{Q}_{p,\infty}^{\mathrm{ur}}/\mathbb{Q}_{p,\infty})$ and the eigenvalues of the Frobenius map are the square roots of $-\epsilon(p)$. By our assumption, this is not 1, so we are done. □

We now give two immediate corollaries.

Corollary 4.5. *The projection $\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(j)) \to H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(j))$ is surjective for all j and n.*

Proof. It is enough to show that $\mathrm{cor}_{n/m} : H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(j)) \to H^1(\mathbb{Q}_{p,m}, T_{\bar{f}}(j))$ is surjective for all $n \geqslant m$. On taking the Pontryagin dual, it is equivalent to showing that

$$\mathrm{res}_{m/n} : H^1(\mathbb{Q}_{p,m}, V_f/T_f(k-1-j)) \to H^1(\mathbb{Q}_{p,n}, V_f/T_f(k-1-j))$$

is injective. But this immediately follows from the inflation–restriction exact sequence and the fact that $V_f/T_f(k-1-j)^{G_{\mathbb{Q}_{p,\infty}}} = 0$ as given by Lemma 4.4. □

Corollary 4.6. *For all n and j as above, $H^1(\mathbb{Q}_{p,n}, T_f(j)) \hookrightarrow H^1(\mathbb{Q}_{p,n}, V_f(j))$.*

Proof. From the short exact sequence $0 \to T_f(j) \to V_f(j) \to V_f/T_f(j) \to 0$, we obtain a long exact sequence

$$\cdots \to (V_f/T_f(j))^{G_{\mathbb{Q}_{p,n}}} \to H^1(\mathbb{Q}_{p,n}, T_f(j)) \to H^1(\mathbb{Q}_{p,n}, V_f(j)) \to \cdots .$$

Hence, the result follows by Lemma 4.4. □

In particular, $H^1(\mathbb{Q}_{p,n}, T_f(j))$ can be identified as an $\mathcal{O}_E$-lattice of $H^1(\mathbb{Q}_{p,n}, V_f(j))$. Another property of H^1 which we need is the injectivity of the restriction

$$H^1(\mathbb{Q}_{p,m}, V_f(j)) \xrightarrow{\mathrm{res}} H^1(\mathbb{Q}_{p,n}, V_f(j))$$

for $n \geqslant m$, which follows from the inflation–restriction sequence and $V_f(j)^{G_{\mathbb{Q}_{p,\infty}}} = 0$ (immediate from Lemma 4.4). In particular, the same can be said about H^1_f. We regard $H^1_f(\mathbb{Q}_{p,m}, A)$ as a subgroup of $H^1_f(\mathbb{Q}_{p,n}, A)$ for $A = T_f(j)$ or $V_f(j)$ in the next section.

4.3 Some subgroups of H^1_f

Let $\eta^{\pm}$ be as defined in § 3. For $1 \leqslant j \leqslant k-1$, recall that $\mathbb{D}^0(V_f(j)) = E \cdot \omega_j$. Using the shorthand introduced in § 3.4.2, we define two $E[G_n]$-modules

$$\begin{aligned} R^+_{n,j} &= \sum_{\sigma \in G_n} E \cdot \gamma_{n,j}(\eta_j^+)^\sigma \mod \omega \subset \mathbb{Q}_{p,n} \otimes \mathbb{D}(V_f(j))/\mathbb{D}^0(V_f(j)), \\ R^-_{n,j} &= \sum_{\sigma \in G_n} E \cdot \gamma_{n,j}(\eta_j^-)^\sigma \mod \omega \subset \mathbb{Q}_{p,n} \otimes \mathbb{D}(V_f(j))/\mathbb{D}^0(V_f(j)). \end{aligned} \tag{9}$$

Remark 4.7. For $1 \leqslant j \leqslant k-1$, we have isomorphisms of $E[G_n]$-modules

$$H^1_f(\mathbb{Q}_{p,n}, V_f(j)) \cong \mathbb{Q}_{p,n} \otimes_{\mathbb{Q}_p} \mathbb{D}(V_f(j))/\mathbb{D}^0(V_f(j)) \cong \mathbb{Q}_{p,n} \otimes E.$$

Under this identification, the corestriction $\mathrm{cor}_{n/m} : H^1_f(\mathbb{Q}_{p,n}, V_f(j)) \to H^1_f(\mathbb{Q}_{p,m}, V_f(j))$ corresponds to $\mathrm{Tr}_{n/m} \otimes \mathrm{id} : \mathbb{Q}_{p,n} \otimes E \to \mathbb{Q}_{p,m} \otimes E$.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

By Remark 4.7, we can identify $R^{\pm}_{n,j}$ with subsets of $\mathbb{Q}_{p,n} \otimes E$ and we have the following description.

LEMMA 4.8. *By identifying* $\mathbb{Q}_{p,n} \otimes \mathbb{D}(V(j))/\mathbb{D}^0(V(j))$ *with* $\mathbb{Q}_{p,n} \otimes E$, *we have*

$$\begin{aligned} R^{+}_{n,j} &= \sum_{m \text{ even}} \sum_{\sigma \in G_m} E \cdot \zeta^{\sigma}_{p^m} + E, \\ R^{-}_{n,j} &= \sum_{m \text{ odd}} \sum_{\sigma \in G_m} E \cdot \zeta^{\sigma}_{p^m} + E, \end{aligned} \tag{10}$$

where $m \leqslant n$ *in the summands.*

Proof. Recall that $\gamma_{n,j} = p^{-n}(\sum_{i=0}^{n-1} \zeta_{p^{n-i}} \otimes \varphi^{i-n} + (1-\varphi)^{-1})$ and $\eta^{\pm}$ are given by the following:

$$\eta^{+} = \frac{\varphi(\omega)}{[\varphi(\omega), \bar{\omega}]} \quad \text{and} \quad \eta^{-} = \frac{\omega}{[\varphi(\omega), \bar{\omega}]}.$$

Hence, we can apply Corollary 4.2 to $R^{\pm}_{n,j}$ provided that

$$(p-1)(1-\varphi)^{-1}(\eta^{\pm}_j) \not\equiv \varphi^{-1}(\eta^{\pm}_j) \mod \omega,$$

which can be checked under Assumption 1. Recall that $\varphi^m(\omega) \equiv 0 \bmod \omega$ if and only if m is an even integer (cf. proof of Proposition 3.14), hence the result. □

In particular, (8) and (10) imply that

$$R^{+}_{n,j} + R^{-}_{n,j} = \mathbb{Q}_{p,n} \otimes E \quad \text{and} \quad R^{+}_{n,j} \cap R^{-}_{n,j} = E$$

under the identification given by Remark 4.7. Let

$$\mathbb{Q}^{\pm}_{p,n} = \{x \in \mathbb{Q}_{p,n} : \mathrm{Tr}_{n/m+1}(x) \in \mathbb{Q}_{p,m} \ \forall m \in S^{\pm}_n\},$$

where $S^{\pm}_n$ are defined by

$$\begin{aligned} S^{+}_n &= \{m \in [0, n-1] : m \text{ even}\}, \\ S^{-}_n &= \{m \in [0, n-1] : m \text{ odd}\}. \end{aligned}$$

Then, $R^{\pm}_{n,j}$ can be identified with $\mathbb{Q}^{\pm}_{p,n} \otimes E$.

LEMMA 4.9. *For* j *and* n *as above,* $\mathbb{Q}^{\pm}_{p,n} \otimes E = R^{\pm}_{n,j}$.

Proof. By (10), it is easy to check that $R^{\pm}_{n,j} \subset \mathbb{Q}^{\pm}_{p,n} \otimes E$, so $\dim_E R^{\pm}_{n,j} \leqslant \dim_E(\mathbb{Q}^{\pm}_{p,n} \otimes E)$. Since $R^{+}_{n,j} + R^{-}_{n,j} = \mathbb{Q}_{p,n} \otimes E$, we have

$$\mathbb{Q}^{+}_{p,n} \otimes E + \mathbb{Q}^{-}_{p,n} \otimes E = R^{+}_{n,j} + R^{-}_{n,j} = \mathbb{Q}_{p,n} \otimes E.$$

If $x \in \mathbb{Q}^{+}_{p,n} \cap \mathbb{Q}^{-}_{p,n}$, then $\mathrm{Tr}_{n/m+1}(x) \in \mathbb{Q}_{p,m}$ for all $m \leqslant n-1$; hence, $x \in \mathbb{Q}_p$. Therefore, we have $\mathbb{Q}^{+}_{p,n} \cap \mathbb{Q}^{-}_{p,n} = \mathbb{Q}_p$. Hence, by the formula $\dim A + \dim B = \dim(A+B) + \dim(A \cap B)$, we deduce that $\dim_E(\mathbb{Q}^{\pm}_{p,n} \otimes E) = \dim_E R^{\pm}_{n,j}$ and we are done. □

Let $H^1_f(\mathbb{Q}_{p,n}, V_f(j))^{\pm}$ denote the image of $R^{\pm}_{n,j}$ under $\exp_{n,j}$; then Remark 4.7 and Lemma 4.9 imply that it is equal to

$$\{x \in H^1_f(\mathbb{Q}_{p,n}, V_f(j)) : \mathrm{cor}_{n/m+1}(x) \in H^1_f(\mathbb{Q}_{p,n}, V_f(j)) \ \forall m \in S^{\pm}_n\}.$$

By Corollary 4.6, if we define

$$H^1_f(\mathbb{Q}_{p,n}, T_f(j))^{\pm} = H^1_f(\mathbb{Q}_{p,n}, V_f(j))^{\pm} \cap H^1_f(\mathbb{Q}_{p,n}, T_f(j)),$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

then it is equal to

$$\{x \in H^1_f(\mathbb{Q}_{p,n}, T_f(j)) : \mathrm{cor}_{n/m+1}(x) \in H^1_f(\mathbb{Q}_{p,m}, T_f(j)) \ \forall m \in S_n^{\pm}\},$$

generalising the definition of $E^{\pm}$ in [Kob03].

4.4 Description of the kernels

Let $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$. Under the notation of § 3, we have $\mathcal{L}_{\eta^{\pm}}(\mathbf{z}) = O(\log_p^{(k-1)/2})$, so we have $\mathcal{L}_{\eta^{\pm}}(\mathbf{z}) = 0$ if and only if $P_{n,r}(\eta^{\pm}, z_{-r,n}) = 0$ for all $n \geqslant 0$ and more than $(k-1)/2$ different values of r with $0 \leqslant r \leqslant k-2$. Recall that

$$P_{n,r}(\cdot, z_{-r,n}) = r! \sum_{\sigma \in G_n} [\exp_{n,r+1}(\gamma_{n,r+1}(\cdot)^{\sigma}), z_{-r,n}]_n \sigma.$$

Hence, $\ker P_{n,r}(\eta^{\pm}, \cdot)$ is just the annihilator of $\{\exp_{n,r+1}(\gamma_{n,r+1}(\eta^{\pm})^{\sigma}) : \sigma \in G_n\}$ under the pairing

$$H^1(\mathbb{Q}_{p,n}, V_f(r+1)) \times H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to E,$$

which coincides with the annihilator of $H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm}$ under the pairing

$$H^1(\mathbb{Q}_{p,n}, T_f(r+1)) \times H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to \mathcal{O}_E. \tag{11}$$

We denote this annihilator by $H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$.

Define $\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1-r)) = \varprojlim H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$. As $\log^{\pm}_{p,k} \neq 0$ and $\mathcal{L}_{\eta^{\pm}} = \log^{\pm}_{p,k} \mathrm{Col}^{\pm}$, Corollary 4.5 implies that

$$\ker \mathcal{L}_{\eta^{\pm}} = \ker(\mathrm{Col}^{\pm}) = \bigcap_{r=0}^{k-2} \mathrm{Tw}_r(\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1-r))).$$

In fact, by the proposition below, it suffices to take just one term in the intersection.

Proposition 4.10. $\mathrm{Tw}_r(\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1-r))) = \mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))$ *for all integers* r *such that* $0 \leqslant r \leqslant k-2$.

Proof. Since $\mathrm{Col}^{\pm}(\mathbf{z}) = O(1)$ for all $\mathbf{z} \in \mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$, it is uniquely determined by its values at an infinite number of characters (see e.g. [Pol03, Lemma 3.2]). Hence, if there exists a fixed r such that $P_{n,r}(\eta^{\pm}, z_{n,-r}) = 0$ for all n, then $\mathrm{Col}^{\pm}(\mathbf{z}) = 0$. Therefore, we have

$$\ker(\mathrm{Col}^{\pm}) = \mathrm{Tw}_r(\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1-r)))$$

and we are done. □

Corollary 4.11. *We have* $\ker \mathcal{L}_{\eta^{\pm}} = \ker(\mathrm{Col}^{\pm}) = \mathrm{Tw}_r(\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1-r)))$ *for any integer* $0 \leqslant r \leqslant k-2$.

4.5 Pontryagin duality

We have seen that $\ker(\mathrm{Col}^{\pm})$ can be written in terms of $H^1_{\pm}$, about which we now say a little bit more. The Pontryagin duality gives a pairing

$$H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1)) \times H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to E/\mathcal{O}_E. \tag{12}$$

We can describe the annihilator of $H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$ under this pairing explicitly.

Lemma 4.12. $H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm} \otimes E/\mathcal{O}_E \hookrightarrow H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1))$ *and it can be identified as the annihilator of* $H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))$ *under (12).*

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Proof. By definitions, we have an exact sequence

$$0 \to H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r)) \to \mathrm{Hom}(H^1_{\bar{f}}(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm}, \mathcal{O}_E).$$

Taking Pontryagin duals, we have

$$H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm} \otimes E/\mathcal{O}_E \to H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1)) \to H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1-r))^{\vee} \to 0.$$

Therefore, the second part of the lemma follows from the first. Recall that $(V_f/T_f(r+1))^{G_{\mathbb{Q}_{p,n}}} = 0$ by Lemma 4.4, so we have

$$H^1_f(\mathbb{Q}_{p,n}, T_f(r+1)) \otimes E/\mathcal{O}_E \hookrightarrow H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(r+1)) \subset H^1(\mathbb{Q}_{p,n}, V_f/T_f(r+1)).$$

Hence, it suffices to show that we have the inclusion

$$H^1_f(\mathbb{Q}_{p,n}, T_f(r+1))^{\pm} \otimes E/\mathcal{O}_E \hookrightarrow H^1_f(\mathbb{Q}_{p,n}, T_f(r+1)) \otimes E/\mathcal{O}_E.$$

But this follows from [Kob03, Lemma 8.17]. □

We write $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(j))^{\pm}$ for $H^1_f(\mathbb{Q}_{p,n}, T_f(j))^{\pm} \otimes E/\mathcal{O}_E$, which is identified as a subgroup of $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(j))$. Note that it corresponds to the definition of $E^{\pm}(\mathbb{Q}_{p,n}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ given in [Kob03] and this is used to define $\mathrm{Sel}_p^{\pm}$ in § 6.

5. Images of the Coleman maps

In this section, we describe the images of $\mathrm{Col}^{\pm}$. By Corollary 4.5, any elements of $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ can be lifted to a global element of $\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$. Hence, we can in fact think of $\mathcal{L}_{\eta^{\pm},n}$ and $\mathrm{Col}_n^{\pm}$ as maps from $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ to $E[G_n]$. This allows us to give a description of $\mathrm{Im}(\mathrm{Col}^{\pm})$ by studying $\mathrm{Im}(\mathrm{Col}_n^{\pm})$.

In [Kob03, § 8], the images of the plus and minus Coleman maps for elliptic curves over $\mathbb{Q}$ are shown to be the following:

$$\mathrm{Im}(\mathrm{Col}^{+}) = (\gamma - 1)\Lambda_{\mathcal{O}_E}(G_\infty) + \left(\sum_{\sigma \in \Delta} \sigma\right)\Lambda_{\mathcal{O}_E}(G_\infty),$$

$$\mathrm{Im}(\mathrm{Col}^{-}) = \Lambda_{\mathcal{O}_E}(G_\infty).$$

In particular, the Δ-invariant part of $\mathrm{Im}(\mathrm{Col}^{\pm})$ is the whole of $(\sum_{\sigma\in\Delta}\sigma)\Lambda_{\mathcal{O}_E}(G_\infty)$ (which we identify with $\Lambda_{\mathcal{O}_E}(\Gamma)$). For a general f, we unfortunately do not know whether the images of the Coleman maps are inside $\Lambda_{\mathcal{O}_E}(G_\infty)$ or not. However, after multiplying by a power of ϖ, we show that the Δ-invariant part of $\mathrm{Im}(\mathrm{Col}^{\pm})$ agrees with the above descriptions and the same can be said for the whole of $\mathrm{Im}(\mathrm{Col}^{-})$.

5.1 Divisibility by $\Phi_m(\gamma)$

We have seen that the image of $\mathcal{L}_{\eta^{\pm}}$ is divisible by $\log_{p,k}^{\pm}$. We give a necessary and sufficient condition for such divisibility at the finite level below.

Recall that $G_\infty = \mathrm{Gal}(k_\infty/\mathbb{Q}) \cong \Delta \times \Gamma$, where Δ is a finite group of order $p-1$, $\Gamma \cong \mathbb{Z}_p$ and γ is a fixed topological generator of Γ. We have

$$\mathcal{O}_E[G_n] \cong \mathcal{O}_E[\Delta][\gamma]/(\gamma^{p^{n-1}} - 1) \quad \text{and} \quad \Phi_m(\gamma) = 1 + \gamma^{p^{m-1}} + \gamma^{2p^{m-1}} + \cdots + \gamma^{(p-1)p^{m-1}}.$$

Therefore, if $m \geqslant n$, then $\Phi_m(\gamma) = p$ in $\mathcal{O}_E[G_n]$, so we only consider $m < n$ here.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Lemma 5.1. *Let $m < n$ and*

$$f = \sum_{\substack{r \bmod p^{n-1} \\ \sigma \in \Delta}} c_{r,\sigma} \cdot \sigma \cdot \gamma^r \in \mathcal{O}_E[G_n].$$

For each $\sigma \in \Delta$ and $r \bmod p^m$, write

$$b_{r,\sigma} = c_{r,\sigma} + c_{r+p^m,\sigma} + \cdots + c_{r-p^m,\sigma}.$$

Then, f is divisible by $\Phi_m(\gamma)$ in $\mathcal{O}_E[G_n]$ if and only if $b_{r,\sigma} = b_{s,\sigma}$ whenever $r \equiv s \bmod p^{m-1}$.

Proof. Let $f = g\Phi_m(\gamma)$ and $g = \sum a_{r,\sigma} \cdot \sigma \cdot \gamma^r \in \mathcal{O}_E[G_n]$. Then, the coefficient of $\sigma\gamma^r$ in f is

$$a_{r,\sigma} + a_{r-p^{m-1},\sigma} + \cdots + a_{r-(p-1)p^{m-1},\sigma}.$$

Hence, $b_{r,\sigma}$ as defined in the statement of the lemma is just the sum of the coefficients $a_{s,\sigma}$ of g with $s \equiv r \bmod p^{m-1}$. Hence, $b_{r,\sigma} = b_{s,\sigma}$ whenever $r \equiv s \bmod p^{m-1}$.

Conversely, let $\sum c_{r,\sigma} \cdot \sigma \cdot \gamma^r \in \mathcal{O}_E[G_n]$ and define $b_{r,\sigma}$ as in the statement of the lemma. Assume that $b_{r,\sigma} = b_{s,\sigma}$ for all $r \equiv s \bmod p^{m-1}$. Let $f_\sigma(\gamma) = \sum_r c_{r,\sigma} \cdot \gamma^r$, so $f = \sum f_\sigma \cdot \sigma$. We have

$$\begin{aligned} f_\sigma(\zeta_{p^m}) &= \sum_{r \bmod p^m} \left(\sum_{s \equiv r(p^m)} c_{s,\sigma} \right) \zeta_{p^m}^r \\ &= \sum_{r \bmod p^m} b_{r,\sigma} \zeta_{p^m}^r \\ &= \sum_{s \bmod p^{m-1}} b_{s,\sigma} \sum_{r \equiv s(p^{m-1})} \zeta_{p^m}^r \\ &= 0. \end{aligned}$$

Hence, $\Phi_m(\gamma)$ divides f and we are done. □

Applying this to the image of $\mathcal{L}_{\eta^\pm,n}$, we have the following corollary.

Corollary 5.2. *For any $z \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$, $\mathcal{L}_{\eta^\pm,n}(z)$ is divisible by $\Phi_m(\gamma)$ in $E[G_n]$ if $m \in S_n^\pm$.*

Proof. The image of $\mathcal{L}_{\eta^\pm,n}(z)$ is given by the following composition:

$$H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}_E}(H^1(\mathbb{Q}_{p,n}, T_f(1)), \mathcal{O}_E) \to E[G_n],$$

where the first isomorphism is induced by the pairing (11) and the second map is given by

$$\begin{aligned} \mathrm{Hom}_{\mathcal{O}_E}(H^1(\mathbb{Q}_{p,n}, T_f(1)), \mathcal{O}_E) &\to E[G_n], \\ \theta &\mapsto \sum_{\tau \in G_n} \theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^\pm)^\tau)\tau, \end{aligned} \tag{13}$$

with θ extended to an element of $\mathrm{Hom}_E(H^1(\mathbb{Q}_{p,n}, V_f(1)), E)$ in the natural way. Hence, it is enough to show that the coefficients $\theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^\pm)^\tau)$, as $\tau \in G_n$ varies, satisfy the relations described in Lemma 5.1. Recall that $\exp_{n,1}$ gives an isomorphism

$$\mathbb{Q}_{p,n} \otimes \mathbb{D}(V_f(1))/E \cdot \omega_1 \to H_f^1(\mathbb{Q}_{p,n}, V_f(1)).$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Therefore, it is in fact enough to show that $\gamma_{n,1}(\eta_1^{\pm})^{\tau} \bmod \omega$ satisfy the relations in Lemma 5.1. Let $\sigma \in \Delta$ and $r \in \mathbb{Z}/p^m\mathbb{Z}$. For $\eta = \eta^{\pm}$, we write

$$\begin{aligned}\eta_{r,\sigma} &= \sum_{s \equiv r(p^m)} \gamma_{n,1}(\eta_1)^{\sigma\gamma^s} \\ &= p^{-m-1}((1-\varphi)^{-1}(\eta_1) + \zeta_p \otimes \varphi^{-1}(\eta_1) + \cdots + \zeta_{p^{m+1}} \otimes \varphi^{-m-1}(\eta_1))^{\sigma\gamma^r}.\end{aligned}$$

Therefore, if $\varphi^{-m-1}(\eta_1) \equiv 0 \bmod \omega$, then $\eta_{r,\sigma} = \eta_{s,\sigma}$ for $r \equiv s \bmod p^{m-1}$, as $(\zeta_{p^m})^{\sigma\gamma^r} = (\zeta_{p^m})^{\sigma\gamma^s}$. Hence, by the definitions of $\eta^{\pm}$ as given in the proof of Proposition 3.14, we are done. □

By considering its image modulo $(u^{-j}\gamma)^{p^{n-1}} - 1$ similarly, one can deduce Proposition 3.14. We can in fact say a bit more about the image of $\mathcal{L}_{\eta^+,n}$.

LEMMA 5.3. *If $\mathcal{L}_{\eta^+,n}(z) = \sum c_{r,\sigma} \cdot \sigma \cdot \gamma^r$, then $\sum_r c_{r,\sigma}$ is independent of σ.*

Proof. For each $\sigma \in \Delta$, we have

$$\sum_r \gamma_{n,1}(\eta_1^+)^{\sigma\gamma^r} = p^{-1}((1-\varphi)^{-1}(\eta_1^+) + \zeta_p \otimes \varphi^{-1}(\eta_1^+))^{\sigma}.$$

But $\varphi^{-1}(\eta_1^+) \equiv 0 \bmod \omega$, so we are done. □

We will see later on that these conditions in fact characterise the images of $\mathcal{L}_{\eta^{\pm},n}$ completely.

5.2 Images of $\log_{p,k}^{\pm}$ in $\mathcal{O}_E[G_n]$

We now fix an integer j such that $0 < j \leqslant k-2$.

LEMMA 5.4. *Let $x \in 1 + p\mathbb{Z}_p$. There exists a constant c such that for any positive integer n, $v_p(x^{p^n} - 1) = n + c$.*

Proof. Let $x = 1 + m$, where $m \in p\mathbb{Z}_p$, so $v_p(m) \geqslant 1$. We have the expansion

$$x^{p^n} - 1 = (1+m)^{p^n} - 1 = m^{p^n} + \binom{p^n}{p^n - 1} m^{p^n - 1} + \cdots + \binom{p^n}{1} m.$$

For $r > 0$, $v_p(\binom{p^n}{r}) = n - v_p(r)$, so

$$v_p\left(\binom{p^n}{r} m^r\right) = r v_p(m) - v_p(r) + n.$$

If $r = p^s a$, where $p \nmid a$ and $a > 1$, then

$$v_p\left(\binom{p^n}{r} m^r\right) > v_p\left(\binom{p^n}{p^s} m^{p^s}\right).$$

Therefore, the set $\{v_p(\binom{p^n}{r} m^r) : r > 0\}$ takes its minimum value at $r = p^s$ for some s.

Consider the curve $f(t) = p^t v_p(m) - t$, for $t \in \mathbb{R}$. It has a unique global minimum when $p^t = (v_p(m) \log p)^{-1}$, so the curve is strictly increasing on $t \geqslant 0$. Therefore, for a fixed n, the minimum of the values

$$v_p\left(\binom{p^n}{p^s} m^{p^s}\right) = p^s v_p(m) - s + n$$

is just $v_p(m) + n$, which is attained at a unique s, hence the result. □

COROLLARY 5.5. *If $m \geqslant n$, then $\Phi_m(u^{-j}\gamma)/p$ is congruent to a unit of $\mathbb{Z}_p$ modulo $\gamma^{p^{n-1}} - 1$.*

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Proof. By definition,

$$\Phi_m(u^{-j}\gamma) = \frac{(u^{-j}\gamma)^{p^m} - 1}{(u^{-j}\gamma)^{p^{m-1}} - 1},$$

so, as elements of $\mathcal{O}_E[G_n]$, we have

$$\frac{1}{p}\Phi_m(u^{-j}\gamma) = \frac{u^{-jp^m} - 1}{p(u^{-jp^{m-1}} - 1)}.$$

But $u \in 1 + p\mathbb{Z}_p$ by definition, so we are done by Lemma 5.4. □

Remark 5.6. We have $\log_{p,k}^{\pm} \equiv p^{1-k}\lambda_{\pm} \prod_{j=0}^{k-2} \omega_n^{\pm}(u^{-j}\gamma) \bmod(\gamma^{p^{n-1}} - 1)$, where $\lambda_{\pm}$ is a unit of $\mathbb{Z}_p$ and $\omega_n^{\pm}$ is defined by

$$\omega_n^{+}(1+X) = \prod_{1 \leqslant m < n/2} \Phi_{2m}(1+X)/p,$$

$$\omega_n^{-}(1+X) = \prod_{1 \leqslant m < (n+1)/2} \Phi_{2m-1}(1+X)/p.$$

5.3 The images of $\mathrm{Col}_n^{\pm}$

Let $R_{n,j}^{\pm}$ be the E-vector spaces defined by (9). We have the following lemma.

Lemma 5.7. *The dimensions of the E-vector spaces $R_{n,j}^{\pm}$ are given by*

$$\dim_E R_{n,j}^{+} = 1 + \sum_{1 \leqslant m \leqslant n/2} p^{2m-2}(p-1)^2,$$

$$\dim_E R_{n,j}^{-} = p - 1 + \sum_{1 \leqslant m \leqslant (n-1)/2} p^{2m-1}(p-1)^2.$$

Proof. By (10), we have

$$\dim_E R_{n,j}^{+} = \dim_{\mathbb{Q}_p} \mathbb{Q}_p + \sum_{1 \leqslant m \leqslant n/2} \dim_{\mathbb{Q}_p} \mathbb{Q}_p^{(2m)},$$

$$\dim_E R_{n,j}^{-} = \dim_{\mathbb{Q}_p} \mathbb{Q}_p + \sum_{1 \leqslant m \leqslant (n-1)/2} \dim_{\mathbb{Q}_p} \mathbb{Q}_p^{(2m+1)}.$$

For $m > 1$, (8) implies that

$$\begin{aligned}\dim_{\mathbb{Q}_p} \mathbb{Q}_p^{(m)} &= \dim_{\mathbb{Q}_p} \mathbb{Q}_{p,m} - \dim_{\mathbb{Q}_p} \mathbb{Q}_{p,m-1} \\ &= p^{m-1}(p-1) - p^{m-2}(p-1) \\ &= p^{m-2}(p-1)^2\end{aligned}$$

and $\dim_{\mathbb{Q}_p} \mathbb{Q}_p^{(1)} = p - 2$, so we are done. □

The dimensions of these vector spaces enable us to obtain the following.

Proposition 5.8. *Let $f = \sum_{\sigma \in \Delta} \sum_{r=0}^{p^{n-1}-1} a_{r,\sigma} \cdot \sigma \cdot u^r \in E[G_n]$. If $\omega_n^{\pm}$ is as defined in Remark 5.6, then:*

(a) *there exists $z \in H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$ such that $\mathrm{Col}_n^{-}(z) \equiv f \bmod \omega_n^{+}(\gamma)$;*

(b) *if moreover $\sum_r a_{r,\sigma_1} = \sum_r a_{r,\sigma_2}$ for all $\sigma_1, \sigma_2 \in \Delta$, then there exists $z \in H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$ such that $\mathrm{Col}_n^{+}(z) \equiv f \bmod \omega_n^{-}(\gamma)$.*

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Proof. We only prove (b), as (a) can be proved in the same way. Define

$$U_n = \left\{ g = \sum c_{r,\sigma} \cdot \sigma \cdot \gamma^r \in E[G_n] : \log_{p,k}^+ | g, \sum_r c_{r,\sigma_1} = \sum_r c_{r,\sigma_1} \forall \sigma_1, \sigma_2 \in \Delta \right\}.$$

Then, U_n is a vector subspace of $E[G_n]$ over E. By Remark 5.6,

$$\log_{p,k}^+ \equiv p^{1-k} \lambda_+ \prod_{j=0}^{k-2} \omega_n^+(u^{-j}\gamma) \mod (\gamma^{p^{n-1}} - 1)$$

for some $\lambda_+ \in \mathcal{O}_E^\times$. Since $\omega_n^+(u^{-j}(1+X))$ and $(1+X)^{p^{n-1}} - 1$ are coprime for $j > 0$, $\log_{p,k}^+ | g$ if and only if $\omega_n^+(\gamma) | g$. But Φ_{m_1} and Φ_{m_2} are coprime if $m_1 \neq m_2$, so $\omega_n^+(\gamma) | g$ if and only if $\Phi_m(\gamma) | g$ for all even $m < n$.

Let $g = \sum c_{r,\sigma} \cdot \sigma \cdot u^r$. For each even $m < n$, let

$$b_{r,\sigma}^{(m)} = c_{r,\sigma} + c_{r+p^m,\sigma} + \cdots + c_{r-p^m,\sigma}.$$

Then, by Lemma 5.1, $\Phi_m(\gamma) | g$ if and only if $b_{r,\sigma}^{(m)} = b_{s,\sigma}^{(m)}$ for all $\sigma \in \Delta$ and $r \equiv s \bmod p^{m-1}$. For each such m and $\sigma \in \Delta$, there are p^{m-1} values of modulo p^{m-1}; each is equated to $p-1$ different values. Since $|\Delta| = p-1$, there are $p^{m-1}(p-1)^2$ linearly independent equations for each m. Together with the equations of $\sum_r c_{r,\sigma}$, there are in total

$$p - 2 + \sum_{1 \leqslant m \leqslant n/2} p^{2m-1}(p-1)^2$$

equations describing the coefficients of elements of the U_n, which give the codimension of U_n over E in $E[G_n]$.

By Corollary 5.2 and Lemma 5.3, for $z \in H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$, $\mathcal{L}_{\eta^+,n}(z)$ lies inside the above subspace. But the dimension of the image is given by $\dim_E R_{n,1}^+$, which is the same as the dimension of U_n by Lemma 5.7, so $\mathcal{L}_{\eta^+,n}(H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))) = U_n$ as E-vector spaces and there exists some z such that $\mathcal{L}_{\eta^+,n}(z) = g$. This implies that

$$\log_{p,k}^+ \operatorname{Col}_n^+(z) \equiv f \log_{p,k}^+ \mod (\gamma^{p^{n-1}} - 1).$$

The factors of $\omega_n^+(u^{-j}\gamma)$ on both sides can be cancelled out for $j > 0$, as $\omega_n^+(u^{-j}\gamma)$ is coprime to $\omega_n^+(\gamma)$. Since $p^{n-1}(\gamma-1)\omega_n^+(\gamma)\omega_n^-(\gamma) = \gamma^{p^{n-1}} - 1$, we deduce that $\operatorname{Col}_n^+(z) \equiv f \bmod ((\gamma - 1)\omega_n^-(\gamma))$, which implies (b). □

5.4 The images of $\operatorname{Col}^\pm$

In the previous section, we studied the images of $H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$ under $\operatorname{Col}_n^\pm$. To understand the images of $\operatorname{Col}^\pm$, we have to understand those of $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ as well.

LEMMA 5.9. *For all n, there exist $r_n^\pm \in \mathbb{Z}$ such that*

$$\mathcal{L}_{\eta^\pm,n}(H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))) = \mathcal{L}_{\eta^\pm,n}(H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))) \cap \varpi^{r_n^\pm} \mathcal{O}_E[G_n].$$

Proof. Note that $\exp_{n,1}(\gamma_{n,1}(\eta_1^\pm)) \neq 0$. As an element of $H^1(\mathbb{Q}_{p,n}, T_f(1))$, it lifts to a cocycle on $G_{\mathbb{Q}_{p,n}}$. By considering the image of this cocycle in $V_f(1)$, which is invariant under the action of G_n, there exist $r_n^\pm$ such that

$$\varpi^{-r_n^\pm} \exp_{n,1}(\gamma_{n,1}(\eta^\pm)^\tau) \in H^1(\mathbb{Q}_{p,n}, T_f(1)) \backslash \varpi H^1(\mathbb{Q}_{p,n}, T_f(1))$$

for all $\tau \in G_n$.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Recall from (13) that $\mathcal{L}_{\eta^{\pm},n}$ is given by

$$\begin{aligned}\mathrm{Hom}_E(H^1(\mathbb{Q}_{p,n}, V_f(1)), E) &\to E[G_n],\\ \theta &\mapsto \sum_{\tau\in G_n} \theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau})\tau,\end{aligned}$$

where we have identified $\mathrm{Hom}_E(H^1(\mathbb{Q}_{p,n}, V_f(1)), E)$ with $H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$. Under this identification, $H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ corresponds to the set of maps which send $H^1(\mathbb{Q}_{p,n}, T_f(1))$ (which is identified as a subset of $H^1(\mathbb{Q}_{p,n}, V_f(1))$ as discussed in § 4) to $\mathcal{O}_E$. Therefore, we have

$$\{\theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau}) : \theta \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))\} = \varpi^{r_n^{\pm}}\mathcal{O}_E$$

for all $\tau \in G_n$. This implies that the left-hand side of the equation in the statement of the lemma is contained in the right-hand side.

Conversely, if x is an element of the right-hand side of the equation, there exists $\theta \in H^1(\mathbb{Q}_{p,n}, V_{\bar{f}}(k-1))$ such that $\sum_{\tau\in G_n} \theta(\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau})\tau = x$ by Proposition 5.8. In particular,

$$\theta(\varpi^{-r_n^{\pm}} \exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau}) \in \mathcal{O}_E$$

for all $\tau \in G_n$. Hence, there exists $\tilde{\theta} \in H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$ which agrees with θ on the set $\{\varpi^{-r_n^{\pm}} \exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^{\tau}) : \tau \in G_n\}$, so $x \in$ the left-hand side. □

Lemma 5.10. *Let $r_n^{\pm}$ be the integers defined in Lemma 5.9; then there exist $c_{\pm}$ such that $r_n^{\pm} = -e(k-1)\lfloor n/2\rfloor + c_{\pm}$ for n sufficiently large, where e is the ramification degree of E.*

Proof. By Remark 3.11,

$$\Omega_{V_f(1),1}((1+X)\otimes\eta_1^{\pm}) = O(\log_p^{(k-1)/2}),$$

which implies that the nth component of $\Omega_{V_f(1),1}((1+X)\otimes\eta_1^{\pm})$, which is $\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm}))$, satisfies

$$\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})) \in \varpi^{-e(k-1)\lfloor n/2\rfloor + c_{\pm}} H^1(\mathbb{Q}_{p,n}, T_f(1))$$

for some constant $c_{\pm}$ independent of n.

Recall that $\mathbb{H}^1_{\mathrm{Iw}}(T_f(1))$ is free of rank two over $\Lambda_{\mathcal{O}_E}(G_\infty)$. Fix a basis z_1, z_2, say. Note that $(1+X)\otimes\eta_1^{\pm}$ form a $\Lambda_E(G_\infty)$-basis for $\mathbb{D}_\infty(V_f)$. The determinant of

$$\Omega_{V_f(1),1} : \mathcal{H}_\infty(G_\infty)\otimes\mathbb{D}_\infty(V_f(1)) \to \mathcal{H}_\infty(G_\infty)\otimes\mathbb{H}^1_{\mathrm{Iw}}(T_f(1))$$

with respect to these bases, as a $\mathcal{H}_\infty(G_\infty)$-homomorphism, is given by

$$\prod_{j=0}^{k-2} \log_p(u^j\gamma) \sim \log_p^{k-1}$$

up to a unit of $\Lambda_E(G_\infty)$ (this is the $\delta(V)$-conjecture of [Per94], which can be deduced from the explicit reciprocity law of Colmez [Col98]). But Theorem 3.12 says that $\log_{p,k}^{\pm} \sim \log_p^{(k-1)/2}$. Hence, we in fact have

$$\Omega_{V_f(1),1}((1+X)\otimes\eta^{\pm}) \sim \log_p^{(k-1)/2}.$$

Therefore, we can choose $c_{\pm}$ such that

$$\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})) \notin \varpi^{-e(k-1)\lfloor n/2\rfloor + c_{\pm}+1} H^1(\mathbb{Q}_{p,n}, T_f(1)),$$

so $r_n^{\pm} = -e(k-1)\lfloor n/2\rfloor + c_{\pm}$, for n sufficiently large. □

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

On combining these two lemmas, we have the following corollary.

COROLLARY 5.11. *If θ is the trivial character on Δ, then there exist $s^{\pm}$ such that*

$$\mathrm{Col}^{\pm}(\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1)))^{\theta} = \varpi^{s_{\pm}}\Lambda_{\mathcal{O}_E}(\Gamma).$$

Proof. By Proposition 5.8 and Lemma 5.9, for sufficiently large n,

$$\varpi^{r_n^{\pm}}\left(\sum_{\sigma\in\Delta}\sigma\right)\prod_{j=0}^{k-2}\tilde{\omega}_n^{\pm}(u^{-j}\gamma) \in \mathcal{L}_{\eta^{\pm},n}(H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))),$$

where

$$\tilde{\omega}_n^{+}(1+X) = \prod_{1\leqslant m<n/2}\Phi_{2m}(1+X),$$
$$\tilde{\omega}_n^{-}(1+X) = \prod_{1\leqslant m<(n+1)/2}\Phi_{2m-1}(1+X).$$

Hence, by Remark 5.6 and Lemma 5.10, there exist constants $s^{\pm}$ (independent of n) such that

$$\varpi^{s^{\pm}}\left(\sum_{\sigma\in\Delta}\sigma\right)\log_{p,k}^{\pm} \in \mathcal{L}_{\eta^{\pm},n}(H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)))$$

and

$$\mathcal{L}_{\eta^{\pm},n}(H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))) \subset \varpi^{s^{\pm}}\log_{p,k}^{\pm}\mathcal{O}_E[G_n].$$

But $\log_{p,k}^{\pm}\mathrm{Col}^{\pm} = \mathcal{L}_{\eta^{\pm}}$, so we have

$$\varpi^{s^{\pm}}\sum_{\sigma\in\Delta}\sigma \in \mathrm{Col}^{\pm}(H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) \mod \tilde{\omega}_n^{\mp}(\gamma).$$

Therefore, we are done, since

$$\varprojlim \Lambda_{\mathcal{O}_E}(G_\infty)/\tilde{\omega}_n^{\pm}(\gamma) = \Lambda_{\mathcal{O}_E}(G_\infty) \quad \text{and} \quad \Lambda_{\mathcal{O}_E}(G_\infty)^{\theta} = \left(\sum_{\sigma\in\Delta}\sigma\right)\Lambda_{\mathcal{O}_E}(G_\infty). \qquad \square$$

Remark 5.12. It is clear that we can replace θ by an arbitrary character on Δ for the minus map in the corollary.

6. ±-Selmer groups

Throughout this section, with the exception of §§ 6.3.2 and 6.4, Assumptions 1 and 2 are not necessary.

Let f be a modular form as in § 2.4 and K a number field; the p-Selmer groups of f over K are defined by the following:

$$\mathrm{Sel}_p^0(f/K) = \ker\left(H^1(K, V_f/T_f(1)) \to \prod_v H^1(K_v, V_f/T_f(1))\right),$$
$$\mathrm{Sel}_p(f/K) = \ker\left(H^1(K, V_f/T_f(1)) \to \prod_v \frac{H^1(K_v, V_f/T_f(1))}{H^1_f(K_v, V_f/T_f(1))}\right),$$

where v runs through the places of K.

We write k_n for $\mathbb{Q}$ adjoining all the p^nth roots of unity and $k_\infty = \cup k_n$. Since there is a unique place above p in k_n, we write this place as p as well. Note that the completion of k_n at p is

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

isomorphic to $\mathbb{Q}_{p,n}$. For f satisfying Assumptions 1 and 2, let $H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(1))^{\pm}$ be as defined in § 4.5. For all $n \geqslant 0$, we define the plus and minus Selmer groups by

$$\mathrm{Sel}_p^{\pm}(f/k_n) = \ker\left(\mathrm{Sel}_p(f/k_n) \to \frac{H^1(\mathbb{Q}_{p,n}, V_f/T_f(1))}{H^1_f(\mathbb{Q}_{p,n}, V_f/T_f(1))^{\pm}}\right).$$

In this section, we show that $\mathrm{Sel}_p(f/k_\infty)$ is not $\Lambda_{\mathcal{O}_E}(G_\infty)$-cotorsion when f is supersingular at p. When f satisfies Assumptions 1 and 2, we show that $\mathrm{Sel}_p^{\pm}(f/k_\infty) = \varinjlim \mathrm{Sel}_p^{\pm}(f/k_n)$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-cotorsion.

6.1 Restricted ramification

We now describe the Selmer groups defined above using restricted ramification. Let S be a finite set of places of a number field K containing all infinite places, all primes above p and those dividing N. Then, by [Rub00, Lemma I.5.3],

$$H^1(G_{S,K}, V_f/T_f(1)) = \ker\left(H^1(K, V_f/T_f(1)) \to \prod_{v \notin S} \frac{H^1(K_v, V_f/T_f(1))}{H^1_f(K_v, V_f/T_f(1))}\right), \tag{14}$$

where $G_{S,K}$ is the Galois group of the maximal extension of K unramified outside S. Therefore, we can rewrite Sel_p as

$$\mathrm{Sel}_p(f/K) = \ker\left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v \in S} \frac{H^1(K_v, V_f/T_f(1))}{H^1_f(K_v, V_f/T_f(1))}\right). \tag{15}$$

If f satisfies Assumptions 1 and 2, we write $H^1_f(k_{n,v}, V_f/T_f(1))^{\pm} = H^1_f(k_{n,v}, V_f/T_f(1))$ for $v \nmid p$. Then,

$$\mathrm{Sel}_p^{\pm}(f/k_n) = \ker\left(H^1(G_{S,k_n}, V_f/T_f(1)) \to \bigoplus_{v \in S} \frac{H^1(k_{n,v}, V_f/T_f(1))}{H^1_f(k_{n,v}, V_f/T_f(1))^{\pm}}\right). \tag{16}$$

The next lemma enables us to give a similar alternative description of Sel_p^0 as well.

Lemma 6.1. *With the notation as above, we have $H^1_f(K_v, V_f/T_f(1)) = 0$ for $v \nmid pN$.*

Proof. If v is an infinite place, we in fact have $H^1(K_v, V_f/T_f(1)) = 0$ as p is odd (see e.g. [Rub00, § I.3.7]).

We now assume that v is a finite place not dividing pN. Since $v \nmid p$,

$$H^1_f(K_v, V_f(1)) = H^1_{\mathrm{ur}}(K_v, V_f(1))$$

by definition and $H^1_f(K_v, V_f/T_f(1))$ is defined to be the image of $H^1_{\mathrm{ur}}(K_v, V_f(1))$ in $H^1(K_v, V_f/T_f(1))$ under the natural map $H^1(K_v, V_f(1)) \to H^1(K_v, V_f/T_f(1))$. By [Rub00, § I.3.2],

$$H^1_{\mathrm{ur}}(K_v, V_f(1)) \cong V_f(1)^I/(\mathrm{Fr} - 1)V_f(1)^I,$$

where I is the inertia group of K_v and Fr is the Frobenius map of K_v^{ur}/K_v. Hence, it suffices to show that 1 is not an eigenvalue of Fr. But v is a good prime (i.e. $v \nmid N$), so the eigenvalues have absolute value $q_v^{(k-1)/2}$, where q_v is the rational prime lying below v. Hence, we are done. □

If S is as above, Lemma 6.1 and (14) imply that

$$H^1(G_{S,K}, V_f/T_f(1)) = \ker\left(H^1(K, V_f/T_f(1)) \to \prod_{v \notin S} H^1(K_v, V_f/T_f(1))\right).$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Therefore, by the definition of Sel_p^0, we have

$$\mathrm{Sel}_p^0(f/K) = \ker\left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v\in S} H^1(K_v, V_f/T_f(1))\right). \tag{17}$$

As stated in the proof of Lemma 6.1, $H^1(K_v, V_f/T_f(1)) = 0$ if v is an infinite place. We can therefore simplify (17) further:

$$\mathrm{Sel}_p^0(f/K) = \ker\left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v\in S_f} H^1(K_v, V_f/T_f(1))\right), \tag{18}$$

where S_f denotes the set of finite places in S.

6.2 Poitou–Tate exact sequences

We now briefly review results on Poitou–Tate exact sequences. Details can be found in [Per95, § A.3].

With the above notation, let S be a finite set of places of K containing those above p and the infinite places; then we have an exact sequence

$$\begin{aligned}\bigoplus_{v\in S_f} H^0(K_v, V_f/T_f(1)) &\to H^2(G_{S,K}, T_{\bar f}(k-1))^\vee \\ &\to H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v\in S_f} H^1(K_v, V_f/T_f(1)),\end{aligned} \tag{19}$$

where S_f is again the set of finite places in S. On combining (19) and (18), we have

$$\bigoplus_{v\in S_f} H^0(K_v, V_f/T_f(1)) \to H^2(G_{S,K}, T_{\bar f}(k-1))^\vee \to \mathrm{Sel}_p^0(f/K).$$

By taking duals and using the fact that $H^0(K_v, V_f/T_f(1))^\vee = H^2(K_v, T_{\bar f}(k-1))$, we obtain

$$\mathrm{Sel}_p^0(f/K)^\vee = \ker\left(H^2(G_{S,K}, T_{\bar f}(k-1)) \to \bigoplus_{v\in S_f} H^2(K_v, T_{\bar f}(k-1))\right). \tag{20}$$

For each $v \in S_f$, let $A_v \subset H^1(K_v, T_{\bar f}(k-1))$ and $B_v \subset H^1(K_v, V_f/T_f(1))$ be $\mathcal{O}_E$-modules so that they are orthogonal complements to each other under the Pontryagin duality. Define

$$H^1_B(K, V_f/T_f(1)) = \ker\left(H^1(G_{S,K}, V_f/T_f(1)) \to \bigoplus_{v\in S_f} \frac{H^1(K_v, V_f/T_f(1))}{B_v}\right).$$

Then, [Per95, Proposition A.3.2] says that we have an exact sequence

$$\begin{aligned}H^1(G_{S,K}, T_{\bar f}(k-1)) \to \bigoplus_{v\in S_f} \frac{H^1(K_v, T_{\bar f}(k-1))}{A_v} &\to H^1_B(K, V_f/T_f(1))^\vee \\ &\to H^2(G_{S,K}, T_{\bar f}(k-1)) \to \bigoplus_{v\in S_f} H^2(K_v, T_{\bar f}(k-1)).\end{aligned} \tag{21}$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Hence, we can combine (20) and (21) to obtain the following exact sequence:

$$H^1(G_{S,K}, T_{\bar{f}}(k-1)) \to \bigoplus_{v\in S_f} \frac{H^1(K_v, T_{\bar{f}}(k-1))}{A_v} \to H^1_B(K, V_f/T_f(1))^\vee \to \mathrm{Sel}_p^0(f/K)^\vee \to 0. \tag{22}$$

6.3 Cotorsionness

6.3.1 $\mathrm{Sel}_p(f/k_\infty)$ *is not* $\Lambda_{\mathcal{O}_E}(G_\infty)$*-cotorsion.* We now prove our claim about $\mathrm{Sel}_p(f/k_\infty)^\vee$ in the introduction. Let $K = k_n$. Take $B_v = H^1_f(k_{n,v}, V_f/T_f(1))$ for $v \in S_f$ in (22); then $A_v = H^1_f(k_{n,v}, T_{\bar{f}}(k-1))$ by [BK90, Proposition 3.8]. Hence, on combining (15) and (22), we have an exact sequence

$$H^1(G_{S,k_n}, T_{\bar{f}}(k-1)) \to \frac{H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))}{H^1_f(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))} \oplus \bigoplus_{v|N} \frac{H^1(k_{n,v}, T_{\bar{f}}(k-1))}{H^1_f(k_{n,v}, T_{\bar{f}}(k-1))} \to \mathrm{Sel}_p(f/k_n)^\vee \to \mathrm{Sel}_p^0(f/k_n)^\vee \to 0. \tag{23}$$

We are interested in taking inverse limits over n. For the terms coming from places dividing N, we can apply the following.

Lemma 6.2. *For each integer $n \geqslant 0$, fix a prime $v(n)$ of $\mathbb{Q}_{p,n}$ not dividing p such that $v(n+1)$ lies above $v(n)$; then*

$$\varprojlim_{n,\mathrm{cor}} \frac{H^1(k_{n,v(n)}, T_{\bar{f}}(k-1))}{H^1_f(k_{n,v(n)}, T_{\bar{f}}(k-1))} = 0.$$

Proof. The Pontryagin dual of the said inverse limit is $\varinjlim H^1_f(k_{n,v(n)}, V_f/T_f(1))$, so the result follows immediately from Lemma 6.1 if $v(n) \nmid N$. The general case is proved in [Kat04, § 17.10] by considering p-cohomological dimensions. □

Therefore, on taking inverse limits in (23), we have the following exact sequence:

$$\mathbb{H}^1_S(T_{\bar{f}}(k-1)) \to \frac{\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))}{\mathbb{H}_f(T_{\bar{f}}(k-1))} \to \mathrm{Sel}_p(f/k_\infty)^\vee \to \mathrm{Sel}_p^0(f/k_\infty)^\vee \to 0, \tag{24}$$

where $\mathbb{H}_f(\cdot) = \varprojlim_n H^1_f(\mathbb{Q}_{p,n}, \cdot)$ and $\mathbb{H}^1_S(\cdot) = \varprojlim_n H^1(G_{k_n,S}, \cdot) \cong \mathbb{H}^1(\cdot)$ (see [Kob03, Proposition 7.1]).

Proposition 6.3. $\mathrm{Sel}_p(f/k_\infty)^\vee$ *is not torsion over* $\Lambda_{\mathcal{O}_E}(G_\infty)$.

Proof. We consider the rank of each term appearing in (24). By Theorem 3.7, $\mathbb{H}^1_S(T_{\bar{f}}(k-1))$ is a torsion-free $\Lambda_{\mathcal{O}_E}(G_\infty)$-module of rank one. By [Per00, Theorem 0.6], $\mathbb{H}_f(T_{\bar{f}}(k-1)) = 0$. By [Per94, Proposition 3.2.1], $\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))$ is of rank two over $\Lambda_{\mathcal{O}_E}(G_\infty)$. By [Kob03, proof of Proposition 7.1], which is a purely algebraic proof and generalises to modular forms directly, $\mathrm{Sel}_p^0(f/k_\infty)^\vee$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-torsion. Therefore, $\mathrm{Sel}_p(f/k_\infty)^\vee$ has $\Lambda_{\mathcal{O}_E}(G_\infty)$-rank at least one and we are done. □

6.3.2 $\mathrm{Sel}_p^\pm(f/k_\infty)$ *is* $\Lambda_{\mathcal{O}_E}(G_\infty)$*-cotorsion.* We again set $K = k_n$. Let

$$B_v = \begin{cases} H^1_f(k_{n,v}, V_f/T_f(1)) & \text{if } v|N, \\ H^1(\mathbb{Q}_{p,n}, V_f/T_f(1))^\pm & \text{if } v = p. \end{cases}$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

By [BK90, Proposition 3.8] and Lemma 4.12, we have

$$A_v = \begin{cases} H^1_f(k_{n,v}, T_{\bar{f}}(k-1)) & \text{if } v|N, \\ H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1)) & \text{if } v = p. \end{cases}$$

Hence, on combining (16) with (22), we obtain the following exact sequence:

$$H^1(G_{S,k_n}, T_{\bar{f}}(k-1)) \to \frac{H^1(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))}{H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))} \oplus \bigoplus_{v|N} \frac{H^1(k_{n,v}, T_{\bar{f}}(k-1))}{H^1_f(k_{n,v}, T_{\bar{f}}(k-1))} \to \mathrm{Sel}^{\pm}_p(f/k_n)^{\vee} \to \mathrm{Sel}^0_p(f/k_n)^{\vee} \to 0. \tag{25}$$

Therefore, on taking inverse limits in (25) and applying Lemma 6.2, we have the exact sequence

$$\mathbb{H}^1_S(T_{\bar{f}}(k-1)) \to \frac{\mathbb{H}^1_{\mathrm{Iw}}(T_{\bar{f}}(k-1))}{\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))} \to \mathrm{Sel}^{\pm}_p(f/k_\infty)^{\vee} \to \mathrm{Sel}^0_p(f/k_\infty)^{\vee} \to 0, \tag{26}$$

where $\mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))$ is as defined in § 4, i.e. $\varprojlim H^1_{\pm}(\mathbb{Q}_{p,n}, T_{\bar{f}}(k-1))$.

PROPOSITION 6.4. *$\mathrm{Sel}^{\pm}_p(f/k_\infty)$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-cotorsion.*

Proof. Recall that $\ker(\mathrm{Col}^{\pm}) = \mathbb{H}^1_{\mathrm{Iw},\pm}(T_{\bar{f}}(k-1))$ from § 4 and $\mathrm{Col}^{\pm}(\mathbf{z}^{\mathrm{Kato}}) = L^{\pm}_p$ by (7). Therefore, the cokernel of the first map in (26) is killed by $L^{\pm}_p$. Therefore, if $L^{\pm}_p \neq 0$, it would imply that the said cokernel is $\Lambda_{\mathcal{O}_E}(G_\infty)$-torsion and the result would follow from the fact that $\mathrm{Sel}^0_p(f/k_\infty)^{\vee}$ is $\Lambda_{\mathcal{O}_E}(G_\infty)$-torsion. Hence, we are done by the following lemma. □

LEMMA 6.5. $L^{\pm}_p \neq 0$.

Proof. The case when f corresponds to an elliptic curve is proved in [Pol03, Corollary 5.11]. The general case can be proved similarly.

By [Pol03], if θ is a character on G_n which does not factor through G_{n-1} and $0 \leqslant r \leqslant k-2$,

$$\chi^r\theta(L^+_p) = C^+_{n,r}(\theta)L(f,\theta,r+1) \quad \text{if } n \text{ is even},$$
$$\chi^r\theta(L^-_p) = C^-_{n,r}(\theta)L(f,\theta,r+1) \quad \text{if } n \text{ is odd},$$

where $C^{\pm}_{n,r}(\theta)$ are non-zero constants. By [Roh88], $L(f,\theta,1) = 0$ for finitely many θ if $k = 2$. If $k \geqslant 3$, $L(f,\theta,r+1) \neq 0$ for $r+1 \leqslant (k-1)/2$ by [Shi76, Proposition 2]. Hence, we are done. □

COROLLARY 6.6. *The first map in (26) is injective.*

Proof. It follows from Theorem 3.7 and Lemma 6.5. □

Remark 6.7. It is clear from the proof of Lemma 6.5 that $L^{\pm,\theta}_p \neq 0$ for any character θ on Δ. Therefore, $\mathrm{Sel}^{\pm}_p(f/k_\infty)^{\theta}$ is $\Lambda_{\mathcal{O}_E}(\Gamma)$-cotorsion and we can associate to it a characteristic ideal, namely $\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}^{\pm}_p(f/k_\infty)^{\vee,\theta})$.

6.4 Main conjectures

We now formulate a main conjecture and relate it to that of Kato. By Corollary 6.6 and the fact that $\mathrm{Sel}^0_p(f/k_\infty)^{\vee} \cong \mathbb{H}^2(T_{\bar{f}}(k-1))$ (see [Kur02]), we have an exact sequence

$$0 \to \mathbb{H}^1_S(T_{\bar{f}}(k-1)) \to \mathrm{Im}(\mathrm{Col}^{\pm}) \to \mathrm{Sel}^{\pm}_p(f/k_\infty)^{\vee} \to \mathbb{H}^2(T_{\bar{f}}(k-1)) \to 0.$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

If θ is a character on Δ, then

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^1_S(T_{\bar{f}}(k-1))^\theta/\mathbb{Z}(T_{\bar{f}}(k-1))^\theta) = \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathbb{H}^2(T_{\bar{f}}(k-1))^\theta)$$

if and only if

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}_p^{\pm}(f/k_\infty)^{\vee,\theta}) = \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Im}(\mathrm{Col}^{\pm,\theta})/L_p^{\pm,\theta}).$$

In other words, Kato's main conjecture (for $\bar{f}$) is equivalent to the following conjecture.

Conjecture 6.8. $\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}_p^{\pm}(f/k_\infty)^{\vee,\theta}) = \mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Im}(\mathrm{Col}^{\pm,\theta})/L_p^{\pm,\theta})$.

Moreover, by Corollary 5.11 and Remark 5.12, we have the following corollary.

Corollary 6.9. *Let $\delta = \pm$. When $\theta = 1$ or $\delta = -$, Conjecture 6.8 is equivalent to*

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_E}(\Gamma)}(\mathrm{Sel}_p^{\pm}(f/k_\infty)^{\vee,\theta}) = (\varpi^{-s^{\pm}} L_p^{\pm,\theta}).$$

Remark 6.10. It is clear that the right-hand sides in Conjectures 6.8 and 6.9 are contained in the left-hand sides if the homomorphism $G_{\mathbb{Q}} \to \mathrm{GL}_{\mathcal{O}_E}(T_{\bar{f}})$ is surjective or if we replace $\Lambda_{\mathcal{O}_E}(\Gamma)$ by $\Lambda_E(G_\infty)$ by Theorem 3.8.

7. CM forms

We now follow the strategy of [PR04] to prove that equality holds in Corollary 6.9 (with $\theta = 1$) for CM forms.

7.1 Generality of CM forms

We first briefly review the theory of CM modular forms. Details can be found in [Kat04, § 15].

Let K be an imaginary quadratic field with idele class group C_K. A Hecke character of K is simply a continuous homomorphism $\phi : C_K \to \mathbb{C}^\times$ with complex L-function

$$L(\phi, s) = \prod_v (1 - \phi(v)N(v)^{-s})^{-1},$$

where the product runs through the finite places v of K at which ϕ is unramified, $\phi(v)$ is the image of the uniformiser of K_v under ϕ and $N(v)$ is the norm of v.

Let f be a modular form as defined in § 2.4 with complex multiplication, i.e. $L(f, s) = L(\phi, s)$ for some Hecke character ϕ of an imaginary quadratic field K. Then, for a good prime p,

$$1 - a_p p^{-s} + \epsilon(p)p^{k-1-2s} = \begin{cases} 1 - \phi(p)p^{-2s} & \text{if } p \text{ is inert in } K, \\ (1 - \phi(\mathfrak{P})p^{-s})(1 - \phi(\bar{\mathfrak{P}})p^{-s}) & \text{if } (p) = \mathfrak{P}\bar{\mathfrak{P}} \text{ in } K. \end{cases}$$

Therefore, $a_p = 0$ if p is inert in K. If p splits into $\mathfrak{P}\bar{\mathfrak{P}}$, $a_p = \phi(\mathfrak{P}) + \phi(\bar{\mathfrak{P}})$. It is known that $\phi(\mathfrak{P}) + \phi(\bar{\mathfrak{P}})$ is a p-adic unit; hence, f is ordinary at p. Therefore, for a good prime $p \nmid N$, $a_p = 0$ if and only if f is supersingular at p. We fix such a p which is odd.

Let $\mathcal{O}$ be the ring of integers of K. We denote the conductor of ϕ by $\mathfrak{f}$. For an ideal $\mathfrak{a}$ of K, $K(\mathfrak{a})$ denotes the ray class field of K of conductor $\mathfrak{a}$. We write $\mathcal{K}$ for the union $\cup_n K(p^n\mathfrak{f})$. Then, the action of $G_{\mathbb{Q}}$ on V_f factors through $\mathrm{Gal}(\mathcal{K}/\mathbb{Q})$. The same is then true for $V_f(j)$ for all j as $k_\infty \subset \mathcal{K}$.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

More specifically, $V_f \cong V(\phi) \oplus \tau V(\phi)$, where $V(\phi)$ is the one-dimensional E-representation of G_K associated to ϕ and τ is the complex conjugation. The action of $G_{\mathbb{Q}}$ is given by

$$\sigma(x,y) = \begin{cases} (\sigma(x), \tau(\tau\sigma\tau)(y)) & \text{if } \sigma \in G_K, \\ ((\tau\sigma\tau)(y), \tau\sigma(x)) & \text{otherwise.} \end{cases}$$

In addition to Assumptions 1 and 2, we assume for simplicity that the following holds.

ASSUMPTION 3. The modular form f is defined over $\mathbb{Q}$ (i.e. $a_n \in \mathbb{Z}$ for all n) and K has class number 1.

This is essential for the properties of elliptic units which we need to hold. Note that as a vector space, V_f is isomorphic to K_p (where K_p denotes the completion of K at p) and we can take T_f to be the lattice corresponding to $\mathcal{O}_p$. We write ρ for the character given by

$$\rho : G_K \to \mathrm{Aut}(V_f/T_f(1)) \cong \mathcal{O}_p^{\times}.$$

For simplicity, we write A for $V_f/T_f(1)$ from now on.

Recall that K_c denotes the $\mathbb{Z}_p$-cyclotomic extension of K. We write K_m for the unique $\mathbb{Z}_p^2$-extension of K and $\mathfrak{L}$ denotes $\mathcal{O}_p[[\mathrm{Gal}(K_m/K)]]$. Given a $\mathbb{Z}_p[[\mathrm{Gal}(\mathcal{K}/K)]]$-module Y, we write Y_F for $Y \otimes_{\mathbb{Z}_p[[\mathrm{Gal}(\mathcal{K}/K)]]} \mathbb{Z}_p[[\mathrm{Gal}(F/K)]]$ and $Y_F^{\rho} = Y_F(\rho^{-1})$, where $F = K_c$ or K_m.

Let F be an extension of $\mathbb{Q}$. Following [Rub85], we define a modified Selmer group:

$$\mathrm{Sel}_p'(f/F) = \ker\left(H^1(F,A) \to \prod_{v \nmid p} \frac{H^1(F_v,A)}{H_f^1(F_v,A)} \right).$$

For a finite abelian extension F of K, we define groups C_F, E_F and U_F as in [PR04]: U_F is the pro-p part of the local unit group $(\mathcal{O}_F \otimes \mathbb{Z}_p)^{\times}$, E_F is the closure of the projection of the global units $\mathcal{O}_F^{\times}$ into U_F and C_F is the closure of the projection of the subgroup of elliptic units (as defined in [Rub91, § 1], see also § 7.1.1 below) into U_F. We then define

$$\mathcal{C} = \varprojlim C_F, \quad \mathcal{E} = \varprojlim E_F \quad \text{and} \quad \mathcal{U} = \varprojlim U_F,$$

where the inverse limits are taken over finite extensions F of K inside $\mathcal{K}$ and the connecting map is the norm map.

Finally, let M be the maximal abelian p-extension of $\mathcal{K}$ which is unramified outside p and write $\mathcal{X}$ for the Galois group of M over $\mathcal{K}$.

7.1.1 *Elliptic units.* We now briefly review the definition of elliptic units associated to K. Let $\mathfrak{a}$ and $\mathfrak{b}$ be non-zero ideals of $\mathcal{O}_K$ such that $\mathfrak{a}$ is prime to $6\mathfrak{b}$ and the natural map $\mathcal{O}_K^{\times} \to (\mathcal{O}_K/\mathfrak{b})^{\times}$ is injective. There exists an elliptic function on $\mathbb{C}/\mathfrak{b}$ with zeros and poles given by 0 (with multiplicity $N(\mathfrak{a})$) and the $\mathfrak{a}$-division points, respectively. There exists a unique such function if we impose some norm compatibility condition on its values as $\mathfrak{a}$ varies. We write ${}_{\mathfrak{a}}\theta_{\mathfrak{b}}$ for this unique function and let ${}_{\mathfrak{a}}z_{\mathfrak{b}} = {}_{\mathfrak{a}}\theta_{\mathfrak{b}}(1)^{-1}$. Then, ${}_{\mathfrak{a}}z_{\mathfrak{b}} \in K(\mathfrak{b})^{\times}$ for any $\mathfrak{a}$ and $\mathfrak{b}$ as above. For a fixed $\mathfrak{b}$, the group of elliptic units in $K(\mathfrak{b})$ is defined to be the group generated by ${}_{\mathfrak{a}}z_{\mathfrak{b}}^{\sigma}$, where $\sigma \in \mathrm{Gal}(K(\mathfrak{b})/K)$, and the roots of unity in $K(\mathfrak{b})$.

7.2 Properties of Sel_p'

In this section, we generalise [PR04, Theorem 2.1]. We do this by generalising three results of [Rub85].

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Lemma 7.1. *There is an isomorphism* $\mathrm{Sel}_p'(f/K_c) \cong \mathrm{Sel}_p(f/K_c)$.

Proof. By definitions, we have the following exact sequence:

$$0 \to \mathrm{Sel}_p(f/K_c) \to \mathrm{Sel}_p'(f/K_c) \to \frac{H^1(K_{c,p}, A)}{H_f^1(K_{c,p}, A)}.$$

Therefore, it suffices to show that $H^1(K_{c,p}, A) = H_f^1(K_{c,p}, A)$. By [BK90, Proposition 3.8],

$$\left(\frac{H^1(K_{c,p}, A)}{H_f^1(K_{c,p}, A)}\right)^\vee = \varprojlim H_f^1(K_p^{(n)}, T_{\bar{f}}(k-1)).$$

Hence, it suffices to show that the said inverse limit is 0.

Note that $\mathrm{Gal}(K_{p,n}/K_p^{(n-1)}) \cong \Delta$; we have the inflation–restriction exact sequence

$$\begin{aligned} 0 \to H^1(\Delta, T_{\bar{f}}(k-1)^{G_{K_{p,n}}}) \to H^1(K_p^{(n-1)}, T_{\bar{f}}(k-1)) \\ \to H^1(K_{p,n}, T_{\bar{f}}(k-1))^\Delta \to H^2(\Delta, T_{\bar{f}}(k-1)^{G_{K_{p,n}}}). \end{aligned}$$

As $K_p/\mathbb{Q}_p$ is unramified, the proof of Lemma 4.4 implies that $T_{\bar{f}}(k-1)^{G_{K_{p,n}}} = 0$ for all n. Therefore,

$$H^1(K_p^{(n-1)}, T_{\bar{f}}(k-1)) \cong H^1(K_{p,n}, T_{\bar{f}}(k-1))^\Delta.$$

By [Per00, Theorem 0.6], we have $\varprojlim H_f^1(K_{n,p}, T_{\bar{f}}(k-1)) = 0$; hence, we are done. □

This corresponds to [Rub85, Theorem 2.1], which holds for any infinite extensions of K contained in $\mathcal{K}$. Since we have used a result on the inverse limit of H_f^1 over $K_{p,n}$, the proof above would unfortunately not work in such generality.

We now generalise [Rub85, Proposition 1.1].

Lemma 7.2. *There is an isomorphism* $\mathrm{Sel}_p'(f/\mathcal{K}) \cong \mathrm{Hom}(\mathcal{X}, A)$.

Proof. Since the action of G_K on A factors through $\mathrm{Gal}(\mathcal{K}/K)$, we have $H^1(\mathcal{K}, A) \cong \mathrm{Hom}(G_\mathcal{K}, A)$. We can therefore identify $\mathrm{Sel}_p'(f/\mathcal{K})$ with a subgroup of $\mathrm{Hom}(G_\mathcal{K}, A)$. Also, the triviality of the action implies that A is unramified at all places of $\mathcal{K}$. Therefore, $H_f^1(\mathcal{K}_v, A) = H_{\mathrm{ur}}^1(\mathcal{K}_v, A)$ for all $v \nmid p$ by [Rub00, Lemma 3.5(iv)]. Hence, $\mathrm{Sel}_p'(f/\mathcal{K})$ corresponds to the subgroup $\mathrm{Hom}(\mathcal{X}, A) \subset \mathrm{Hom}(G_\mathcal{K}, A)$. □

Before we continue, we state a result of Rubin.

Lemma 7.3. *For* $i = 1, 2$, $H^i(\mathcal{K}/K_c, A) = 0$.

Proof. See [Rub85, proof of Proposition 1.2]. □

This allows us to generalise [Rub85, Proposition 1.2].

Lemma 7.4. *There is an isomorphism* $\mathrm{Sel}_p'(f/K_c) \cong \mathrm{Sel}_p'(f/\mathcal{K})^{\mathrm{Gal}(\mathcal{K}/K_c)}$.

Proof. We have the inflation–restriction exact sequence:

$$0 \to H^1(\mathcal{K}/K_c, A) \to H^1(K_c, A) \xrightarrow{r} H^1(\mathcal{K}, A)^{\mathrm{Gal}(\mathcal{K}/K_c)} \to H^2(\mathcal{K}/K_c, A),$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

where r is the restriction map. Consider the following commutative diagram:

$$\begin{array}{ccc} H^1(K_c, A) & \xrightarrow{\quad r \quad} & H^1(\mathcal{K}, A) \\ \downarrow & & \downarrow \\ H^1(K_{c,v}, A)/H^1_f(K_{c,v}, A) & \longrightarrow & H^1(\mathcal{K}_{v'}, A)/H^1_f(\mathcal{K}_{v'}, A) \end{array}$$

where $v \nmid p$ is a place of K_c and v' is a place of $\mathcal{K}$ above v. It clearly implies that

$$r(\mathrm{Sel}'_p(f/K_c)) \subset \mathrm{Sel}'_p(f/\mathcal{K}).$$

Write v' for the place of $K_c(\mathfrak{f})$ below v'; then v' is unramified in $\mathcal{K}/K_c(\mathfrak{f})$. Therefore, the map

$$r_{v'} : H^1(I_{K_c(\mathfrak{f})_{v'}}, A) \to H^1(I_{\mathcal{K}_{v'}}, A),$$

where I denotes the inertia group, is injective. This implies that

$$H^1(K_c(\mathfrak{f})_{v'}, A)/H^1_f(K_c(\mathfrak{f})_{v'}, A) \to H^1(\mathcal{K}_{v'}, A)/H^1_f(\mathcal{K}_{v'}, A)$$

is injective because the H^1_f coincide with H^1_{ur}. But $\mathrm{Gal}(K_c(\mathfrak{f})/K_c)$ has trivial Sylow p-subgroup; hence, the bottom row of the commutative diagram above is injective. Therefore, we have

$$r^{-1}(\mathrm{Sel}'_p(f/\mathcal{K})) \subset \mathrm{Sel}'_p(f/K_c).$$

Hence, we have an exact sequence:

$$0 \to H^1(\mathcal{K}/K_c, A) \to \mathrm{Sel}'_p(f/K_c) \xrightarrow{r} \mathrm{Sel}'_p(f/\mathcal{K})^{\mathrm{Gal}(\mathcal{K}/K_c)} \to H^2(\mathcal{K}/K_c, A).$$

Hence, we are done by Lemma 7.3. □

We can now give a generalisation of [PR04, Theorem 2.1].

COROLLARY 7.5. $\mathrm{Sel}_p(f/K_c) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{X}^{\rho}_{K_c}, K_p/\mathcal{O}_p)$.

Proof. On combining Lemmas 7.1, 7.2 and 7.4, we have

$$\begin{aligned} \mathrm{Sel}_p(f/K_c) &\cong \mathrm{Sel}'_p(f/K_c) \\ &\cong \mathrm{Sel}'_p(f/\mathcal{K})^{\mathrm{Gal}(\mathcal{K}/K_c)} \\ &\cong \mathrm{Hom}(\mathcal{X}, A)^{\mathrm{Gal}(\mathcal{K}/K_c)}. \end{aligned}$$

But $A|_{G_K} \cong K_p/\mathcal{O}_p(\rho)$; hence, the result. □

7.3 Reciprocity law

In this section, we generalise the reciprocity law given by [PR04, Theorem 5.1]. We first review a result of Rubin.

THEOREM 7.6. *The $\mathfrak{L}$-module $\mathcal{C}^{\rho}_{K_m}$ is free of rank one.*

Proof. It follows from [Rub91, Theorem 7.7]. □

We now generalise [PR04, Proposition 4.1].

LEMMA 7.7. $H^1_f(K_{c,p}, A) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{U}^{\rho}_{K_c}, K_p/\mathcal{O}_p)$.

Proof. As in the proof of Lemma 7.2, we have $H^1(\mathcal{K}_p, A) \cong \mathrm{Hom}(G_{\mathcal{K}_p}, A)$. But we also have an isomorphism $H^1(K_{c,p}, A) \cong H^1(\mathcal{K}_p, A)^{\mathrm{Gal}(\mathcal{K}_p/K_{c,p})}$ by the inflation–restriction sequence and

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Lemma 7.3. Hence, by local class field theory, we have

$$\begin{aligned} H^1(K_{c,p}, A) &\cong \mathrm{Hom}(G_{\mathcal{K}_p}, A)^{\mathrm{Gal}(\mathcal{K}_p/K_{c,p})} \\ &\cong \mathrm{Hom}_{\mathcal{O}_p}(\mathcal{U}, A) \end{aligned}$$

(see [Rub87, Proposition 5.2]). By the proof of Lemma 7.1, we have $H^1_f(K_{c,p}, A) \cong H^1(K_{c,p}, A)$; hence, we are done. □

In particular, we have a pairing $\langle\,,\rangle : H^1_f(K_{c,p}, A) \times \mathcal{U}^\rho_{K_c} \to K_p/\mathcal{O}_p$. We now prove the explicit reciprocity law.

Proposition 7.8. *There exists a generator ξ of $\mathcal{C}^\rho_{K_m}$ over $\mathfrak{L}$ such that for any finite extension F of K contained in K_c, θ a character on $G = \mathrm{Gal}(F/K)$, $x \in H^1_f(F_p, A)$ and r a non-negative integer, we have*

$$\sum_{\sigma\in G} \theta(\sigma)\langle x^\sigma \otimes p^{-r}, \xi\rangle = p^{-r}\frac{L(f_{\theta^{-1}}, 1)}{\Omega^{\pm}_f}\left[\sum_{\sigma\in G}\theta(\sigma)\exp^{-1}_{F_p, V_f(1)}(x^\sigma), \bar{\omega}_{-1}\right], \tag{27}$$

where $\theta(-1) = \pm$ and $\exp^{-1}_{F_p,V_f(1)}$ is the inverse of the exponential map

$$\exp_{F_p,V_f(1)} : F_p \otimes \mathbb{D}(V_f(1))/\mathbb{D}^0(V_f(1)) \xrightarrow{\sim} H^1_f(F_p, V_f(1)).$$

Proof. Let $z_{p^\infty\mathfrak{f}} = (z_{p^n\mathfrak{f}})_n$ be the system of norm-compatible elliptic units in $\varprojlim K(p^n\mathfrak{f})$ defined in [Kat04, § 16.5]; then ${}_\mathfrak{a} z_{p^n\mathfrak{f}}$ is a multiple of $z_{p^n\mathfrak{f}}$ for all $\mathfrak{a}$ and $p^n\mathfrak{f}$ satisfying the conditions in § 7.1.1. Therefore, if we write ξ as its image in $\mathcal{C}^\rho_{K_m}$, it must be a generator of $\mathcal{C}^\rho_{K_m}$ over $\mathfrak{L}$ by Theorem 7.6.

Let $x \in H^1_f(F_p, T_f(1))$ and $y \in H^1(F_p, T_{\bar{f}}(k-1))$; we have

$$\begin{aligned} \sum_{\sigma\in G}\theta(\sigma)[x^\sigma, y] &= \sum_{\sigma\in G}\theta(\sigma)\mathrm{Tr}_{F/K}[\exp^{-1}_{F_p,V_f(1)}(x^\sigma), \exp^*_{F_p,V_{\bar{f}(k-1)}}(y)] \\ &= \sum_{\sigma,\tau\in G}\theta(\sigma)[\exp^{-1}_{F_p,V_f(1)}(x^{\sigma\tau}), \exp^*_{F_p,V_{\bar{f}(k-1)}}(y^\tau)] \\ &= \sum_{\sigma,\tau\in G}\theta(\sigma\tau)\theta^{-1}(\tau)[\exp^{-1}_{F_p,V_f(1)}(x^{\sigma\tau}), \exp^*_{F_p,V_{\bar{f}(k-1)}}(y^\tau)] \\ &= \left[\sum_{\sigma\in G}\theta(\sigma)\exp^{-1}_{F_p,V_f(1)}(x^\sigma), \sum_{\tau\in G}\theta^{-1}(\tau)\exp^*_{F_p,V_{\bar{f}(k-1)}}(y^\tau)\right]. \end{aligned}$$

Consider the Kummer exact sequences

$$\begin{array}{ccc} \mathcal{C} & \longrightarrow & \mathcal{U} \\ \downarrow & & \downarrow \\ \varprojlim H^1(\mathcal{O}_{K'}[1/p], \mathcal{O}_p(1)) & \longrightarrow & \varprojlim H^1(K'_p, \mathcal{O}_p(1)) \\ \downarrow{\scriptstyle \otimes\rho\chi^{k-2}} & & \downarrow{\scriptstyle \otimes\rho\chi^{k-2}} \\ \varprojlim H^1(\mathcal{O}_{K'}[1/p], T_{\bar{f}}(k-1)) & \longrightarrow & \varprojlim H^1(K'_p, T_{\bar{f}}(k-1)) \end{array}$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

By [Kat04, Proposition 15.9 and (15.16.1)], the image of $z_{p^\infty \mathfrak{f}}$ in $\varprojlim H^1(\mathcal{O}_{K'}[1/p], T_{\bar{f}}(k-1))$ is $\mathbf{z}^{\mathrm{Kato}}$ (up to a twist) and so ξ satisfies

$$\sum_{\tau \in G} \theta^{-1}(\tau) \exp^*_{F_p, V_{\bar{f}}(k-1)}(\xi^\tau) = \frac{L(f_{\theta^{-1}}, 1)\bar{\omega}_{-1}}{\Omega_f^{\pm}}.$$

Therefore, we have

$$\sum_{\sigma \in G} \theta(\sigma) \langle x^\sigma \otimes p^{-r}, \xi \rangle = p^{-r} \left[\sum_{\sigma \in G} \theta(\sigma) \exp^{-1}_{F, V_f(1)}(x^\sigma), \frac{L(f_{\theta^{-1}}, 1)\bar{\omega}_{-1}}{\Omega_f^{\pm}} \right],$$

as required. □

7.4 Proof of the main conjecture

On replacing $\mathbb{Q}_{p,n}$ by $K_{p,n}$, we define $H^1_f(K_{p,n}, W)^{\pm}$ and hence $\mathrm{Sel}_p^{\pm}(f/K_\infty)$ as in § 6, where $W = A$ or $T_f(1)$. Let $\mathcal{G} = \mathrm{Gal}(K/\mathbb{Q})$. As in the proof of Lemma 7.1, the inflation–restriction exact sequence implies that $H^1(\mathbb{Q}_{p,n}, W) \cong H^1(K_{p,n}, W)^{\mathcal{G}}$ for $W = A$ or $T_f(1)$, so we recover $\mathrm{Sel}_p^{\pm}(f/k_\infty)$ on taking $\mathcal{G}$-invariants. Similarly, on replacing $\mathbb{Q}_{p,n}$ and $K_{p,n}$ by $\mathbb{Q}_p^{(n-1)}$ and $K_p^{(n-1)}$, respectively, we define the $\pm$-Selmer groups $\mathrm{Sel}_p^{\pm}(f/\mathbb{Q}_c)$ and $\mathrm{Sel}_p^{\pm}(f/K_c)$. Under our assumptions, they coincide with the Δ-invariants of $\mathrm{Sel}_p^{\pm}(f/k_\infty)$ and $\mathrm{Sel}_p^{\pm}(f/K_\infty)$, respectively. Analogously, we have $H^1_{\pm}(F, T_{\bar{f}}(k-1))$ for $F = K_{p,n}$, $K_p^{(n-1)}$ or $\mathbb{Q}_p^{(n-1)}$. Since $K_p/\mathbb{Q}_p$ is unramified, all the results from the previous sections generalise directly on replacing $\mathbb{Q}_p$ by K.

Via the isomorphism defined in Lemma 7.7, we define $\mathcal{V}^{\pm} \subset \mathcal{U}^{\rho}_{K_c}$ to be the subgroup corresponding to the elements of $\mathrm{Hom}_{\mathcal{O}}(H^1_f(K_{c,p}, A), K_p/\mathcal{O}_p)$ which factor through $H^1_f(K_{c,p}, A)^{\pm}$. Then, by [PR04, Theorem 4.3], $\mathrm{Sel}_p^{\pm}(f/K_c) \cong \mathrm{Hom}_{\mathcal{O}}(\mathcal{X}^{\rho}_{K_c}/\alpha(\mathcal{V}^{\pm}), K_p/\mathcal{O}_p)$, where α is the Artin map on $\mathcal{U}$, which enables us to generalise [PR04, Theorem 7.2].

THEOREM 7.9. *Let $s^{\pm}$ be as given by Corollary 5.11; then*

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_p}(\Gamma)}(\mathrm{Hom}_{\mathcal{O}}(\mathrm{Sel}_p^{\pm}(f/K_c), K_p/\mathcal{O}_p)) = (p^{-s^{\pm}} L_p^{\pm}).$$

Proof. By the above isomorphism and [PR04, Theorem 6.3], we have

$$\begin{aligned} \mathrm{Char}_{\Lambda_{\mathcal{O}_p}(\Gamma)}(\mathrm{Hom}_{\mathcal{O}}(\mathrm{Sel}_p^{\pm}(f/K_c), K_p/\mathcal{O}_p)) &= \mathrm{Char}_{\Lambda_{\mathcal{O}_p}(\Gamma)}(\mathcal{X}^{\rho}_{K_c}/\alpha(\mathcal{V}^{\pm})) \\ &= \mathrm{Char}_{\Lambda_{\mathcal{O}_p}(\Gamma)}(\mathcal{U}^{\rho}_{K_c}/(\mathcal{V}^{\pm} + \mathcal{C}^{\rho}_{K_c})). \end{aligned}$$

By Corollary 5.11, the quotient $H^1(\mathbb{Q}_{c,p}, T_{\bar{f}}(k-1))/H^1_{\pm}(\mathbb{Q}_{c,p}, T_{\bar{f}}(k-1))$ is free of rank one over $\Lambda(\Gamma)$. Hence, by (13) and the proofs of Lemma 5.9 and Corollary 5.11, the $\Lambda(\Gamma)$-module $\mathrm{Hom}(H^1_f(\mathbb{Q}_{c,p}, T_f(1))^{\pm}, \mathbb{Z}_p)$ is also free of rank one and it has a generator $f_{\pm}$ such that

$$\sum_{\sigma \in G_n} f_{\pm}(\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm})^\sigma))\sigma \equiv p^{s^{\pm}} \log^{\pm}_{p,k} \mod(\gamma^{p^{n-1}} - 1). \tag{28}$$

Note that we have abused notation by writing $\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm}))$ for its image in $H^1(\mathbb{Q}_p^{(n-1)}, T_f(1))$ under the corestriction.

As in [PR04, Theorems 7.1 and 7.2], we have

$$\begin{aligned} \mathrm{Hom}(H^1_f(\mathbb{Q}_{c,p}, A)^{\pm}, \mathbb{Q}_p/\mathbb{Z}_p) &\cong \mathrm{Hom}(H^1_f(\mathbb{Q}_{c,p}, T_f(1))^{\pm}, \mathbb{Z}_p), \\ \mathrm{Hom}_{\mathcal{O}}(H^1_f(K_{c,p}, A)^{\pm}, K_p/\mathcal{O}_p) &\cong \mathrm{Hom}(H^1_f(\mathbb{Q}_{c,p}, A)^{\pm}, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{O}_p. \end{aligned}$$

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Let $\mu^{\pm}$ and $\vartheta^{\pm}$ be the images of $f_{\pm}$ and ξ from Proposition 7.8 in $\mathrm{Hom}_{\mathcal{O}}(H^1_f(K_{c,p},A)^{\pm}, K_p/\mathcal{O}_p)$, respectively. Then, $\vartheta^{\pm}=h^{\pm}\mu^{\pm}$ for some $h^{\pm}\in\Lambda_{\mathcal{O}_p}(\Gamma)$. As in [PR04, proof of Theorem 7.2], there is an isomorphism $\mathcal{U}^{\rho}_{K_c}/(\mathcal{V}^{\pm}+\mathcal{C}^{\rho}_{K_c})\cong\Lambda_{\mathcal{O}_p}(\Gamma)/h^{\pm}\Lambda_{\mathcal{O}_p}(\Gamma)$. Hence, we have

$$\mathrm{Char}_{\Lambda_{\mathcal{O}_p}(\Gamma)}(\mathrm{Hom}_{\mathcal{O}}(\mathrm{Sel}^{\pm}_p(f/K_c),K_p/\mathcal{O}_p))=h^{\pm}\Lambda_{\mathcal{O}_p}(\Gamma).$$

Let F be a finite extension of K contained in K_c, θ a character of G, the Galois group of F over K, $x\in H^1_f(F_p,A)$ and r an integer; then $\vartheta^{\pm}=h^{\pm}\mu^{\pm}$ implies that

$$\sum_{\sigma\in G}\theta(\sigma)\vartheta^{\pm}(x^{\sigma}\otimes p^{-r})=\theta(h^{\pm})\sum_{\sigma\in G}\theta(\sigma)\mu^{\pm}(x^{\sigma}\otimes p^{-r}). \tag{29}$$

We now take $x=\exp_{n,1}(\gamma_{n,1}(\eta_1^{\pm}))$. By (28), the right-hand side of (29) is just $p^{-r+s^{\pm}}\theta(h^{\pm})\theta(\log^{\pm}_{p,k})$. Then, (27) implies that the left-hand side of (29) equals the following:

$$p^{-r}\frac{L(f_{\theta^{-1}},1)}{\Omega^{\delta}_f}\left[\sum_{\sigma\in G}\theta(\sigma)\gamma_{n,1}(\eta_1^{\pm})^{\sigma},\bar{\omega}_{-1}\right],$$

where $\delta=\theta(-1)$. We now compute $\sum_{\sigma\in G}\theta(\sigma)\gamma_{n,1}(\eta_1^{\pm})^{\sigma}$.

Take F to be $K_p^{(n-1)}$ and θ a character of conductor p^n. Then,

$$\begin{aligned}\sum_{\sigma\in G}\theta(\sigma)\gamma_{n,1}(\eta^{\pm})^{\sigma}&=\sum_{\sigma\in G}\frac{\theta(\sigma)}{p^n}\left(\sum_{i=0}^{n-1}\zeta^{\sigma}_{p^{n-i}}\otimes\varphi^{i-n}(\eta_1^{\pm})+(1-\varphi)^{-1}(\eta_1^{\pm})\right)\\&=p^{-n}\sum_{\sigma\in G}\theta(\sigma)\zeta^{\sigma}_{p^n}\otimes\varphi^{-n}(\eta_1^{\pm})\\&=p^{-n}\tau(\theta)\varphi^{-n}(\eta_1^{\pm}),\end{aligned}$$

where $\tau(\theta)$ denotes the Gauss sum of θ. Since $\varphi^2+\epsilon(p)p^{k-3}=0$ on $\mathbb{D}(V_f(1))$, we have

$$\begin{aligned}\varphi^{-n}(\eta_1^{-})&=(-\epsilon(p)p^{k-3})^{(-n-1)/2}p^{-1}\varphi(\omega)_1/[\varphi(\omega),\bar{\omega}]\quad(\text{for } n \text{ odd}),\\\varphi^{-n}(\eta_1^{+})&=(-\epsilon(p)p^{k-3})^{-n/2}\varphi(\omega)_1/[\varphi(\omega),\bar{\omega}]\quad(\text{for } n \text{ even}).\end{aligned}$$

Hence, (29) implies that

$$\begin{aligned}p^{s^-}\theta(h^-)\theta(\log^-_{p,k})&=(-\epsilon(p)p^{k-1})^{(-n-1)/2}\tau(\theta)\frac{L(f_{\theta^{-1}},1)}{\Omega^{\delta}_f}\quad(\text{for } n \text{ odd}),\\p^{s^+}\theta(h^+)\theta(\log^+_{p,k})&=(-\epsilon(p)p^{k-1})^{-n/2}\tau(\theta)\frac{L(f_{\theta^{-1}},1)}{\Omega^{\delta}_f}\quad(\text{for } n \text{ even}).\end{aligned}$$

Therefore, by the interpolating properties of $L_p^{\pm}$ at these characters, we have

$$\begin{aligned}p^{s^-}\theta(h^-)&=\theta(L_p^-)\quad(\text{for } n \text{ odd}),\\p^{s^+}\theta(h^+)&=\theta(L_p^+)\quad(\text{for } n \text{ even}).\end{aligned}$$

But $h^{\pm}$ and $L_p^{\pm}$ are both $O(1)$ and the above holds for infinitely many n, so $h^{\pm}=p^{-s^{\pm}}L_p^{\pm}$. Hence, we are done. □

By taking $\mathcal{G}$-invariants, we have the following corollary.

Corollary 7.10. $\mathrm{Char}_{\Lambda(\Gamma)}(\mathrm{Sel}^{\pm}_p(f/\mathbb{Q}_c)^{\vee})=(p^{-s^{\pm}}L_p^{\pm})$.

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press

Acknowledgements

The author would like to thank Prof. Tony Scholl for suggesting the study of this topic and his patient guidance and tremendous help. The author is also indebted to Alex Bartel, Tobias Berger, Michael Fester and Byoung Du Kim for very helpful discussions. Finally, the author is extremely grateful to the anonymous referees for their very useful comments and suggestions.

References

AV75 Y. Amice and J. Vélu, *Distributions p-adiques associées aux séries de Hecke*, in *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974)* (Soc. Math. France, Paris, 1975), 119–131, Astérisque, Nos. 24–25.

BLZ04 L. Berger, H. Li and H. J. Zhu, *Construction of some families of 2-dimensional crystalline representations*, Math. Ann. **329** (2004), 365–377.

BK90 S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, in *The Grothendieck Festschrift, Vol. I*, Progress in Mathematics, vol. 86 (Birkhäuser, Boston, MA, 1990), 333–400.

Bre01 C. Breuil, *p-adic hodge theory, deformations and local langlands*, cours au C.R.M. de Barcelone (http://www.ihes.fr/∼breuil/), 2001.

Col98 P. Colmez, *Théorie d'Iwasawa des représentations de de Rham d'un corps local*, Ann. of Math. (2) **148** (1998), 485–571.

Del69 P. Deligne, *Formes modulaires et représentations l-adiques*, Séminaire Bourbaki (1968/69), Exp. No. 355, 139–172.

Kat93 K. Kato, *Lectures on the approach to Iwasawa theory for Hasse–Weil L-functions via* B_{dR}. *I*, in *Arithmetic algebraic geometry (Trento, 1991)*, Lecture Notes in Mathematics, vol. 1553 (Springer, Berlin, 1993), 50–163.

Kat04 K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in *Cohomologies p-adiques et applications arithmétiques. III*, Astérisque **295** (2004), 117–290.

Kob03 S. Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1–36.

Kur02 M. Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*, Invent. Math. **149** (2002), 195–224.

MTT86 B. Mazur, J. Tate and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), 1–48.

Per93 B. Perrin-Riou, *Fonctions L p-adiques d'une courbe elliptique et points rationnels*, Ann. Inst. Fourier (Grenoble) **43** (1993), 945–995.

Per94 B. Perrin-Riou, *Théorie d'Iwasawa des représentations p-adiques sur un corps local*, Invent. Math. **115** (1994), 81–161.

Per95 B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques*, Astérisque **229** (1995).

Per00 B. Perrin-Riou, *Représentations p-adiques et normes universelles. I. Le cas cristallin*, J. Amer. Math. Soc. **13** (2000), 533–551.

Pol03 R. Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), 523–558.

PR04 R. Pollack and K. Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), 447–464.

Roh88 D. E. Rohrlich, *L-functions and division towers*, Math. Ann. **281** (1988), 611–632.

Rub85 K. Rubin, *Elliptic curves and* $\mathbb{Z}_p$*-extensions*, Compositio Math. **56** (1985), 237–250.

Rub87 K. Rubin, *Local units, elliptic units, Heegner points and elliptic curves*, Invent. Math. **88** (1987), 405–422.

Rub91 K. Rubin, *The 'main conjecture' of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25–68.

Rub00 K. Rubin, *Euler systems*, Annals of Mathematics Studies, vol. 147 (Princeton University Press, Princeton, NJ, 2000).

Shi76 G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), 783–804.

Spr09 F. Sprung, *Iwasawa theory for elliptic curves at supersingular primes: beyond the case* $a_p = 0$, arXiv:0903.3419, 2009.

Antonio Lei antonio.lei@monash.edu
Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK

Current address: School of Mathematical Sciences, Monash University, Clayton, VIC 3800, Australia

https://doi.org/10.1112/S0010437X10005130 Published online by Cambridge University Press