Compositio Math. 140 (2004) 1439–1472
DOI: 10.1112/S0010437X04000569

The Heegner point Kolyvagin system

Benjamin Howard

Abstract

In Bull. Soc. Math. France **115** (1987), 399–456, Perrin-Riou formulates a form of the Iwasawa main conjecture which relates Heegner points to the Selmer group of an elliptic curve defined over $\mathbb{Q}$, as one goes up the anticyclotomic $\mathbb{Z}_p$-extension of a quadratic imaginary field K. Building on the earlier work of Bertolini on this conjecture, and making use of the recent work of Mazur and Rubin on Kolyvagin's theory of Euler systems, we prove one divisibility of Perrin-Riou's conjectured equality. As a consequence, one obtains an upper bound on the rank of the Mordell–Weil group $E(K)$ in terms of Heegner points.

Introduction

In this paper we modify the notion of a Kolyvagin system, as defined in [MR04], to include the system of cohomology classes which result from the application of Kolyvagin's derivative operators to the Heegner point Euler system. The resulting theory yields a simplified proof of a theorem of Kolyvagin, stated below as Theorem A. Our true sights, however, are set on the Iwasawa theory of Heegner points in the anticyclotomic $\mathbb{Z}_p$-extension of a quadratic imaginary field.

Fix forever a rational prime p. If E is an elliptic curve defined over a number field L, we denote by $\mathrm{Sel}_{p^\infty}(E/L)$ and $S_p(E/L)$ the usual p-power Selmer groups which fit into the descent sequences

$$0 \to E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/L) \to Ш_{p^\infty} \to 0,$$
$$0 \to E(L) \otimes \mathbb{Z}_p \to S_p(E/L) \to \varprojlim Ш_{p^n} \to 0.$$

Fix once and for all an elliptic curve $E/\mathbb{Q}$ with conductor N and a quadratic imaginary field K of discriminant $D \neq -3, -4$ satisfying the Heegner hypothesis that all primes dividing N are split in K. Let $T = T_p(E)$ be the p-adic Tate module of E. The theory of complex multiplication gives a family of points on the modular curve $X_0(N)$ which are rational over abelian extensions of K. More precisely, in § 1.7 we will attach to every square-free product n of rational primes inert in K a point $h_n \in X_0(N)(K[n])$, where $K[n]$ is the ring class field of K of conductor n. Fixing a modular parametrization of E by $X_0(N)$ yields a family of points $P[n] \in E(K[n])$ which satisfy Euler system-like relations relative to the norm operators. To each point $P[n]$ one applies first the Kummer map and then Kolyvagin's derivative operator D_n to obtain a cohomology class over K,

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

where $G_n = \bigotimes_{\ell|n} \mathrm{Gal}(K[\ell]/K[1])$, I_n is an ideal of $\mathbb{Z}_p$, and

$$H^1_{\mathcal{F}(n)}(K, T/I_nT) \subset H^1(K, T/I_nT)$$

Received 25 November 2002, accepted in final form 31 July 2003, published online 15 October 2004.
2000 Mathematics Subject Classification 11G05, 11R23.
Keywords: Iwasawa theory, elliptic curves, Heegner points, Euler systems.
This research is derived from the author's PhD thesis, and was conducted under the supervision of Karl Rubin. The author extends his thanks both to Professor Rubin and to the Mathematics Department of Stanford University. This research was partially conducted by the author for the Clay Mathematics Institute, to whom he also gives his thanks.

is the generalized Selmer group of Definition 1.2.2 obtained by modifying the usual local conditions which define $S_p(E/K)$ at primes of K dividing n. The classes κ_n form a Kolyvagin system, as defined in § 1.2. The class $\kappa_1 \in H^1_{\mathcal{F}(1)}(K,T) = S_p(E/K)$ is just the image under the Kummer map of the norm of $P[1]$, and the celebrated theorem of Gross and Zagier says that $\mathrm{ord}_{s=1} L(s,E/K) = 1$ if and only if κ_1 has infinite order. In § 1 we will give a proof of the following theorem.

Theorem A (Kolyvagin). *Assume p is odd and the integers p, D, and N are pairwise coprime. Assume also that $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective. If $\kappa_1 \neq 0$ then $S_p(E/K)$ is free of rank one over $\mathbb{Z}_p$ and there is a finite $\mathbb{Z}_p$-module M such that*

$$\mathrm{Sel}_{p^\infty}(E/K) \cong (\mathbb{Q}_p/\mathbb{Z}_p) \oplus M \oplus M$$

with

$$\mathrm{length}_{\mathbb{Z}_p}(M) \leqslant \mathrm{length}_{\mathbb{Z}_p}(S_p(E/K)/\mathbb{Z}_p\kappa_1).$$

Assume now that E is ordinary at p. Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K, $\Gamma = \mathrm{Gal}(K_\infty/K)$, and $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Let $K_n \subset K_\infty$ be the unique subfield with $[K_n : K] = p^n$. In § 2.2 we define, in the manner of [Gre89], two generalized Selmer groups

$$H^1_{\mathcal{F}_\Lambda}(K,\mathbf{T}) \subset \varprojlim H^1(K_n,T), \quad H^1_{\mathcal{F}_\Lambda}(K,\mathbf{A}) \subset \varinjlim H^1(K_n,E[p^\infty]),$$

where $\mathbf{T} \cong T \otimes \Lambda$ and $\mathbf{A} \cong \mathrm{Hom}(\mathbf{T},\mu_{p^\infty})$, such that there are pseudo-isomorphisms of Λ-modules

$$H^1_{\mathcal{F}_\Lambda}(K,\mathbf{T}) \sim \varprojlim S_p(E/K_n), \quad H^1_{\mathcal{F}_\Lambda}(K,\mathbf{A}) \sim \varinjlim \mathrm{Sel}_{p^\infty}(E/K_n).$$

Define $X = \mathrm{Hom}(H^1_{\mathcal{F}_\Lambda}(K,\mathbf{A}),\mathbb{Q}_p/\mathbb{Z}_p)$, and let $X_{\Lambda\text{-tors}}$ denote the Λ-torsion submodule of X. In the spirit of the Iwasawa Main Conjecture we view the characteristic ideal $\mathrm{char}(X_{\Lambda\text{-tors}})$ as a sort of algebraically defined p-adic L-function.

In § 2.3 we use Heegner points to construct a Kolyvagin system κ^{Hg} for the Λ-module $\mathbf{T}$. The class $\kappa_1^{\mathrm{Hg}} \in H^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ is nonzero by the work of Cornut and Vatsal. At a height-one prime $\mathfrak{P}$ of Λ, a Kolyvagin system for $\mathbf{T}$ reduces to a Kolyvagin system for $\mathbf{T} \otimes_\Lambda S_\mathfrak{P}$ where $S_\mathfrak{P}$ is the integral closure of $\Lambda/\mathfrak{P}$. Applying at every prime of Λ the same machinery used to prove Theorem A gives the following result.

Theorem B. *Keep the assumptions on T, p, D, and N of Theorem A, and assume also that p does not divide the class number of K. We continue to assume that E is ordinary at p. Let $\mathbf{H}$ denote the Λ-submodule of $H^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ generated by κ_1^{Hg}, and let $\iota : \Lambda \to \Lambda$ be the involution induced by inversion in Γ.*

The Λ-module $H^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})$ is torsion-free of rank one, and there is a finitely generated torsion Λ-module M such that

a) $\mathrm{char}(M) = \mathrm{char}(M)^\iota$,
b) $X \sim \Lambda \oplus M \oplus M$,
c) $\mathrm{char}(M)$ *divides* $\mathrm{char}(H^1_{\mathcal{F}_\Lambda}(K,\mathbf{T})/\mathbf{H})$,

where char *denotes characteristic ideal.*

We remark that parts a and b of the theorem are already known by the combined results of Bertolini, Cornut, and Nekovář [Ber95, Cor02, Nek01b] and have the following important consequence: by Mazur's control theorem one has

$$\mathrm{rank}_{\mathbb{Z}_p} X/(\gamma-1)X = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K),$$

and therefore the corank of the Selmer group over K odd. This is compatible with the Birch and Swinnerton-Dyer conjecture: the Heegner hypothesis forces the sign of the functional equation of

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

$L(s, E/K)$ to be -1, and so $\mathrm{ord}_{s=1} L(s, E/K)$ is odd. Similarly, part c of the theorem, together with the control theorem, gives the inequality

$$\mathrm{rank}_{\mathbb{Z}_p} S_p(E/K) \leqslant 1 + 2\,\mathrm{ord}_J(\mathbf{L}), \tag{1}$$

where $J \subset \Lambda$ is the augmentation ideal and $\mathbf{L} = \mathrm{char}\left(H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\mathbf{H}\right)$. One does not typically expect equality to hold; see (2) below. Theorem B can be generalized in many ways, for example by replacing E by an abelian variety with real multiplication, replacing the modular curve $X_0(N)$ by an appropriate Shimura curve (allowing one to weaken the Heegner hypothesis), and replacing K by a CM-field. See [How04b] for work in this direction.

The Main Conjecture for Heegner points was formulated by Perrin-Riou in [Per87] and predicts that

$$\mathrm{char}(M) = c^{-1}\,\mathrm{char}(H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\mathbf{H}),$$

where $c \in \mathbb{Z}_p$ is the Manin constant associated to our choice of modular parametrization of E (the proof that our $\mathbf{H}$ agrees with the module considered by Perrin-Riou is part of the content of Theorem 2.3.7). The theory of derived p-adic height pairings, introduced by Bertolini and Darmon and further developed by the author [BD01b, How04a], leads one to conjecture that the torsion module M of Theorem B has the form

$$M \sim (\Lambda/J)^{e_1} \oplus (\Lambda/J^2)^{e_2} \oplus M'$$

for a Λ-module M' with characteristic ideal prime to J, and

$$e_1 = \min(r^+, r^-), \quad e_2 = \frac{|r^+ - r^-| - 1}{2},$$

where $r^\pm$ is the rank of the $\pm$-eigenspace of $S_p(E/K)$ under complex conjugation. Combining this with the Main Conjecture, we see that one should expect

$$\mathrm{ord}_J(\mathbf{L}) = e_1 + 2e_2 = \max(r^+, r^-) - 1. \tag{2}$$

Since the left-hand side of (1) is $1 + 2e_1 + 2e_2$ by Mazur's control theorem, one expects equality to hold there exactly when $e_2 = 0$.

The following conventions will remain in effect throughout. By a coefficient ring, R, we mean a complete, Noetherian, local ring with finite residue field of characteristic p. The cases of interest are when R is the ring of integers $\mathcal{O}$ of a finite extension of $\mathbb{Q}_p$, a quotient of $\mathcal{O}$, or the Iwasawa algebra Λ. The maximal ideal of R is denoted $\mathfrak{m}$. We denote by $R(1)$ the Tate twist of R, i.e. the free, rank-one R-module on which Galois acts through the cyclotomic character.

If M is any R-module and $I \subset R$ is an ideal then $M[I]$ is the submodule of M consisting of elements annihilated by every $r \in I$. We define $M(1) = M \otimes_R R(1)$. If L is a perfect field (which is all we shall ever have need to consider), then $\bar{L}$ denotes the algebraic closure of L, and $G_L = \mathrm{Gal}(\bar{L}/L)$. If L is a local field we let L^{unr} denote the maximal unramified extension of L and denote by Fr the Frobenius automorphism of L^{unr}/L.

1. Kolyvagin systems

Throughout § 1 we fix a coefficient ring R and a quadratic imaginary field K. If L is a perfect field, we denote by $\mathrm{Mod}_{R,L}$ the category of finitely generated R-modules equipped with continuous, linear actions of G_L, assumed to be unramified outside of a finite set of primes in the case where L is a global field. The letter T will always denote an object of this category (for some field L). Let $\tau \in G_{\mathbb{Q}}$ be a fixed complex conjugation.

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Sections 1.1, 1.2, and 1.3 follow [MR04] very closely. Sections 1.5 and 1.6 do as well, but with modifications unique to the case of Heegner points. The results of § 1.4, which rely crucially on the self-duality of the Tate module $T_p(E)$, have no analogue in [MR04].

1.1 Selmer groups

Fix a finite place v of K, and denote by $\mathcal{I}_v$ the inertia subgroup of G_{K_v}, $\mathrm{Fr}_v \in \mathrm{Gal}(K_v^{\mathrm{unr}}/K_v)$ the Frobenius element, and $\mathbf{k}_v$ the residue field of K_v. Let T be an object of Mod_{R,K_v}.

Definition 1.1.1. A *local condition* on T (over K_v) is a choice of R-submodule of $H^1(K_v,T)$. We will frequently use $\mathcal{F}$ to denote a local condition, in which case the submodule will be denoted $H^1_{\mathcal{F}}(K_v,T) \subset H^1(K_v,T)$.

Given an $R[[G_{K_v}]]$-submodule (respectively quotient) S of T and a local condition $\mathcal{F}$ on T we define the *propagated* condition, still denoted by $\mathcal{F}$, on S to be the preimage (respectively image) of $H^1_{\mathcal{F}}(K_v,T)$ under the natural map

$$H^1(K_v,S) \to H^1(K_v,T)$$

(respectively $H^1(K_v,T) \to H^1(K_v,S)$).

We will be concerned primarily (but not entirely) with local conditions of the following types:

a) the *relaxed* and *strict* conditions (respectively)

$$H^1_{\mathrm{rel}}(K_v,T) = H^1(K_v,T), \quad H^1_{\mathrm{str}}(K_v,T) = 0,$$

b) the *unramified* condition

$$H^1_{\mathrm{unr}}(K_v,T) = \ker(H^1(K_v,T) \to H^1(K_v^{\mathrm{unr}},T)),$$

c) the *L-transverse* condition

$$H^1_{L\text{-tr}}(K_v,T) = \ker(H^1(K_v,T) \to H^1(L,T)),$$

where K_v has residue characteristic $\neq p$ and L is a maximal totally tamely ramified abelian p-extension of K_v.

If K_v has residue characteristic different from p and T is unramified (i.e. the inertia group $\mathcal{I}_v$ acts trivially on T), then we shall also refer to the unramified condition on T as the *finite* condition $H^1_{\mathrm{f}}(K_v,T)$. We then define the *singular quotient* $H^1_{\mathrm{s}}(K_v,T)$ by exactness of

$$0 \to H^1_{\mathrm{f}}(K_v,T) \to H^1(K_v,T) \to H^1_{\mathrm{s}}(K_v,T) \to 0.$$

If $\mathcal{T}$ is a subcategory of Mod_{R,K_v} then by a *local condition functorial over* $\mathcal{T}$ we mean a subfunctor of $H^1(K_v,\ \ )$,

$$T \mapsto H^1_{\mathcal{F}}(K_v,T) \subset H^1(K_v,T).$$

The local conditions defined above are all functorial over Mod_{R,K_v}.

Definition 1.1.2. A local condition $\mathcal{F}$ functorial over a subcategory $\mathcal{T}$ of Mod_{R,K_v} is *cartesian* if for any injective morphism $\alpha : S \to T$ the local condition $\mathcal{F}$ on S is the same as the local condition obtained by propagating $\mathcal{F}$ from T to S.

Definition 1.1.3. For T an object of Mod_{R,K_v} we define the *quotient category* of T, $\mathrm{Quot}(T)$, to be the category whose objects are quotients T/IT of T by ideals of R and the morphisms from T/IT to T/JT are the maps induced by scalar multiplications $r \in R$ with $rI \subset J$.

Any local condition on T defines a local condition functorial over $\mathrm{Quot}(T)$ by propagation.

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Remark 1.1.4. Of special interest is the case where R is principal and Artinian of length k and T is a free R-module. Let $\mathfrak{m} = \pi R$ be the maximal ideal of R. A local condition on $\mathrm{Quot}(T)$ being cartesian implies that for $i < k$ the local condition on the submodule $T[\mathfrak{m}^i]$ (propagated from T) agrees with the local condition on $T/\mathfrak{m}^i T$ when the two modules are identified via the isomorphism

$$T/\mathfrak{m}^i T \xrightarrow{\pi^{k-i}} T[\mathfrak{m}^i].$$

Lemma 1.1.5. *The unramified local condition is cartesian on any subcategory of* Mod_{R,K_v} *whose objects are unramified* G_{K_v}*-modules.*

Proof. This is Lemma 1.1.9 of [MR04]. □

Definition 1.1.6. Set $T^* = \mathrm{Hom}(T, R(1))$. We give T^* the structure of a G_{K_v}-module by letting $\sigma \in G_{K_v}$ act on $f(t)$ by $f(t) \mapsto \sigma f(\sigma^{-1}t)$. Local Tate duality gives a perfect R-bilinear pairing

$$\langle , \rangle : H^1(K_v, T) \times H^1(K_v, T^*) \to H^2(K_v, R(1)) \xrightarrow{\mathrm{inv}} R,$$

and for any local condition $\mathcal{F}$ on T we define the *dual local condition*, $\mathcal{F}^*$, on T^* to be the orthogonal complement of $\mathcal{F}$ under the above local pairing.

Proposition 1.1.7. *Assume that* v *does not divide* p*, that* T *is unramified at* v*, and that* $|\mathbf{k}_v^\times| \cdot T = 0$*. There are canonical isomorphisms*

$$H^1_{\mathrm{f}}(K_v, T) \cong T/(\mathrm{Fr}_v - 1)T, \quad H^1_{\mathrm{s}}(K_v, T) \otimes \mathbf{k}_v^\times \cong T^{\mathrm{Fr}_v = 1}.$$

Proof. This is Lemma 1.2.1 of [MR04]. The first map is given on cocycles by evaluation at the Frobenius automorphism, and the second by $c \otimes \alpha \mapsto c(\sigma_\alpha)$ where $\sigma_\alpha \in \mathrm{Gal}(K_v^{\mathrm{ab}}/K_v^{\mathrm{unr}})$ is the Artin symbol of any lift of α to K. □

Definition 1.1.8. If v does not divide p, G_{K_v} acts trivially on T, and $|\mathbf{k}_v^\times| \cdot T = 0$, we define the *finite-singular comparison map* to be the isomorphism

$$\phi_v^{\mathrm{fs}} : H^1_{\mathrm{f}}(K_v, T) \cong T \cong H^1_{\mathrm{s}}(K_v, T) \otimes \mathbf{k}_v^\times$$

given by Proposition 1.1.7.

Proposition 1.1.9. *Keep the assumptions of Definition 1.1.8. We fix a maximal totally tamely ramified abelian* p*-extension* L/K_v*, and hence a choice of* L*-transverse condition on* T*. The transverse submodule* $H^1_{\mathrm{tr}}(K_v, T)$ *projects isomorphically onto* $H^1_{\mathrm{s}}(K_v, T)$ *giving a splitting*

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

Furthermore, under the local Tate pairing

a) $H^1_{\mathrm{f}}(K_v, T)$ *and* $H^1_{\mathrm{f}}(K_v, T^*)$ *are exact orthogonal complements,*

b) $H^1_{\mathrm{tr}}(K_v, T)$ *and* $H^1_{\mathrm{tr}}(K_v, T^*)$ *are exact orthogonal complements.*

Proof. These statements are Lemma 1.2.4 and Proposition 1.3.2 of [MR04]. □

We now consider global cohomology groups. Fix an object T of $\mathrm{Mod}_{R,K}$.

Definition 1.1.10. By a *Selmer structure* $\mathcal{F}$ on T (over K) we mean a finite set of places $\Sigma(\mathcal{F})$ of K containing p, all archimedean places, and all places at which T is ramified, and for each $v \in \Sigma(\mathcal{F})$ a choice of local condition $H^1_{\mathcal{F}}(K_v, T)$. Given a Selmer structure $\mathcal{F}$ on T we define the associated *Selmer module*

$$H^1_{\mathcal{F}}(K, T) \subset H^1(K, T)$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

to be the kernel of

$$H^1(K_{\Sigma(\mathcal{F})}/K,T) \to \bigoplus_{v\in\Sigma(\mathcal{F})} H^1(K_v,T)/H^1_{\mathcal{F}}(K_v,T),$$

where $K_{\Sigma(\mathcal{F})}$ is the maximal extension of K unramified away from the places of $\Sigma(\mathcal{F})$.

Given a Selmer structure $\mathcal{F}$ we will usually write $H^1_{\mathcal{F}}(K_v,T)$ for $H^1_{\mathrm{f}}(K_v,T)$ for a prime $v\notin\Sigma(\mathcal{F})$. Then $H^1_{\mathcal{F}}(K,T)$ is nothing more than the set of classes in $H^1(K,T)$ whose localization lives in $H^1_{\mathcal{F}}(K_v,T)$ at every place v. There is a natural partial ordering on the set of all Selmer structures, namely we write $\mathcal{F}\leqslant\mathcal{G}$ if and only if $H^1_{\mathcal{F}}(K_v,T)\subset H^1_{\mathcal{G}}(K_v,T)$ for every place v of K. Clearly if $\mathcal{F}\leqslant\mathcal{G}$ we have $H^1_{\mathcal{F}}(K,T)\subset H^1_{\mathcal{G}}(K,T)$. If $\mathcal{F}$ is a Selmer structure on T then the collection of dual local conditions gives a Selmer structure $\mathcal{F}^*$ on T^* with $\Sigma(T)=\Sigma(T^*)$. The following theorem is the fundamental tool which turns Kolyvagin systems into bounds on Selmer groups.

Theorem 1.1.11 (Poitou–Tate global duality). *Suppose $\mathcal{F}\leqslant\mathcal{G}$ are Selmer structures on T. There are exact sequences*

$$0\to H^1_{\mathcal{F}}(K,T)\to H^1_{\mathcal{G}}(K,T)\xrightarrow{\mathrm{loc}}\bigoplus_v H^1_{\mathcal{G}}(K_v,T)/H^1_{\mathcal{F}}(K_v,T),$$

$$0\to H^1_{\mathcal{G}^*}(K,T^*)\to H^1_{\mathcal{F}^*}(K,T^*)\xrightarrow{\mathrm{loc}}\bigoplus_v H^1_{\mathcal{F}^*}(K_v,T^*)/H^1_{\mathcal{G}^*}(K_v,T^*),$$

and the images of the rightmost arrows are exact orthogonal complements under the sum of the local pairings of Definition 1.1.6.

Proof. See [Mil86, I.4.10] or [Rub00, 1.7.3]. □

1.2 Kolyvagin systems

Let T be an object of $\mathrm{Mod}_{R,K}$, and denote by $\mathcal{L}_0=\mathcal{L}_0(T)$ the set of degree-two primes of K which do not divide p or any prime at which T is ramified. We will consistently confuse a prime of $\mathcal{L}_0$ with the rational prime below it, and if the distinction needs to be made we will write $\ell|\lambda\in\mathcal{L}_0$ to indicate that ℓ is the rational prime and λ the prime of K.

Definition 1.2.1.

a) For each $\ell|\lambda\in\mathcal{L}_0$, define I_ℓ to be the smallest ideal of R containing $\ell+1$ for which Fr_λ acts trivially on $T/I_\ell T$.
b) For every $k\in\mathbb{Z}^+$ define $\mathcal{L}_k=\mathcal{L}_k(T)=\{\ell\in\mathcal{L}_0\mid I_\ell\subset p^k\mathbb{Z}_p\}$.
c) For $\ell|\lambda\in\mathcal{L}_0$ let $G_\ell=\mathbf{k}_\lambda^\times/\mathbf{k}_\ell^\times$ where $\mathbf{k}_\ell$ and $\mathbf{k}_\lambda$ are the residue fields of ℓ and λ, respectively.
d) Let $\mathcal{N}_k$ denote the set of square-free products of primes of $\mathcal{L}_k$. For $n\in\mathcal{N}_0$ define

$$I_n=\sum_{\ell|n} I_\ell\subset R,\quad G_n=\bigotimes_{\ell|n} G_\ell.$$

By convention $1\in\mathcal{N}_k$ for every k, $I_1=0$, and $G_1=\mathbb{Z}$.

For $\ell|\lambda\in\mathcal{L}_0$ we denote by $K[\ell]$ the ring class field of conductor ℓ. Since λ splits completely in the Hilbert class field of K, the maximal p-subextension of the local extension $K[\ell]_\lambda/K_\lambda$ (call it L) is a maximal totally tamely ramified abelian p-extension of K_λ whose Galois group is canonically identified with the p-Sylow subgroup of G_ℓ by class field theory. For such a λ we therefore have a canonical choice of L-transverse condition as in § 1.1, which we denote by $H^1_{\mathrm{tr}}(K_\ell,T)$.

By a *Selmer triple* $(T,\mathcal{F},\mathcal{L})$ we mean an object T of $\mathrm{Mod}_{R,K}$, a choice of Selmer structure $\mathcal{F}$ on T, and a (typically infinite) subset $\mathcal{L}\subset\mathcal{L}_0$ which is disjoint from $\Sigma(\mathcal{F})$. We define $\mathcal{N}=\mathcal{N}(\mathcal{L})$ to be the set of square-free products of primes of $\mathcal{L}$, with the convention that $1\in\mathcal{N}(\mathcal{L})$.

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Definition 1.2.2. Given a Selmer triple $(T,\mathcal{F},\mathcal{L})$ and $abc\in\mathcal{N}(\mathcal{L})$ we define a new Selmer triple $(T,\mathcal{F}_b^a(c),\mathcal{L}(abc))$ by taking $\Sigma(\mathcal{F}_b^a(c))$ to be $\Sigma(\mathcal{F})$ together with all prime divisors of abc, and taking $\mathcal{L}(abc)$ to be $\mathcal{L}$ with all prime divisors of abc removed. At any place λ of K define the local condition $\mathcal{F}_b^a(c)$ to be

$$H^1_{\mathcal{F}_b^a(c)}(K_\lambda,T)=\begin{cases}H^1_{\mathrm{rel}}(K_\lambda,T) & \text{if } \lambda|a,\\ H^1_{\mathrm{str}}(K_\lambda,T) & \text{if } \lambda|b,\\ H^1_{\mathrm{tr}}(K_\lambda,T) & \text{if } \lambda|c,\end{cases}$$

and retain the original local condition

$$H^1_{\mathcal{F}_b^a(c)}(K_\lambda,T)=H^1_{\mathcal{F}}(K_\lambda,T)$$

if λ does not divide abc. If any one of a, b, or c is 1 we omit it from the notation.

For any $n\ell\in\mathcal{N}_0$, we may identify the p-Sylow subgroups of G_ℓ and $\mathbf{k}_\lambda^\times/\mathbf{k}_\ell^\times$ via the Artin symbol, and let

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

be the finite-singular comparison map at ℓ. We have maps as follows.

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

Definition 1.2.3. Given a Selmer triple $(T,\mathcal{F},\mathcal{L})$ we define a *Kolyvagin system* κ for $(T,\mathcal{F},\mathcal{L})$ to be a collection of cohomology classes

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

one for each $n\in\mathcal{N}(\mathcal{L})$, such that for any $n\ell\in\mathcal{N}(\mathcal{L})$ the images of κ_n and $\kappa_{n\ell}$ in $H^1_{\mathrm{s}}(K_\ell,T/I_{n\ell}T)\otimes G_{n\ell}$ under the maps of (3) agree. We denote the R-module of all Kolyvagin systems for $(T,\mathcal{F},\mathcal{L})$ by $\mathbf{KS}(T,\mathcal{F},\mathcal{L})$.

Remark 1.2.4. The module of Kolyvagin systems has the following functorial properties:

a) if $\mathcal{L}'\subset\mathcal{L}$ then there is a map $\mathbf{KS}(T,\mathcal{F},\mathcal{L})\to\mathbf{KS}(T,\mathcal{F},\mathcal{L}')$;

b) if $H^1_{\mathcal{F}}(K_v,T)\subset H^1_{\mathcal{G}}(K_v,T)$ at every place v then there is a map

$$\mathbf{KS}(T,\mathcal{F},\mathcal{L})\to\mathbf{KS}(T,\mathcal{G},\mathcal{L});$$

c) if $R\to R'$ is a ring homomorphism then there is a map

$$\mathbf{KS}(T,\mathcal{F},\mathcal{L})\otimes_R R'\to\mathbf{KS}(T\otimes_R R',\mathcal{F}\otimes_R R',\mathcal{L})$$

where the local condition $\mathcal{F}\otimes_R R'$ is defined as the image of

$$H^1_{\mathcal{F}}(K_v,T)\otimes_R R'\to H^1(K_v,T\otimes_R R')$$

for $v\in\Sigma(\mathcal{F})$, and $\Sigma(\mathcal{F}\otimes_R R')=\Sigma(\mathcal{F})$.

1.3 Hypotheses

In this subsection R is a coefficient ring and T is an object of Mod_{R,G_K}. The maximal ideal of R is denoted $\mathfrak{m}$, and $\bar{T}=T/\mathfrak{m}T$ is the residual representation of T. We denote by $\mathrm{Tw}(T)$ the G_K-module

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

whose underlying R-module is T and on which G_K acts through the automorphism conjugation by τ. The identity map on the underlying R-modules $T \to \mathrm{Tw}(T)$ and the automorphism of G_K given by conjugation by τ induce a 'change of group' $(G_K, T) \rightsquigarrow (G_K, \mathrm{Tw}(T))$ which induces an isomorphism on cohomology

$$H^i(K, T) \cong H^i(K, \mathrm{Tw}(T)).$$

Similarly at any place v of K conjugation by τ induces an isomorphism

$$H^i(K_{\bar{v}}, T) \cong H^i(K_v, \mathrm{Tw}(T))$$

where $\bar{v} = v^\tau$.

We fix a Selmer triple $(T, \mathcal{F}, \mathcal{L})$ and record some desirable hypotheses which it may satisfy.

H.0) T is a free, rank-two R-module.

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

H.2) There is a Galois extension $F/\mathbb{Q}$ such that $K \subset F$, G_F acts trivially on T, and

$$H^1(F(\mu_{p^\infty})/K, \bar{T}) = 0.$$

H.3) For every $v \in \Sigma(\mathcal{F})$ the local condition $\mathcal{F}$ at v is cartesian on the category $\mathrm{Quot}(T)$ (see Definitions 1.1.2 and 1.1.3).

H.4) There is a perfect, symmetric, R-bilinear pairing

$$(\ ,\ ) : T \times T \to R(1)$$

which satisfies $(s^\sigma, t^{\tau\sigma\tau^{-1}}) = (s, t)^\sigma$ for every $s, t \in T$ and $\sigma \in G_K$. Equivalently there is a G_K-invariant pairing

$$T \times \mathrm{Tw}(T) \to R(1)$$

which is symmetric when the underlying group of $\mathrm{Tw}(T)$ is identified with that of T. We assume that the local condition $\mathcal{F}$ is its own exact orthogonal complement under the induced local pairing

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

for every place v of K.

H.5) a) The action of G_K on $\bar{T}$ extends to an action of $G_{\mathbb{Q}}$ and the action of τ splits $\bar{T} = \bar{T}^+ \oplus \bar{T}^-$ into one-dimensional eigenspaces.

b) The condition $\mathcal{F}$ propagated to $\bar{T}$ is stable under the action of $G_{\mathbb{Q}}$.

c) If hypothesis H.4 is assumed to hold then the residual pairing

$$\bar{T} \times \bar{T} \to (R/\mathfrak{m})(1)$$

satisfies $(s^\tau, t^\tau) = (s, t)^\tau$ for all $s, t \in T$.

While hypotheses H.0–H.3 are similar to hypotheses used in [MR04], hypothesis H.4, the self-duality of T (up to a twist), is not used by those authors, but plays an essential role here. Hypothesis H.5 is made to overcome a technical difficulty: in the applications to Iwasawa theory, we will want to deal with $T = T_p(E) \otimes \Lambda$, where $E_{/\mathbb{Q}}$ is an elliptic curve and Λ is the Iwasawa algebra associated to the anticyclotomic $\mathbb{Z}_p$-extension of K. The natural action of G_K on $T_p(E) \otimes \Lambda$ does not extend naturally to an action of $G_{\mathbb{Q}}$, but the action on the residual representation does.

We remark that the choice of $\mathcal{L}$ plays no role in any of the hypotheses. Hypothesis H.3 implies that the local condition $\mathcal{F}$ is cartesian on $\mathrm{Quot}(T)$ at every place of K by Lemma 1.1.5. When hypothesis H.4 holds, it can be shown that the local pairing

$$H^1(K_\lambda, T) \times H^1(K_\lambda, T) \to R$$

at any degree-two prime λ of K is symmetric.

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Remark 1.3.1. It is easily seen that hypotheses H.0–H.5 are stable under base change in the obvious sense. See Remark 1.2.4.

Remark 1.3.2. The reader who is puzzled by the pairing of hypothesis H.4 would do well to keep the following example in mind. If $R = \mathbb{Z}_p$, T is the p-adic Tate module of an elliptic curve over $\mathbb{Q}$, and $e : T \times T \to \mathbb{Z}_p(1)$ is the Weil pairing, then the pairing $(s,t) = e(s,t^\tau)$ has the desired properties. The function $t \mapsto t^\tau$ defines a G_{K_v}-module isomorphism $\mathrm{Tw}(T) \to T$ such that the composition of isomorphisms

$$H^1(K_{\bar{v}}, T) \to H^1(K_v, \mathrm{Tw}(T)) \to H^1(K_v, T)$$

is the usual action of complex conjugation. Using this identification the local pairing of hypothesis H.4 is exactly the usual local Tate pairing.

More generally, whenever the action of G_K on T extends to an action of $G_{\mathbb{Q}}$, the existence of a pairing of the type described in hypothesis H.4 is equivalent to the existence of a skew-symmetric, Galois-equivariant pairing on T. As noted above, in the applications to Iwasawa theory we will want to deal with modules for which the action does not extend.

Lemma 1.3.3. *Suppose R is principal and Artinian of length k, and that hypotheses H.1 and H.3 hold. If $0 \leqslant i \leqslant k$ and π is a generator of $\mathfrak{m}$, then the maps*

$$T/\mathfrak{m}^i T \xrightarrow{\pi^{k-i}} T[\mathfrak{m}^i] \to T$$

induce isomorphisms

$$H^1_{\mathcal{F}}(K, T/\mathfrak{m}^i T) \to H^1_{\mathcal{F}}(K, T[\mathfrak{m}^i]) \to H^1_{\mathcal{F}}(K,T)[\mathfrak{m}^i].$$

Proof. See Remark 1.1.4 above, and Lemma 3.5.4 of [MR04]. □

1.4 The Cassels–Tate pairing

In this subsection we construct a generalized form of the Cassels–Tate pairing. Our exposition closely follows that of [Fla90]. See also [Guo93] and [Mil86].

Let R be a principal Artinian coefficient ring of length k and T an object of Mod_{R,G_K}. Fix a generator π of the maximal ideal $\mathfrak{m}$ of R. Let $T^* = \mathrm{Hom}(T, R(1))$ and fix a Selmer structure $\mathcal{F}$ on T. Let $\mathcal{F}^*$ denote the dual Selmer structure on T^*. In all that follows we assume that $(T, \mathcal{F})$ and $(T^*, \mathcal{F}^*)$ satisfy hypotheses H.0–H.5.

At every place v of K set

$$H^1_{/\mathcal{F}}(K_v, T) = H^1(K_v, T)/H^1_{\mathcal{F}}(K_v, T)$$

and similarly for T^*. Hypothesis H.3 implies that for any positive integers s and t with $s + t \leqslant k$, and any place v of K, there are exact sequences

$$0 \to H^1_{/\mathcal{F}}(K_v, T/\mathfrak{m}^t T) \xrightarrow{\xi} H^1_{/\mathcal{F}}(K_v, T/\mathfrak{m}^{s+t}T) \to H^1_{/\mathcal{F}}(K_v, T/\mathfrak{m}^s T), \tag{4}$$

$$H^1_{\mathcal{F}^*}(K_v, T^*[\mathfrak{m}^s]) \to H^1_{\mathcal{F}^*}(K_v, T^*[\mathfrak{m}^{s+t}]) \xrightarrow{\xi} H^1_{\mathcal{F}^*}(K_v, T^*[\mathfrak{m}^t]) \to 0, \tag{5}$$

where the arrows labeled ξ are induced by $\pi^s : T \to T$.

We want to construct a pairing

$$H^1_{\mathcal{F}}(K, T/\mathfrak{m}^s T) \times H^1_{\mathcal{F}^*}(K, T^*[\mathfrak{m}^t]) \to R$$

for any positive integers s and t with $s + t \leqslant k$. Suppose we are given classes in $H^1_{\mathcal{F}}(K, T/\mathfrak{m}^s T)$ and $H^1_{\mathcal{F}^*}(K, T^*[\mathfrak{m}^t])$ represented by cocycles

$$a \in Z^1(K, T/\mathfrak{m}^s T), \quad b \in Z^1(K, T^*[\mathfrak{m}^t]).$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

We will repeatedly use the fact that for any topological group G the continuous cochain functor $C^i(G,\ \ )$ from R-modules to R-modules is exact, and so in particular we have surjective maps

$$C^1(K,T/\mathfrak{m}^{s+t}T) \to C^1(K,T/\mathfrak{m}^sT), \quad C^1(K,T^*[\mathfrak{m}^{s+t}]) \xrightarrow{\pi^s} C^1(K,T^*[\mathfrak{m}^t]).$$

Choose cochains $\alpha \in C^1(K,T/\mathfrak{m}^{s+t}T)$ and $\beta \in C^1(K,T^*[\mathfrak{m}^{s+t}])$ which map to a and b respectively. Let d be the coboundary operator. From $\pi^s\, d\beta = db$ it follows that $d\beta$ is killed by π^s, and similarly $d\alpha$ reducing to zero in $C^2(K,T/\mathfrak{m}^sT)$ implies that $d\alpha$ is divisible by π^s in $C^2(K,T/\mathfrak{m}^{s+t}T)$. Therefore $d\alpha \cup d\beta = 0$ and

$$d(d\alpha \cup \beta) = d^2\alpha \cup \beta + d\alpha \cup d\beta = 0,$$

so that $d\alpha \cup \beta$ lives in $Z^3(K,R(1))$ (we view the cup product as taking values in $R(1)$-valued cochains using the natural pairing $T \otimes T^* \to R(1)$). By Theorem I.4.10 of [Mil86], $H^3(K,R(1)) = 0$, and so there is an $\epsilon \in C^2(K,R(1))$ with

$$d\epsilon = d\alpha \cup \beta.$$

By the exact sequence (5) there is a $\beta_v' \in Z^1_{\mathcal{F}^*}(K_v,T^*[\mathfrak{m}^{s+t}])$ such that $\pi^s\beta_v' = b_v$, where $Z^1_{\mathcal{F}^*}(K_v,T^*[\mathfrak{m}^{s+t}]) \subset Z^1(K_v,T^*[\mathfrak{m}^{s+t}])$ is the preimage of $H^1_{\mathcal{F}^*}(K_v,T^*[\mathfrak{m}^t])$ under multiplication by π^s. The cochain $\alpha_v \cup \beta_v' - \epsilon_v \in C^2(K_v,R(1))$ is in fact a coboundary, and we define the pairing

$$(a,b)_{s,t} = \sum_v \mathrm{inv}_v(\alpha_v \cup \beta_v' - \epsilon_v). \tag{6}$$

It can be checked that this is independent of all choices made.

Proposition 1.4.1. *For positive integers s and t with $s+t \leqslant k$ there is a pairing*

$$(\ ,\ )_{s,t} : H^1_{\mathcal{F}}(K,T/\mathfrak{m}^sT) \times H^1_{\mathcal{F}^*}(K,T^*[\mathfrak{m}^t]) \to R$$

whose kernels on the left and right are the images of

$$H^1_{\mathcal{F}}(K,T/\mathfrak{m}^{s+t}T) \to H^1_{\mathcal{F}}(K,T/\mathfrak{m}^sT),$$
$$H^1_{\mathcal{F}^*}(K,T^*[\mathfrak{m}^{s+t}]) \xrightarrow{\pi^s} H^1_{\mathcal{F}^*}(K,T^*[\mathfrak{m}^t]).$$

Proof. The construction of the pairing is above. The computation of the kernels is a straightforward modification of the methods of [Fla90]. □

Theorem 1.4.2. *There is an R-module M and an integer ϵ such that*

$$H^1_{\mathcal{F}}(K,T) \cong R^\epsilon \oplus M \oplus M.$$

By the structure theorem for finitely generated modules over R, we may assume $\epsilon \in \{0,1\}$.

Proof. Abbreviate $\mathcal{H} = H^1_{\mathcal{F}}(K,T)$, and for $1 \leqslant s < k$ define

$$V_s = \mathcal{H}[\mathfrak{m}^s]/\mathfrak{m}\mathcal{H}[\mathfrak{m}^{s+1}], \quad W_s = \mathcal{H}[\mathfrak{m}]/\mathfrak{m}^s\mathcal{H}[\mathfrak{m}^{s+1}].$$

We claim that for $0 \leqslant s < k$, the $R/\mathfrak{m}$-vector space V_s is even dimensional. The theorem then follows easily from this and the structure theorem for finitely generated R-modules.

There is an exact sequence

$$0 \to V_{s-1} \to V_s \xrightarrow{\pi^{s-1}} W_s.$$

Using hypothesis H.4 and Lemma 1.3.3, we may identify

$$H^1_{\mathcal{F}^*}(K,T^*[\mathfrak{m}]) \cong H^1_{\mathcal{F}}(K,T[\mathfrak{m}]) \cong \mathcal{H}[\mathfrak{m}]$$

and

$$H^1_{\mathcal{F}}(K,T/\mathfrak{m}^sT) \cong \mathcal{H}[\mathfrak{m}^s].$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Proposition 1.4.1 therefore gives a nondegenerate pairing of $R/\mathfrak{m}$-vector spaces

$$(\ ,\ )_{s,1} : V_s \times W_s \cong \mathcal{H}[\mathfrak{m}^s]/\mathfrak{m}\mathcal{H}[\mathfrak{m}^{s+1}] \times \mathcal{H}[\mathfrak{m}]/\mathfrak{m}^s\mathcal{H}[\mathfrak{m}^{s+1}] \to R[m].$$

We define a pairing

$$\langle\ ,\ \rangle : V_s \times V_s \to R[m]$$

by $\langle a, b\rangle = (a, \pi^{s-1}b)_{s,1}$. The kernel on the right is V_{s-1}. If we can show that this pairing is alternating, then V_s/V_{s-1} is even dimensional for every $1 \leqslant s < k$, and the theorem follows. To check that this is alternating we must verify

$$(a, \pi^{s-1}b)_{s,1} = -(b, \pi^{s-1}a)_{s,1}.$$

We denote by $\phi : T \to \mathrm{Tw}(T)$ the identity map on underlying groups and by ψ the change of group isomorphisms

$$(G_K, T) \to (G_K, \mathrm{Tw}(T)), \quad (G_{K_v}, T) \to (G_{K_{\bar{v}}}, \mathrm{Tw}(T))$$

of § 1.3. We also denote by ψ the induced map on cochains and cohomology. Fix α and β in $C^1(F, T[\mathfrak{m}^{s+1}])$ with $\pi\alpha = a$ and $\pi\beta = b$, and choose ϵ_1 and ϵ_2 in $C^2(F, R(1))$ satisfying

$$d\alpha \cup \psi(\beta) = d\epsilon_1, \quad d\beta \cup \psi(\alpha) = d\epsilon_2$$

and for every place v of F elements α'_v and β'_v in $H^1_{\mathcal{F}}(F_v, T[\mathfrak{m}^{s+1}])$ which map to a_v and b_v under multiplication by π. Then

$$(a, \pi^{s-1}b)_{s,1} = \sum_v \mathrm{inv}_v(\alpha_v \cup \psi(\beta'_{\bar{v}}) - \epsilon_{1,v}),$$
$$(b, \pi^{s-1}a)_{s,1} = \sum_v \mathrm{inv}_v(\beta_v \cup \psi(\alpha'_{\bar{v}}) - \epsilon_{2,v}),$$

where unprimed cochains are localizations of global cochains, and primed cochains are (typically) not. Both $\alpha_v - \alpha'_v$ and $\beta_v - \beta'_v$ lie in $C^1(F_v, T[\mathfrak{m}])$, and so

$$(\alpha_v - \alpha'_v) \cup \psi(\beta_{\bar{v}} - \beta'_{\bar{v}}) = 0,$$

which implies

$$\alpha_v \cup \psi(\beta_{\bar{v}}) + \alpha'_v \cup \psi(\beta'_{\bar{v}}) = \alpha_v \cup \psi(\beta'_{\bar{v}}) + \alpha'_v \cup \psi(\beta_{\bar{v}}). \tag{7}$$

Given a topological group G, if $\mathcal{R}^*$ is the standard resolution of $\mathbb{Z}$ by projective G-modules, then one can form the tensor square resolution $\mathcal{R}^* \otimes \mathcal{R}^*$. For a topological G-module M denote by $CC^*(G, M)$ the cochain complex $\mathrm{Hom}(\mathcal{R}^* \otimes \mathcal{R}^*, M)$ of continuous homomorphisms. The cohomology of CC^* agrees with the usual continuous cohomology (see [Fla90]) and the automorphism ρ of CC^* induced by the automorphism $r_1 \otimes r_2 \mapsto r_2 \otimes r_1$ of $\mathcal{R}^* \otimes \mathcal{R}^*$ induces the identity on cohomology. It follows from [Bro82, V.3.6] that there is a commutative diagram of complexes

$$\begin{array}{ccccc}
C^*(K_v, T) \otimes C^*(K_v, \mathrm{Tw}(T)) & \xrightarrow{\cup} & CC^*(K_v, T \otimes \mathrm{Tw}(T)) & \longrightarrow & CC^*(K_v, R(1)) \\
\downarrow{\scriptstyle s} & & \downarrow{\scriptstyle (\rho,\mathrm{tr})} & & \downarrow{\scriptstyle \rho} \\
C^*(K_v, \mathrm{Tw}(T)) \otimes C^*(K_v, T) & \xrightarrow{\cup} & CC^*(K_v, \mathrm{Tw}(T) \otimes T) & \longrightarrow & CC^*(K_v, R(1)) \\
\downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle -\tau} \\
C^*(K_{\bar{v}}, T) \otimes C^1(K_{\bar{v}}, \mathrm{Tw}(T)) & \xrightarrow{\cup} & CC^*(K_{\bar{v}}, T \otimes \mathrm{Tw}(T)) & \longrightarrow & CC^*(K_{\bar{v}}, R(1))
\end{array}$$

in which $\mathrm{tr} : T \otimes \mathrm{Tw}(T) \to \mathrm{Tw}(T) \otimes T$ takes $t_1 \otimes t_2$ to $t_2 \otimes t_1$, s is the map

$$a \otimes b \to (-1)^{\deg(a)\deg(b)} b \otimes a,$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

and τ is the change of group $(G_{K_v}, R(1)) \to (G_{K_{\bar{v}}}, R(1))$ which is conjugation by τ on the groups and action by τ on $R(1)$. Commutativity of the bottom right square follows from the symmetry $(t_1, \phi(t_2)) = (t_2, \phi(t_1))$ of the pairing of hypothesis H.4. The upshot of the diagram is the relation

$$x \cup \psi(y) = (-1)^{\deg(x)\deg(y)+1}(y \cup \psi(x))^{\tau}, \tag{8}$$

where x and y are in $C^*(K_v, T)$ and $C^*(K_{\bar{v}}, T)$, respectively. There is a similar global diagram obtained by ignoring all the v and $\bar{v}$, and the relation (8) holds for $x, y \in C^*(K, T)$.

From (7) we now deduce

$$(\alpha \cup \psi(\beta) - \epsilon_1 - (\epsilon_2)^{\tau})_v + \alpha'_v \cup \psi(\beta'_{\bar{v}}) = \alpha_v \cup \psi(\beta'_{\bar{v}}) - \epsilon_{1,v} + \alpha'_v \cup \psi(\beta_{\bar{v}}) - (\epsilon_{2,\bar{v}})^{\tau}. \tag{9}$$

It follows from (8) and the definition of ϵ_i that $\alpha \cup \psi(\beta) - \epsilon_1 + (\epsilon_2)^{\tau}$ is a 2-cocycle, and so by the reciprocity law of class field theory the sum of its local invariants is zero. The local invariant of $\alpha'_v \cup \psi(\beta'_{\bar{v}})$ is zero by the assumption that $\mathcal{F}$ is everywhere self-orthogonal under the local pairing. Again using (8) we obtain

$$\sum_v \mathrm{inv}_v(\alpha_v \cup \psi(\beta'_{\bar{v}}) - \epsilon_{1,v}) = -\sum_v \mathrm{inv}_v((\beta_{\bar{v}} \cup \psi(\alpha'_v) - \epsilon_{2,\bar{v}})^{\tau})$$

and the theorem now follows from Galois invariance of the local invariant map. □

1.5 Modules over principal Artinian rings

Throughout § 1.5 we fix a coefficient ring R which is assumed to be principal and Artinian of length k. Let $(T, \mathcal{F}, \mathcal{L})$ be a Selmer triple satisfying hypotheses H.0–H.5. We assume that $\mathcal{L} \subset \mathcal{L}_k(T)$, so that $I_n R = 0$ for every $n \in \mathcal{N} = \mathcal{N}(\mathcal{L})$. By hypothesis H.0 and Proposition 1.1.7, this implies that the local conditions $H^1_{\mathrm{f}}(K_\lambda, T)$ and $H^1_{\mathrm{tr}}(K_\lambda, T)$ are free rank-two R-modules.

Set $\bar{T} = T/\mathfrak{m}T$, and abbreviate

$$\mathcal{H}^a_b(c) = H^1_{\mathcal{F}^a_b(c)}(K, T), \quad \bar{\mathcal{H}}^a_b(c) = H^1_{\mathcal{F}^a_b(c)}(K, \bar{T}),$$

for $abc \in \mathcal{N} = \mathcal{N}(\mathcal{L})$. For any $c \in H^1(K, T)$ and any place v of K we denote by c_v the image of c in $H^1(K_v, T)$ and by $\langle\ ,\ \rangle_v$ the local Tate pairing

$$H^1(K_v, T) \times H^1(K_{\bar{v}}, T) \to R$$

of hypothesis H.4. For any integer n, $\nu(n)$ denotes the number of prime divisors of n. Recall that $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is a fixed complex conjugation. If M is any $R/\mathfrak{m}$-vector space on which τ acts we denote by M^+ and M^- the subspaces on which τ acts by $+1$ and -1 respectively.

Lemma 1.5.1. *The Selmer triple $(T, \mathcal{F}(n), \mathcal{L}(n))$ satisfies hypotheses H.0–H.5 for any $n \in \mathcal{N}$.*

Proof. See Lemma 3.7.4 of [MR04] for the case of hypothesis H.3. The other cases are trivial. □

Definition 1.5.2. For any $n \in \mathcal{N}$ we let $\rho(n)^{\pm}$ be the $R/\mathfrak{m}$-dimension of $\bar{\mathcal{H}}(n)^{\pm}$, and set $\rho(n) = \rho(n)^+ + \rho(n)^-$.

Lemma 1.5.3. *For any $n\ell \in \mathcal{N}$,*

a) *if $\mathrm{loc}_\ell(\bar{\mathcal{H}}(n)^{\pm}) \neq 0$ then $\rho(n\ell)^{\pm} = \rho(n)^{\pm} - 1$ and $\mathrm{loc}_\ell(\bar{\mathcal{H}}(n\ell)^{\pm}) = 0$,*
b) *if $\mathrm{loc}_\ell(\bar{\mathcal{H}}(n)^{\pm}) = 0$ then $\rho(n\ell)^{\pm} = \rho(n)^{\pm} + 1$.*

In particular this implies that $\rho(n) \pmod 2$ is independent of $n \in \mathcal{N}$.

Proof. Assume that $\mathrm{loc}_\ell(H^1_{\mathcal{F}(n)}(K, \bar{T})^{\pm}) \neq 0$ and consider the exact sequences

$$\begin{aligned} 0 \to H^1_{\mathcal{F}_\ell(n)}(K, \bar{T}) \to H^1_{\mathcal{F}(n)}(K, \bar{T}) \to H^1_{\mathrm{f}}(K_\ell, \bar{T}), \\ 0 \to H^1_{\mathcal{F}(n)}(K, \bar{T}) \to H^1_{\mathcal{F}^\ell(n)}(K, \bar{T}) \to H^1_{\mathrm{s}}(K_\ell, \bar{T}). \end{aligned} \tag{10}$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

By global duality (Theorem 1.1.11) the images of the rightmost arrows are exact orthogonal complements under the $G_{\mathbb{Q}}$-invariant local Tate pairing. Furthermore the action of complex conjugation splits $H^1_{\mathrm{f}}(K_\ell, \bar{T})$ and $H^1_{\mathrm{s}}(K_\ell, \bar{T})$ each into one-dimensional eigenspaces by hypothesis H.5 and the isomorphisms

$$H^1_{\mathrm{f}}(K_\ell, \bar{T}) \cong \bar{T} \cong H^1_{\mathrm{s}}(K_\ell, \bar{T}) \otimes \mathbf{k}^\times$$

of Proposition 1.1.7. It follows that $H^1_{\mathcal{F}(n)}(K, \bar{T})^\pm = H^1_{\mathcal{F}^\ell(n)}(K, \bar{T})^\pm$ and therefore $H^1_{\mathcal{F}_\ell(n)}(K, \bar{T})^\pm = H^1_{\mathcal{F}(\ell n)}(K, \bar{T})^\pm$. This proves part a.

Assume that $\mathrm{loc}_\ell(H^1_{\mathcal{F}(n)}(K, \bar{T})^\pm) = 0$. Again applying global duality to the exact sequences (10) we see that it suffices to show $H^1_{\mathcal{F}^\ell(n)}(K, \bar{T})^\pm = H^1_{\mathcal{F}(n\ell)}(K, \bar{T})^\pm$. If $c \in H^1_{\mathcal{F}^\ell(n)}(K, \bar{T})^\pm$ then the local image of c at ℓ is self-orthogonal under the local pairing. Indeed, the reciprocity law of class field theory and the isotropy of the local conditions $\mathcal{F}(n)$ (by hypothesis H.4) imply

$$\langle c_\ell, c_\ell \rangle_\ell = \sum_v \langle c_v, c_{\bar{v}} \rangle_v = 0,$$

where the sum is over all places of K. Therefore the localization of $H^1_{\mathcal{F}^\ell(n)}(K, \bar{T})^\pm$ at ℓ is a maximal isotropic subspace of $H^1(K_\ell, \bar{T})^\pm$ and an elementary linear algebra exercise shows that the only two such subspaces are $H^1_{\mathrm{f}}(K_\ell, \bar{T})^\pm$ and $H^1_{\mathrm{tr}}(K_\ell, \bar{T})^\pm$. Therefore $H^1_{\mathcal{F}^\ell(n)}(K, \bar{T})^\pm$ is equal to either $H^1_{\mathcal{F}(n)}(K, \bar{T})^\pm$ or $H^1_{\mathcal{F}(n\ell)}(K, \bar{T})^\pm$. Returning to the exact sequences (10) we see that the first possibility contradicts the assumption $\mathrm{loc}_\ell(H^1_{\mathcal{F}(n)}(K, \bar{T})^\pm) = 0$. □

By Theorem 1.4.2 and Lemma 1.5.1, for each $n \in \mathcal{N}$ there is an R-module $M(n)$ and an integer ϵ such that

$$\mathcal{H}(n) \cong R^\epsilon \oplus M(n) \oplus M(n). \tag{11}$$

By the structure theorem for finitely generated modules over R, we can (and do) take $\epsilon \in \{0, 1\}$. It will be seen momentarily that ϵ is independent of n.

Definition 1.5.4. For $n \in \mathcal{N}$, and with notation as in the preceding theorem, we define

a) $\lambda(n) = \mathrm{length}(M(n))$,
b) the *stub Selmer module* $\mathcal{S}(n) = \mathfrak{m}^{\lambda(n)}\mathcal{H}(n)$.

The reader is invited to compare the above definitions with Definitions 4.1.2 and 4.3.1 of [MR04].

Proposition 1.5.5. *The integer ϵ appearing in the decomposition (11) is congruent to $\rho(n) \pmod 2$ and is therefore independent of $n \in \mathcal{N}$ by Lemma 1.5.3.*

Proof. We have

$$\epsilon + 2\dim_{R/\mathfrak{m}} M(n)[\mathfrak{m}] = \dim_{R/\mathfrak{m}} \mathcal{H}(n)[\mathfrak{m}] = \rho(n),$$

the second equality by Lemma 1.3.3. □

Lemma 1.5.6. *For $mn \in \mathcal{N}$, the image of $\mathcal{H}^m(n)$ in $\bigoplus_{\lambda|m} H^1(K_\lambda, T)$ is maximal isotropic under the sum of the local Tate pairings.*

Proof. Let A be the image of $\mathcal{H}^m(n)$ in $\bigoplus_{\lambda|m} H^1(K_\lambda, T)$. The local condition $\mathcal{F}^m(n)$ is maximal isotropic away from m under the local Tate pairing, and the reciprocity law of class field theory implies that for any $c, d \in H^1_{\mathcal{F}^m(n)}(K, T)$

$$\sum_{\lambda|m} \langle c_\lambda, d_\lambda \rangle_\lambda = \sum_{\text{all } v} \langle c_v, d_{\bar{v}} \rangle_v = 0,$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

which shows that $A \subset A^\perp$. By global duality (Theorem 1.1.11)

$$\begin{aligned}\text{length}(A) &= \text{length}(\mathcal{H}^m(n)/\mathcal{H}(n)) + \text{length}(\mathcal{H}(n)/\mathcal{H}_m(n)) \\ &= 2k\nu(n).\end{aligned}$$

The sum of the lengths of A and $A^\perp$ must be $4k\nu(m)$ and we conclude that $\text{length}(A) = \text{length}(A^\perp)$ and so $A = A^\perp$. □

Lemma 1.5.7. *For some $\delta \geqslant 0$, $\mathcal{H}^\ell(n)/(\mathcal{H}(n) + \mathcal{H}(\ell n)) \cong (R/\mathfrak{m}^\delta)^2$.*

Proof. We first construct a nondegenerate, alternating, R-bilinear, R-valued pairing on the module $\mathcal{H}^\ell(n)/(\mathcal{H}(n)+\mathcal{H}(\ell n))$. Let A be the local image of $\mathcal{H}^\ell(n)$ in $H^1(K_\ell, T)$. Then A is maximal isotropic by the previous lemma. Write A_{f} and A_{tr} for the intersections of A with $H^1_{\text{f}}(K_\ell, T)$ and $H^1_{\text{tr}}(K_\ell, T)$, respectively. Localization at ℓ gives an isomorphism

$$\mathcal{H}^\ell(n)/(\mathcal{H}(n) + \mathcal{H}(\ell n)) \cong A/(A_{\text{f}} + A_{\text{tr}}),$$

and it is on this R-module that we define the pairing.

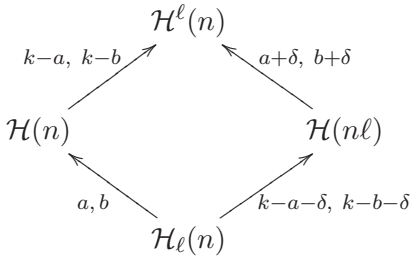
If $x \in A$ write x_{f} and x_{tr} for the projections of x onto the finite and transverse submodules. For $x, y \in A$ we define the symbol $[x, y] \in R$ by $[x, y] = \langle x_{\text{f}}, y_{\text{tr}}\rangle$. That $[x, y] = -[y, x]$ follows immediately from $\langle x, y\rangle = 0$ and the isotropy of the finite and transverse submodules. Suppose $x \in A$ is in the kernel of this pairing, then $0 = \langle x_{\text{f}}, y_{\text{tr}}\rangle = \langle x_f, y\rangle$ for every $y \in A$ and so $x_{\text{f}} \in A$ by maximal isotropy of A. It follows that $x_{\text{tr}} \in A$ and so $x \in A_{\text{f}} + A_{\text{tr}}$, proving that the pairing is nondegenerate.

We now have that

$$\mathcal{H}^\ell(n)/(\mathcal{H}(n) + \mathcal{H}(\ell n)) \cong D \oplus D$$

for some R-module D. Since $\mathcal{H}^\ell(n)/\mathcal{H}(n)$ injects into $H^1_{\text{s}}(K_\ell, T)$ which is free of rank two, it follows that $\mathcal{H}^\ell(n)/(\mathcal{H}(n) + \mathcal{H}(\ell n))$ can be generated by two elements. Therefore D is cyclic. □

Lemma 1.5.8. *There are a, b, and δ greater than or equal to zero such that in the following diagram the cokernel of each inclusion is a direct sum of two cyclic R-modules of the indicated lengths.*



Proof. The relation between the lower left and upper left quotients follows from global duality, and similarly for the lower and upper right quotients. The relation between lower left and upper right quotients, and also the relation between lower right and upper left, follows from the preceding lemma. □

Proposition 1.5.9. *For $n\ell \in \mathcal{N}$,*

$$\text{loc}_\ell(\mathcal{S}(n)) = 0 \implies \text{loc}_\ell(\mathcal{S}(\ell n)) = 0.$$

Proof. Keeping the notation as in the diagram of Lemma 1.5.8, $\text{loc}_\ell(\mathcal{S}(n)) = 0$ implies that $\mathfrak{m}^{\lambda(n)}$ kills the lower left quotient, and so $a, b \leqslant \lambda(n)$. The diagram immediately implies

$$\begin{aligned}\lambda(n\ell) &= \lambda(n) + k - a - b - \delta \\ &\geqslant k - a - \delta,\ k - b - \delta,\end{aligned}$$

so that $\mathfrak{m}^{\lambda(n\ell)}$ kills the lower right quotient. The proposition follows. □

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

1.6 Bounding the Selmer group

Throughout this subsection R is a fixed discrete valuation ring with uniformizing parameter π. Let $(T, \mathcal{F}, \mathcal{L})$ be a Selmer triple satisfying hypotheses H.0–H.5, and suppose $\mathcal{L}_s(T) \subset \mathcal{L}$ for $s \gg 0$. If Φ denotes the field of fractions of R, $\mathcal{D} = \Phi/R$, and $A = T \otimes_R \mathcal{D}$, then we obtain a Selmer structure on A, still denoted $\mathcal{F}$, by propagating $\mathcal{F} \otimes \Phi$ from $T \otimes \Phi$ to A. The following theorem is the technical core of this paper.

Theorem 1.6.1. *Suppose there is a Kolyvagin system $\kappa \in \mathbf{KS}(T, \mathcal{F}, \mathcal{L})$ with $\kappa_1 \neq 0$. Then $H^1_{\mathcal{F}}(K, T)$ is a free rank-one R module, and there is a finite R-module M such that*

$$H^1_{\mathcal{F}}(K, A) \cong \mathcal{D} \oplus M \oplus M.$$

Furthermore $\mathrm{length}_R(M) \leqslant \mathrm{length}_R(H^1_{\mathcal{F}}(K, T)/R \cdot \kappa_1)$.

We will prove this through a series of lemmas (the proof of Theorem 1.6.1 being given after the proof of Lemma 1.6.4). For any $k \geqslant 0$ we define

$$R^{(k)} = R/\mathfrak{m}^k, \quad T^{(k)} = T/\mathfrak{m}^k T, \quad \mathcal{L}^{(k)} = \mathcal{L} \cap \mathcal{L}_k(T).$$

By Remark 1.3.1, the Selmer triple $(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$ satisfies hypotheses H.0–H.5, and we may invoke the definitions and results of the preceding section. In particular for $\ell \in \mathcal{N}^{(k)} = \mathcal{N}(\mathcal{L}^{(k)})$ we have a decomposition

$$H^1_{\mathcal{F}(n)}(K, T^{(k)}) \cong R^{(k),\epsilon} \oplus M^{(k)}(n) \oplus M^{(k)}(n)$$

in which $\epsilon \in \{0, 1\}$ is independent of both n and k (by Lemma 1.5.3). We define

$$\lambda^{(k)}(n) = \mathrm{length}_R(M^{(k)}(n)), \quad \mathcal{S}^{(k)}(n) = \mathfrak{m}^{\lambda^{(k)}(n)} H^1_{\mathcal{F}(n)}(K, T^{(k)}).$$

We obtain, by Remark 1.2.4, a Kolyvagin system $\kappa^{(k)} \in \mathbf{KS}(T^{(k)}, \mathcal{F}, \mathcal{L}^{(k)})$.

Lemma 1.6.2. *Suppose we are given elements*

$$c^+ \in H^1(K, \bar{T})^+, \quad c^- \in H^1(K, \bar{T})^-.$$

There are infinitely many primes $\lambda \in \mathcal{L}^{(2k-1)}$ such that $c^\pm \neq 0 \implies \mathrm{loc}_\lambda(c^\pm) \neq 0$.

Proof. We consider only the case where c^+, c^- are both nonzero, the other case being entirely similar. Let $F/\mathbb{Q}$ be the extension of hypothesis H.2, and let L be the Galois closure (over $\mathbb{Q}$) of $K(T^{(2k-1)}, \mu_{p^{2k-1}})$. Since $F/\mathbb{Q}$ is Galois by hypothesis, $L \subset F(\mu_{p^\infty})$, and so restriction

$$H^1(K, \bar{T}) \to H^1(L, \bar{T})^{\mathrm{Gal}(L/K)} \cong \mathrm{Hom}(G_L, \bar{T})^{\mathrm{Gal}(L/K)}$$

is an injection. We identify $c^\pm$ with its image under restriction. Let E be the smallest extension of L with $c^\pm(G_E) = 0$, and set $G = \mathrm{Gal}(E/L)$. Then G is an $\mathbf{F}_p$-vector space with a natural action of $\mathrm{Gal}(L/\mathbb{Q})$, and we let $G^\pm$ be the $\pm$-eigenspace for the action of τ.

We claim that the maps

$$c^+ : G^+ \to \bar{T}^+, \quad c^- : G^+ \to \bar{T}^- \tag{12}$$

are nontrivial. Indeed, if $c^+(G^+) = 0$ then $c^+(G) = c^+(G^-) \subset \bar{T}^-$, and so $R \cdot c^+(G)$ is an $R[G_K]$-submodule of $\bar{T}$ contained in $\bar{T}^-$. This contradicts hypotheses H.1 and H.5, part a. Similar considerations apply to c^-.

The kernels of the maps (12) have codimension $\geqslant 1$, and so there is an $\eta \in G^+$ for which $c^\pm(\eta)$ are both nonzero, and we may choose some $\sigma \in G$ such that $\eta = (\tau\sigma)^2$. By the Cebotarev theorem, there are infinitely many primes ℓ of $\mathbb{Q}$ whose Frobenius class in $\mathrm{Gal}(E/\mathbb{Q})$ is equal to $\tau\sigma$, and at which the localizations of $c^\pm$ are unramified. For such an ℓ, the image of $c^\pm$ under

$$H^1(K, \bar{T}) \to H^1(K_\ell, \bar{T}) \to H^1_{\mathrm{unr}}(K_\ell, \bar{T}) \cong \bar{T}$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

(the final isomorphism being evaluation at the Frobenius of the prime of K above ℓ) is equal to $\phi(c^{\pm}) \neq 0$. □

Lemma 1.6.3. *If $n \in \mathcal{N}^{(2k-1)}$ and $\mathcal{S}^{(k)}(n) \neq 0$ then the image of*

$$H^1_{\mathcal{F}(n)}(K, T^{(2k-1)}) \to H^1_{\mathcal{F}(n)}(K, T^{(k)})$$

is a free, rank-one $R^{(k)}$-submodule.

Proof. Under the identification $H^1_{\mathcal{F}(n)}(K, T^{(k)}) \cong H^1_{\mathcal{F}(n)}(K, T^{(2k-1)})[\mathfrak{m}^k]$ of Lemma 1.3.3, the above map is identified with

$$H^1_{\mathcal{F}(n)}(K, T^{(2k-1)}) \xrightarrow{\pi^{k-1}} H^1_{\mathcal{F}(n)}(K, T^{(2k-1)})[\mathfrak{m}^k].$$

The hypothesis $\mathcal{S}^{(k)}(n) \neq 0$ implies that $\mathrm{length}_R(M^{(2k-1)}) < k$ and that $\epsilon = 1$, hence the image is isomorphic as an R-module to $\mathfrak{m}^{k-1}R^{(2k-1)} \cong R^{(k)}$. □

Lemma 1.6.4. *If $n \in \mathcal{N}^{(2k-1)}$ then $\kappa_n^{(k)} \in \mathcal{S}^{(k)}(n) \otimes G_n$.*

Proof. We argue by induction on both k and $\rho^{(k)}(n)$. Let $k > 0$ be the minimal integer for which the claim is false (for some n), and fix a generator for the cyclic group G_ℓ for every $\ell \in \mathcal{N}^{(2k-1)}$ so that we may identify $H^1_{\mathcal{F}(n)}(K, T^{(k)}) \otimes G_n \cong H^1_{\mathcal{F}(n)}(K, T^{(k)})$.

First suppose $\mathcal{S}^{(k)}(n) \neq 0$, so that in particular we are in the case $\epsilon = 1$, and $\lambda^{(k)}(n) < k$. Let $i = \lambda^{(k)}(n)$. By minimality of k, $\kappa_n^{(i)} \in \mathcal{S}^{(i)}(n)$. By Lemma 1.3.3 we have an isomorphism of R-modules $M^{(i)} \cong M^{(k)}[\mathfrak{m}^i] = M^{(k)}$, so that $\lambda^{(i)}(n) = \lambda^{(k)}(n) = i$. This implies that $\mathcal{S}^{(i)}(n) = 0$, and so $\kappa_n^{(i)} = 0$. Appealing again to Lemma 1.3.3, this is equivalent to $\pi^{k-i}\kappa_n^{(k)} = 0$. Now by Lemma 1.6.3, $\kappa_n^{(k)}$ is divisible by π^i in $H^1_{\mathcal{F}(n)}(K, T^{(k)})$, proving this special case.

Now keep k fixed as above and suppose that $n \in \mathcal{L}^{(2k-1)}$ gives a counterexample with $\rho(n)$ minimal. The above case shows that $\mathcal{S}^{(k)}(n) = 0$. By Lemma 1.3.3, $\rho(n) = 0$ or 1 implies that $\mathcal{S}^{(k)}(n) = H^1_{\mathcal{F}(n)}(K, T^{(k)})$, and so we must have $\rho(n) > 1$.

Case i: $\rho(n)^+$ and $\rho(n)^-$ are both nonzero. Using Lemma 1.3.3 we identify $H^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}] \cong H^1_{\mathcal{F}(n)}(K, \bar{T})$. If $\kappa^{(k)}(n) \neq 0$ then it has some nonzero multiple $d \in H^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}]$. This d has nontrivial projection onto one of the τ-eigencomponents of $H^1_{\mathcal{F}(n)}(K, \bar{T})$. Assume that $d^+ \neq 0$. By Lemma 1.6.2 we may choose a prime $\ell \in \mathcal{L}^{(2k-1)}$ at which both d^+ and some element of $H^1_{\mathcal{F}(n)}(K, \bar{T})^-$ have nontrivial localization. By Lemma 1.5.3, $\rho(n\ell) = \rho(n) - 2$, and so by induction $\kappa^{(k)}(n\ell) \in \mathcal{S}^{(k)}(n\ell)$. By Proposition 1.5.9, $\mathrm{loc}_\ell(\kappa^{(k)}(n\ell)) = 0$, but then the Kolyvagin system relations imply that $\mathrm{loc}_\ell(\kappa_n^{(k)}) = 0$, contradicting the choice of ℓ.

Case ii: one of $\rho(n)^\pm$ is equal to zero. Suppose $\rho(n)^- = 0$, so that $\rho(n)^+ > 1$. If $\kappa^{(k)}(n) \neq 0$ then choose a nonzero multiple of $\kappa^{(k)}(n)$, $d \in H^1_{\mathcal{F}(n)}(K, T^{(k)})[\mathfrak{m}]^+$, and a prime $\ell \in \mathcal{L}^{(2k-1)}$ for which $\mathrm{loc}_\ell(d) \neq 0$. By Lemma 1.5.3, $\rho(n\ell)^\pm$ are both nonzero and $\rho(n\ell) = \rho(n)$. Thus, by case i, $\kappa_{n\ell}^{(k)} \in \mathcal{S}^{(k)}(n\ell)$. By Proposition 1.5.9, $\mathrm{loc}_\ell(\mathcal{S}^{(k)}(n\ell)) = 0$, but the Kolyvagin system relations guarantee that $\mathrm{loc}_\ell(\kappa_{n\ell}^{(k)}) \neq 0$. This is a contradiction. □

Proof of Theorem 1.6.1. Since $H^1_{\mathcal{F}}(K, T) \cong \varprojlim H^1_{\mathcal{F}}(K, T^{(k)})$, we must have $\kappa_1^{(k)}$ nonzero for $k \gg 0$. Fix such a k. Taking $n = 1$ in Lemma 1.6.4, we have $\kappa_1^{(k)} \in \mathcal{S}^{(k)}$, and in particular $\mathcal{S}^{(k)} \neq 0$. Lemma 1.3.3 implies that there are isomorphisms

$$H^1_{\mathcal{F}}(K, T^{(k)}) \cong H^1_{\mathcal{F}}(K, A[\mathfrak{m}^k]) \cong H^1_{\mathcal{F}}(K, A)[\mathfrak{m}^k],$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

and we conclude that

$$H^1_{\mathcal{F}}(K,A)[\mathfrak{m}^k] \cong R/\mathfrak{m}^k \oplus M^{(k)} \oplus M^{(k)}$$

with $\mathrm{length}_R(M^{(k)}) < k$, and so for some finite R-module $M \cong M^{(k)}$ there is an isomorphism $H^1_{\mathcal{F}}(K,A) \cong \mathcal{D} \oplus M \oplus M$.

The compact Selmer group $H^1_{\mathcal{F}}(K,T)$ is the π-adic Tate module of $H^1_{\mathcal{F}}(K,A)$, and is therefore a free, rank-one R-module. Let $\lambda = \mathrm{length}_R(M) = \lambda^{(k)}(1)$. By Lemma 1.6.4, $\kappa_1^{(k)} \in \mathfrak{m}^\lambda H^1_{\mathcal{F}}(K,T^{(k)})$, and so by the injectivity of

$$H^1_{\mathcal{F}}(K,T)/\mathfrak{m}^k H^1_{\mathcal{F}}(K,T) \to H^1_{\mathcal{F}}(K,T^{(k)})$$

(which is deduced from Lemma 1.3.3), $\kappa_1 \in \mathfrak{m}^\lambda H^1_{\mathcal{F}}(K,T)$. The theorem follows. □

Let $E/\mathbb{Q}$ be an elliptic curve as in the statement of Theorem A of the Introduction, and let $\mathrm{Sel}_{p^\infty}(E/K)$ and $S_p(E/K)$ be the p-power Selmer groups defined there. Define a Selmer structure $\mathcal{F}$ on $V = T_p(E) \otimes \mathbb{Q}_p$ by taking the unramified local condition at each place v of K which does not divide p, and at $v|p$ take the image of the local Kummer map

$$E(K_v) \otimes \mathbb{Q}_p \to H^1(K,V).$$

Define local conditions on $T_p(E)$ and $E[p^\infty] \cong V/T_p(E)$ by propagating $\mathcal{F}$. By Proposition 1.6.8 of [Rub00], $H^1_{\mathcal{F}}(K, E[p^\infty]) = \mathrm{Sel}_{p^\infty}(E/K)$.

Theorem 1.6.5 (Kolyvagin). *Suppose there is an integer s for which the Selmer triple $(T_p(E), \mathcal{F}, \mathcal{L}_s)$ admits a Kolyvagin system with $\kappa_1 \neq 0$. Then $S_p(E/K)$ is free of rank one over $\mathbb{Z}_p$ and there is a finite $\mathbb{Z}_p$-module M such that*

$$\mathrm{Sel}_{p^\infty}(E/K) \cong (\mathbb{Q}_p/\mathbb{Z}_p) \oplus M \oplus M$$

with $\mathrm{length}_{\mathbb{Z}_p}(M) \leqslant \mathrm{length}_{\mathbb{Z}_p}(S_p(E/K)/\mathbb{Z}_p \cdot \kappa_1)$.

Proof. By Theorem 1.6.1 we need only verify that hypotheses H.0–H.5 hold. Hypothesis H.0 is trivial. Hypothesis H.1 follows from our assumption that G_K surjects onto $\mathrm{Aut}_{\mathbb{Z}_p}(T_p(E))$. This assumption also implies that

$$H^1(K(E[p^\infty])/K, E[p]) \cong H^1(GL_2(\mathbb{Z}_p), \mathbf{F}_p^2) = 0$$

(for the second equality, apply the inflation-restriction sequence to the subgroup $\mu_{p-1} \subset GL_2(\mathbb{Z}_p)$ embedded diagonally.) Hence hypothesis H.2 holds with $F = K(E[p^\infty])$. The fact that $\mathcal{F}$ is obtained by propagation from V implies that the quotient of $H^1(K_v, T_p(E))$ by $H^1_{\mathcal{F}}(K_v, T_p(E))$ is torsion-free for every place v, and hence hypothesis H.3 holds by Lemma 3.7.1 of [MR04]. The pairing of hypothesis H.4 is the Weil pairing, modified as in Remark 1.3.2. The orthogonality relations of that hypothesis are equivalent to Tate local duality, by the same remark. All of the conditions of hypothesis H.5 hold for $T_p(E)$, hence also for $\bar{T} \cong E[p]$, using the fact that E is defined over $\mathbb{Q}$. The splitting of part a of hypothesis H.5 follows from the τ-invariance of the Weil pairing on $T_p(E)$; part b of hypothesis H.5 says that the images of the local Kummer maps are stable under the $G_{\mathbb{Q}}$-action on (semi-)local cohomology; part c of hypothesis H.5 follows from

$$(s^\tau, t^\tau) = e(s^\tau, t) = e(s, t^\tau)^\tau = (s,t)^\tau,$$

where e is the Weil pairing. □

In the next section we will construct a Kolyvagin system from the Euler system of Heegner points. Applying Theorem 1.6.5 to this Kolyvagin system proves Theorem A of the Introduction.

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

1.7 Heegner points

In this subsection we show that our theory is nonvacuous by constructing a Kolyvagin system for $T = T_p(E)$ from the Heegner point Euler system. Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N and K a quadratic imaginary field of discriminant prime to p and $\neq -3, -4$. Assume that p does not divide N and that all prime divisors of N are split in K. Fix an integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$ satisfying $\mathcal{O}_K/\mathfrak{a} \cong \mathbb{Z}/N\mathbb{Z}$. Let $\mathcal{L} = \mathcal{L}_1(T)$ and $\mathcal{N} = \mathcal{N}_1$. For $\ell \in \mathcal{L}$, we denote by $a_\ell \in \mathbb{Z}$ the trace of the Frobenius at ℓ on $T_p(E)$. The ideal $I_\ell \subset \mathbb{Z}_p$ is the smallest ideal containing $\ell+1$ for which $\mathrm{Fr}_\lambda = \mathrm{Fr}_\ell^2$ acts trivially on $T/I_\ell T$, and hence on which Fr_ℓ acts with characteristic polynomial X^2-1. Therefore I_ℓ is generated by a_ℓ and $\ell+1$.

For every integer of the form $m = p^k n$ with $n \in \mathcal{N}$ we let $h_m \in X_0(N)$ be the point corresponding to the cyclic N-isogeny of complex tori

$$h_m = [\mathbb{C}/\mathcal{O}_m \to \mathbb{C}/(\mathcal{O}_m \cap \mathfrak{a})^{-1}],$$

where $\mathcal{O}_m$ is the order of conductor m in $\mathcal{O}_K$ and $(\mathcal{O}_m \cap \mathfrak{a})^{-1}$ is the inverse of the invertible $\mathcal{O}_m$-ideal $(\mathcal{O}_m \cap \mathfrak{a})$. The point h_m is rational over the ring class field of conductor m, which we denote by $K[m]$. Let $J_0(N)$ be the Jacobian of $X_0(N)$, and embed $X_0(N) \hookrightarrow J_0(N)$ by sending the cusp at ∞ to the origin. The image of h_m in $J_0(N)$ is again denoted by h_m. Fix a modular parametrization

$$J_0(N) \to E.$$

The image of h_m is now denoted by $P[m] \in E(K[m])$, the *Heegner point of conductor* m. If $n\ell \in \mathcal{N}$ we have the Euler system relation ([Gro91, Proposition 3.7] or [Per87, Section 3.3], for example)

$$\mathrm{Norm}_{K[n\ell]/K[n]} P[n\ell] = a_\ell P[n]$$

and the congruence

$$P[n\ell] \equiv \left(\frac{\lambda'}{K[n\ell]/\mathbb{Q}}\right) P[n] \pmod{\lambda'}, \tag{13}$$

where λ' is any prime of $K[n\ell]$ above ℓ.

If $n \in \mathcal{N}$ we set $\mathcal{G}(n) = \mathrm{Gal}(K[n]/K)$ and $G(n) = \prod_{\ell|n} G_\ell$. Then for m dividing n we have the equality

$$\mathrm{Gal}(K[n]/K[m]) \cong \prod_{\ell|(n/m)} G_\ell \cong G(n/m).$$

Define the derivative operator $D_\ell \in \mathbb{Z}_p[G(\ell)]$ by $D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i$, where σ_ℓ is a fixed generator of $G(\ell)$, and let $D_n = \prod_{\ell|n} D_\ell \in \mathbb{Z}_p[G(n)]$. One has the easy telescoping identity

$$(\sigma_\ell - 1)D_\ell = \ell + 1 - \mathrm{Norm}_\ell\,.$$

Choosing a set of coset representatives S for $G(n) \subset \mathcal{G}(n)$, we define

$$\tilde{\kappa}_n = \sum_{s \in S} sD_n(P[n]) \in E(K[n]).$$

Lemma 1.7.1. *The image of $\tilde{\kappa}_n$ in $E(K[n])/I_nE(K[n])$ is fixed by $\mathcal{G}(n)$.*

Proof. For each $\ell|n$ we have the equalities in $E(K[n])/I_nE(K[n])$:

$$\begin{aligned}(\sigma_\ell - 1)D_n(P[n]) &= (\sigma_\ell - 1)D_\ell D_{n/\ell} P[n] \\ &= -D_{n/\ell}\,\mathrm{Norm}_\ell(P[n]) \\ &= -a_\ell D_{n/\ell}(P[n/\ell]).\end{aligned}$$

Since $a_\ell \in I_\ell \subset I_n$, the lemma follows. □

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Our assumption that the map $G_K \to \mathrm{Aut}(T)$ is surjective guarantees that $E(K[n])[p] = 0$, and so, by the Hochschild–Serre spectral sequence, restriction gives an isomorphism

$$H^1(K, T/I_nT) \xrightarrow{\mathrm{res}} H^1(K[n], T/I_nT)^{\mathcal{G}(n)}.$$

If $\delta_n : E(K[n])/I_nE(K[n]) \to H^1(K[n], T/I_nT)$ is the Kummer map, we define κ_n to be the unique preimage of $\delta_n(\tilde{\kappa}_n)$ under restriction.

Lemma 1.7.2. *The class $\kappa_n \in H^1(K, T/I_nT)$ may be given as an explicit cocycle as follows. Let $I_n = p^{M_n}\mathbb{Z}_p$ and fix a p^{M_n}-divisor of $\tilde{\kappa}_n$, $\tilde{\kappa}_n/p^{M_n} \in E(\bar{K})$. For $\sigma \in G_K$ let $(\sigma-1)\tilde{\kappa}_n/p^{M_n}$ be the unique p^{M_n}-divisor of $(\sigma-1)\tilde{\kappa}_n$ in $E(K[n])$. Then*

$$\kappa_n(\sigma) = (\sigma-1)\frac{\tilde{\kappa}_n}{p^{M_n}} - \frac{(\sigma-1)\tilde{\kappa}_n}{p^{M_n}}.$$

Proof. This is Lemma 4.1 of [McC91]. □

Lemma 1.7.3. *Fix $n \in \mathcal{N}$ and let $\mathcal{F}$ denote the Selmer structure of Theorem 1.6.5 on T, so that $H^1_{\mathcal{F}}(K, T) = S_p(E/K)$. Then $\kappa_n \in H^1_{\mathcal{F}(n)}(K, T/I_nT)$.*

Proof. The statement that $\mathrm{loc}_v(\kappa_n) \in H^1_{\mathcal{F}}(K_v, T/I_nT)$ for v not dividing n is Proposition 6.2 of [Gro91].

Assume that $\ell | n$ and let λ be the prime of K above ℓ. We must show that the restriction of κ_n to $H^1(K[\ell]_{\lambda'}, T/I_nT)$ is trivial, where λ' is the unique prime of $K[\ell]$ above ℓ. The prime λ of K above ℓ splits completely in $K[n/\ell]$, and so λ' splits completely in $K[n]$. Fixing a prime λ'' of $K[n]$ above λ', we have $K[\ell]_{\lambda'} = K[n]_{\lambda''}$. Therefore it suffices to show that $\sum_{s\in S} sD_n(\delta_n(P[n]))$ has trivial restriction to $H^1(K[n]_{\lambda''}, T/I_nT)$.

Let

$$c = \delta_n(P[n]) \in H^1_{\mathrm{unr}}(K[\ell]_{\lambda'}, T/I_nT) = H^1_{\mathrm{unr}}(K[n]_{\lambda''}, T/I_nT)$$

and extend σ_ℓ to a generator of $\mathrm{Gal}(K[\ell]^{\mathrm{unr}}_{\lambda'}/K^{\mathrm{unr}}_{\lambda})$. By definition of I_n, the Frobenius automorphism, $\mathrm{Fr}_\lambda \in \mathrm{Gal}(K^{\mathrm{unr}}_\lambda/K_\lambda)$ acts trivially on T/I_nT, and so by Proposition 1.1.7 it suffices to show that $(D_\ell c)(\mathrm{Fr}_\lambda) \in T/I_nT$ is zero. Since σ_ℓ acts trivially on T/I_nT, we have

$$(D_\ell c)(\mathrm{Fr}_\lambda) = \sum_{i=1}^{\ell} ic(\mathrm{Fr}_\lambda) = \frac{\ell(\ell+1)}{2}c(\mathrm{Fr}_\lambda) = 0.$$ □

Proposition 1.7.4. *For every $\ell|\lambda \in \mathcal{L}$ there is an automorphism*

$$\chi_\ell : T/I_\ell T \to T/I_\ell T$$

such that for $n\ell \in \mathcal{N}$, $\chi_\ell(\kappa_n(\mathrm{Fr}_\lambda)) = \kappa_{n\ell}(\sigma_\ell)$ as elements of $T/I_{n\ell}T$.

Proof. Fix a prime λ' of $\bar{K}$ above λ. Identify

$$T/I_\ell T \cong E[I_\ell] \cong \tilde{E}(\mathbf{F})[I_\ell],$$

where $\tilde{E}$ is the reduction of E at ℓ and $\mathbf{F}$ is the residue field of K at λ. By Lemma 1.7.2 (and using the notation of that lemma) the right-hand side is given by the congruence

$$\kappa_{n\ell}(\sigma_\ell) \equiv -\frac{(\sigma_\ell - 1)\tilde{\kappa}_{n\ell}}{p^{M_{n\ell}}} \pmod{\lambda'}.$$

Combining this with the Euler system relations and the congruence (13) gives

$$\kappa_{n\ell}(\sigma_\ell) \equiv \frac{a_\ell - (\ell+1)\,\mathrm{Fr}_\ell}{p^{M_{n\ell}}}\tilde{\kappa}_n \pmod{\lambda'}$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

(see the proof of Proposition 4.4 of [McC91]). Define χ_ℓ to be the composition

$$E(K_\lambda) \to \tilde{E}(\mathbf{F}) \to \tilde{E}(\mathbf{F})[p^\infty] \xrightarrow{p^{-M_\ell}(a_\ell-(\ell+1)\,\mathrm{Fr}_\ell)} \tilde{E}(\mathbf{F})[I_\ell] \to E[I_\ell],$$

where the first arrow is reduction, the second is projection onto the p-Sylow subgroup, and the last is the canonical lift to $E(\bar{K}_\lambda)[I_\ell]$. The action of Fr_ℓ splits the p-Sylow subgroup of $\tilde{E}(\mathbf{F})$ into cyclic eigencomponents whose lengths are the orders at p of $\ell+1-a_\ell$ and $\ell+1+a_\ell$. It follows that χ_ℓ is a surjection. Since $E[I_\ell]$ is defined over K_λ, the map χ_ℓ factors through to an isomorphism

$$E(K_\lambda)/I_\ell E(K_\lambda) \to E[I_\ell].$$

Identifying

$$E(K_\lambda)/I_\ell E(K_\lambda) \cong H^1(K_\lambda^{\mathrm{unr}}/K_\lambda, E[I_\ell]) \cong E[I_\ell],$$

we obtain the desired automorphism of $E[I_\ell]$. □

The above proposition shows that the classes κ_n almost form a Kolyvagin system. Only a slight modification is needed:

Theorem 1.7.5. *There is a Kolyvagin system κ' for $(T,\mathcal{F},\mathcal{L})$ with $\kappa'_1=\kappa_1$.*

Proof. For $n\in\mathcal{N}$ define an automorphism

$$\chi_n : H^1(K,T/I_nT) \to H^1(K,T/I_nT)$$

as follows. For each ℓ dividing n, the automorphism χ_ℓ of $T/I_\ell T$ induces an automorphism of $H^1(K,T/I_nT)$, again denoted by χ_ℓ. It is clear from construction in the proof of Proposition 1.7.4 that the maps χ_ℓ pairwise commute, and we define χ_n to be the composition of the χ_ℓ as ℓ runs over all divisors of n. We now define

$$\kappa'_n = \chi_n^{-1}(\kappa_n)\otimes_{\ell|n}\sigma_\ell \in H^1_{\mathcal{F}(n)}(K,T/I_nT)\otimes G_n.$$ □

The class κ'_1 is the image of $\mathrm{Norm}_{K[1]/K}P[1]$ under the Kummer map $E(K)\to H^1(K,T)$, and so is nonzero provided that $L'(E/K,1)\neq 0$, by the results of Gross and Zagier [GZ86].

2. Iwasawa theory

Fix an elliptic curve $E_{/\mathbb{Q}}$ with good, ordinary reduction at p, and let K be a quadratic imaginary field satisfying the Heegner hypothesis and with discriminant $\neq -3,-4$ and prime to p. Let K_∞/K be the anticyclotomic $\mathbb{Z}_p$-extension,

$$\Gamma=\mathrm{Gal}(K_\infty/K),\quad \Lambda=\mathbb{Z}_p[[\Gamma]],$$

so that K_∞/K is characterized as the unique $\mathbb{Z}_p$-extension of K such that complex conjugation acts as $\tau\sigma\tau=\sigma^{-1}$ for all $\sigma\in\Gamma$. Fix a topological generator $\gamma\in\Gamma$ so that we may identify Λ with the power series ring $\mathbb{Z}_p[[T]]$. Let K_n denote the unique subfield of K_∞ with $[K_n:K]=p^n$. Set

$$T=T_p(E),\quad V=T\otimes\mathbb{Q}_p,\quad A=V/T.$$

We assume throughout that the map $\mathrm{Gal}(\bar{K}/K)\to\mathrm{Aut}_{\mathbb{Z}_p}(T)$ is surjective, and that each prime of K above p is totally ramified in K_∞.

We denote by $f\mapsto f^\iota$ the involution of Λ induced by $\gamma\mapsto\gamma^{-1}$. We regard Λ as a G_K-module in the obvious way. The symbol Σ_Λ will always be used to indicate a finite set of height-one prime ideals of Λ, and $\mathfrak{P}$ will always denote a height-one prime of Λ.

For a height-one prime $\mathfrak{P}\neq p\Lambda$ of Λ, denote by $S_\mathfrak{P}$ the integral closure of $\Lambda/\mathfrak{P}$, by $\Phi_\mathfrak{P}$ the field of fractions of $S_\mathfrak{P}$, and by $\mathcal{D}_\mathfrak{P}$ the quotient $\Phi_\mathfrak{P}/S_\mathfrak{P}$. For any $\mathbb{Z}_p$-module N, let $N_\mathfrak{P}=N\otimes_{\mathbb{Z}_p}S_\mathfrak{P}$.

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

If N has a G_K-action, we let G_K act on $N_{\mathfrak{P}}$ by acting on both factors in the tensor product, the action on $S_{\mathfrak{P}}$ being given by the natural map $G_K \to \Lambda \to S_{\mathfrak{P}}$.

Our basic tool for studying the Iwasawa module $\mathbf{T} = T_p(E) \otimes \Lambda$ and its cohomology is, following [MR04], to consider the $S_{\mathfrak{P}}$-module $T_{\mathfrak{P}} \cong \mathbf{T} \otimes_\Lambda S_{\mathfrak{P}}$ for each height-one prime $\mathfrak{P}$ of Λ. The results of § 1 allow one to control certain Selmer groups associated to $T_{\mathfrak{P}}$, defined using the ideas of [CG96], and from this one may recover information about the structure of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$.

2.1 Kolyvagin systems at height-one primes

Throughout § 2.1 we work with a fixed height-one prime $\mathfrak{P} \neq p\Lambda$ of Λ. Let $\mathfrak{m}$ be the maximal ideal of $S_{\mathfrak{P}}$. If $\mathfrak{d}$ is a generator for the absolute different of $\Phi_{\mathfrak{P}}$, the trace from $\Phi_{\mathfrak{P}}$ to $\mathbb{Q}_p$ defines a surjective map

$$\mathcal{D}_{\mathfrak{P}} = \Phi_{\mathfrak{P}}/S_{\mathfrak{P}} \xrightarrow{\mathfrak{d}^{-1}} \Phi_{\mathfrak{P}}/\mathfrak{d}^{-1}S_{\mathfrak{P}} \xrightarrow{\mathrm{Tr}} \mathbb{Q}_p/\mathbb{Z}_p$$

whose kernel contains no $S_{\mathfrak{P}}$-submodules. This map induces an isomorphism of $S_{\mathfrak{P}}$-modules

$$\mathrm{Hom}_{S_{\mathfrak{P}}}(N, \mathcal{D}_{\mathfrak{P}}(1)) \cong \mathrm{Hom}_{\mathbb{Z}_p}(N, \mu_{p^\infty})$$

for any finitely or cofinitely generated $S_{\mathfrak{P}}$-module N.

If v is a prime of K above p, we define $\mathrm{Fil}_v T$ to be the kernel of the reduction map $T_p(E) \to T_p(\tilde{E})$ where $\tilde{E}$ is the reduction of E at v. Let

$$\mathrm{Fil}_v T_{\mathfrak{P}} = (\mathrm{Fil}_v T) \otimes S_{\mathfrak{P}}, \quad \mathrm{Fil}_v V_{\mathfrak{P}} = (\mathrm{Fil}_v T) \otimes \Phi_{\mathfrak{P}}.$$

We define the *ordinary* local condition at v, $H^1_{\mathrm{ord}}(K_v, V_{\mathfrak{P}})$, to be the image of

$$H^1(K_v, \mathrm{Fil}_v V_{\mathfrak{P}}) \to H^1(K_v, V_{\mathfrak{P}}).$$

Lemma 2.1.1. *There is a perfect $S_{\mathfrak{P}}$-bilinear pairing*

$$e_{\mathfrak{P}} : T_{\mathfrak{P}} \times T_{\mathfrak{P}} \to S_{\mathfrak{P}}(1)$$

which satisfies $e_{\mathfrak{P}}(s^\sigma, t^{\tau\sigma\tau}) = e_{\mathfrak{P}}(s,t)^\sigma$ for $s, t \in T_{\mathfrak{P}}$ and $\sigma \in G_K$ (here we regard $S_{\mathfrak{P}}(1)$ as the Tate twist of the module $S_{\mathfrak{P}}$ with trivial *Galois action). The submodule $\mathrm{Fil}_v T_{\mathfrak{P}}$ is its own exact orthogonal complement under this pairing.*

Proof. If $e : T \times T \to \mathbb{Z}_p(1)$ is the Weil pairing, we define $e_{\mathfrak{P}}$ by

$$e_{\mathfrak{P}}(t_1 \otimes \alpha_1, t_2 \otimes \alpha_2) = e(t_1, t_2^\tau) \otimes \alpha_1\alpha_2$$

for $t_i \in T$ and $\alpha_i \in S_{\mathfrak{P}}$. Since $\mathrm{Fil}_v T$ is maximal isotropic under the Weil pairing, the same is true of $\mathrm{Fil}_v T_{\mathfrak{P}}$. □

Definition 2.1.2. Define a Selmer structure $\mathcal{F}_{\mathfrak{P}}$ on $V_{\mathfrak{P}}$ by

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

We denote also by $\mathcal{F}_{\mathfrak{P}}$ the Selmer structures obtained by propagating this to $T_{\mathfrak{P}}$ and to $A_{\mathfrak{P}} \cong V_{\mathfrak{P}}/T_{\mathfrak{P}}$.

Proposition 2.1.3. *Fix a positive integer s and a set of primes $\mathcal{L} \supset \mathcal{L}_s(T_{\mathfrak{P}})$, and suppose the Selmer triple $(T_{\mathfrak{P}}, \mathcal{F}_{\mathfrak{P}}, \mathcal{L})$ admits a nontrivial Kolyvagin system κ. Then $H^1_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}})$ is a free, rank-one $S_{\mathfrak{P}}$-module, and*

$$H^1_{\mathcal{F}_{\mathfrak{P}}}(K, A_{\mathfrak{P}}) \cong \mathcal{D}_{\mathfrak{P}} \oplus M_{\mathfrak{P}} \oplus M_{\mathfrak{P}},$$

where $M_{\mathfrak{P}}$ is a finite $S_{\mathfrak{P}}$-module with

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

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Proof. By Theorem 1.6.1, we need only verify that hypotheses H.0–H.5 hold. Hypothesis H.0 is trivial. For hypothesis H.1, observe that $\bar{T}_{\mathfrak{P}} \cong E[p] \otimes S_{\mathfrak{P}}/\mathfrak{m}$. The action of G_K on $S_{\mathfrak{P}}/\mathfrak{m}$ factors through $G_K \to \Lambda/(p, \gamma - 1) \to S_{\mathfrak{P}}/\mathfrak{m}$, and so is trivial on the second factor of the tensor product. Therefore, the surjectivity of $G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(E[p])$ implies that $G_K \to \mathrm{Aut}_{S_{\mathfrak{P}}}(\bar{T}_{\mathfrak{P}})$ is also surjective. For hypothesis H.2 we take $F = K_\infty(E[p^\infty])$. Since $\mu_{p^\infty} \subset F$ and $\bar{T}_{\mathfrak{P}} \cong E[p] \otimes S_{\mathfrak{P}}/\mathfrak{m}$, we must show that $H^1(F/K, E[p]) = 0$. From the surjectivity of $G_K \to \mathrm{Aut}_{\mathbb{Z}_p}(E[p])$, one may deduce that $E(K_\infty)[p] = 0$ and that

$$H^1(F/K_\infty, E[p]) \cong H^1(K(E[p^\infty])/K, E[p]) \cong H^1(GL_2(\mathbb{Z}_p), \mathbf{F}_p^2) = 0$$

(as in Theorem 1.6.5) and so the claim follows from the exactness of the inflation-restriction sequence

$$H^1(K_\infty/K, E(K_\infty)[p]) \to H^1(F/K, E[p]) \to H^1(F/K_\infty, E[p]).$$

Hypothesis H.3 follows from Lemma 3.7.1 of [MR04] and the fact that the Selmer structure $\mathcal{F}_{\mathfrak{P}}$ on $T_{\mathfrak{P}}$ is obtained by propagation from $V_{\mathfrak{P}}$. Hypothesis H.4 follows from Lemma 2.1.1, and hypothesis H.5 follows from the isomorphism $\bar{T}_{\mathfrak{P}} \cong E[p] \otimes S_{\mathfrak{P}}/\mathfrak{m}$ (with G_K acting trivially on the second factor). □

2.2 Kolyvagin systems over Λ

Definition 2.2.1. If M is any group on which G_K acts and L/K is a finite Galois extension we define the induced representation

$$M_{L/K} = \mathrm{Ind}_{L/K} M = \{f : G_K \to M \mid f(\sigma x) = f(x)^\sigma \forall x \in G_K,\ \sigma \in G_L\}.$$

This comes equipped with commuting actions of G_K and $\mathrm{Gal}(L/K)$ defined by

$$(f^\sigma)(x) = f(x\sigma), \quad (\gamma \cdot f)(x) = f(\tilde{\gamma}^{-1}x)^{\tilde{\gamma}},$$

where $\sigma \in G_K$, $\gamma \in \mathrm{Gal}(L/K)$, and $\tilde{\gamma}$ is any lift of γ to G_K.

We view $\mathrm{Ind}_{L/K}$ as an exact functor from the category of G_K-modules to the category of G_K-modules with commuting $\mathrm{Gal}(L/K)$-action. For M a G_K-module, we define G_K-module maps

$$\mathrm{res} : M \to M_{L/K}, \quad \mathrm{cor} : M_{L/K} \to M$$

by $\mathrm{res}(m)(x) = x \cdot m$ and $\mathrm{cor}(f) = (\mathrm{Norm}_{L/K} f)(\mathrm{id}_{G_K})$. Under the canonical identification of Shapiro's lemma $H^q(L, M) \cong H^q(K, M_{L/K})$, res and cor induce restriction and corestriction.

Lemma 2.2.2. *If F is any extension of L, there is a canonical isomorphism*

$$H^q(F, M_{L/K}) \cong \mathrm{Ind}_{L/K} H^q(F, M).$$

Proof. This follows from Proposition B.4.2 of [Rub00]. □

Definition 2.2.3. Define Λ-modules $\mathbf{T}$ and $\mathbf{A}$ by

$$\mathbf{T} = \varprojlim \mathrm{Ind}_{K_n/K} T, \quad \mathbf{A} = \varinjlim \mathrm{Ind}_{K_n/K} A,$$

the limits with respect to corestriction and restriction, respectively. We remark that there is a canonical isomorphism of Λ and G_K-modules $\mathbf{T} \cong T \otimes \Lambda$, where G_K acts on both factors in the tensor product and Λ acts only on the second factor.

Proposition 2.2.4. *The Weil pairing $e : T \times A \to \mu_{p^\infty}$ induces a perfect G_K-equivariant pairing*

$$e_\Lambda : \mathbf{T} \times \mathbf{A} \to \mu_{p^\infty}$$

satisfying $e_\Lambda(\lambda \cdot t, a) = e_\Lambda(t, \lambda^\iota \cdot a)$ for $t \in \mathbf{T}$, $a \in \mathbf{A}$, and $\lambda \in \Lambda$.

Proof. Let $T_n = \mathrm{Ind}_{K_n/K} T$ and $A_n = \mathrm{Ind}_{K_n/K} A$. Define a pairing

$$\tilde{e}_n : T_n \times A_n \to \mathrm{Ind}_{K_n/K}(\mu_{p^\infty})$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

by $\tilde{e}_n(f,f')(x) = e(f(x),f'(x))$. This pairing is easily seen to be equivariant for the actions of both G_K and Λ, and to satisfy

$$\mathrm{cor}(\tilde{e}_n(f,\mathrm{res}(a))) = e(\mathrm{cor}(f),a)$$

for $f \in T_n$ and $a \in A$. Define a pairing $e_n : T_n \times A_n \to \mu_{p^\infty}$ by the composition

$$T_n \times A_n \to \mathrm{Ind}_{K_n/K}(\mu_{p^\infty}) \xrightarrow{\mathrm{cor}} \mu_{p^\infty}.$$

Passing to the limit as $n \to \infty$ yields the desired pairing e_Λ. □

Definition 2.2.5. If v is a place of K dividing p, let $\mathrm{Fil}_v T$ be the kernel of the reduction map $T \to T_p(\tilde{E})$ where $\tilde{E}$ is the reduction of E at v. Define $\mathrm{Fil}_v V = \mathrm{Fil}_v T \otimes \mathbb{Q}_p \subset V$ and $\mathrm{Fil}_v A = \mathrm{Fil}_v V/\mathrm{Fil}_v T \subset A$. Define $\mathrm{Fil}_v \mathbf{T} \subset \mathbf{T}$ and $\mathrm{Fil}_v \mathbf{A} \subset \mathbf{A}$ by

$$\mathrm{Fil}_v \mathbf{T} = \varprojlim \mathrm{Ind}_{K_n/K} \mathrm{Fil}_v T, \quad \mathrm{Fil}_v \mathbf{A} = \varinjlim \mathrm{Ind}_{K_n/K} \mathrm{Fil}_v A.$$

If N is any object for which $\mathrm{Fil}_v N$ is defined, set $\mathrm{gr}_v N = N/\mathrm{Fil}_v N$.

The submodules $\mathrm{Fil}_v T$ and $\mathrm{Fil}_v A$ are exact orthogonal complements under the Weil pairing, and it follows that the same is true of $\mathrm{Fil}_v \mathbf{T}$ and $\mathrm{Fil}_v \mathbf{A}$ under the pairing of Proposition 2.2.4.

Definition 2.2.6. Define a Selmer structure $\mathcal{F}_\Lambda$ on $\mathbf{T}$ by taking the unramified condition at primes of K not dividing p, and taking the image of

$$H^1(K_v, \mathrm{Fil}_v \mathbf{T}) \to H^1(K_v, \mathbf{T})$$

at primes above p. Define a Selmer structure, also denoted $\mathcal{F}_\Lambda$, on $\mathbf{A}$ in a similar manner.

It follows from the comment following Definition 2.2.5 that the local conditions $\mathcal{F}_\Lambda$ on $\mathbf{T}$ and $\mathbf{A}$ are everywhere exact orthogonal complements under the local Tate pairing.

For any height-one prime $\mathfrak{P} \neq p\Lambda$, the involution of Λ induces a map $S_\mathfrak{P} \to S_{\mathfrak{P}^\iota}$ which we continue to denote by ι. Define a bijection $\psi : T_\mathfrak{P} \to T_{\mathfrak{P}^\iota}$ by $\psi(t \otimes \alpha) = t^\tau \otimes \alpha^\iota$. This map satisfies

$$\psi(\lambda x) = \lambda^\iota \psi(x), \quad \psi(x^\sigma) = \psi(x)^{\tau\sigma\tau}$$

for any $x \in T_\mathfrak{P}$, $\lambda \in \Lambda$, and $\sigma \in G_K$. If $e_\mathfrak{P} : T_\mathfrak{P} \times A_\mathfrak{P} \to \mu_{p^\infty}$ is the pairing induced by that of Lemma 2.1.1 and the trace form, then $(x,y) \mapsto e_\mathfrak{P}(\psi^{-1}(x),y)$ defines a perfect, G_K-invariant pairing

$$T_{\mathfrak{P}^\iota} \times A_\mathfrak{P} \to \mu_{p^\infty}$$

satisfying $(\lambda x, y) = (x, \lambda^\iota y)$. Dualizing the natural map $\mathbf{T}/\mathfrak{P}^\iota\mathbf{T} \to T_{\mathfrak{P}^\iota}$ and using the above pairing and the pairing of Proposition 2.2.4, we obtain a map of G_K and Λ-modules

$$A_\mathfrak{P} \to \mathbf{A}[\mathfrak{P}]. \tag{14}$$

Lemma 2.2.7. *For every height-one prime $\mathfrak{P} \neq p\Lambda$ of Λ and every place v of K, the map $\mathbf{T} \to T_\mathfrak{P}$ and the map (14) induce maps*

$$H^1_{\mathcal{F}_\Lambda}(K_v, \mathbf{T}/\mathfrak{P}\mathbf{T}) \to H^1_{\mathcal{F}_\mathfrak{P}}(K_v, T_\mathfrak{P}),$$
$$H^1_{\mathcal{F}_\mathfrak{P}}(K_v, A_\mathfrak{P}) \to H^1_{\mathcal{F}_\Lambda}(K_v, \mathbf{A}[\mathfrak{P}])$$

with finite kernels and cokernels which are bounded by constants depending only on $[S_\mathfrak{P} : \Lambda/\mathfrak{P}]$.

Proof. The case where v does not divide p is covered by Lemma 5.3.13 of [MR04], so we assume that v divides p. The kernel of the first map is bounded by the size of $H^0(K_v, T \otimes S_\mathfrak{P}/(\Lambda/\mathfrak{P}))$ and so causes no problems. To bound the cokernel, it suffices to bound each cokernel in the composition

$$H^1(K_v, \mathrm{Fil}_v(\mathbf{T})) \to H^1(K_v, \mathrm{Fil}_v(T) \otimes \Lambda/\mathfrak{P}) \to H^1(K_v, \mathrm{Fil}_v(T_\mathfrak{P})) \to H^1_{\mathcal{F}_\mathfrak{P}}(K_v, T_\mathfrak{P}). \tag{15}$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

The cokernel of the first map is controlled by $H^2(K_v, \mathrm{Fil}_v \mathbf{T})[\mathfrak{P}]$, and by local duality it suffices to bound

$$H^0(K_v, \mathrm{gr}_v \mathbf{A}) \cong H^0(K_{\infty,v}, \mathrm{gr}_v A).$$

This last group is isomorphic to the p-power torsion of the reduction of E at v rational over the residue field of K_v, and this is finite.

The cokernel of the second arrow of (15) is controlled by $H^1(K_v, T \otimes S_{\mathfrak{P}}/(\Lambda/\mathfrak{P}))$. This group has a bound of the desired sort, using the fact that K_v has only finitely many extensions of a given degree.

For the third arrow of (15) it suffices to bound the kernel of

$$H^1(K_v, \mathrm{gr}_v T_{\mathfrak{P}}) \to H^1(K_v, \mathrm{gr}_v V_{\mathfrak{P}}),$$

which is controlled by

$$\begin{aligned} H^0(K_v, \mathrm{gr}_v A_{\mathfrak{P}}) &\cong H^0(K_v, (\mathrm{gr}_v A) \otimes S_{\mathfrak{P}}) \\ &\subset H^0(K_{\infty,v}, (\mathrm{gr}_v A) \otimes S_{\mathfrak{P}}) \\ &\cong H^0(K_{\infty,v}, \mathrm{gr}_v A) \otimes S_{\mathfrak{P}} \\ &\cong H^0(K_v, \mathrm{gr}_v A) \otimes S_{\mathfrak{P}}, \end{aligned}$$

where the last isomorphism uses the fact that $K_{\infty,v}/K_v$ is totally ramified, while $\mathrm{gr}_v A$ is unramified. Since $H^0(K_v, \mathrm{gr}_v A)$ is isomorphic to the p-power torsion of E defined over the residue field of K_v, we obtain a bound of the desired sort.

Finally, to deal with the second map in the statement of the lemma, observe that the kernel and cokernel of $H^1(K_v, \mathbf{T}/\mathfrak{P}^\iota \mathbf{T}) \to H^1(K_v, T_{\mathfrak{P}^\iota})$ are finite and have bounds of the desired sort, and so the same is true of

$$H^1(K_v, \mathbf{T}/\mathfrak{P}^\iota \mathbf{T})/H^1_{\mathcal{F}_\Lambda}(K_v, \mathbf{T}/\mathfrak{P}^\iota \mathbf{T}) \to H^1(K_v, T_{\mathfrak{P}^\iota})/H^1_{\mathcal{F}_{\mathfrak{P}^\iota}}(K_v, T_{\mathfrak{P}^\iota}).$$

Now apply local duality. □

Proposition 2.2.8. *For every height-one prime $\mathfrak{P} \neq p\Lambda$ of Λ, the map $\mathbf{T} \to T_{\mathfrak{P}}$ and the map (14) induce maps*

$$H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\mathfrak{P} H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T}) \to H^1_{\mathcal{F}_{\mathfrak{P}}}(K, T_{\mathfrak{P}}),$$
$$H^1_{\mathcal{F}_{\mathfrak{P}}}(K, A_{\mathfrak{P}}) \to H^1_{\mathcal{F}_\Lambda}(K, \mathbf{A})[\mathfrak{P}].$$

There is a finite set of primes Σ_Λ of Λ such that for $\mathfrak{P} \notin \Sigma_\Lambda$ the kernels and cokernels of these maps are finite and bounded by a constant depending only on $[S_{\mathfrak{P}} : \Lambda/\mathfrak{P}]$.

Proof. This is deduced from the preceding lemma exactly as in the proof of Proposition 5.3.14 of [MR04]. □

Lemma 2.2.9. *The Λ-module $H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ is torsion-free.*

Proof. Let K_S be the maximal extension of K unramified outside of all primes dividing p and the conductor of E. Then $H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ is a submodule of $H^1(K_S/K, \mathbf{T})$ which has no Λ-torsion by [Per00, § 1.3.3] and the fact that $E(K_\infty)[p] = 0$ (by the surjectivity of $G_K \to \mathrm{Aut}(T)$). □

Theorem 2.2.10. *Let $X = \mathrm{Hom}(H^1_{\mathcal{F}_\Lambda}(K, \mathbf{A}), \mathbb{Q}_p/\mathbb{Z}_p)$ and suppose that for some s the Selmer triple $(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L}_s)$ admits a Kolyvagin system κ with $\kappa_1 \neq 0$. Then*

a) *$H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ is a torsion-free, rank-one Λ-module,*
b) *there is a torsion Λ-module M such that $\mathrm{char}(M) = \mathrm{char}(M)^\iota$ and a pseudo-isomorphism*

$$X \sim \Lambda \oplus M \oplus M,$$

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

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Proof. At every height-one prime $\mathfrak{P} \neq p\Lambda$, Remark 1.2.4 and Lemma 2.2.7 yield a map

$$\mathbf{KS}(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L}_s(\mathbf{T})) \to \mathbf{KS}(T_\mathfrak{P}, \mathcal{F}_\mathfrak{P}, \mathcal{L}_s(T_\mathfrak{P})).$$

Let $\kappa^{(\mathfrak{P})}$ be the image of κ under this map. It follows from Proposition 2.2.8 and Lemma 2.2.9 that $\kappa_1^{(\mathfrak{P})}$ generates an infinite $S_\mathfrak{P}$-submodule of $H^1_{\mathcal{F}_\mathfrak{P}}(K, T_\mathfrak{P})$ for all but finitely many height-one primes. We let Σ_Λ be a finite set of height-one primes of Λ containing those primes for which $\kappa_1^{(\mathfrak{P})}$ has finite order, all prime divisors of the characteristic ideal of the Λ-torsion submodule of X, the exceptional set of primes of Proposition 2.2.8, and the prime $p\Lambda$.

Let $\mathfrak{P} \notin \Sigma_\Lambda$ be a height-one prime. Since $\kappa_1^{(\mathfrak{P})} \neq 0$, Proposition 2.1.3 implies that $H^1_{\mathcal{F}_\mathfrak{P}}(K, T_\mathfrak{P})$ is a free rank-one $S_\mathfrak{P}$-module, and by Proposition 2.2.8 so is $H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T}) \otimes_\Lambda S_\mathfrak{P}$. Part a of the theorem follows immediately from this. Similarly, the $S_\mathfrak{P}$-corank of $H^1_{\mathcal{F}_\mathfrak{P}}(K, A_\mathfrak{P})$ is one, and it follows from Proposition 2.2.8 that the Λ-corank of $H^1_{\mathcal{F}_\Lambda}(K, \mathbf{A})$ is also one.

Now let $f_\Lambda = \mathrm{char}(H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})/\Lambda \cdot \kappa_1)$ and take $\mathfrak{P} \neq p\Lambda$ to be a prime divisor of f_Λ. We want to determine the order of the characteristic ideal of X at $\mathfrak{P}$, following ideas of [MR04]. We consider an auxiliary ideal $\mathfrak{Q} \notin \Sigma_\Lambda$, determine the structure of the Selmer group $H^1_{\mathcal{F}_\mathfrak{Q}}(K, A_\mathfrak{Q})$ (or rather the order of the quotient by the maximal divisible subgroup), and then consider what happens as $\mathfrak{Q}$ 'approaches' $\mathfrak{P}$. Fix a generator g of $\mathfrak{P}$, and let $\mathfrak{Q} = (g + p^m)\Lambda$ for some integer m. By Hensel's lemma, for $m \gg 0$ there is an isomorphism of rings (but not Λ-modules) $\Lambda/\mathfrak{P} \cong \Lambda/\mathfrak{Q}$, and we take m large enough that this is so. In particular $\mathfrak{Q}$ is a height-one prime, and, increasing m if needed, we assume that $\mathfrak{Q}$ is not contained in Σ_Λ and does not divide f_Λ.

Let d denote the Weierstrass degree of $\mathfrak{P}$ (i.e. the $\mathbb{Z}_p$-rank of $\Lambda/\mathfrak{P}$). We now argue as in the proof of [MR04, Proposition 5.3.10]. Using the notation of Proposition 2.1.3, Proposition 2.2.8 and the equality of ideals $(\mathfrak{Q}, \mathfrak{P}^n) = (\mathfrak{Q}, p^{mn})$ imply that one has the equalities

$$\begin{aligned}
\mathrm{length}_{\mathbb{Z}_p} H^1_{\mathcal{F}_\mathfrak{Q}}(K, T_\mathfrak{Q})/S_\mathfrak{Q}\kappa_1^{(\mathfrak{Q})} &= \mathrm{length}_{\mathbb{Z}_p} \Lambda/(f_\Lambda, \mathfrak{Q}) \\
&= \mathrm{length}_{\mathbb{Z}_p} \Lambda/(\mathfrak{P}^{\mathrm{ord}_\mathfrak{P}(f_\Lambda)}, \mathfrak{Q}) \\
&= md\,\mathrm{ord}_\mathfrak{P}(f_\Lambda)
\end{aligned}$$

up to $O(1)$ as m varies. Similarly, we have

$$\begin{aligned}
2\,\mathrm{length}_{\mathbb{Z}_p} M_\mathfrak{Q} &= \mathrm{length}_{\mathbb{Z}_p} H^1_{\mathcal{F}_\mathfrak{Q}}(K, A_\mathfrak{Q})_{/\mathrm{div}} \\
&= \mathrm{length}_{\mathbb{Z}_p} (X/\mathfrak{Q}X)_{\mathbb{Z}_p\text{-tors}} \\
&= md\,\mathrm{ord}_\mathfrak{P}(\mathrm{char}(X_{\Lambda\text{-tors}}))
\end{aligned}$$

up to $O(1)$ as m varies. Here $H^1_{\mathcal{F}_\mathfrak{Q}}(K, A_\mathfrak{Q})_{/\mathrm{div}}$ denotes the quotient of $H^1_{\mathcal{F}_\mathfrak{Q}}(K, A_\mathfrak{Q})$ by its maximal $\mathbb{Z}_p$-divisible submodule. Applying Proposition 2.1.3 at the prime $\mathfrak{Q}$ and letting $m \to \infty$ we deduce that

$$\mathrm{ord}_\mathfrak{P}(\mathrm{char}(X_{\Lambda\text{-tors}})) \leqslant 2\,\mathrm{ord}_\mathfrak{P}(f_\Lambda). \tag{16}$$

The case $\mathfrak{P} = p\Lambda$ is dealt with in an entirely similar fashion, taking $\mathfrak{Q} = T^m + p \in \mathbb{Z}_p[[T]]$. This shows that part c of the theorem follows from part b.

To prove part b, keep $\mathfrak{P} \neq p\Lambda$ and $\mathfrak{Q}$ as above. Fix a pseudo-isomorphism

$$X_{\Lambda\text{-tors}} \sim N \oplus N_\mathfrak{P},$$

where $\mathrm{char}(N)$ is prime to $\mathfrak{P}$, and $N_\mathfrak{P}$ is isomorphic to $\bigoplus_i \Lambda/\mathfrak{P}^{e_i}$. The dual of the second map of Proposition 2.2.8 induces the third arrow of the composition

$$N_\mathfrak{P} \otimes_\Lambda S_\mathfrak{Q} \to X_{\Lambda\text{-tors}} \otimes_\Lambda S_\mathfrak{Q} \to (X \otimes_\Lambda S_\mathfrak{Q})_{\mathbb{Z}_p\text{-tors}} \to M_\mathfrak{Q} \oplus M_\mathfrak{Q},$$

and this composition has finite kernel and cokernel, bounded as m varies. Fixing a ring isomorphism

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

$S_{\mathfrak{P}} \cong S_{\mathfrak{Q}}$ (which will not be an isomorphism of Λ-modules), we may view $N_{\mathfrak{P}} \otimes_{\Lambda} S_{\mathfrak{Q}}$ as an $S_{\mathfrak{P}}$-module, isomorphic to $\bigoplus_i S_{\mathfrak{P}}/p^{me_i}S_{\mathfrak{P}}$. Letting D_m denote $M_{\mathfrak{Q}}$, viewed as an $S_{\mathfrak{P}}$-module, we now have $S_{\mathfrak{P}}$-module maps

$$\bigoplus_i S_{\mathfrak{P}}/p^{me_i}S_{\mathfrak{P}} \to D_m \oplus D_m$$

with kernels and cokernels bounded as m varies. An elementary argument shows that, for a given e, $\{i \mid e_i = e\}$ has an even number of elements. The case $\mathfrak{P} = p\Lambda$ is dealt with similarly, again taking $\mathfrak{Q} = T + p^m \in \mathbb{Z}_p[[T]]$.

The functional equation $\mathrm{char}(M) = \mathrm{char}(M)^{\iota}$ follows from the functional equation of [Nek01a]

$$\mathrm{char}(X_{\Lambda\text{-tors}}) = \mathrm{char}(X_{\Lambda\text{-tors}})^{\iota}. \qquad \square$$

2.3 The anticyclotomic Euler system

We retain all notation and assumptions from the introduction to § 2, and in addition assume that p does not divide the class number of K. Denote by K_k the subfield of the anticyclotomic extension K_∞/K satisfying $[K_k : K] = p^k$. By the assumption on the class number of K, K_∞/K is linearly disjoint from the Hilbert class field $K[1]$, and K_k is the maximal p-power subextension of $K[p^{k+1}]/K$. Let $\mathbf{T}$ and $\mathbf{A}$ be as in Definition 2.2.3 and let $\mathcal{F}_\Lambda$ be the Selmer structure of Definition 2.2.6. Define $\mathcal{L} = \mathcal{L}_1(\mathbf{T})$. The majority of this subsection is devoted to the proof of the following theorem, which involves a series of lemmas and a further theorem.

Theorem 2.3.1. *There exists a Kolyvagin system $\kappa^{\mathrm{Hg}} \in \mathbf{KS}(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L})$ such that $\kappa_1^{\mathrm{Hg}} \in H^1_{\mathcal{F}_\Lambda}(K, \mathbf{T})$ is nonzero.*

For $n \in \mathcal{N}$ let $K_k[n]$ be the compositum of K_k and $K[n]$, and let $K_\infty[n]$ be the union over all k of $K_k[n]$. There is a canonical isomorphism

$$(\mathcal{O}_K/p\mathcal{O}_K)^\times/(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathrm{Gal}(K[np^{k+1}]/K_k[n]),$$

and we denote this group by Δ. Let $\delta = |\Delta|$. If p is split in K we let σ and σ^* denote the Frobenius automorphisms in $\mathcal{G}(n) = \mathrm{Gal}(K[n]/K)$ of the primes above p. Define $\gamma_k, \Phi \in \mathbb{Z}_p[\mathcal{G}(n)]$ by the formulas

$$\Phi = \begin{cases} (p+1)^2 - a_p^2 & \text{inert case,} \\ (p - a_p\sigma + \sigma^2)(p - a_p\sigma^* + \sigma^{*2}) & \text{split case,} \end{cases}$$

$$\gamma_0 = \begin{cases} a_p & \text{inert case,} \\ a_p - \sigma - \sigma^* & \text{split case,} \end{cases}$$

$$\gamma_1 = a_p\gamma_0 - \delta,$$

$$\gamma_k = a_p\gamma_{k-1} - p\gamma_{k-2} \quad \text{for } k > 1,$$

where split and inert refer to the behavior of the rational prime p in K.

Define points $P_k[n] \in E(K_k[n])$ by

$$P_k[n] = \mathrm{Norm}_{K[np^{k+1}]/K_k[n]} P[np^{k+1}]$$

for $k \geqslant 0$, and denote by $H_k[n]$ the $\mathbb{Z}_p[\mathrm{Gal}(K_k[n]/K)]$-submodule of $E(K_k[n]) \otimes \mathbb{Z}_p$ generated by

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

$P[n]$ and $P_j[n]$ for all $j \leqslant k$. It follows from § 3.1 of [Per87] that one has the relations

$$P_0[n] = \gamma_0 P[n],$$
$$\mathrm{Norm}_{K_{k+1}[n]/K_k[n]}\, P_{k+1}[n] = \begin{cases} a_p P_k[n] - P_{k-1}[n] & \text{for } k > 0, \\ \gamma_1 P[n] & \text{for } k = 0, \end{cases}$$
$$\mathrm{Norm}_{K_k[n\ell]/K_k[n]}\, P_k[n\ell] = a_\ell P_k[n],$$

and an easy inductive argument using the first two of these relations shows that

$$\mathrm{Norm}_{K_k[n]/K[n]}\, P_k[n] = \gamma_k P[n] \quad \text{for } k \geqslant 0.$$

We observe also that the norm from $K_{k+1}[n]$ to $K_k[n]$ takes $H_{k+1}[n]$ into $H_k[n]$, and so we may define for every $n \in \mathcal{N}$ a $\Lambda[\mathcal{G}(n)]$-module

$$\mathbf{H}[n] = \varprojlim H_k[n].$$

Lemma 2.3.2. *If M is any finitely generated $\mathbb{Z}_p[\mathcal{G}(n)]$-module, the intersection of $\gamma_k M$ for $k \geqslant 1$ is equal to ΦM.*

Proof. This is Corollary 5 of § 3.3 of [Per87]. □

Lemma 2.3.3. *There exists a family*

$$\{Q[n] = \varprojlim Q_k[n] \in \mathbf{H}[n]\}_{n \in \mathcal{N}}$$

such that $Q_0[n] = \Phi P[n]$, and for any $n\ell \in \mathcal{N}$

$$\mathrm{Norm}_{K_\infty[n\ell]/K_\infty[n]}\, Q[n\ell] = a_\ell Q[n].$$

Proof. Fix an $n \in \mathcal{N}$ and let $\tilde{H}_k$ be the free $\mathbb{Z}_p[\mathrm{Gal}(K_k[n]/K)]$-module on generators $\{x, x_j \mid 0 \leqslant j \leqslant k\}$, modulo relations of the form:

a) x is fixed by $\mathrm{Gal}(K_k[n]/K[n])$, and x_j is fixed by $\mathrm{Gal}(K_k[n]/K_j[n])$ for every $j \leqslant k$,
b) for $j > 1$, $\mathrm{Norm}_{K_j[n]/K_{j-1}[n]}\, x_j = a_p x_{j-1} - x_{j-2}$,
c) $\mathrm{Norm}_{K_1[n]/K_0[n]}\, x_1 = \gamma_1 x$, and $x_0 = \gamma_0 x$.

Then for each $j \leqslant k$,

$$\mathrm{Norm}_{K_j[n]/K_0[n]}\, x_j = \gamma_j x. \tag{17}$$

There is a natural inclusion $\tilde{H}_k \to \tilde{H}_{k+1}$ and a natural norm $\tilde{H}_{k+1} \to \tilde{H}_k$. By Lemma 2.3.2 and the relation (17), $\Phi x \in \tilde{H}_0$ is a norm from every $\tilde{H}_k$.

Let $y \in \tilde{\mathbf{H}} = \varprojlim \tilde{H}_k$ be a lift of Φx, and define, for any $m|n$, $Q[m]$ to be the image of y under the map $\phi(m) : \tilde{\mathbf{H}} \to \mathbf{H}[m]$ which sends $x_k \mapsto P_k[m]$ and $x \mapsto P[m]$. For any $m\ell|n$, the diagram

$$\begin{array}{ccc} \tilde{\mathbf{H}} & \xrightarrow{\phi(m\ell)} & \mathbf{H}[m\ell] \\ \downarrow{\scriptstyle a_\ell} & & \downarrow \\ \tilde{\mathbf{H}} & \xrightarrow{\phi(m)} & \mathbf{H}[m] \end{array}$$

commutes, where the right vertical arrow is the norm from $K_\infty[m\ell]$ to $K_\infty[m]$, and so we obtain a family $\{Q[m]\}_{m|n}$ with the desired properties.

An easy argument shows that the Λ-module of such 'partial' families (i.e. where m runs through divisors of a fixed n) is compact, and so the inverse limit over all $n \in \mathcal{N}$ is nonempty. □

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Fix a family $Q[n]$ as in Lemma 2.3.3. Exactly as in § 1.7, we fix a generator σ_ℓ of $G(\ell)$ for every $\ell \in \mathcal{L}$ and define derivative operators

$$D_n \in \mathbb{Z}_p[G(n)] \subset \Lambda[G(n)].$$

Fix a set of coset representatives S of $G(n) \subset \mathcal{G}(n)$. Let

$$\tilde{\kappa}_n = \sum_{s \in S} sD_nQ[n] \in \mathbf{H}[n].$$

For $\ell \in \mathcal{L}$, the ideal $I_\ell \subset \mathbb{Z}_p$ is generated by $\ell + 1$ and a_ℓ, and the image of $\tilde{\kappa}_n$ in $\mathbf{H}[n]/I_n\mathbf{H}[n]$ is fixed by $\mathcal{G}(n)$ (see Lemma 1.7.1).

The Kummer map $\delta_k(n) : E(K_k[n]) \otimes \mathbb{Z}_p \to H^1(K_k[n], T_p(E))$ induces a map

$$\begin{aligned}\delta(n) = \varprojlim \delta_k(n) : \mathbf{H}[n] &\to \varprojlim H^1(K_k[n], T_p(E)) \\ &\cong H^1(K[n], \mathbf{T}),\end{aligned}$$

and we define κ_n to be the unique preimage of $\delta(n)(\tilde{\kappa}_n)$ under the isomorphism

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

(the bijectivity being a consequence of

$$H^0(K[n], \mathbf{T}/I_n\mathbf{T}) \cong \varprojlim H^0(K_k[n], E[I_n]) = 0,$$

since E has no p-torsion defined over any abelian extension of K).

Lemma 2.3.4. *For every $n \in \mathcal{N}$, $\kappa_n \in H^1_{\mathcal{F}_\Lambda(n)}(K, \mathbf{T}/I_n\mathbf{T})$.*

Proof. The proof that the localization of κ_n at primes of K dividing n lies in the transverse subspace is exactly as in the proof of Lemma 1.7.3.

It remains to show that at every prime v of K not dividing n, the localization of κ_n at v is contained in $H^1_{\mathcal{F}_\Lambda}(K_v, \mathbf{T}/I_n\mathbf{T})$, the image of the map

$$H^1_{\mathcal{F}_\Lambda}(K_v, \mathbf{T}) \to H^1(K_v, \mathbf{T}/I\mathbf{T}).$$

Fix a prime v of K not dividing n and let w be a prime of $K[n]$ above v.

Case i: $v \nmid pN$. We first observe that

$$H^1_{\mathcal{F}_\Lambda}(K_v, \mathbf{T}/I_n\mathbf{T}) = H^1_{\mathrm{unr}}(K_v, \mathbf{T}/I_n\mathbf{T}).$$

Indeed, since $\mathrm{Gal}(K_v^{\mathrm{unr}}/K_v)$ has cohomological dimension one, the map

$$H^1_{\mathrm{unr}}(K_v, \mathbf{T}) \to H^1_{\mathrm{unr}}(K_v, \mathbf{T}/I_n\mathbf{T})$$

is surjective. Using the injectivity of torsion points in the reduction of E at w, the image of the Kummer map

$$\delta_k(N) : H_k[n] \to \bigoplus_{w'|w} H^1(K_k[n]_{w'}, T) \cong H^1(K[n]_w, \mathrm{Ind}_{K_k/K} T)$$

is unramified, and passing to the limit shows that the image of

$$\delta(n) : \mathbf{H}[n] \to H^1(K[n], \mathbf{T}) \to H^1(K[n]_w, \mathbf{T})$$

is unramified at w. Therefore $\delta(n)(\tilde{\kappa}_n)$ is unramified, and so also is κ_n.

Case ii: $v|N$. In this case the Heegner hypothesis implies that the prime w is finitely decomposed in $K_\infty[n]$. Proposition B.3.4 of [Rub00] gives the equality

$$H^1(K_v, \mathbf{T}) = H^1_{\mathrm{unr}}(K_v, \mathbf{T}),$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

and we must therefore show that $\mathrm{loc}_v(\kappa_n)$ is in the image of

$$H^1(K_v, \mathbf{T}) \to H^1(K_v, \mathbf{T}/I_n\mathbf{T}).$$

On the other hand, the restriction of κ_n to $H^1(K[n]_w, \mathbf{T}/I_n\mathbf{T})$ comes from $H^1(K[n]_w, \mathbf{T})$ (namely from the localization of $\delta(n)(\tilde{\kappa}_n)$) and so it suffices to check that the right vertical arrow in the exact and commutative diagram

$$\begin{array}{ccccc} H^1(K_v, \mathbf{T}) & \longrightarrow & H^1(K_v, \mathbf{T}/I_n\mathbf{T}) & \longrightarrow & H^2(K_v, \mathbf{T}) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(K[n]_w, \mathbf{T}) & \longrightarrow & H^1(K[n]_w, \mathbf{T}/I_n\mathbf{T}) & \longrightarrow & H^2(K[n]_w, \mathbf{T}) \end{array}$$

is an injection. Applying local duality and Shapiro's lemma, this is equivalent to the surjectivity of the norm map

$$\bigoplus_{w'|w} E(K_\infty[n]_{w'})[p^\infty] \to \bigoplus_{v'|v} E(K_{\infty,v'})[p^\infty],$$

which is a consequence of the observation that the degree of $K_\infty[n]_{w'}$ over $K_{\infty,v'}$ is prime to p. Indeed, any intermediary extension

$$K_{\infty,v'} \subset F \subset K_\infty[n]_{w'}$$

of p-power order over $K_{\infty,v'}$ would be contained in the union of all unramified p-power extensions of K_v, and this union is $K_{\infty,v'}$, the unique $\mathbb{Z}_p$-extension of K_v.

Case iii: $v|p$. For each prime w of $K[n]$, fix an extension of w to $\bar{K}$ and denote by $\mathrm{Fil}_w(T)$ the kernel of the reduction map $T \to T_p(\tilde{E})$ at that place. Set $\mathrm{gr}_w(T) = T/\mathrm{Fil}(T)$. Let

$$\mathrm{Fil}_w(\mathbf{T}) = \mathrm{Fil}_w(T) \otimes \Lambda \subset \mathbf{T}, \quad \mathrm{gr}_w(\mathbf{T}) = \mathbf{T}/\mathrm{Fil}_w(\mathbf{T}),$$

and define

$$H^1_{\mathrm{ord}}(K[n]_w, \mathbf{T}) = \mathrm{image}(H^1(K[n]_w, \mathrm{Fil}_w(\mathbf{T})) \to H^1(K[n]_w, \mathbf{T})).$$

We first claim that the image of the composition

$$\mathbf{H}[n] \xrightarrow{\delta(n)} H^1(K[n], \mathbf{T}) \to H^1(K[n]_w, \mathbf{T})$$

lies in $H^1_{\mathrm{ord}}(K[n]_w, \mathbf{T})$. To see this, let $L_k = K_k[n]_w$ and consider the composition

$$H_k[n] \to H^1(L_k, T) \to H^1(L_k, \mathrm{gr}_w(T)) \to H^1(L_k^{\mathrm{unr}}, \mathrm{gr}_w(T)).$$

It is clear from the definition of the Kummer map that this composition is trivial, and so any $Q_k \in H_k[n]$ yields a class in the kernel of the final arrow,

$$H^1(L_k^{\mathrm{unr}}/L_k, \mathrm{gr}_w(T)) \cong \mathrm{gr}_w(T)/(\mathrm{Fr} - 1)\,\mathrm{gr}_w(T) \cong \tilde{E}(\mathbf{F}[n])[p^\infty],$$

where $\mathbf{F}[n]$ is the residue field of $K[n]_w$, and using the fact that $L_k/K[n]_w$ is totally ramified. If the point Q_k can be lifted to a universal norm in $\mathbf{H}[n]$, then this class can be lifted to an element of the p-adic Tate module of the finite group $\tilde{E}(\mathbf{F}[n])[p^\infty]$, which is trivial. The composition

$$\mathbf{H}[n] \to H^1(L_k, T) \to H^1(L_k, \mathrm{gr}_w(T))$$

is therefore trivial, and the claim follows.

The above shows that the restriction of κ_n to $H^1(L_0, \mathbf{T}/I_n\mathbf{T})$ lies in the image of $H^1(L_0, \mathrm{Fil}_w(\mathbf{T}))$ under the natural map. For brevity, we write

$$\mathbf{T}^+ = \mathrm{Fil}_w(\mathbf{T}), \quad \mathbf{T}^- = \mathrm{gr}_w(\mathbf{T}).$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Consider the following exact and commutative diagram.

$$\begin{array}{ccccc} H^1(K_v, \mathbf{T}^+/I_n\mathbf{T}^+) & \longrightarrow & H^1(K_v, \mathbf{T}/I_n\mathbf{T}) & \longrightarrow & H^1(K_v, \mathbf{T}^-/I_n\mathbf{T}^-) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(L_0, \mathbf{T}^+/I_n\mathbf{T}^+) & \longrightarrow & H^1(L_0, \mathbf{T}/I_n\mathbf{T}) & \longrightarrow & H^1(L_0, \mathbf{T}^-/I_n\mathbf{T}^-) \end{array}$$

The image $\mathrm{loc}_v(\kappa_n)$ in the lower right corner is trivial, and the kernel of the right-hand vertical map is

$$\varprojlim H^1(K_\infty[n]_w/K_{\infty,v}, \tilde{E}(\mathbf{F}[n])[I_n]),$$

where the inverse limit is with respect to multiplication by p. This is clearly zero, and so we may choose an $\alpha \in H^1(K_v, \mathbf{T}^+/I_n\mathbf{T}^+)$ which lifts κ_n. It is easily seen that the bottom left horizontal arrow is injective, and so the image of α under the left vertical arrow is the unique lift to $H^1(L_0, \mathbf{T}^+/I_n\mathbf{T}^+)$ of the restriction of κ_n to $H^1(L_0, \mathbf{T}/I_n\mathbf{T})$, which is already known to be in the image of $H^1(L_0, \mathbf{T}^+)$. In other words, in the diagram

$$\begin{array}{ccccc} H^1(K_v, \mathbf{T}^+) & \longrightarrow & H^1(K_v, \mathbf{T}^+/I_n\mathbf{T}^+) & \longrightarrow & H^2(K_v, \mathbf{T}^+) \\ \downarrow & & \downarrow & & \downarrow \\ H^1(L_0, \mathbf{T}^+) & \longrightarrow & H^1(L_0, \mathbf{T}^+/I_n\mathbf{T}^+) & \longrightarrow & H^2(L_0, \mathbf{T}^+) \end{array}$$

the image of α in the lower right corner is trivial.

To complete the proof of the lemma, we need only show that the right vertical arrow is injective. By local duality, the injectivity of this map is equivalent to surjectivity of the norm map

$$\tilde{E}(\mathbf{F}[n])[p^\infty] \to \tilde{E}(\mathbf{F})[p^\infty]$$

(where $\mathbf{F}$ is the residue field of K_v), and this follows from

$$H^1(\mathbf{F}[n]/\mathbf{F}, \tilde{E}(\mathbf{F}[n])[p^\infty]) \hookrightarrow H^1(\mathbf{F}, \tilde{E}[p^\infty]) \cong \tilde{E}[p^\infty]/(\mathrm{Fr} - 1)\tilde{E}[p^\infty] = 0$$

and the fact that the Herbrand quotient of a finite cyclic group acting on a finite module is equal to 1. This completes the proof of Lemma 2.3.4. □

Fix $n\ell \in \mathcal{N}$ and let λ be the prime of K above ℓ and λ' a fixed place of $\bar{K}$ above λ. Such a choice gives a canonical extension of each prime w of K_k above λ to a prime w' of $K_k[n\ell]$. Namely the unique place which restricts to w in K_k and to λ' in $K[n\ell]$ (recall that λ splits completely in $K_\infty[n\ell]$). This determines a map of Λ-modules

$$\Psi : \mathbf{H}[n\ell] \to \varprojlim \bigoplus_w \tilde{E}(\mathbf{F}_w), \tag{18}$$

where the limit is over k, the sum is over primes of K_k above λ, and $\mathbf{F}_w$ is the residue field of w. Each summand is canonically identified with the points of $\tilde{E}$ rational over the residue field of K at λ (which we denote by $\mathbf{F}_\lambda$), and Λ acts by permuting summands. The module on the right-hand side of (18) comes equipped with a natural involution Fr_ℓ which acts as the nontrivial automorphism of $\mathbf{F}_w/\mathbf{F}_\ell$ on each summand. The action of Fr_ℓ commutes with the action of Λ.

The following is the analogue of the congruence (13) of § 1.7.

Lemma 2.3.5. *For any $t \in \Lambda[\mathcal{G}(n\ell)]$, $\Psi(t \cdot Q[n\ell]) = \mathrm{Fr}_\ell\, \Psi(t \cdot Q[n])$.*

Proof. Exactly as in (13), for any prime w' of $K_k[n\ell]$ above ℓ and any $j \leqslant k$, we have

$$P_j[n\ell] \equiv \left(\frac{w'}{K_k[n\ell]/\mathbb{Q}}\right) P_j[n] \pmod{w'},$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

which implies that for any $t \in \mathbb{Z}_p[\mathrm{Gal}(K_k[n\ell]/K)]$

$$\Psi_k(t \cdot P_j[n\ell]) = \mathrm{Fr}_\ell\, \Psi_k(t \cdot P_j[n]),$$

where $\Psi_k : H_k[n\ell] \to \bigoplus_w \tilde{E}(\mathbf{F}_w)$ (the sum is over primes of K_k above λ) is the map Ψ at finite levels. By construction of $Q[n\ell]$ there are elements

$$\{t_j \in \mathbb{Z}_p[\mathrm{Gal}(K_k[n\ell]/K)] \mid 0 \leqslant j \leqslant k\}$$

such that $Q_k[m] = \sum_{j=0}^k t_j P_j[m]$ for every $m | n\ell$ (in particular the t_j do not depend on m), and the lemma follows easily. □

Our choice of λ' also fixes an isomorphism

$$E[I_{n\ell}] \otimes \Lambda \cong \mathbf{T}/I_{n\ell}\mathbf{T} \cong \varprojlim \bigoplus_w \tilde{E}(\mathbf{F}_w)[I_{n\ell}] \tag{19}$$

which sends elements of the form $P \otimes \sigma$ to the reduction of P at λ' living in the summand attached to the prime $\sigma\lambda'$ of K_∞. Exactly as in the proof of Proposition 1.7.4 we have an explicit description of the image of $\kappa_{n\ell} \otimes \sigma_\ell$ under the isomorphism

$$H^1_{\mathrm{s}}(K_\lambda, \mathbf{T}/I_{n\ell}\mathbf{T}) \otimes G_\ell \to \mathbf{T}/I_{n\ell}\mathbf{T} \cong E[I_{n\ell}] \otimes \Lambda \to \varprojlim \bigoplus_w \tilde{E}(\mathbf{F}_w)[I_{n\ell}],$$

namely

$$\kappa_{n\ell} \otimes \sigma_\ell \mapsto \Psi\left(-\frac{(\sigma_\ell - 1)\tilde{\kappa}_{n\ell}}{p^{M_{n\ell}}}\right),$$

where $p^{M_{n\ell}}\mathbb{Z}_p = I_{n\ell}$, and the right-hand side is interpreted as the image of the unique $p^{M_{n\ell}}$-divisor of $-(\sigma_\ell - 1)\tilde{\kappa}_{n\ell}$ in $H[n\ell]$ under the map (18) (uniqueness follows from the fact that our assumptions on E imply that E has no p-torsion defined over any abelian extension of K).

Lemma 2.3.6. *We have that*

$$\Psi\left(-\frac{(\sigma_\ell - 1)\tilde{\kappa}_{n\ell}}{p^{M_{n\ell}}}\right) = \frac{a_\ell - (\ell+1)\,\mathrm{Fr}_\ell}{p^{M_{n\ell}}}\Psi(\tilde{\kappa}_n).$$

Proof. In $\mathbf{H}[n\ell]$ we have the equalities

$$\begin{aligned}
-\frac{(\sigma_\ell - 1)\tilde{\kappa}_{n\ell}}{p^{M_{n\ell}}} &= -\frac{\sum_{s\in S}(\ell + 1 - \mathrm{Norm}_\ell)sD_nQ[n\ell]}{p^{M_{n\ell}}} \\
&= \sum_{s\in S} sD_n\left(\frac{a_\ell}{p^{M_{n\ell}}}Q[n] - \frac{\ell+1}{p^{M_{n\ell}}}Q[n\ell]\right) \\
&= \frac{a_\ell}{p^{M_{n\ell}}}\tilde{\kappa}_n - \frac{\ell+1}{p^{M_{n\ell}}}\sum_{s\in S} sD_nQ[n\ell].
\end{aligned}$$

Now apply the preceding lemma. □

As in the proof of Proposition 1.7.4, we define a map χ_ℓ as the composition

$$\varprojlim \bigoplus_w E(K_{k,w}) \to \varprojlim \bigoplus_w \tilde{E}(\mathbf{F}_w)[p^\infty] \to \varprojlim \bigoplus_w \tilde{E}(\mathbf{F}_w)[I_\ell] \cong \mathbf{T}/I_\ell\mathbf{T},$$

where the second arrow is given by the action of $[a_\ell - (\ell+1)\,\mathrm{Fr}_\ell]/p^{M_\ell}$. This map factors through

$$\left(\varprojlim \bigoplus_w E(K_{k,w})\right) \otimes_\Lambda \Lambda/I_\ell \cong H^1_{\mathrm{f}}(K_\lambda, \mathbf{T}/I_\ell\mathbf{T}) \cong \mathbf{T}/I_\ell\mathbf{T},$$

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

where the first map is the Kummer map and the second is evaluation of cocycles at Frobenius. The resulting automorphism of $\mathbf{T}/I_\ell\mathbf{T}$ is again called χ_ℓ, and satisfies

$$\chi_\ell(\kappa_n(\mathrm{Fr}_\lambda)) = \frac{a_\ell - (\ell+1)\,\mathrm{Fr}_\ell}{p^{M_{n\ell}}}\Psi(\tilde{\kappa}_n) = \kappa_{n\ell}(\sigma_\ell).$$

The classes κ_n may now be modified exactly as in Theorem 1.7.5 to produce a Kolyvagin system $\kappa^{\mathrm{Hg}} \in \mathbf{KS}(\mathbf{T}, \mathcal{F}_\Lambda, \mathcal{L})$ with $\kappa_1^{\mathrm{Hg}} = \kappa_1$.

Now we turn our attention to the proof that κ_1^{Hg} is nontrivial. Let

$$H_k \subset E(K_k) \otimes \mathbb{Z}_p$$

be the Λ-submodule generated by $\mathrm{Norm}_{K[1]/K} P[1]$ and $\mathrm{Norm}_{K_k[1]/K_k} P_j[1]$ for $0 \leqslant j \leqslant k$, and let $\mathbf{H} = \varprojlim H_k$. Since κ_1^{Hg} is the image of $\tilde{\kappa}_1$ under the injective Kummer map $\mathbf{H} \to H^1(K, \mathbf{T})$, to complete the proof of Theorem 2.3.1 it suffices to prove the following theorem.

Theorem 2.3.7. *The Λ-module $\mathbf{H}$ is free of rank one, generated by $\tilde{\kappa}_1$.*

Proof. By the main result of [Cor02], one of the points $\mathrm{Norm}_{K_k[1]/K_k} P_k[1]$ has infinite order, and so Proposition 10 of § 3 of [Per87] implies that $\mathbf{H}$ is free of rank one. We show that $\tilde{\kappa}_1$ is a generator.

Recall the construction of $\tilde{\kappa}_1$. There is a canonical decomposition

$$\mathrm{Gal}(K_k[1]/K) \cong \Gamma_k \times \mathcal{G},$$

where $\Gamma_k = \mathrm{Gal}(K_k/K)$ and $\mathcal{G} = \mathcal{G}(1)$ is the ideal class group of K (which has no p-torsion by assumption). We let $\mathrm{Norm}_{\mathcal{G}}$ be the norm element in $\mathbb{Z}_p[\mathcal{G}] \subset \Lambda[\mathcal{G}]$. Let $\tilde{H}_k$ be the $\mathbb{Z}_p[\Gamma_k \times \mathcal{G}]$-module defined in the proof of Lemma 2.3.3 (with $n = 1$), and let $\tilde{\mathbf{H}} = \varprojlim \tilde{H}_k$, the limit with respect to the norm maps. We may choose an element $y \in \tilde{\mathbf{H}}$ which lifts $\Phi x \in \tilde{H}_0$. Let

$$x_j^{\mathcal{G}} = \mathrm{Norm}_{\mathcal{G}(1)}\, x_j \in \tilde{H}_k^{\mathcal{G}}, \quad y^{\mathcal{G}} = \mathrm{Norm}_{\mathcal{G}(1)}\, y \in \tilde{\mathbf{H}}^{\mathcal{G}}$$

(including the case where j is the empty subscript).

We have the following commutative diagram in which all arrows are surjective and the vertical arrows are $\mathrm{Norm}_{\mathcal{G}(1)}$.

$$\begin{array}{ccc} \tilde{\mathbf{H}} & \longrightarrow & \mathbf{H}[1] \\ \downarrow & & \downarrow \\ \tilde{\mathbf{H}}^{\mathcal{G}} & \longrightarrow & \mathbf{H} \end{array}$$

The top arrow takes x_j to $P_j[1]$, and the bottom arrow takes $x_j^{\mathcal{G}}$ to $\mathrm{Norm}_{\mathcal{G}(1)} P_j[1]$ and $y^{\mathcal{G}}$ to $\tilde{\kappa}_1$.

Fix a topological generator $\gamma \in \Gamma$. By Nakayama's lemma we will be done once we show that

$$\tilde{\mathbf{H}}^{\mathcal{G}} = \Lambda y^{\mathcal{G}} + (\gamma - 1)\tilde{\mathbf{H}}^{\mathcal{G}}.$$

This is immediate from the following two lemmas.

Lemma 2.3.8. *Let $\mathrm{aug} : \mathbb{Z}_p[\mathcal{G}(1)] \to \mathbb{Z}_p$ be the augmentation map. The image of the natural map $\tilde{\mathbf{H}}^{\mathcal{G}} \to \tilde{H}_0^{\mathcal{G}}$ is a free rank-one $\mathbb{Z}_p$-module generated by $\mathrm{aug}(\Phi)x^{\mathcal{G}}$, the image of $y^{\mathcal{G}}$.*

Proof. The $\mathbb{Z}_p$-module $\tilde{H}_0^{\mathcal{G}}$ is free of rank one, generated by $x^{\mathcal{G}}$, and one has the relations

$$\mathrm{Norm}_{K_k/K}(x_k^{\mathcal{G}}) = \mathrm{aug}(\gamma_k)x^{\mathcal{G}}.$$

Lemma 2.3.2 implies that $\bigcap_{k>0} \mathrm{aug}(\gamma_k)\mathbb{Z}_p = \mathrm{aug}(\Phi)\mathbb{Z}_p$, and an elementary argument using the recursion relation defining γ_k shows that $\mathrm{aug}(\gamma_k)\mathbb{Z}_p = \mathrm{aug}(\Phi)\mathbb{Z}_p$ for $k \gg 0$. The lemma follows. □

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press

Lemma 2.3.9. *The map of the preceding lemma induces an isomorphism*

$$\tilde{\mathbf{H}}^{\mathcal{G}}/(\gamma-1)\tilde{\mathbf{H}}^{\mathcal{G}} \to \mathrm{aug}(\Phi)\tilde{H}_0^{\mathcal{G}}.$$

Proof. We have seen that it is a surjection, so suppose $h = \varprojlim h_k$ is in the kernel of $\tilde{\mathbf{H}}^{\mathcal{G}} \to \tilde{H}_0^{\mathcal{G}}$. The Λ-module $\tilde{H}_k^{\mathcal{G}}$ is generated by $x_k^{\mathcal{G}}$ and $x_{k-1}^{\mathcal{G}}$, and so h_k may be written in the form

$$h_k = \alpha_k x_k^{\mathcal{G}} + \beta_k x_{k-1}^{\mathcal{G}} + (\gamma-1)z_k$$

for α_k and β_k in $\mathbb{Z}_p$. Taking the norm to $\tilde{H}_0^{\mathcal{G}}$ and using the fact that $x^{\mathcal{G}}$ has infinite order yields

$$0 = \alpha_k \,\mathrm{aug}(\gamma_k) + p\beta_k \,\mathrm{aug}(\gamma_{k-1})$$

and so

$$\mathrm{aug}(\gamma_k)h_k \in \beta_k s_k + (\gamma-1)\tilde{H}_k^{\mathcal{G}},$$

where $s_k = -p\,\mathrm{aug}(\gamma_{k-1})x_k^{\mathcal{G}} + \mathrm{aug}(\gamma_k)x_{k-1}^{\mathcal{G}}$. The recursion relation for the γ_j and the norm relations for the x_j imply that the norm from $\tilde{H}_{k+1}^{\mathcal{G}}$ to $\tilde{H}_k^{\mathcal{G}}$ takes s_{k+1} to ps_k. If we take k large enough that $\mathrm{aug}(\gamma_\ell) = \mathrm{aug}(\Phi)$ for all $\ell \geqslant k$, and take $\ell \gg k$

$$\mathrm{aug}(\gamma_k)h_k = \mathrm{aug}(\gamma_\ell)\,\mathrm{Norm}_{\ell/k}\, h_\ell \in \beta_\ell p^{\ell-k} s_k + (\gamma-1)\tilde{H}_k^{\mathcal{G}}.$$

Letting $\ell \to \infty$ shows that $h_k \in (\gamma-1)\tilde{H}_k^{\mathcal{G}}$ for every k and the lemma follows. □

This completes the proof of Theorem 2.3.1 and 2.3.7 (and thus of Theorem 2.3.1). □

References

BD01b M. Bertolini and H. Darmon, *p-adic L-functions of modular elliptic curves*, in *Mathematics Unlimited – 2001 and Beyond* (Springer, Berlin, 2001).

Ber95 M. Bertolini, *Selmer groups and Heegner points in anticyclotomic* $\mathbf{Z}_p$*-extensions*, Compositio Math. **99** (1995), 153–182.

Bro82 K. Brown, *Cohomology of Groups* (Springer, Berlin, 1982).

CG96 J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), 129–174.

Cor02 C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2003), 495–523.

Fla90 M. Flach, *A generalisation of the Cassels–Tate pairing*, J. reine angew. Math. **412** (1990), 113–127.

Gre89 R. Greenberg, *Iwasawa theory for p-adic representations*, in *Algebraic number theory*, Advanced Studies in Pure Mathematics, vol. 17 (Princeton University Press, Princeton, NJ, 1989).

Gro91 B. Gross, *Kolyvagin's work on modular elliptic curves*, in *L-functions and arithmetic*, eds J. Coates and M. Taylor (Cambridge University Press, Cambridge, 1991), 235–256.

Guo93 L. Guo, *On a generalization of Tate dualities with applications to Iwasawa theory*, Compositio Math. **85** (1993), 125–161.

GZ86 B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

How04a B. Howard, *Derived p-adic heights and p-adic L-functions*, Amer. J. Math., to appear.

How04b B. Howard, *Iwasawa theory of Heegner points on abelian varieties of* GL_2 *type*, Duke Math. J., to appear.

McC91 W. McCallum, *Kolyvagin's work on Shafarevich–Tate groups*, in *L-functions and arithmetic*, eds J. Coates and M. Taylor (Cambridge University Press, Cambridge, 1991), 296–316.

Mil86 J. Milne, *Arithmetic duality theorems* (Academic Press, New York, 1986).

MR04 B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc., vol. 168, no. 799 (American Mathematical Society, Providence, RI, 2004).

Nek01a J. Nekovář, *Selmer complexes*, Unpublished manuscript (2001).

Nek01b J. Nekovář, *On the parity of ranks of Selmer groups II*, C. R. Acad. Sci. Paris Sér. 1 Math. **332** (2001), 99–104.

Per87 B. Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), 399–456.
Per00 B. Perrin-Riou, *p-adic L-functions and p-adic representations* (American Mathematical Society, Providence, RI, 2000).
Rub00 K. Rubin, *Euler systems* (Princeton University Press, Princeton, NJ, 2000).

Benjamin Howard howard@math.harvard.edu
Department of Mathematics, Stanford University, Stanford, CA 94305, USA
Current address: Department of Mathematics, Harvard University, Cambridge, MA 02138, USA

https://doi.org/10.1112/S0010437X04000569 Published online by Cambridge University Press