ANTICYCLOTOMIC IWASAWA THEORY OF CM ELLIPTIC CURVES

ADEBISI AGBOOLA AND BENJAMIN HOWARD

WITH AN APPENDIX BY KARL RUBIN

Abstract. We study the Iwasawa theory of a CM elliptic curve E in the anticyclotomic $\mathbf{Z}_p$-extension of the CM field, where p is a prime of good, ordinary reduction for E. When the complex L-function of E vanishes to even order, Rubin's proof of the two variable main conjecture of Iwasawa theory implies that the Pontryagin dual of the p-power Selmer group over the anticyclotomic extension is a torsion Iwasawa module. When the order of vanishing is odd, work of Greenberg shows that it is not a torsion module. In this paper we show that in the case of odd order of vanishing the dual of the Selmer group has rank exactly one, and we prove a form of the Iwasawa main conjecture for the torsion submodule.

0. Introduction and statement of results

Let K be an imaginary quadratic field of class number one, and let $E_{/\mathbf{Q}}$ be an elliptic curve with complex multiplication by the maximal order $\mathcal{O}_K$ of K. Let ψ denote the K-valued grossencharacter associated to E, and fix a rational prime $p > 3$ at which E has good, ordinary reduction.

Write $\mathbf{Q}_p^{\mathrm{unr}} \subset \mathbf{C}_p$ for the maximal unramified extension of $\mathbf{Q}_p$, and let R_0 denote the completion of its ring of integers. If F/K is any Galois extension, then we write $\Lambda(F) = \mathbf{Z}_p[[\mathrm{Gal}(F/K)]]$ for the generalised Iwasawa algebra, and we set $\Lambda(F)_{R_0} = R_0[[\mathrm{Gal}(F/K)]]$. Let C_∞ and D_∞ be the cyclotomic and anticyclotomic $\mathbf{Z}_p$-extensions of K, respectively, and let $K_\infty = C_\infty D_\infty$ be the unique $\mathbf{Z}_p^2$-extension of K.

As p is a prime of ordinary reduction for E, it follows that p splits into two distinct primes $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}^*$ over K. A construction of Katz gives a canonical measure

$$\mathcal{L} \in \Lambda(K_\infty)_{\mathrm{R}_0},$$

the two-variable p-adic L-function, denoted $\mu_{\mathfrak{p}^*}(K_\infty, \psi_{\mathfrak{p}^*})$ in the text, which interpolates the value at $s = 0$ of twists of $L(\psi^{-1}, s)$ by characters of $\mathrm{Gal}(K_\infty/K)$. It is a theorem of Coates [3] that the Pontryagin dual of the Selmer group $\mathrm{Sel}_{\mathfrak{p}^*}(E/K_\infty) \subset H^1(K_\infty, E[\mathfrak{p}^{*\infty}])$ is a torsion $\Lambda(K_\infty)$-module, and a fundamental theorem of Rubin, the two-variable Iwasawa main conjecture, asserts that the characteristic ideal of

---

Date: Final version. January 11, 2006.

2000 *Mathematics Subject Classification.* 11G05, 11R23, 11G16.

The first author is partially supported by NSF grant DMS-0070449.

The second author is supported by a National Science Foundation Mathematical Sciences Postdoctoral Research Fellowship.

The author of the appendix is partially supported by NSF grant DMS-0140378.

this torsion module is generated by $\mathcal{L}$. In many cases this allows one to deduce properties of the $\mathfrak{p}^*$-power Selmer group of E over subfields of K_∞. For example, if we identify

$$\Lambda(K_\infty) \cong \Lambda(D_\infty)[[\mathrm{Gal}(C_\infty/K)]]$$

and choose a topological generator $\gamma \in \mathrm{Gal}(C_\infty/K)$, then we may expand $\mathcal{L}$ as a power series in $(\gamma - 1)$

$$\mathcal{L} = \mathcal{L}_0 + \mathcal{L}_1(\gamma - 1) + \mathcal{L}_2(\gamma - 1)^2 + \cdots$$

with $\mathcal{L}_i \in \Lambda(D_\infty)_{\mathrm{R}_0}$. Standard "control theorems" imply that the characteristic ideal of

$$X^*(D_\infty) \stackrel{\mathrm{def}}{=} \mathrm{Hom}\big(\mathrm{Sel}_{\mathfrak{p}^*}(E/D_\infty), \mathbf{Q}_p/\mathbf{Z}_p\big)$$

(the reader should note Remark 1.1.8) is then generated by the constant term $\mathcal{L}_0$. If the sign in the functional equation of $L(E/\mathbf{Q}, s)$ is equal to 1, then theorems of Greenberg imply that $\mathcal{L}_0 \neq 0$, and so $X^*(D_\infty)$ is a torsion $\Lambda(D_\infty)$-module. In sharp contrast to this, when the sign of the functional equation is -1, the constant term vanishes and $X^*(D_\infty)$ is not torsion, as was proved by Greenberg even before Rubin's proof of the main conjecture (see [6]).

The following is the main result of this paper (which appears in the text as Theorems 2.4.17 and 3.1.5) and was inspired by conjectures of Mazur [12], Perrin-Riou [18] and Mazur-Rubin [15] concerning Heegner points.

Theorem A. *Suppose the sign of the functional equation of $L(E/\mathbf{Q}, s)$ is -1. Then $X^*(D_\infty)$ is a rank one $\Lambda(D_\infty)$-module. If $\mathcal{X} \subset \Lambda(D_\infty)$ is the characteristic ideal of the torsion submodule of $X^*(D_\infty)$, then*

$$\mathcal{X} \cdot \mathcal{R} = (\mathcal{L}_1)$$

as ideals of $\Lambda(D_\infty)_{R_0} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, where $\mathcal{R}$ is the regulator of the $\Lambda(D_\infty)$-adic height pairing (defined in Section 3).

A different statement of the Iwasawa main conjecture over D_∞, involving elliptic units and including the case where the sign in the functional equation is equal to 1, is also contained in Theorem 2.4.17. Similar results in the Heegner point case alluded to above can be found in [8]. T. Arnold [1] has recently generalized Theorem A from the case of elliptic curves with complex multiplication to CM modular forms of higher weight.

The following result is due to K. Rubin. It establishes a conjecture made in an earlier version of this paper, and a proof is given in the Appendix.

Theorem B. *Under the assumptions and notation of the Theorem A, the linear term $\mathcal{L}_1$ is nonzero.*

While we have stated our results in terms of the $\mathfrak{p}^*$-adic Selmer group, they may equally well be stated in terms of the $\mathfrak{p}$-adic Selmer group. If one replaces $\mathfrak{p}^*$ by $\mathfrak{p}$ in the above theorem, then $\mathcal{X}$, $\mathcal{L}_1$, and $\mathcal{R}$ are replaced by $\mathcal{X}^\iota$, $\mathcal{L}_1^\iota$, and $\mathcal{R}^\iota$, respectively, where ι is the involution of $\Lambda(D_\infty)$ induced by inversion on $\mathrm{Gal}(D_\infty/K)$. The decomposition $E[p^\infty] \cong E[\mathfrak{p}^\infty] \oplus E[\mathfrak{p}^{*\infty}]$ of $\mathrm{Gal}(K^{\mathrm{al}}/K)$-modules induces a decomposition of $\Lambda(D_\infty)$-modules

$$\mathrm{Sel}_p(E/D_\infty) \cong \mathrm{Sel}_{\mathfrak{p}}(E/D_\infty) \oplus \mathrm{Sel}_{\mathfrak{p}^*}(E/D_\infty)$$

which shows that, when the sign in the functional equation is -1, the full p-power Selmer group $\mathrm{Sel}_p(E/D_\infty)$ has $\Lambda(D_\infty)$-corank 2, as was conjectured by Mazur [12].

An outline of this paper is as follows. The first section gives definitions and fundamental properties of various Selmer groups associated to E, with special attention to the anticyclotomic tower. In the second section, we recall the definition of Katz's p-adic L-function and the Euler system of elliptic units, and we state a theorem of Yager which relates the two. Our discussion of these topics closely follows the excellent book of de Shalit [4]. Work of Rubin allows one to "twist" the elliptic unit Euler system into an Euler system for the $\mathfrak{p}$-adic Tate module $T_{\mathfrak{p}}(E)$, and we show, using nonvanishing results of Greenberg, that the restriction of the resulting Euler system to the anticyclotomic extension is nontrivial. Applying the main results of [25] shows that a certain "restricted" Selmer group, contained in $\mathrm{Sel}_{\mathfrak{p}^*}(E/D_\infty)$, is a cotorsion module; using this we show that $X^*(D_\infty)$ has rank one. Using a form of Mazur's control theorem, we then deduce that the characteristic ideal of a restricted Selmer group over K_∞ does not have an anticyclotomic zero. This restricted two-variable Selmer group is related to elliptic units by Rubin's proof of the two-variable main conjecture, and the nonvanishing of its characteristic ideal along the anticyclotomic line allows us to descend to the anticyclotomic extension and relate the restricted Selmer group over D_∞ to the elliptic units. In the third section we use results of Perrin-Riou and Rubin on the p-adic height pairing to relate the twisted elliptic units to the linear term $\mathcal{L}_1$ of Katz's L-function.

Acknowledgments. We are very grateful to Karl Rubin for writing an appendix to this paper.

0.1. **Notation and conventions.** We write ψ for the K-valued grossencharacter associated to E, and we let $\mathfrak{f}$ denote its conductor. Note that since p is a prime of good reduction for E, it follows that p is coprime to $\mathfrak{f}$.

Let $\mathbf{Q}^{\mathrm{al}} \subset \mathbf{C}$ be the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$, and let τ be complex conjugation, also denoted by $z \mapsto \bar{z}$. Fix an embedding $i_{\mathfrak{p}} : \mathbf{Q}^{\mathrm{al}} \hookrightarrow \mathbf{C}_p$ lying above the prime $\mathfrak{p}$, and let $i_{\mathfrak{p}^*} = i_{\mathfrak{p}} \circ \tau$ be the conjugate embedding.

We write R for the field of fractions of R_0. If M is any $\mathbf{Z}_p$-module, we define

$$M_{\mathrm{R}_0} = M \hat{\otimes}_{\mathbf{Z}_p} \mathrm{R}_0, \qquad M_{\mathrm{R}} = M_{\mathrm{R}_0} \otimes_{\mathrm{R}_0} \mathrm{R}.$$

The Pontryagin dual of M is denoted

$$M^\vee \stackrel{\mathrm{def}}{=} \mathrm{Hom}_{\mathbf{Z}_p}(M, \mathbf{Q}_p/\mathbf{Z}_p).$$

If M is any $\mathbf{Z}_p$-module of finite or cofinite type equipped with a continuous action of $G_K = \mathrm{Gal}(\mathbf{Q}^{\mathrm{al}}/K)$ and F is a (possibly infinite) Galois extension of K, we let

$$\mathcal{H}^i(F, M) = \varprojlim H^i(F', M)$$

where the inverse limit is over all subfields $F' \subset F$ finite over K and is taken with respect to the natural corestriction maps. If $\mathfrak{q}$ is $\mathfrak{p}$ or $\mathfrak{p}^*$, we define

$$\mathcal{H}^i(F_{\mathfrak{q}}, M) = \varprojlim \bigoplus_{w|\mathfrak{q}} H^i(F'_w, M), \qquad H^i(F_{\mathfrak{q}}, M) = \varinjlim \bigoplus_{w|\mathfrak{q}} H^i(F'_w, M).$$

(Here the inverse (respectively, direct) limit is taken with respect to the corestriction (respectively, restriction) maps.) These groups have natural $\Lambda(F) := \mathbf{Z}_p[[\mathrm{Gal}(F/K)]]$-module structures.

For a positive integer n, C_n is the unique subfield of C_∞ with $[C_n : K] = p^n$; the field D_n is defined similarly. If $\mathfrak{m}$ is an ideal of K, we denote by $K(\mathfrak{m})$ the ray class field of conductor $\mathfrak{m}$. If $\mathfrak{n}$ is another ideal of K, we let $K(\mathfrak{m}\mathfrak{n}^\infty) = \cup_k K(\mathfrak{m}\mathfrak{n}^k)$. We write $\mathrm{N}(\mathfrak{m})$ for the absolute norm of the ideal $\mathfrak{m}$.

1. A little cohomology

We define canonical generators π and π^* of the ideals $\mathfrak{p}$ and $\mathfrak{p}^*$ by $\pi = \psi(\mathfrak{p})$ and $\pi^* = \psi(\mathfrak{p}^*)$, so that $\pi^* = \pi^\tau$. Define G_K-modules

$$W_{\mathfrak{p}} = E[\mathfrak{p}^\infty] \qquad W_{\mathfrak{p}^*} = E[\mathfrak{p}^{*\infty}],$$

and let $T_{\mathfrak{p}}$ and $T_{\mathfrak{p}^*}$ be the π and π^*-adic Tate modules, respectively. Note that the action of τ on $E[p^\infty]$ interchanges $W_{\mathfrak{p}}$ and $W_{\mathfrak{p}^*}$, and so induces a group isomorphism $T_{\mathfrak{p}} \cong T_{\mathfrak{p}^*}$. If we set $V_{\mathfrak{p}} = T_{\mathfrak{p}} \otimes \mathbf{Q}_p$ and $V_{\mathfrak{p}^*} = T_{\mathfrak{p}^*} \otimes \mathbf{Q}_p$, then there is an exact sequence

$$0 \to T_{\mathfrak{q}} \to V_{\mathfrak{q}} \to W_{\mathfrak{q}} \to 0 \tag{1.1}$$

where $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$. For every place v of K and any finite extension F of K or K_v, the G_F-cohomology of this sequence implies that

$$H^0(F, W_{\mathfrak{p}})_{/\mathrm{div}} \cong H^1(F, T_{\mathfrak{p}})_{\mathrm{tor}},$$

where the subscript $/\mathrm{div}$ indicates the quotient by the maximal divisible submodule, and the subscript tor indicates the $\mathbf{Z}_p$-torsion submodule. The Weil pairing restricts to a perfect pairing $T_{\mathfrak{p}} \times T_{\mathfrak{p}^*} \to \mathbf{Z}_p(1)$.

1.1. **Selmer modules.** Let $\mathfrak{q}$ be either $\mathfrak{p}$ or $\mathfrak{p}^*$ and set $\mathfrak{q}^* = \tau(\mathfrak{q})$.

Lemma 1.1.1. *The primes of K above p are finitely decomposed in K_∞.*

Proof. This follows from Proposition II.1.9 of [4]. □

Lemma 1.1.2. *The degree of $K_{\mathfrak{q}}(E[\mathfrak{q}])$ over $K_{\mathfrak{q}}$ is $p-1$.*

Proof. This follows from the theory of Lubin-Tate groups. See for example Chapter 1 of [4]. □

Lemma 1.1.3. *For any intermediate field $K \subset F \subset K_\infty$ the $\Lambda(F)$-module*

$$A_{\mathfrak{f}}(F) = \bigoplus_{v|\mathfrak{f}} H^0(F_v, W_{\mathfrak{p}})$$

has finite exponent. If all primes dividing $\mathfrak{f}$ are finitely decomposed in F, then $A_{\mathfrak{f}}(F)$ is finite.

Proof. Fix a place $v|\mathfrak{f}$ of F. The extension F_v/K_v is unramified, while $W_{\mathfrak{p}}$ is a ramified $\mathrm{Gal}(K_v^{\mathrm{alg}}/K_v)$-module (by the criterion of Néron-Ogg-Shafarevich). Since $W_{\mathfrak{p}} \cong \mathbf{Q}_p/\mathbf{Z}_p$ has no proper infinite submodules we conclude that $E(F_v)[\mathfrak{p}^\infty]$ is finite, and so $\bigoplus_{v|\mathfrak{f}} H^0(F_v, W_{\mathfrak{p}^*})$ has finite exponent. This group is finite if all primes above $\mathfrak{f}$ are finitely decomposed in F. □

Lemma 1.1.4. *Let F/K be a finite extension, let v be a prime of F not dividing p, and let V be a finite dimensional $\mathbf{Q}_p$-vector space with a linear action of G_{F_v}. If V and $\mathrm{Hom}(V, \mathbf{Q}_p(1))$ both have no G_{F_v}-invariants then $H^1(F_v, V) = 0$.*

Proof. This follows from Corollary 1.3.5 of [25] and local duality, or from standard properties of local Euler characteristics. □

In particular, Lemma 1.1.4 implies that $H^1(F_v, V_\mathfrak{q}) = 0$ for v not dividing p. If v is any place of F, we define the *finite* or *Bloch-Kato* local conditions

$$H^1_f(F_v, T_\mathfrak{q}) = \begin{cases} H^1(F_v, T_\mathfrak{q})_{\mathrm{tor}} & \text{if } v \mid \mathfrak{q}^* \\ H^1(F_v, T_\mathfrak{q}) & \text{else} \end{cases}$$

$$H^1_f(F_v, V_\mathfrak{q}) = \begin{cases} H^1(F_v, V_\mathfrak{q}) & \text{if } v \mid \mathfrak{q} \\ 0 & \text{else} \end{cases}$$

$$H^1_f(F_v, W_\mathfrak{q}) = \begin{cases} H^1(F_v, W_\mathfrak{q})_{\mathrm{div}} & \text{if } v \mid \mathfrak{q} \\ 0 & \text{else} \end{cases}$$

The submodules $H^1_f(F_v, T_\mathfrak{q})$ and $H^1_f(F_v, W_\mathfrak{q})$ are the preimage and image, respectively, of $H^1_f(F_v, V_\mathfrak{q})$ under the maps on cohomology induced by the exact sequence (1.1). If M is any object for which we have defined $H^1_f(F_v, M)$, we define the *relaxed* Selmer group $\mathrm{Sel}_{\mathrm{rel}}(F, M)$ to be the set of all $c \in H^1(F, M)$ such that $\mathrm{loc}_v(c) \in H^1_f(F_v, M)$ for every place v not dividing p. We define the *true* Selmer group $\mathrm{Sel}(F, M)$ to be the subgroup consisting of all $c \in \mathrm{Sel}_{\mathrm{rel}}(F, M)$ such that $\mathrm{loc}_v(c) \in H^1_f(F_v, M)$ for all v, including those above p. Finally, we define the *strict* Selmer group to be all those $c \in \mathrm{Sel}(F, M)$ such that $\mathrm{loc}_v(c) = 0$ at the v lying above p. By definition there are inclusions

$$\mathrm{Sel}_{\mathrm{str}}(F, M) \subset \mathrm{Sel}(F, M) \subset \mathrm{Sel}_{\mathrm{rel}}(F, M)$$

and all are $\Lambda(F)$-modules. Our definitions of $\mathrm{Sel}(F, T_\mathfrak{q})$ and $\mathrm{Sel}(F, W_\mathfrak{q})$ agree with the usual definitions of the Selmer groups defined by the local images of the Kummer maps; see Section 6.5 of [25].

Lemma 1.1.5. *Let S denote the set of places of K dividing $\mathfrak{p}\mathfrak{f}$ and let K_S/K be the maximal extension of K unramified outside S. For any $K \subset F \subset K_S$ finite over K,*

$$H^1(K_S/F, T_\mathfrak{p}) = \mathrm{Sel}_{\mathrm{rel}}(F, T_\mathfrak{p}).$$

Proof. For any $v \notin S$, the local condition $H^1_f(F_v, T_\mathfrak{p})$ is exactly the subgroup of unramified classes by [25] Lemma 1.3.5, while for $v \in S$ the local condition defining the relaxed Selmer group is all of $H^1(F_v, T_\mathfrak{p})$. □

If F/K is a (possibly infinite) extension we define $\Lambda(F)$-modules

$$\mathcal{S}(F, T_\mathfrak{q}) = \varprojlim \mathrm{Sel}(F', T_\mathfrak{q}) \qquad \mathrm{Sel}(F, W_\mathfrak{q}) = \varinjlim \mathrm{Sel}(F', W_\mathfrak{q})$$

where the limits are with respect to corestriction and restriction respectively, and are taken over all subfields $F' \subset F$ finite over K. We also define strict and relaxed Selmer groups over F in the obvious way, e.g. $\mathcal{S}_{\mathrm{str}}(F, T_\mathfrak{q}) = \varprojlim \mathrm{Sel}_{\mathrm{str}}(F', T_\mathfrak{q})$, and so on. Recall the notation

$$\mathcal{H}^i(F_\mathfrak{q}, M) = \varprojlim \bigoplus_{v \mid \mathfrak{q}} H^i(F'_v, M),$$

and set

$$\mathcal{H}^1_f(F_\mathfrak{q}, M) = \varprojlim \bigoplus_{v \mid \mathfrak{q}} H^1_f(F'_v, M), \quad H^1_f(F_\mathfrak{q}, M) = \varinjlim \bigoplus_{v \mid \mathfrak{q}} H^1_f(F'_v, M).$$

The canonical involution of $\Lambda(F)$ which is inversion on group-like elements is denoted $\iota : \Lambda(F) \to \Lambda(F)$. This involution induces a functor from the category of $\Lambda(F)$-modules to itself, which on objects is written as $M \mapsto M^\iota$. If $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$, there is a perfect local Tate pairing

$$\mathcal{H}^1(F_\mathfrak{q}, T_\mathfrak{p}) \times H^1(F_\mathfrak{q}, W_{\mathfrak{p}^*}) \to \mathbf{Q}_p/\mathbf{Z}_p \tag{1.2}$$

which satisfies $(\lambda x, y) = (x, \lambda^\iota y)$ for $\lambda \in \Lambda(F)$. Under this pairing, the submodules $\mathcal{H}^1_f(F_\mathfrak{q}, T_\mathfrak{p})$ and $H^1_f(F_\mathfrak{q}, W_{\mathfrak{p}^*})$ are exact orthogonal complements.

Proposition 1.1.6. *Suppose F/K is a $\mathbf{Z}_p$-extension in which $\mathfrak{p}^*$ ramifies. Then $\mathcal{H}^1(F_\mathfrak{p}, T_\mathfrak{p})$ and $\mathcal{H}^1(F_{\mathfrak{p}^*}, T_\mathfrak{p})$ are rank one, torsion-free $\Lambda(F)$-modules.*

Proof. Let $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$. The claim that $\mathcal{H}^1(F_\mathfrak{q}, T_\mathfrak{p})$ has rank 1 is Proposition 2.1.3 of [19]. By Proposition 2.1.6 of the same, the $\Lambda(F)$-torsion submodule of $\mathcal{H}^1(F_\mathfrak{q}, T_\mathfrak{p})$ is isomorphic to $H^0(F_\mathfrak{q}, T_\mathfrak{p})$, so it suffices to show that $E(F_v)[\mathfrak{p}^\infty]$ is finite for every place v of F above $\mathfrak{q}$. If $\mathfrak{q} = \mathfrak{p}$ this is immediate from Lemma 1.1.2. If $\mathfrak{q} = \mathfrak{p}^*$ then $E[\mathfrak{p}^\infty]$ generates an unramified extension of $K_\mathfrak{q}$, and by hypothesis the intersection of this extension with F_v is of finite degree over $K_\mathfrak{q}$. Hence $E(F_v)[\mathfrak{p}^\infty]$ is finite. □

Proposition 1.1.7. *If F/K is an abelian extension such that $\mathcal{H}^1_f(F_{\mathfrak{p}^*}, T_\mathfrak{p}) = 0$, then there are exact sequences*

$$0 \to \mathcal{S}(F, T_\mathfrak{p}) \to \mathcal{S}_{\mathrm{rel}}(F, T_\mathfrak{p}) \xrightarrow{\mathrm{loc}_{\mathfrak{p}^*}} \mathcal{H}^1(F_{\mathfrak{p}^*}, T_\mathfrak{p}) \tag{1.3}$$

$$0 \to \mathrm{Sel}_{\mathrm{str}}(F, W_{\mathfrak{p}^*}) \to \mathrm{Sel}(F, W_{\mathfrak{p}^*}) \xrightarrow{\mathrm{loc}_{\mathfrak{p}^*}} H^1(F_{\mathfrak{p}^*}, W_{\mathfrak{p}^*}), \tag{1.4}$$

and the images of the rightmost arrows are exact orthogonal complements under the local Tate pairing. Under the same hypotheses there are exact sequences

$$0 \to \mathcal{S}_{\mathrm{str}}(F, T_\mathfrak{p}) \to \mathcal{S}(F, T_\mathfrak{p}) \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} \mathcal{H}^1(F_\mathfrak{p}, T_\mathfrak{p}) \tag{1.5}$$

$$0 \to \mathrm{Sel}(F, W_{\mathfrak{p}^*}) \to \mathrm{Sel}_{\mathrm{rel}}(F, W_{\mathfrak{p}^*}) \xrightarrow{\mathrm{loc}_{\mathfrak{p}}} H^1(F_\mathfrak{p}, W_{\mathfrak{p}^*}), \tag{1.6}$$

and again the images of the rightmost arrows are exact orthogonal complements under the sum of the local pairings. The hypotheses hold if F contains a $\mathbf{Z}_p$-extension in which $\mathfrak{p}^*$ ramifies.

Proof. If $\mathcal{H}^1_f(F_{\mathfrak{p}^*}, T_\mathfrak{p}) = 0$ then $H^1_f(F_{\mathfrak{p}^*}, W_{\mathfrak{p}^*}) = H^1(F_{\mathfrak{p}^*}, W_{\mathfrak{p}^*})$ by local duality. The exactness of the sequences is now just a restatement of the definitions. The claims concerning orthogonal complements are consequences of Poitou-Tate global duality, c.f. Theorem 1.7.3 of [25].

Let v be a place of F above $\mathfrak{p}^*$ and let $F' \subset F_v$ be finite over $K_{\mathfrak{p}^*}$. From the cohomology of (1.1) and the fact that $H^0(F', V_\mathfrak{p}) = 0$ we have

$$H^1_f(F', T_\mathfrak{p}) \cong H^0(F', W_\mathfrak{p}) \cong E(F')[\mathfrak{p}^\infty].$$

Taking the inverse limit over $F' \subset F_v$, we see that

$$\varprojlim H^1_f(F', T_\mathfrak{p}) = 0$$

whenever F_v contains an infinite pro-p extension of $K_{\mathfrak{p}^*}$ whose intersection with $K_{\mathfrak{p}^*}(E[\mathfrak{p}^\infty])$ is of finite degree over $K_{\mathfrak{p}^*}$. The extension of $K_{\mathfrak{p}^*}$ generated by $E[\mathfrak{p}^\infty]$ is unramified, so this will be the case whenever F contains a $\mathbf{Z}_p$-extension in which $\mathfrak{p}^*$ ramifies. □

If F/K is an abelian extension we define $\Lambda(F)$-modules

$$\begin{aligned} X(F) &= \mathrm{Sel}(F, W_{\mathfrak{p}})^{\vee} \\ X_{\mathrm{rel}}(F) &= \mathrm{Sel}_{\mathrm{rel}}(F, W_{\mathfrak{p}})^{\vee} \\ X_{\mathrm{str}}(F) &= \mathrm{Sel}_{\mathrm{str}}(F, W_{\mathfrak{p}})^{\vee}. \end{aligned}$$

Define $X^*(F)$, $X^*_{\mathrm{rel}}(F)$, and $X^*_{\mathrm{str}}(F)$ similarly, replacing $\mathfrak{p}$ by $\mathfrak{p}^*$.

Remark 1.1.8. Because of the behavior of the local pairing (1.2) under the action of $\Lambda(F)$, we adopt, for the entirety of the paper, the convention that $\Lambda(F)$ acts on $X(F)$ via $(\lambda \cdot f)(x) = f(\lambda^{\iota} x)$. Thus the map

$$\mathcal{H}^1(F_{\mathfrak{p}^*}, T_{\mathfrak{p}}) \to X^*(F)$$

induced by localization at $\mathfrak{p}^*$ and the local pairing is a map of $\Lambda(D_\infty)$-modules. The same convention is adopted for $X^*(F)$, $X_{\mathrm{rel}}(F)$, etc.

Lemma 1.1.9. *Let F/K be a $\mathbf{Z}_p$ or $\mathbf{Z}_p^2$ extension of K. There is a canonical isomorphism of $\Lambda(F)$-modules*

$$\mathcal{S}_{\mathrm{rel}}(F, T_{\mathfrak{p}}) \cong \mathrm{Hom}_{\Lambda(F)}(X_{\mathrm{rel}}(F), \Lambda(F)).$$

In particular $\mathcal{S}_{\mathrm{rel}}(F, T_{\mathfrak{p}})$ and $X_{\mathrm{rel}}(F)$ have the same $\Lambda(F)$-rank, and $\mathcal{S}_{\mathrm{rel}}(F, T_{\mathfrak{p}})$ is torsion-free.

Proof. The proof is essentially the same as that of [19] Proposition 4.2.3. Suppose that $L \subset F$ is finite over K. Let S denote the set of places of K consisting of the infinite place and the prime divisors of $p\mathfrak{f}$, and let K_S/K be the maximal extension of K unramified outside S. By Lemma 1.1.5

$$\mathcal{S}_{\mathrm{rel}}(L, T_{\mathfrak{p}}) \cong H^1(K_S/L, T_{\mathfrak{p}}) \cong \varprojlim H^1(K_S/L, E[\mathfrak{p}^k]).$$

On the other hand, Lemma 1.1.2 shows that $E(L)[\mathfrak{p}] = 0$ (since $[L : K]$ is a power of p), and so the $\mathrm{Gal}(K_S/L)$-cohomology of

$$0 \to E[\mathfrak{p}^k] \to W_{\mathfrak{p}} \xrightarrow{\pi^k} W_{\mathfrak{p}} \to 0$$

shows that $H^1(K_S/L, E[\mathfrak{p}^k]) \cong H^1(K_S/L, W_{\mathfrak{p}})[\mathfrak{p}^k]$.

If we define

$$X_S(L) = H^1(K_S/L, W_{\mathfrak{p}})^{\vee}$$

then

$$\mathrm{Hom}_{\Lambda(L)}(X_S(L), \Lambda(L)) \cong \mathrm{Hom}_{\mathbf{Z}_p}(X_S(L), \mathbf{Z}_p)$$

via the augmentation map $\Lambda(L) \to \mathbf{Z}_p$. The right hand side is isomorphic to the p-adic Tate module of $H^1(K_S/L, W_{\mathfrak{p}})$, so by the above

$$\mathcal{S}_{\mathrm{rel}}(L, T_{\mathfrak{p}}) \cong \mathrm{Hom}_{\Lambda(L)}(X_S(L), \Lambda(L)). \tag{1.7}$$

As in the proof of Lemma 1.1.5, for any $v \notin S$ the unramified classes in $H^1(L_v, W_{\mathfrak{p}})$ agree with the local condition $H^1_f(L_v, W_{\mathfrak{p}})$, and so we have the exact sequence

$$0 \to \mathrm{Sel}_{\mathrm{rel}}(L, W_{\mathfrak{p}}) \to H^1(K_S/L, W_{\mathfrak{p}}) \to \bigoplus_{v \mid \mathfrak{f}} H^1(L_v, W_{\mathfrak{p}}). \tag{1.8}$$

The Pontryagin dual of the final term is isomorphic to

$$\bigoplus_{v \mid \mathfrak{f}} H^1(L_v, T_{\mathfrak{p}^*}) \cong \bigoplus_{v \mid \mathfrak{f}} H^0(L_v, W_{\mathfrak{p}^*}),$$

where we have used Lemma 1.1.4 and the cohomology of the short exact sequence relating $T_{\mathfrak{p}^*}$, $V_{\mathfrak{p}^*}$, and $W_{\mathfrak{p}^*}$.

If $A^*_{\mathfrak{f}}(F)$ denotes the module of Lemma 1.1.3, with $\mathfrak{p}$ replaced by $\mathfrak{p}^*$, we may take the limit as L varies, and the dual sequence to (1.8) reads

$$A^*_{\mathfrak{f}}(F)^\vee \to X_S(F) \to X_{\mathrm{rel}}(F) \to 0$$

where the first term is a torsion $\Lambda(F)$-module (even a torsion $\mathbf{Z}_p$-module) by Lemma 1.1.3. Applying the functor $\mathrm{Hom}_{\Lambda(F)}(\cdot, \Lambda(F))$ and combining this with (1.7) gives the result. □

Remark 1.1.10. A similar argument can be used to show that $\mathcal{S}(F, T_{\mathfrak{p}})$ and $X(F)$ have the same $\Lambda(F)$-rank, and similarly for the strict Selmer groups. See [19] Proposition 4.2.3, for example. When $F = D_\infty$, these facts will fall out during the more detailed analysis of the relationship between X_{str} and and X_{rel} given in Theorem 1.2.2.

1.2. **Anticyclotomic Iwasawa modules.**

Lemma 1.2.1. *There are isomorphisms of $\Lambda(D_\infty)$-modules*

$$\mathcal{S}(D_\infty, T_{\mathfrak{p}})^\iota \cong \mathcal{S}(D_\infty, T_{\mathfrak{p}^*}) \qquad X(D_\infty)^\iota \cong X^*(D_\infty),$$

and similarly for the relaxed and restricted Selmer groups.

Proof. The action of G_K on the full Selmer group

$$\mathrm{Sel}(D_\infty, E[p^\infty]) \cong \mathrm{Sel}(D_\infty, W_{\mathfrak{p}}) \oplus \mathrm{Sel}(D_\infty, W_{\mathfrak{p}^*})$$

extends to an action of $G_{\mathbf{Q}}$, and complex conjugation interchanges the $\mathfrak{p}$ and $\mathfrak{p}^*$-primary components. Since $\mathrm{Gal}(D_\infty/\mathbf{Q})$ is of dihedral type, we may view complex conjugation as an isomorphism

$$\mathrm{Sel}(D_\infty, W_{\mathfrak{p}})^\iota \cong \mathrm{Sel}(D_\infty, W_{\mathfrak{p}^*}),$$

and so $X(D_\infty)^\iota \cong X^*(D_\infty)$. The other claims are proved similarly. □

The remainder of this subsection is devoted to a proof of the following result.

Theorem 1.2.2. *If $r(\cdot)$ denotes $\Lambda(D_\infty)$-rank, then $r(X(D_\infty)) = r(\mathcal{S}(D_\infty))$ and the same holds for the strict and relaxed Selmer groups. Furthermore,*

$$r(X_{\mathrm{rel}}(D_\infty)) = 1 + r(X_{\mathrm{str}}(D_\infty))$$

and the $\Lambda(D_\infty)$-torsion submodules of $X_{\mathrm{rel}}(D_\infty)$ and $X_{\mathrm{str}}(D_\infty)$ have the same characteristic ideals, up to powers of $p\Lambda(D_\infty)$.

Let $\mathcal{O}$ be the ring of integers of some finite extension $\Phi/\mathbf{Q}_p$, and let

$$\chi : \mathrm{Gal}(D_\infty/K) \to \mathcal{O}^\times$$

be a continuous character of $\mathrm{Gal}(D_\infty/K)$. If M is any $\mathbf{Z}_p$-module, define $M(\chi) = M \otimes \mathcal{O}(\chi)$. From Lemma 1.1.2 it follows that $\psi_{\mathfrak{q}} : G_K \to \mathbf{Z}_p^\times \to (\mathbf{Z}_p/p\mathbf{Z}_p)^\times$ is surjective, and from this it is easy to see that the residual representation of $T_{\mathfrak{q}}(\chi)$ is nontrivial and absolutely irreducible. Combining this with Lemma 1.1.4 and the duality

$$V_{\mathfrak{p}}(\chi) \times V_{\mathfrak{p}^*}(\chi^{-1}) \to \mathbf{Q}_p(1),$$

we have that $H^1(K_v, V_{\mathfrak{q}}(\chi)) = 0$ for every v not dividing p. We define generalized Selmer groups

$$H^1_{\mathrm{rel}}(K, W_{\mathfrak{q}}(\chi)) \qquad H^1_{\mathrm{str}}(K, W_{\mathfrak{q}}(\chi)),$$

where the first group consists of classes which are everywhere trivial at primes not dividing p, and which lie in the maximal divisible subgroup of $H^1(K_v, W_{\mathfrak{q}}(\chi))$ at primes v above p, and the second group consists of classes which are everywhere locally trivial.

If χ is the trivial character, then $H^1_{\mathrm{str}}(K, W_{\mathfrak{q}}) = \mathrm{Sel}_{\mathrm{str}}(K, W_{\mathfrak{q}})$, but $H^1_{\mathrm{rel}}(K, W_{\mathfrak{q}})$ may be slightly smaller than $\mathrm{Sel}_{\mathrm{rel}}(K, W_{\mathfrak{q}})$. If we define

$$\mathrm{Sel}_{\mathrm{rel}}(K, W_{\mathfrak{q}}(\chi)) \subset H^1(K, W_{\mathfrak{q}}(\chi))$$

to be the subgroup of classes which are locally trivial at all primes not dividing p, and impose no conditions at all above p (so that this agrees with our previous definition when χ is trivial), then we can bound the index of

$$H^1_{\mathrm{rel}}(K, W_{\mathfrak{q}}(\chi)) \subset \mathrm{Sel}_{\mathrm{rel}}(K, W_{\mathfrak{q}}(\chi)) \tag{1.9}$$

as follows. The quotient injects into

$$H^1(K_{\mathfrak{p}}, W_{\mathfrak{q}}(\chi)) \oplus H^1(K_{\mathfrak{p}^*}, W_{\mathfrak{q}}(\chi))$$

modulo its maximal divisible subgroup. Thus, using the exact sequence (1.1) and local duality, the order of the quotient is bounded by the order of

$$H^0(K_{\mathfrak{p}}, W_{\mathfrak{q}^*}(\chi^{-1})) \oplus H^0(K_{\mathfrak{p}^*}, W_{\mathfrak{q}^*}(\chi^{-1})).$$

It is easy to see that this group is finite, and bounded by some constant which does not depend on χ, provided $\mathcal{O}$ remains fixed.

Our reason for working with the slightly smaller group H^1_{rel} is the following

Proposition 1.2.3. *(Mazur-Rubin) For every character χ there is a non-canonical isomorphism of $\mathcal{O}$-modules*

$$H^1_{\mathrm{rel}}(K, W_{\mathfrak{p}}(\chi)) \cong (\Phi/\mathcal{O}) \oplus H^1_{\mathrm{str}}(K, W_{\mathfrak{p}^*}(\chi^{-1})).$$

Proof. All references in this proof are to [14]. It follows from Theorem 4.1.13 and Lemma 3.5.3 that

$$H^1_{\mathrm{rel}}(K, W_{\mathfrak{p}}(\chi))[p^i] \cong (\Phi/\mathcal{O})^r[p^i] \oplus H^1_{\mathrm{str}}(K, W_{\mathfrak{p}^*}(\chi^{-1}))[p^i]$$

for every i, where r is the core rank (Definition 4.1.11) of the local conditions defining the Selmer group $H^1_{\mathrm{rel}}(K, W_{\mathfrak{p}}(\chi))$. A formula of Wiles, Proposition 2.3.5, shows that the core rank is equal to

$$\mathrm{corank}\ H^1(K_{\mathfrak{p}}, W_{\mathfrak{p}}(\chi)) + \mathrm{corank}\ H^1(K_{\mathfrak{p}^*}, W_{\mathfrak{p}}(\chi)) - \mathrm{corank}\ H^0(K_v, W_{\mathfrak{p}}(\chi)),$$

in which v denotes the unique archimedean place of K and corank means corank as an $\mathcal{O}$-module. The first two terms are each equal to 1 by the local Euler characteristic formula, and the third is visibly 1. Hence the core rank is 1. Letting $i \to \infty$ proves the claim. □

Restriction gives a map

$$H^1(K, W_{\mathfrak{q}}(\chi)) \ \to \ H^1(D_\infty, W_{\mathfrak{q}})(\chi)^{\mathrm{Gal}(D_\infty/K)},$$

and since $H^0(D_\infty, W_{\mathfrak{q}}(\chi)) = 0$, the Hochschild-Serre sequence (see Proposition B.2.5 of [25]) implies that this map is an isomorphism.

Lemma 1.2.4. *The above restriction isomorphism induces injective maps*

$$\begin{aligned} H^1_{\mathrm{str}}(K, W_{\mathfrak{q}}(\chi)) \quad &\to \quad \mathrm{Sel}_{\mathrm{str}}(D_\infty, W_{\mathfrak{q}})(\chi)^{\mathrm{Gal}(D_\infty/K)} \\ H^1_{\mathrm{rel}}(K, W_{\mathfrak{q}}(\chi)) \quad &\to \quad \mathrm{Sel}_{\mathrm{rel}}(D_\infty, W_{\mathfrak{q}})(\chi)^{\mathrm{Gal}(D_\infty/K)} \end{aligned}$$

whose cokernels are finite and bounded as χ varies (provided $\mathcal{O}$ remains fixed).

Proof. A class $d \in \mathrm{Sel}_{\mathrm{str}}(D_\infty, W_{\mathfrak{q}})(\chi)^{\mathrm{Gal}(D_\infty/K)}$ is the restriction of some class $c \in H^1(K, W_{\mathfrak{q}}(\chi))$ which is in the kernel of

$$H^1(K_v, W_{\mathfrak{q}}(\chi)) \rightarrow H^1(D_{\infty,v}, W_{\mathfrak{q}}(\chi)) \tag{1.10}$$

for every place v of D_∞. Let $\Gamma_v = \mathrm{Gal}(D_{\infty,v}/K_v)$, so that Γ is either trivial or isomorphic to $\mathbf{Z}_p$. If $\Gamma_v = 0$ then (1.10) is an isomorphism. If $\Gamma_v \cong \mathbf{Z}_p$ with generator γ, then the cokernel is trivial and the kernel is isomorphic to $M/(\gamma-1)M$ where $M = H^0(D_{\infty,v}W_{\mathfrak{q}}) \otimes \mathcal{O}$. If v is a prime of good reduction not dividing p, then $D_{\infty,v}$ is the unique unramified $\mathbf{Z}_p$-extension of K_v. It follows that $M = 0$ if $E[\mathfrak{q}] \not\subset K_v$, while $M = W_{\mathfrak{q}}$ if $E[\mathfrak{q}] \subset K_v$. In either case, since $(\gamma - 1)$ acts as a nontrivial scalar on $W_{\mathfrak{q}}$, we must have $M/(\gamma-1)M = 0$. If v is a prime of bad reduction, or if v lies above p, then M is finite. Thus the kernel of (1.10) is trivial for almost all v, and finite and bounded by a constant independent of χ.

A class $d \in \mathrm{Sel}_{\mathrm{rel}}(D_\infty, W_{\mathfrak{q}})(\chi)^{\mathrm{Gal}(D_\infty/K)}$ is the restriction of some class $c \in H^1(K, W_{\mathfrak{q}}(\chi))$ which is in the kernel of (1.10) at every prime not dividing p. The above argument shows that the cokernel of

$$\mathrm{Sel}_{\mathrm{rel}}(K, W_{\mathfrak{q}}(\chi)) \rightarrow \mathrm{Sel}_{\mathrm{rel}}(D_\infty, W_{\mathfrak{q}})(\chi)^{\mathrm{Gal}(D_\infty/K)}$$

is finite with a bound of the desired sort, and so the claim follows from our bound on the index of (1.9). □

Corollary 1.2.5. *For any $\chi : \mathrm{Gal}(D_\infty/K) \rightarrow \mathcal{O}^\times$, the $\mathcal{O}$-coranks of*

$$\mathrm{Sel}_{\mathrm{rel}}(D_\infty, W_{\mathfrak{p}})(\chi)^{\mathrm{Gal}(D_\infty/K)} \qquad \mathrm{Sel}_{\mathrm{str}}(D_\infty, W_{\mathfrak{p}})(\chi)^{\mathrm{Gal}(D_\infty/K)}$$

differ by 1, and the quotients by the maximal $\mathcal{O}$-divisible submodules have the same order, up to $O(1)$ as χ varies.

Proof. By Lemma 1.2.1,

$$\mathrm{Sel}_{\mathrm{str}}(D_\infty, W_{\mathfrak{p}^*})(\chi^{-1})^{\mathrm{Gal}(D_\infty/K)} \cong \mathrm{Sel}_{\mathrm{str}}(D_\infty, W_{\mathfrak{p}})(\chi)^{\mathrm{Gal}(D_\infty/K)}.$$

Combining this with Proposition 1.2.3 and Lemma 1.2.4 gives the stated result. □

Lemma 1.2.6. *We have the equality $r(X_{\mathrm{rel}}(D_\infty)) = 1 + r(X_{\mathrm{str}}(D_\infty))$, and the $\Lambda(D_\infty)$-torsion submodules of $X_{\mathrm{rel}}(D_\infty)$ and $X_{\mathrm{str}}(D_\infty)$ have the same characteristic ideals, up to powers of $p\Lambda(D_\infty)$.*

Proof. Choose a generator $\gamma \in \mathrm{Gal}(D_\infty/K)$ and identify $\Lambda(D_\infty)$ with $\mathbf{Z}_p[[S]]$ via $\gamma - 1 \mapsto S$. Assume $\mathcal{O}$ is chosen large enough that the characteristic ideals of the torsion submodules of $X^*_{\mathrm{str}}(D_\infty)$ and $X^*_{\mathrm{rel}}(D_\infty)$ split into linear factors. Let $\mathfrak{m} \subset \mathcal{O}$ be the maximal ideal, and fix pseudo-isomorphisms

$$X^*_{\mathrm{rel}}(D_\infty) \otimes_{\mathbf{Z}_p} \mathcal{O} \sim A \oplus A_p \qquad X^*_{\mathrm{str}}(D_\infty) \otimes_{\mathbf{Z}_p} \mathcal{O} \sim B \oplus B_p$$

where A_p and B_p are torsion modules with chracteristic ideals generated by powers of p, and A and B are of the form

$$A \cong \mathcal{O}[[S]]^a \oplus \bigoplus_{\xi \in \mathfrak{m}} A_\xi \qquad B \cong \mathcal{O}[[S]]^b \oplus \bigoplus_{\xi \in \mathfrak{m}} B_\xi$$

where each A_ξ is isomorphic to $\bigoplus_i \mathcal{O}[[S]]/(S-\xi)^{e_i}$ for some exponents $e_i = e_i(A, \xi)$, and similarly for B. Define

$$P = \{\xi \in \mathfrak{m} \mid A_\xi \neq 0 \text{ or } B_\xi \neq 0\},$$

and to any $\xi \notin P$ we define a character χ_ξ by $\chi_\xi(\gamma) = (\xi+1)^{-1}$. Then for any $\xi \notin P$ we have

$$a = \mathrm{rank}_{\mathcal{O}}\ A/(S-\xi)A = \mathrm{corank}_{\mathcal{O}}\ \mathrm{Sel}_{\mathrm{rel}}(D_\infty, W_{\mathfrak{p}})(\chi_\xi)^{\mathrm{Gal}(D_\infty/K)}$$

and similarly for B. The corollary above immediately implies that $a = b+1$, hence $r(X_{\mathrm{rel}}(D_\infty)) = r(X_{\mathrm{str}}(D_\infty)) + 1$.

Now fix $\xi \in P$ and choose a sequence $x_k \to \xi$ with $x_k \in \mathfrak{m} - P$ for all k. As k varies, the $\mathcal{O}$-length of the torsion submodule of $A/(S-x_k)A$ is given by

$$v(x_k - \xi)\cdot \sum_i e_i(A,\xi) \ + O(1)$$

where v is the valuation on $\mathcal{O}$, and similarly for B. Applying the corollary, we have

$$v(x_k-\xi)\cdot\sum_i e_i(A,\xi) = v(x_k-\xi)\cdot\sum_i e_i(B,\xi),$$

up to $O(1)$ as k varies. Letting $k\to\infty$ shows that $\sum_i e_i(A,\xi) = \sum_i e_i(B,\xi)$, proving that the torsion submodules of $X_{\mathrm{str}}(D_\infty)$ and $X_{\mathrm{rel}}(D_\infty)$ have the same characteristic ideals, up to powers of $p\Lambda(D_\infty)$. □

The following corollary completes the proof of Theorem 1.2.2.

Corollary 1.2.7. *We have the equality of ranks $r(X(D_\infty)) = r(\mathcal{S}(D_\infty))$, and the same holds for the strict and relaxed Selmer groups.*

Proof. For the relaxed Selmer groups, this equality of ranks was proved in Lemma 1.1.9. Let A and B be the cokernels of

$$\mathcal{S}_{\mathrm{rel}}(D_\infty, T_{\mathfrak{p}}) \ \to\ \mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}}), \qquad \mathcal{S}(D_\infty, T_{\mathfrak{p}}) \ \to\ \mathcal{H}^1(D_{\infty,\mathfrak{p}}, T_{\mathfrak{p}}),$$

respectively. Then Propositions 1.1.7 and 1.2.1 give

$$\begin{aligned} r(A) + r(X_{\mathrm{str}}(D_\infty)) &= r(X(D_\infty)) \\ r(B) + r(X(D_\infty)) &= r(X_{\mathrm{rel}}(D_\infty)) \\ r(A) + r(\mathcal{S}_{\mathrm{rel}}(D_\infty, T_{\mathfrak{p}})) &= 1 + r(\mathcal{S}(D_\infty, T_{\mathfrak{p}})) \\ r(B) + r(\mathcal{S}(D_\infty, T_{\mathfrak{p}})) &= 1 + r(\mathcal{S}_{\mathrm{str}}(D_\infty, T_{\mathfrak{p}})). \end{aligned}$$

By Lemma 1.2.6, the first two equalities imply that $r(A)+r(B) = 1$. The second two equalities then imply that $r(\mathcal{S}_{\mathrm{rel}}(D_\infty,T_{\mathfrak{p}})) = 1 + r(\mathcal{S}_{\mathrm{str}}(D_\infty,T_{\mathfrak{p}}))$. We deduce, using Lemma 1.1.9, that $r(X_{\mathrm{str}}(D_\infty)) = r(\mathcal{S}_{\mathrm{str}}(D_\infty,T_{\mathfrak{p}}))$. Similarly, the equality $r(X(D_\infty)) = r(\mathcal{S}(D_\infty,T_{\mathfrak{p}}))$ is deduced from Lemma 1.1.9 by adding the middle two equalities. □

2. L-functions and Euler systems

In this section we recall the definition of Katz's L-function, the construction of the elliptic units, and state Yager's theorem relating the two. Our presentation follows [4], to which the reader is referred for more details on these topics. Using results of Rubin, we then twist the elliptic units into an Euler system more suitable for our purposes and use the twisted Euler system to compute the corank of the $\mathfrak{p}^*$-power Selmer group over D_∞.

2.1. **The p-adic L-function.** For any integers k, j, we define a grossencharacter (of type A_0, although we shall never consider any other type) of type (k,j) to be a $\mathbf{Q}^{\mathrm{al}}$-valued function, ϵ, defined on integral ideals prime to some ideal $\mathfrak{m}$, such that if $\mathfrak{a} = \alpha\mathcal{O}_K$ with $\alpha \equiv 1 \pmod{\mathfrak{m}}$ then $\epsilon(\mathfrak{a}) = \alpha^k\bar{\alpha}^j$. We have the usual notion of the conductor of a grossencharacter, and the usual L-function defined to be (the analytic continuation of)

$$L(\epsilon, s) = \prod_{\mathfrak{l}} \frac{1}{1-\epsilon(\mathfrak{l})\mathrm{N}(\mathfrak{l})^{-s}}$$

where the product is over all primes $\mathfrak{l}$ of K, with the convention that $\epsilon(\mathfrak{l}) = 0$ for $\mathfrak{l}$ dividing the conductor of ϵ. For any ideal $\mathfrak{m}$, the notation $L_{\mathfrak{m}}(\epsilon, s)$ means the L-function without Euler factors at primes dividing $\mathfrak{m}$, and

$$L_{\infty,\mathfrak{m}}(\epsilon, s) = \frac{\Gamma(s-\min(k,j))}{(2\pi)^{s-\min(k,j)}} L_{\mathfrak{m}}(\epsilon, s).$$

Finally, if ϵ has conductor $\mathfrak{f}_\epsilon$ and type (k,j), set $R(\epsilon, s) = (d_K \mathrm{N}(\mathfrak{f}_\epsilon))^{s/2} L_{\infty,\mathfrak{f}_\epsilon}(\epsilon, s)$, where d_K denotes the discriminant of K. Then we have the functional equation $R(\epsilon, s) = W_\epsilon \cdot R(\bar{\epsilon}, 1+k+j-s)$ for some constant W_ϵ of absolute value one (the "root number" associated to ϵ). If we take $\epsilon = \psi$ to be the grossencharacter of our elliptic curve, then the functional equation reads $R(\psi, s) = W_\psi \cdot R(\psi, 2-s)$, since $\bar{\psi}(\mathfrak{l}) = \psi(\bar{\mathfrak{l}})$ implies that $L(\psi, s) = L(\bar{\psi}, s)$. In particular W_ψ must be ± 1.

To any grossencharacter of conductor dividing $\mathfrak{m}$, we associate p-adic Galois characters

$$\epsilon_{\mathfrak{q}} : \mathrm{Gal}(K(\mathfrak{m}p^\infty)/K) \rightarrow \mathbf{C}_p^\times$$

by the rule $\epsilon_{\mathfrak{q}}(\sigma_{\mathfrak{a}}) = i_{\mathfrak{q}}(\epsilon(\mathfrak{a}))$, where $\mathfrak{q}$ is $\mathfrak{p}$ or $\mathfrak{p}^*$, and $\sigma_{\mathfrak{a}}$ is the Frobenius of $\mathfrak{a}$. The character $\psi_{\mathfrak{q}}$ agrees with the character

$$\mathrm{Gal}(K(\mathfrak{f}\mathfrak{q}^\infty)/K) \rightarrow \mathrm{Aut}(T_{\mathfrak{q}}) \cong \mathbf{Z}_p^\times,$$

and the formalism of the Weil pairing implies that $\psi_{\mathfrak{p}}\psi_{\mathfrak{p}^*}$ is the cyclotomic character.

Theorem 2.1.1. *(Katz) There are measures*

$$\mu_{\mathfrak{p}} \in \Lambda(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0} \qquad \mu_{\mathfrak{p}^*} \in \Lambda(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0} \tag{2.1}$$

such that if ϵ is a grossencharacter of conductor dividing $\mathfrak{f}p^\infty$ of type (k,j) with $0 \le -j < k$, one has the interpolation formula

$$\alpha_{\mathfrak{p}}(\epsilon) \int \epsilon_{\mathfrak{p}} \; d\mu_{\mathfrak{p}} = \left(1 - \frac{\epsilon(\mathfrak{p})}{p}\right) \cdot L_{\infty,\mathfrak{f}\mathfrak{p}^*}(\epsilon^{-1}, 0) \tag{2.2}$$

where $\alpha_{\mathfrak{p}}(\epsilon) \in \mathbf{C}_p$ is a nonzero constant, the integral is over $\mathrm{Gal}(K(\mathfrak{f}p^\infty)/K)$, and the right hand side is interpreted as an element of $\mathbf{C}_p$ via the embedding $i_{\mathfrak{p}}$. As usual, $\epsilon(\mathfrak{p}) = 0$ if $\mathfrak{p}$ divides the conductor of ϵ. Similarly, if ϵ has infinity type (k,j) with $0 \le -j < k$ and conductor dividing $\mathfrak{f}p^\infty$, then

$$\alpha_{\mathfrak{p}^*}(\epsilon) \int \epsilon_{\mathfrak{p}^*} \; d\mu_{\mathfrak{p}^*} = \left(1 - \frac{\epsilon(\mathfrak{p}^*)}{p}\right) \cdot L_{\infty,\mathfrak{f}\mathfrak{p}}(\epsilon^{-1}, 0)$$

for some nonzero $\alpha_{\mathfrak{p}^*}(\epsilon)$ where the right hand side is embedded in $\mathbf{C}_p$ via $i_{\mathfrak{p}^*}$.

Proof. This is Theorem II.4.14 of [4]. $\square$

Remark 2.1.2. Our measure $\mu_{\mathfrak{p}}$ is de Shalit's $\mu_p(\mathfrak{f}\mathfrak{p}^{*\infty})$. The measure $\mu_{\mathfrak{p}}$ is canonically associated to the field K, the ideal $\mathfrak{f}$ and the embedding $i_{\mathfrak{p}}$. In particular it does not depend on the elliptic curve E. The constants $\alpha_{\mathfrak{p}}(\epsilon)$ and $\alpha_{\mathfrak{p}^*}(\epsilon)$ can be made explicit.

Remark 2.1.3. It can be deduced either from the interpolation formulae (2.1), (2.2) or from a result of Yager (see Theorem 2.2.1 below) that the involution of $\Lambda(K(\mathfrak{f}p^{\infty}))_{\mathrm{R}_0}$ induced by complex conjugation interchanges $\mu_{\mathfrak{p}}$ and $\mu_{\mathfrak{p}^*}$.

If ϵ is a grossencharacter of conductor dividing $\mathfrak{f}p^{\infty}$, we define

$$\mathcal{L}_{\mathfrak{p},\mathfrak{f}}(\epsilon) = \int_{\mathrm{Gal}(K(\mathfrak{f}p^{\infty})/K)} \epsilon_{\mathfrak{p}}^{-1}\, d\mu_{\mathfrak{p}},$$

and similarly with $\mathfrak{p}$ replaced by $\mathfrak{p}^*$, so that the interpolation formula reads

$$\mathcal{L}_{\mathfrak{p},\mathfrak{f}}(\epsilon) = \left(1 - \frac{\epsilon(\mathfrak{p})^{-1}}{p}\right) \cdot L_{\infty,\mathfrak{f}\mathfrak{p}^*}(\epsilon, 0) \tag{2.3}$$

up to a nonzero constant, provided that ϵ has infinity type (k, j) with $0 \geq -j > k$.

If χ is a $\mathbf{Z}_p^{\times}$-valued character of $\mathrm{Gal}(F/K)$ for some abelian extension F/K, we let

$$\mathrm{Tw}_{\chi} : \Lambda(F)_{\mathrm{R}_0} \;\to\; \Lambda(F)_{\mathrm{R}_0}$$

be the ring automorphism induced by $\gamma \mapsto \chi(\gamma)\gamma$ on group-like elements. Suppose $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$, F is an extension of K contained in $K(\mathfrak{f}p^{\infty})$, and χ is a $\mathbf{Z}_p^{\times}$-valued character of $\mathrm{Gal}(K(\mathfrak{f}p^{\infty})/K)$. Define $\mu_{\mathfrak{q}}(F;\chi)$ to be the image of $\mathrm{Tw}_{\chi}(\mu_{\mathfrak{q}})$ under the natural projection

$$\Lambda(K(\mathfrak{f}p^{\infty}))_{\mathrm{R}_0} \;\to\; \Lambda(F)_{\mathrm{R}_0},$$

and for any integral $\mathcal{O}_K$-ideal $\mathfrak{a}$ prime to $\mathfrak{f}p$, define $\lambda(F;\chi,\mathfrak{a})$ to be the image of $\mathrm{Tw}_{\chi}(\sigma_{\mathfrak{a}} - \mathrm{N}\mathfrak{a})$. Let

$$\mu_{\mathfrak{q}}(F;\chi,\mathfrak{a}) = \mu_{\mathfrak{q}}(F;\chi)\lambda(F;\chi,\mathfrak{a}).$$

In particular, the measure $\mu_{\mathfrak{q}}(D_{\infty};\psi_{\mathfrak{p}^*},\mathfrak{a})$ will be of crucial interest.

If F/K is any subextension of $K(\mathfrak{f}p^{\infty})$ and ϵ is a grossencharacter such that $\epsilon_{\mathfrak{q}}$ factors through $\mathrm{Gal}(F/K)$, then

$$\begin{aligned} \int \epsilon_{\mathfrak{q}}^{-1}\, d\mu_{\mathfrak{q}}(F;\psi_{\mathfrak{p}^*},\mathfrak{a}) &= \left(\epsilon_{\mathfrak{q}}^{-1}\psi_{\mathfrak{p}^*}(\sigma_{\mathfrak{a}}) - \mathrm{N}\mathfrak{a}\right) \int \epsilon_{\mathfrak{q}}^{-1}\psi_{\mathfrak{p}^*}\, d\mu_{\mathfrak{q}} \\ &= \begin{cases} i_{\mathfrak{p}}\left(\epsilon^{-1}\bar{\psi}(\mathfrak{a}) - \mathrm{N}\mathfrak{a}\right) \cdot \mathcal{L}_{\mathfrak{p},\mathfrak{f}}(\epsilon\bar{\psi}^{-1}) & \text{if } \mathfrak{q} = \mathfrak{p} \\ i_{\mathfrak{p}^*}\left(\epsilon^{-1}\psi(\mathfrak{a}) - \mathrm{N}\mathfrak{a}\right) \cdot \mathcal{L}_{\mathfrak{p}^*,\mathfrak{f}}(\epsilon\psi^{-1}) & \text{if } \mathfrak{q} = \mathfrak{p}^* \end{cases} \end{aligned} \tag{2.4}$$

where the integral on the left is over $\mathrm{Gal}(F/K)$ and the integral on the right is over $\mathrm{Gal}(K(\mathfrak{f}p^{\infty})/K)$.

Fix a generator σ of $\mathrm{Gal}(K_{\infty}/D_{\infty})$. The cyclotomic character defines a canonical isomorphism

$$<>: \mathrm{Gal}(K_{\infty}/D_{\infty}) \cong \mathrm{Gal}(C_{\infty}/K) \cong 1 + p\mathbf{Z}_p.$$

Following Greenberg, we define the *critical divisor*

$$\Theta = \sigma - <\sigma> \sigma^{-1} \in \Lambda(K_{\infty})_{\mathrm{R}_0}.$$

If $\mathfrak{q}$ is $\mathfrak{p}$ or $\mathfrak{p}^*$, we have a canonical factorization $\psi_{\mathfrak{q}} = \chi_{\mathfrak{q}}\eta_q$ where $\chi_{\mathfrak{q}}$ takes values in μ_{p-1} and $\eta_{\mathfrak{q}}$ takes values in $1 + p\mathbf{Z}_p$. It is trivial to verify, using the fact that $\eta_{\mathfrak{p}}\eta_{\mathfrak{p}^*} =<>$, that $\mathrm{Tw}_{\eta_q}(\Theta)$ generates the kernel of the natural projection $\Lambda(K_{\infty})_{\mathrm{R}_0} \;\to\; \Lambda(D_{\infty})_{\mathrm{R}_0}$.

Let $\mathcal{K} = K(E[p^\infty])$ so that $\mathcal{K} \subset K(\mathfrak{f}p^\infty)$ by the theory of complex multiplication. We have a natural isomorphism

$$\mathrm{Gal}(\mathcal{K}/K) \xrightarrow{\psi_{\mathfrak{p}} \times \psi_{\mathfrak{p}^*}} \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times,$$

and hence if we define $\Delta = \mathrm{Gal}(\mathcal{K}/K_\infty)$, every character of Δ is of the form $\chi_{\mathfrak{p}}^a \chi_{\mathfrak{p}^*}^b$ for some unique $0 \le a, b < p-1$. If χ is any character of Δ, we let $e(\chi) \in \Lambda(\mathcal{K})_{\mathrm{R}_0}$ be the associated idempotent, satisfying $\gamma e(\chi) = \chi(\gamma) e(\chi)$ We may also view $e(\chi)$ as a map $\Lambda(\mathcal{K})_{\mathrm{R}_0} \to \Lambda(K_\infty)_{\mathrm{R}_0}$, hopefully without confusion. If χ is the trivial character, this map is the natural projection.

Theorem 2.1.4. *(Greenberg) Let $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$, $\mathfrak{q}^* = \bar{\mathfrak{q}}$, and denote by W the sign in the functional equation of ψ. If 1 denotes the trivial character, so that $\mu_{\mathfrak{q}}(\mathcal{K}, 1)$ is the image of $\mu_{\mathfrak{q}}$ in $\Lambda(\mathcal{K})_{\mathrm{R}_0}$, then*

(1) *the critical divisor divides $e(\chi_{\mathfrak{q}})\mu_{\mathfrak{q}}(\mathcal{K}, 1)$ if and only if $W = -1$,*
(2) *the critical divisor divides $e(\chi_{\mathfrak{q}^*})\mu_{\mathfrak{q}}(\mathcal{K}, 1)$ if and only if $W = 1$.*

Proof. The first claim is exactly the case $k_0 = 0$ of [6], Proposition 6. For the second claim, the case $k_0 = p-2$ of the same proposition shows that the critical divisor divides $e(\chi_{\mathfrak{q}^*})\mu_{\mathfrak{q}}(\mathcal{K}, 1)$ if and only if $W_{p-2} = -1$, where W_{p-2} is the sign in the functional equation of $\psi^{2(p-2)+1}$. Let m denote the number of roots of unity in K. Proposition 1 of [6], together with the fact that $p \equiv 1 \pmod{m}$, implies that $W_{p-2} = -W$. $\square$

Corollary 2.1.5. *The measure $\mu_{\mathfrak{p}}(D_\infty, \psi_{\mathfrak{p}^*})$ is nonzero if and only if $W = -1$. The measure $\mu_{\mathfrak{p}^*}(D_\infty, \psi_{\mathfrak{p}^*})$ is nonzero if and only if $W = 1$.*

Proof. Let $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$. We have $\mu_{\mathfrak{q}}(D_\infty, \psi_{\mathfrak{p}^*}) = 0$ if and only if $\mathrm{Tw}_{\eta_{\mathfrak{p}^*}}(\Theta)$ divides $\mu_{\mathfrak{q}}(K_\infty, \psi_{\mathfrak{p}^*})$, which occurs if and only if Θ divides

$$\begin{aligned}
\mathrm{Tw}_{\eta_{\mathfrak{p}^*}^{-1}}\left(\mu_{\mathfrak{q}}(K_\infty, \psi_{\mathfrak{p}^*})\right) &= \mathrm{Tw}_{\psi_{\mathfrak{p}^*}^{-1}}\left(e(1)\mu_{\mathfrak{q}}(\mathcal{K}, \psi_{\mathfrak{p}^*})\right) \\
&= e(\chi_{\mathfrak{p}^*})\mathrm{Tw}_{\psi_{\mathfrak{p}^*}^{-1}}\left(\mu_{\mathfrak{q}}(\mathcal{K}, \psi_{\mathfrak{p}^*})\right) \\
&= e(\chi_{\mathfrak{p}^*})\mu_{\mathfrak{q}}(\mathcal{K}, 1).
\end{aligned}$$

The claim now follows from Theorem 2.1.4. $\square$

Corollary 2.1.5 shows that one of the measures $\mu_{\mathfrak{p}}(D_\infty, \psi_{\mathfrak{p}^*})$, $\mu_{\mathfrak{p}^*}(D_\infty, \psi_{\mathfrak{p}^*})$ (depending upon the value of W) is non-zero. We conclude this subsection by describing an alternative approach to showing this fact, using root number calculations and non-vanishing theorems for complex-valued L-functions.

Suppose that θ is a $\mathbf{C}^\times$-valued idele class character of K, of conductor f_θ. Then we may write $\theta = \prod_v \theta_v$, where the product is over all places of K. We define the integer $n(\theta)$ by the equality $\theta_\infty(z) = z^{n(\theta)}|z|^s$. Hence, if θ is associated to a grossencharacter of K of type (k, j), then

$$\theta_\infty(z) = z^k \bar{z}^j = z^{k-j}|z|^{2j},$$

and so $n(\theta) = k - j$.

Let W_θ denote the root number associated to θ. It follows easily from standard properties of root numbers (see, for example [10], especially Proposition 2.2 on page 30 and the definition on page 32) that $W_\theta = W_{\theta/|\theta|}$.

Proposition 2.1.6. *(Weil) Suppose that θ_1 and θ_2 are $\mathbf{C}^\times$-valued idele class characters of absolute value* 1. *Assume also that f_{θ_1} and f_{θ_2} are relatively prime. Then*

$$W_{\theta_1}W_{\theta_2}\theta_1(f_{\theta_2})\theta_2(f_{\theta_1}) = \begin{cases} W_{\theta_1\theta_2} & \text{if } n(\theta_1)n(\theta_2) \geq 0; \\ (-1)^\nu W_{\theta_1\theta_2} & \text{if } n(\theta_1)n(\theta_2) < 0, \end{cases}$$

where $\nu = \inf\{|n(\theta_1)|, |n(\theta_1)|\} \mod 2$.

Proof. See [26], pages 151-161 (especially Section 79). □

Let $K[p^n]$ denote the ring class field of K of conductor p^n, and set $K[p^\infty] = \cup_{n\geq 1}K[p^n]$.

Proposition 2.1.7. *Let ξ be a grossencharacter of K whose associated Galois character factors through* $\mathrm{Gal}(K[p^\infty]/K)$ *and is of finite order.*

(a)(Greenberg) The following equality holds

$$W_{\xi\psi} = W_\psi.$$

(b) Let e be a positive integer, and let ϵ be a grossencharacter of type $(-e, e)$ associated to K, of trivial conductor (such a grossencharacter always exists for a suitable choice of e). Then

$$W_{\epsilon\xi\psi} = -W_\psi.$$

Proof. (a) This is proved on page 247 of [6]. (Note that the proof given in [6] assumes that the Galois character associated to ξ factors through $\mathrm{Gal}(D_\infty/K)$. It is easy to see that the same proof holds if we instead assume that the Galois character associated to ξ factors through $\mathrm{Gal}(K[p^\infty]/K)$.)

(b) From part (a), we see that it suffices to show that

$$W_{\epsilon\xi\psi} = -W_{\xi\psi}.$$

The proof of this equality proceeds by applying Proposition 2.1.6 to the idele class characters $\theta_1 = \xi\psi/|\xi\psi|$ and $\theta_2 = \epsilon/|\epsilon|$.

We first note that since ϵ has trivial conductor, the same is true of θ_2, and so $\theta_1(f_{\theta_2}) = 1$. Next, we observe that since E is defined over $\mathbf{Q}$, it follows that $\bar{f}_{\theta_1} = f_{\theta_1}$. Since ϵ is of type $(e, -e)$ and has trivial conductor, this implies that $\theta_2(f_{\theta_1}) = 1$.

Let δ_K denote the different of $K/\mathbf{Q}$. It follows from standard formulae for global root numbers (see [9], Chapter XIV, §8, Corollary 1, for example) that

$$W_\epsilon = i^{-2e}\epsilon(\delta_K^{-1}) = (-1)^e\epsilon(\delta_K^{-1}). \tag{2.5}$$

It is not hard to check that the different of any imaginary quadratic field of class number one has a generator δ satisfying $\delta/|\delta| = i$. This implies (since ϵ has trivial conductor and is of type $(e, -e)$) that $\epsilon(\delta_K^{-1}) = (-1)^e$. It now follows from (2.5) that

$$W_\epsilon = 1 = W_{\theta_2}.$$

Finally, we note that $n(\theta_1) = 1$ and $n(\theta_2) = -2e$, whence it follows that $\nu = 1$. Putting all of the above together gives

$$W_{\theta_1\theta_2} = -W_{\theta_1}W_{\theta_2},$$

from which we deduce that

$$W_{\epsilon\xi\psi} = -W_{\xi\psi} = -W_\psi,$$

as claimed. □

Now suppose that $W_\psi = -1$, and let $\kappa = \epsilon\xi$ be a grossencharacter as in Proposition 2.1.7(b) whose associated Galois character factors through $\mathrm{Gal}(D_\infty/K)$. (Note that once a choice of ϵ is fixed, then there are infinitely many choices of ξ such that the Galois character associated to $\epsilon\xi$ factors through $\mathrm{Gal}(D_\infty/K)$.) Then $\kappa\bar{\psi}^{-1}$ is of type $(-e, e-1)$, and so it lies within the range of interpolation of (2.3). Hence we have (from (2.3) and (2.4))

$$\begin{aligned}\int \kappa_{\mathfrak{p}}^{-1} d\mu_{\mathfrak{p}}(D_\infty; \psi_{\mathfrak{p}^*}, \mathfrak{a}) &= i_{\mathfrak{p}}(\kappa^{-1}\bar{\psi}(\mathfrak{a}) - \mathrm{N}\mathfrak{a})\mathcal{L}_{\mathfrak{p},\mathfrak{f}}(\kappa\bar{\psi}^{-1}) \\ &= i_{\mathfrak{p}}(\kappa^{-1}\bar{\psi}(\mathfrak{a}) - \mathrm{N}\mathfrak{a})\left(1 - \frac{\kappa(\mathfrak{p})^{-1}}{p}\right) L_{\infty,\mathfrak{f}\mathfrak{p}^*}(\kappa\bar{\psi}^{-1}, 0) \\ &= i_{\mathfrak{p}}(\kappa^{-1}\bar{\psi}(\mathfrak{a}) - \mathrm{N}\mathfrak{a})\left(1 - \frac{\kappa(\mathfrak{p})^{-1}}{p}\right) L_{\infty,\mathfrak{f}\mathfrak{p}^*}(\kappa\psi, 1),\end{aligned}$$

where for the last equality we have used the fact that $\psi\bar{\psi} = \mathrm{N}$.

Next we note that Proposition 2.1.7(b) implies that $W_{\kappa\psi} = 1$. It now follows from a theorem of Rohrlich (see page 384 of [20]) that, for all but finitely many choices of κ, we have $L_{\infty,\mathfrak{f}\mathfrak{p}^*}(\kappa\psi, 1) \neq 0$. Hence the measure $\mu_{\mathfrak{p}}(D_\infty; \psi_{\mathfrak{p}^*}, \mathfrak{a})$ is non-zero, and so the same is true of $\mu_{\mathfrak{p}}(D_\infty; \psi_{\mathfrak{p}^*})$.

We now turn to the measure $\mu_{\mathfrak{p}^*}(D_\infty; \psi_{\mathfrak{p}^*})$. Suppose that $W_\psi = 1$, and let ξ be any character of $\mathrm{Gal}(D_\infty/K)$ of finite order. Then the grossencharacter $\xi\psi^{-1}$ is of type $(-1, 0)$, and so lies within the range of interpolation of (2.3). Hence, just as above, we have

$$\begin{aligned}\int \xi_{\mathfrak{p}^*}^{-1} d\mu_{\mathfrak{p}^*}(D_\infty; \psi_{\mathfrak{p}^*}, \mathfrak{a}) &= i_{\mathfrak{p}^*}(\xi^{-1}\psi(\mathfrak{a}) - \mathrm{N}\mathfrak{a})\mathcal{L}_{\mathfrak{p}^*,\mathfrak{f}}(\xi\psi^{-1}) \\ &= i_{\mathfrak{p}^*}(\xi^{-1}\psi(\mathfrak{a}) - \mathrm{N}\mathfrak{a})\left(1 - \frac{\xi(\mathfrak{p}^*)^{-1}}{p}\right) L_{\infty,\mathfrak{f}\mathfrak{p}}(\xi\psi^{-1}, 0) \\ &= i_{\mathfrak{p}^*}(\xi^{-1}\psi(\mathfrak{a}) - \mathrm{N}\mathfrak{a})\left(1 - \frac{\xi(\mathfrak{p}^*)^{-1}}{p}\right) L_{\infty,\mathfrak{f}\mathfrak{p}}(\xi\bar{\psi}, 1).\end{aligned}$$

Now Proposition 2.1.7(a) implies that that $W(\xi\bar{\psi}) = W(\psi) = 1$. It therefore follows from the theorem of Rohrlich quoted above that, for all but finitely many choices of ξ, we have $L_{\infty,\mathfrak{f}\mathfrak{p}}(\xi\bar{\psi}, 1) \neq 0$. This in turn implies that $\mu_{\mathfrak{p}^*}(D_\infty; \psi_{\mathfrak{p}^*}, \mathfrak{a})$ is non-zero, whence it follows that $\mu_{\mathfrak{p}^*}(D_\infty; \psi_{\mathfrak{p}^*})$ is non-zero also.

2.2. **Elliptic units.** If F/K is any finite extension and $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$, we define $U_{\mathfrak{q}}(F)$ to be the direct sum over all places w dividing $\mathfrak{q}$ of the principal units of F_w. If F/K is any (possibly infinite) extension, we define $U_{\mathfrak{q}}(F)$ to be the inverse limit with respect to the norm maps of the groups $U_{\mathfrak{q}}(F')$ as $F' \subset F$ ranges over the finite extensions of K. Let $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal with $(\mathfrak{a}, \mathfrak{f}p) = 1$, and let $I(\mathfrak{a})$ denote the set of all ideals of $\mathcal{O}_K$ prime to $\mathfrak{a}$.

If $L \subset \mathbf{C}$ is a lattice with CM by $\mathcal{O}_K$, we define an elliptic function

$$\Theta(z; L, \mathfrak{a}) = \frac{\Delta(L)}{\Delta(\mathfrak{a}^{-1}L)} \prod \frac{\Delta(L)}{(\wp(z, L) - \wp(u, L))^6}$$

where the product is over the nontrivial $u \in \mathfrak{a}^{-1}L/L$, and Δ is the modular discriminant. For any $\mathfrak{m} \in I(\mathfrak{a})$, let $w_{\mathfrak{m}}$ be the number of roots of unity congruent to 1 modulo $\mathfrak{m}$. If $\mathfrak{m}$ is not a prime power then $\Theta(1; \mathfrak{m}, \mathfrak{a})$ is a unit of $K(\mathfrak{m})$, and if

$\mathfrak{l} \in I(\mathfrak{a})$ is prime we have the distribution relation

$$\mathrm{Norm}_{K(\mathfrak{m}\mathfrak{l})/K(\mathfrak{m})}\Theta(1;\mathfrak{m}\mathfrak{l},\mathfrak{a})^e = \begin{cases} \Theta(1;\mathfrak{m},\mathfrak{a}) & \text{if } \mathfrak{l} \mid \mathfrak{m} \\ \Theta(1;\mathfrak{m},\mathfrak{a})^{1-\sigma_{\mathfrak{l}}^{-1}} & \text{else} \end{cases}$$

where $e = w_{\mathfrak{m}}/w_{\mathfrak{m}\mathfrak{l}}$. In particular, the sequence $\Theta(1;\mathfrak{f}p^k,\mathfrak{a})$ is norm compatible for $k > 0$. We denote by $\beta(\mathfrak{a})$ and $\beta^*(\mathfrak{a})$ the images of this sequence in $U_{\mathfrak{p}}(K(\mathfrak{f}p^\infty))$ and $U_{\mathfrak{p}^*}(K(\mathfrak{f}p^\infty))$, respectively.

Define $J \subset \Lambda(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0}$ to be the annihilator of μ_{p^∞}. Then J is the ideal generated by $\sigma_{\mathfrak{b}} - \mathrm{N}(\mathfrak{b})$ as $\mathfrak{b}$ ranges over integral ideals prime to $\mathfrak{f}p$.

Theorem 2.2.1. *(Yager) There are isomorphisms of $\Lambda(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0}$-modules*

$$U_{\mathfrak{p}}(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0} \cong J, \quad U_{\mathfrak{p}^*}(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0} \cong J,$$

which take

$$\beta(\mathfrak{a}) \mapsto (\sigma_{\mathfrak{a}} - \mathrm{N}(\mathfrak{a}))\cdot\mu_{\mathfrak{p}}, \quad \beta^*(\mathfrak{a}) \mapsto (\sigma_{\mathfrak{a}} - \mathrm{N}(\mathfrak{a}))\cdot\mu_{\mathfrak{p}^*}.$$

Proof. This is Proposition III.1.4 of [4]. □

2.3. **The twisted Euler system.** We continue to denote by $\mathfrak{a}$ a nontrivial $\mathcal{O}_K$-ideal prime to $\mathfrak{f}p$. If $\mathfrak{m} \in I(\mathfrak{a})$, define a unit

$$\vartheta_{\mathfrak{a}}(\mathfrak{m}) = \mathrm{Norm}_{K(\mathfrak{m}\mathfrak{f}p)/K(\mathfrak{m})}\Theta(1;\mathfrak{m}\mathfrak{f}p,\mathfrak{a}).$$

If we let $\mathcal{K}_{\mathfrak{a}} = \cup_{\mathfrak{m}\in I(\mathfrak{a})}K(\mathfrak{m})$, the elements

$$\vartheta_{\mathfrak{a}}(\mathfrak{m}) \in H^1(K(\mathfrak{m}),\mathbf{Z}_p(1)),$$

with $\mathfrak{a}$ fixed, form an Euler system for $(\mathbf{Z}_p(1),\mathfrak{f}p,\mathcal{K}_{\mathfrak{a}})$ in the sense of [25].

Proposition 2.3.1. *Let $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$. There is an Euler system $c = c_{\mathfrak{a}}$ for $(T_{\mathfrak{p}},\mathfrak{f}p,\mathcal{K}_{\mathfrak{a}})$ and an injection (the Coleman map)*

$$\mathrm{Col}_{\mathfrak{q}} : \mathcal{H}^1(K(\mathfrak{f}p^\infty)_{\mathfrak{q}},T_{\mathfrak{p}})_{\mathrm{R}_0} \to \Lambda(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0}$$

with the following property: if we set

$$z = \varprojlim c(K(\mathfrak{f}p^k)) \in \mathcal{H}^1(K(\mathfrak{f}p^\infty),T_{\mathfrak{p}}),$$

and let $\mathrm{loc}_{\mathfrak{q}}(z)$ be its image in $\mathcal{H}^1(K(\mathfrak{f}p^\infty)_{\mathfrak{q}},T_{\mathfrak{p}})$, then $\mathrm{Col}_{\mathfrak{q}}$ sends

$$\mathrm{loc}_{\mathfrak{q}}(z)\otimes 1 \mapsto \mu_{\mathfrak{q}}(K(\mathfrak{f}p^\infty),\psi_{\mathfrak{p}^*},\mathfrak{a}).$$

The image of $\mathrm{Col}_{\mathfrak{q}}$ is $\mathrm{Tw}_{\psi_{\mathfrak{p}^*}}(J)$, the ideal generated by all elements of the form $\sigma_{\mathfrak{b}} - \psi_{\mathfrak{p}}(\sigma_{\mathfrak{b}})$ with $\mathfrak{b}$ prime to $\mathfrak{f}p$.

Proof. This follows from the "twisting" theorems of Chapter 6 of [25]. The G_K-module $T_{\mathfrak{p}}$ is isomorphic to the twist of $\mathbf{Z}_p(1)$ by the character $\omega^{-1}\psi_{\mathfrak{p}} = \psi_{\mathfrak{p}^*}^{-1}$, where ω is the cyclotomic character. A choice of such an isomorphism determines an isomorphism of $\mathbf{Z}_p$-modules

$$\mathcal{H}^1(K(\mathfrak{f}p^\infty),\mathbf{Z}_p(1)) \xrightarrow{\phi} \mathcal{H}^1(K(\mathfrak{f}p^\infty),T_{\mathfrak{p}})$$

satisfying $\phi\circ\mathrm{Tw}_{\psi_{\mathfrak{p}^*}}^{-1}(\lambda) = \lambda\circ\phi$ for any $\lambda \in \Lambda(K(\mathfrak{f}p^\infty))$. Similarly, if $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$, there is an isomorphism of $\mathbf{Z}_p$-modules

$$U_{\mathfrak{q}}(K(\mathfrak{f}p^\infty)) \cong \mathcal{H}^1(K(\mathfrak{f}p^\infty)_{\mathfrak{q}},\mathbf{Z}_p(1)) \xrightarrow{\phi_{\mathfrak{q}}} \mathcal{H}^1(K(\mathfrak{f}p^\infty)_{\mathfrak{q}},T_{\mathfrak{p}})$$

which is compatible with ϕ and the localization map $\mathrm{loc}_{\mathfrak{q}}$.

The Euler system $c_{\mathfrak{a}}$ is the twist of $\vartheta_{\mathfrak{a}}$ by $\psi_{\mathfrak{p}^*}$, and by construction

$$z = \phi(\varprojlim \vartheta_{\mathfrak{a}}(\mathfrak{f}p^k)) = \phi(\varprojlim \Theta(1; \mathfrak{f}p^k, \mathfrak{a})).$$

See Section 6.3 of [25], especially Theorem 6.3.5. In particular, $\mathrm{loc}_{\mathfrak{q}}(z) = \phi_{\mathfrak{q}}(\beta_{\mathfrak{a}})$, and if we define $\mathrm{Col}_{\mathfrak{q}}$ to be the composition

$$\mathcal{H}^1(K(\mathfrak{f}p^\infty)_{\mathfrak{q}}, T_{\mathfrak{p}})_{\mathrm{R}_0} \xrightarrow{\phi_{\mathfrak{q}}^{-1}} U_{\mathfrak{q}}(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0} \cong J \xrightarrow{\mathrm{Tw}_{\psi_{\mathfrak{p}^*}}} \mathrm{Tw}_{\psi_{\mathfrak{p}^*}}(J)$$

then $\mathrm{Col}_{\mathfrak{q}}$ is an isomorphism of $\Lambda(K(\mathfrak{f}p^\infty))_{\mathrm{R}_0}$-modules with the desired properties. □

Definition 2.3.2. We say that the prime p is *anomalous* if p divides

$$(1 - \psi(\mathfrak{p}))(1 - \psi(\mathfrak{p}^*)),$$

or equivalently if there is any p-torsion defined over $\mathbf{Z}/p\mathbf{Z}$ on the reduction of E at p.

Lemma 2.3.3. *Let $F \subset K_\infty$ contain K and let $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$. The natural corestriction map*

$$\mathcal{H}^1(K_{\infty,\mathfrak{q}}, T_{\mathfrak{p}}) \otimes_{\Lambda(K_\infty)} \Lambda(F) \to \mathcal{H}^1(F_{\mathfrak{q}}, T_{\mathfrak{p}}) \tag{2.6}$$

is an isomorphism if either $\mathfrak{q} = \mathfrak{p}^*$ or if $\mathfrak{q} = \mathfrak{p}$ and p is not anomalous. If $F = C_m D_n$ for some $0 \le m, n \le \infty$, then the map is injective with finite cokernel.

Proof. Let v be any place of K_∞ above $\mathfrak{p}^*$, and denote also by v the place of F below it. By Lemma 1.1.2, $E(K_{\infty,v})[\mathfrak{p}^*] = 0$, and the inflation-restriction sequence shows that

$$H^1(F_v, W_{\mathfrak{p}^*}) \to H^1(K_{\infty,v}, W_{\mathfrak{p}^*})^{\mathrm{Gal}(K_{\infty,v}/F_v)}$$

is an isomorphism. This implies that the restriction map

$$H^1(F_{\mathfrak{p}^*}, W_{\mathfrak{p}^*}) \to H^1(K_{\infty,\mathfrak{p}^*}, W_{\mathfrak{p}^*})^{\mathrm{Gal}(K_\infty/F)}$$

is an isomorphism. By local duality, the map

$$\mathcal{H}^1(K_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}}) \otimes_{\Lambda(K_\infty)} \Lambda(F) \to \mathcal{H}^1(F_{\mathfrak{p}^*}, T_{\mathfrak{p}})$$

is an isomorphism. If p is not anomalous then $E(L)[\mathfrak{p}] = 0$ for any p-power extension $L/K_{\mathfrak{p}}$, and the same argument as above shows that

$$\mathcal{H}^1(K_{\infty,\mathfrak{p}}, T_{\mathfrak{p}}) \otimes_{\Lambda(K_\infty)} \Lambda(F) \to \mathcal{H}^1(F_{\mathfrak{p}}, T_{\mathfrak{p}})$$

is an isomorphism.

Now suppose $F = C_m D_n$, let v be a place of K_∞ above $\mathfrak{p}$, and suppose also that p is anomalous; this implies that all $\mathfrak{p}^*$-power torsion of E is defined over $K_{\infty,v}$, and in fact is defined over the unique unramified $\mathbf{Z}_p$-extension of K_v. Set $L = C_\infty D_n$, and define

$$B = H^0(L_v, W_{\mathfrak{p}^*}) = H^0(K_v^{\mathrm{unr}} \cap L_v, W_{\mathfrak{p}^*}).$$

Note that B is finite, since $K_v^{\mathrm{unr}} \cap L_v$ is a finite extension of $\mathbf{Q}_p$. We have the inflation-restriction sequence

$$H^1(L_v/F_v, B) \to H^1(F_v, W_{\mathfrak{p}^*}) \xrightarrow{\mathrm{res}} H^1(L_v, W_{\mathfrak{p}^*})^{\mathrm{Gal}(L_v/F_v)} \to H^2(L_v/F_v, B).$$

Since $\mathrm{Gal}(L_v/F_v) \cong \mathbf{Z}_p$ is of cohomological dimension one, the final term of this sequence is trivial, and so the map res is surjective. The first term of the sequence is isomorphic to $B/(\gamma - 1)B$ for any generator γ of $\mathrm{Gal}(L_v/F_v)$, and this is finite since B is.

Now consider the restriction map

$$H^1(L_v, W_{\mathfrak{p}^*}) \;\to\; H^1(K_{\infty,v}, W_{\mathfrak{p}^*})^{\mathrm{Gal}(K_{\infty,v}/L_v)}.$$

Since $K_{\infty,v}/L_v$ is a $\mathbf{Z}_p$-extension, the restriction is surjective, exactly as above. Similarly, the kernel is isomorphic to $W_{\mathfrak{p}^*}/(\sigma-1)W_{\mathfrak{p}^*}$ for any generator σ of $\mathrm{Gal}(K_{\infty,v}/L_v)$. Such a σ acts on $W_{\mathfrak{p}^*}$ through some scalar $\neq 1$, and since $W_{\mathfrak{p}^*}$ is divisible the kernel of restriction is trivial. As above, local duality gives the stated results. □

Proposition 2.3.4. *Let $F \subset K_\infty$ be a (possibly infinite) extension of K, and let $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$. Suppose that one of the following holds*

(1) $\mathfrak{q} = \mathfrak{p}^*$,
(2) $\mathfrak{q} = \mathfrak{p}$ *and p is not anomalous,*
(3) $\mathfrak{q} = \mathfrak{p}$ *and $F = D_m C_n$ for $0 \leq m, n \leq \infty$.*

There is an injection of $\Lambda_{\mathrm{R}}(F)$-modules

$$\mathcal{H}^1(F_{\mathfrak{q}}, T_{\mathfrak{p}})_{\mathrm{R}} \;\to\; \Lambda(F)_{\mathrm{R}}$$

taking $\mathrm{loc}_{\mathfrak{q}}(c(F)) \otimes 1$ to $\mu_{\mathfrak{q}}(F; \psi_{\mathfrak{p}^*}, \mathfrak{a})$. The image of this map is the ideal generated by $\lambda(F; \psi_{\mathfrak{p}^*}, \mathfrak{a})$ as $\mathfrak{a}$ varies, and if $F = D_\infty$ the map is an isomorphism. If p does not divide $[K(\mathfrak{f}) : K]$ and if either (1) or (2) holds, the result is true with R replaced by R_0.

Proof. Let w be a place of $K(\mathfrak{f}p^\infty)$ above p, set $H = \mathrm{Gal}(K(\mathfrak{f}p^\infty)_w/K_{\infty,w})$ and consider the inflation-restriction sequence

$$H^1(H, W_{\mathfrak{p}^*}) \;\to\; H^1(K_{\infty,w}, W_{\mathfrak{p}^*}) \;\to\; H^1(K(\mathfrak{f}p^\infty)_w, W_{\mathfrak{p}^*}) \;\to\; H^2(H, W_{\mathfrak{p}^*}).$$

The first and last terms are finite. If p does not divide $[K(\mathfrak{f}) : K]$ then p does not divide $|H|$, and so the kernel and cokernel of restriction are trivial. Applying local duality and considering the semi-local cohomology, we see that the map

$$\mathcal{H}^1(K(\mathfrak{f}p^\infty)_{\mathfrak{q}}, T_{\mathfrak{p}}) \otimes_{\Lambda(K(\mathfrak{f}p^\infty))} \Lambda(K_\infty) \;\to\; \mathcal{H}^1(K_{\infty,\mathfrak{q}}, T_{\mathfrak{p}})$$

has finite kernel and cokernel, and is an isomorphism if $[K(\mathfrak{f}) : K]$ is prime to p.

By Lemma 2.3.3 the natural map

$$\mathcal{H}^1(K(\mathfrak{f}p^\infty)_{\mathfrak{q}}, T_{\mathfrak{p}}) \otimes_{\Lambda(K(\mathfrak{f}p^\infty))} \Lambda(F) \;\to\; \mathcal{H}^1(F_{\mathfrak{q}}, T_{\mathfrak{p}})$$

has finite kernel and cokernel, and so becomes an isomorphism upon applying first $\hat{\otimes}\mathrm{R}_0$ and then $\otimes\mathrm{R}$. Tensoring the Coleman map of Proposition 2.3.1 with $\Lambda(F)$ yields the desired map. If $F = D_\infty$ then F is disjoint from the extension of K cut out by $\psi_{\mathfrak{p}}$, and it follows that the image of the map above is the ideal of $\Lambda(F)_{\mathrm{R}}$ generated by all elements of the form $\gamma - \alpha$, where γ runs over $\mathrm{Gal}(D_\infty/K)$ and α runs over $\mathbf{Z}_p^\times$. This ideal is all of $\Lambda(F)_{\mathrm{R}}$. □

2.4. **Main conjectures.** Throughout this subsection we fix a topological generator $\gamma \in \mathrm{Gal}(K_\infty/D_\infty)$, and we let $I = (\gamma - 1)\Lambda(K_\infty)$.

Denote by W the sign in the functional equation of $L(\psi, s)$. Let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$ prime to $p\mathfrak{f}$, and recall that $\mathcal{K}_{\mathfrak{a}}$ is the union of all ray class fields of K of conductor prime to $\mathfrak{a}$. Let $c_{\mathfrak{a}}$ be the Euler system for $(T_{\mathfrak{p}}, \mathfrak{f}p, \mathcal{K}_{\mathfrak{a}})$ of Proposition 2.3.1, and for any $F \subset K_\infty$, let

$$c_{\mathfrak{a}}(F) = \varprojlim c_{\mathfrak{a}}(F') \in \mathcal{H}^1(F, T_{\mathfrak{p}}).$$

be the limit as F' ranges over subfields of F finite over K. Let $\mathcal{C}_{\mathfrak{a}}(F)$ be the $\Lambda(F)$-submodule of $\mathcal{S}_{\mathrm{rel}}(F,T_{\mathfrak{p}})$ generated by $c_{\mathfrak{a}}(F)$, and let $\mathcal{C}(F)$ be the submodule generated by $\mathcal{C}_{\mathfrak{a}}(F)$ as $\mathfrak{a}$ varies over all ideals prime to $p\mathfrak{f}$. Define

$$Z(F)=\mathcal{S}_{\mathrm{rel}}(F,T_{\mathfrak{p}})/\mathcal{C}(F),$$

and define $Z_{\mathfrak{a}}(F)$ similarly, replacing $\mathcal{C}$ by $\mathcal{C}_{\mathfrak{a}}$.

Remark 2.4.1. It is clear from the definitions that $\mathrm{Sel}_{\mathrm{rel}}(F,T_{\mathfrak{p}})=H^1(F,T_{\mathfrak{p}})$ for every extension F/K. In particular $c_{\mathfrak{a}}(F)\in\mathcal{S}_{\mathrm{rel}}(F,T_{\mathfrak{p}})$.

Lemma 2.4.2. *For every $F\subset\mathcal{K}_{\mathfrak{a}}$ finite over K, the class $c_{\mathfrak{a}}(F)$ is unramified at every prime of F not dividing p.*

Proof. This follows from Corollary B.3.5 of [25], and the fact that the class $c_{\mathfrak{a}}(F)$ is a universal norm in the cyclotomic direction. □

Proposition 2.4.3. *The submodule $\mathrm{loc}_{\mathfrak{p}^*}(\mathcal{C}(D_\infty))\subset\mathcal{H}^1(D_{\infty,\mathfrak{p}^*},T_{\mathfrak{p}})$ is nontrivial if and only if $W=1$. The submodule $\mathrm{loc}_{\mathfrak{p}}(\mathcal{C}(D_\infty))\subset\mathcal{H}^1(D_{\infty,\mathfrak{p}},T_{\mathfrak{p}})$ is nontrivial if and only if $W=-1$. In particular, $\mathcal{C}(D_\infty)\neq 0$ regardless of the value of W.*

Proof. Suppose $W=1$. By Corollary 2.1.5,

$$\mu_{\mathfrak{p}}(D_\infty,\psi_{\mathfrak{p}^*})=0 \qquad \mu_{\mathfrak{p}^*}(D_\infty,\psi_{\mathfrak{p}^*})\neq 0.$$

We may choose $\mathfrak{a}$ so that $\lambda(D_\infty;\psi_{\mathfrak{p}^*},\mathfrak{a})\neq 0$, and then Proposition 2.3.4 implies that $\mathrm{loc}_{\mathfrak{p}^*}(\mathcal{C}_{\mathfrak{a}}(D_\infty))\neq 0$. Therefore $\mathrm{loc}_{\mathfrak{p}^*}(\mathcal{C}(D_\infty))\neq 0$. On the other hand, for every choice of $\mathfrak{a}$, $\mu_{\mathfrak{p}}(D_\infty;\psi_{\mathfrak{p}^*},\mathfrak{a})=0$, and so Proposition 2.3.4 implies that $\mathrm{loc}_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{a}}(D_\infty))$ is trivial in $\mathcal{H}^1(D_{\infty,\mathfrak{p}},T_{\mathfrak{p}})_{\mathrm{R}}$ By Proposition 1.1.6, $\mathcal{H}^1(D_{\infty,\mathfrak{p}},T_{\mathfrak{p}})$ is torsion-free, and so $\mathrm{loc}_{\mathfrak{p}}(\mathcal{C}_{\mathfrak{a}}(D_\infty))$ is trivial in $\mathcal{H}^1(D_{\infty,\mathfrak{p}},T_{\mathfrak{p}})$. The case $W=-1$ is entirely similar. □

Now armed with a nontrivial Euler system, we may apply the general theory introduced by Kolyvagin and developed by Kato, Perrin-Riou, and Rubin.

Proposition 2.4.4. *The $\Lambda(D_\infty)$-module $X^*_{\mathrm{str}}(D_\infty)$ is torsion and $\mathcal{S}_{\mathrm{rel}}(D_\infty,T_{\mathfrak{p}})$ is torsion free of rank one. Furthermore, we have the divisibility of characteristic ideals*

$$\mathrm{char}(X^*_{\mathrm{str}}(D_\infty)) \ \text{ divides } \ \mathrm{char}(Z(D_\infty)).$$

If $W=1$ then the $\Lambda(D_\infty)$-module $X^*(D_\infty)$ is torsion. If $W=-1$ then $X^*(D_\infty)$ has rank one and $\mathcal{S}(D_\infty,T_{\mathfrak{p}})=\mathcal{S}_{\mathrm{rel}}(D_\infty,T_{\mathfrak{p}})$.

Proof. By Proposition 2.4.3, we may choose some $\mathfrak{a}$ so that $\mathcal{C}_{\mathfrak{a}}(D_\infty)\neq 0$. The first claim follows from Theorem 2.3.2 of [25] (together with Lemma 2.4.2 and the remarks of Section 9.2 of [25]), and the second then follows from Lemmas 1.1.9 and 1.2.1 and Theorem 1.2.2. Applying Theorem 2.3.3 of [25] as $\mathfrak{a}$ varies over all integral ideals prime to $p\mathfrak{f}$, one obtains the divisibility of characteristic ideals.

Suppose $W=1$. The image of $\mathcal{C}(D_\infty)$ under

$$\mathrm{loc}_{\mathfrak{p}^*}:\mathcal{S}_{\mathrm{rel}}(D_\infty,T_{\mathfrak{p}})\ \to\ \mathcal{H}^1(D_{\infty,\mathfrak{p}^*},T_{\mathfrak{p}})$$

is nontrivial by Proposition 2.4.3, and since both modules are torsion-free of rank one this map must be injective with torsion cokernel. By Proposition 1.1.7 we obtain the exact sequence

$$0\ \to\ \mathcal{S}_{\mathrm{rel}}(D_\infty,T_{\mathfrak{p}})\ \to\ \mathcal{H}^1(D_{\infty,\mathfrak{p}^*},T_{\mathfrak{p}})\ \to\ X^*(D_\infty)\ \to\ X^*_{\mathrm{str}}(D_\infty)\ \to\ 0$$

which shows that $X^*(D_\infty)$ is torsion.

Suppose $W = -1$. By Proposition 2.4.3 and the exact sequence (1.3), $\mathcal{C}(D_\infty) \subset \mathcal{S}(D_\infty, T_\mathfrak{p})$. Since $\mathcal{C}(D_\infty) \neq 0$ and $\mathcal{S}(D_\infty, T_\mathfrak{p}) \subset \mathcal{S}_{\mathrm{rel}}(D_\infty, T_\mathfrak{p})$, it follows that $\mathcal{S}(D_\infty, T_\mathfrak{p})$ is torsion free of rank one. From Lemma 1.2.1 and Proposition 1.2.2, we see that $X^*(D_\infty)$ has rank one. Furthermore, the image of $\mathrm{loc}_{\mathfrak{p}^*}$ in the exact sequence (1.3) (with $F = D_\infty$) must be a torsion module, and hence must be trivial. Therefore $\mathcal{S}(D_\infty, T_\mathfrak{p}) = \mathcal{S}_{\mathrm{rel}}(D_\infty, T_\mathfrak{p})$. □

Let $\mathcal{K} = K(E[p^\infty])$ and define abelian extensions of $\mathcal{K}$ as follows:

- $\mathcal{M}_{\mathrm{rel}}$ is the maximal abelian pro-p-extension of $\mathcal{K}$ unramified outside of p,
- $\mathcal{M}$ is the maximal abelian pro-p-extension of $\mathcal{K}$ unramified outside of $\mathfrak{p}^*$,
- $\mathcal{M}_{\mathrm{str}}$ is the maximal abelian pro-p-extension of $\mathcal{K}$ unramified everywhere.

Let $\mathcal{E}$ be the inverse limit of the groups $\mathcal{O}_F^\times \otimes \mathbf{Z}_p$ over subfields $F \subset \mathcal{K}$ containing K. For any integral ideal $\mathfrak{a}$ of K prime to $p\mathfrak{f}$, let $\mathcal{U}_\mathfrak{a} \subset \mathcal{E}$ be the submodule generated by the (untwisted) elliptic unit Euler system $\vartheta_\mathfrak{a}$ of §2.3. Let $\mathcal{U}$ be the submodule generated by all such $\mathcal{U}_\mathfrak{a}$. By Kummer theory we may view $\mathcal{U} \subset \mathcal{E} \subset \mathcal{H}^1(\mathcal{K}, \mathbf{Z}_p(1))$.

The following result is essentially due to Coates (see [3] Theorem 12).

Lemma 2.4.5. *There is a group isomorphism*

$$\alpha : H^1(\mathcal{K}, \mathbf{Q}_p/\mathbf{Z}_p) \cong H^1(\mathcal{K}, W_{\mathfrak{p}^*})$$

satisfying $\alpha \circ \mathrm{Tw}_{\psi^*}(\lambda) = \lambda \circ \alpha$ *for every* $\lambda \in \Lambda(\mathcal{K})$, *where* $\mathrm{Tw}_{\psi_{\mathfrak{p}^*}} : \Lambda(\mathcal{K}) \to \Lambda(\mathcal{K})$ *is the ring automorphism of §2.1. This map restricts to an isomorphism (of groups, not* $\Lambda(\mathcal{K})$*-modules)*

$$\mathrm{Hom}(\mathrm{Gal}(\mathcal{M}/\mathcal{K}), \mathbf{Q}_p/\mathbf{Z}_p) \cong \mathrm{Sel}(\mathcal{K}, W_{\mathfrak{p}^*})$$

and similarly for the relaxed and restricted Selmer groups, replacing $\mathcal{M}$ *by* $\mathcal{M}_{\mathrm{rel}}$ *and* $\mathcal{M}_{\mathrm{str}}$, *respectively. Similarly, there is a group isomorphism*

$$\beta : \mathcal{H}^1(\mathcal{K}, \mathbf{Z}_p(1)) \cong \mathcal{H}^1(\mathcal{K}, T_\mathfrak{p})$$

satisfying $\beta \circ \mathrm{Tw}^{-1}_{\psi_{\mathfrak{p}^*}}(\lambda) = \lambda \circ \beta$ *for every* $\lambda \in \Lambda(\mathcal{K})$. *This isomorphism identifies* $\mathcal{E}$ *with* $\mathcal{S}_{\mathrm{rel}}(\mathcal{K}, T_\mathfrak{p})$ *and* $\mathcal{U}$ *with* $\mathcal{C}(\mathcal{K})$.

Proof. The existence of

$$\alpha : H^1(\mathcal{K}, \mathbf{Q}_p/\mathbf{Z}_p) \cong H^1(\mathcal{K}, W_{\mathfrak{p}^*})$$

follows from the twisting theorems of [25] §6.2, once one fixes an isomorphism $W_{\mathfrak{p}^*} \cong (\mathbf{Q}_p/\mathbf{Z}_p)(\psi_{\mathfrak{p}^*})$. From the definitions, together with Proposition 1.1.7, we have the following characterizations of our Selmer groups in $H^1(\mathcal{K}, W_{\mathfrak{p}^*})$:

- $\mathrm{Sel}_{\mathrm{rel}}(\mathcal{K}, W_{\mathfrak{p}^*})$ consists of the classes locally trivial away from p,
- $\mathrm{Sel}(\mathcal{K}, W_{\mathfrak{p}^*})$ consists of the classes locally trivial away from $\mathfrak{p}^*$,
- $\mathrm{Sel}_{\mathrm{str}}(\mathcal{K}, W_{\mathfrak{p}^*})$ consists of the classes everywhere locally trivial.

The isomorphism α identifies each of these Selmer groups with the subgroup of classes in $H^1(\mathcal{K}, \mathbf{Q}_p/\mathbf{Z}_p)$ satisfying the same local conditions, and so it suffices to check that for every place v of $\mathcal{K}$, the condition "locally trivial at v" agrees with the condition "unramified at v". For v not dividing p this is [25] Lemma B.3.3, and the case $v|p$ is identical: fix a place v of $\mathcal{K}$ and note that regardless of the rational prime below v, $\mathcal{K}_v$ always contains the unique unramified $\mathbf{Z}_p$-extension of K_v. In particular, if $\mathcal{K}^{\mathrm{unr}}$ is the maximal unramified extension of $\mathcal{K}$, then $\mathrm{Gal}(\mathcal{K}^{\mathrm{unr}}/\mathcal{K})$ has trivial pro-p-part, and so $H^1(\mathcal{K}^{\mathrm{unr}}/\mathcal{K}, \mathbf{Q}_p/\mathbf{Z}_p) = 0$.

For the compact cohomology group $\mathcal{H}^1(\mathcal{K}, T_\mathfrak{p})$ the existence of β is proved in the same fashion, using the fact that $\psi_\mathfrak{p}\psi_{\mathfrak{p}^*}$ is the cyclotomic character. That β identifies the relaxed Selmer group with the unit group is a consequence of the discussion above, since local duality shows that the unramified conditions agree with the relaxed conditions everywhere locally. The identification of $\mathcal{U}_\mathfrak{a}$ with $\mathcal{C}_\mathfrak{a}(\mathcal{K})$ is immediate from the construction of the twisted Euler system $c_\mathfrak{a}$ from the elliptic units $\vartheta_\mathfrak{a}$ in Proposition 2.3.1. □

Decompose

$$\mathrm{Gal}(\mathcal{K}/K) \cong \Delta \times \mathrm{Gal}(K_\infty/K)$$

where $\Delta \cong \mathrm{Gal}(K(E[p])/K)$, and let $\psi_\mathfrak{q} = \chi_\mathfrak{q}\eta_\mathfrak{q}$ be the associated decomposition of $\psi_\mathfrak{q}$, for $\mathfrak{q} = \mathfrak{p}$ of $\mathfrak{p}^*$.

Corollary 2.4.6. *We have the equality of characteristic ideals in* $\Lambda(K_\infty)$

$$\mathrm{Tw}_{\eta_\mathfrak{p}^*}^{-1}\big(\mathrm{char}(\mathrm{Gal}(\mathcal{M}/\mathcal{K})^{\chi_{\mathfrak{p}^*}})\big) = \mathrm{char}(X^*(K_\infty))$$

and similarly for the relaxed and restricted Selmer groups. Also,

$$\mathrm{Tw}_{\eta_\mathfrak{p}^*}^{-1}\big(\mathrm{char}(\mathcal{E}/\mathcal{U})^{\chi_{\mathfrak{p}^*}}\big) = \mathrm{char}(Z(K_\infty)).$$

Proof. This follows easily by taking Δ-invariants of the $\Lambda(\mathcal{K}/K)$-modules of the Lemma above (cf. e.g. [25] Lemma 6.1.2). One must remember our convention, Remark 1.1.8, about the $\Lambda(\mathcal{K})$-action on $X^*(\mathcal{K})$. □

Theorem 2.4.7. *(Rubin) The* $\Lambda(K_\infty)$*-module* $X^*(K_\infty)$ *is torsion,* $\mathcal{S}_{\mathrm{rel}}(K_\infty, T_\mathfrak{p})$ *has rank one, and*

$$\begin{aligned}\mathrm{char}(X^*(K_\infty)) &= \mathrm{char}\big(\mathcal{H}^1(K_{\infty,\mathfrak{p}^*}, T_\mathfrak{p})/\mathrm{loc}_{\mathfrak{p}^*}\mathcal{C}(K_\infty)\big)\\ \mathrm{char}(X^*_{\mathrm{str}}(K_\infty)) &= \mathrm{char}(Z(K_\infty)).\end{aligned}$$

Proof. In view of Lemma 2.4.5 and its corollary, this is a twisted form of the main results of [21]. □

Remark 2.4.8. The fact that $X^*(K_\infty)$ is torsion is originally due to Coates [3].

The following proposition follows from a deep result of Greenberg. Strictly speaking, it is not needed to prove the main result of this section, Theorem 2.4.17 below, but it is helpful for understanding the case $W = 1$. See Remark 2.4.18.

Proposition 2.4.9. *The* $\Lambda(K_\infty)$*-modules* $X^*_{\mathrm{rel}}(K_\infty)$ *and* $X^*(K_\infty)$ *have no nonzero pseudo-null submodules.*

Proof. It is a theorem of Greenberg [5] that $\mathrm{Gal}(\mathcal{M}_{\mathrm{rel}}/\mathcal{K})$ has no non-zero pseudo-null submodules, and so Lemma 2.4.5 implies that $X^*_{\mathrm{rel}}(K_\infty)$ also has none. By [17] §II.2 Théorème 23, $X^*(K_\infty)$ also has no nontrivial pseudo-null submodules. □

Lemma 2.4.10. *For* $\mathfrak{q} = \mathfrak{p}$ *or* $\mathfrak{p}^*$*, the kernel of the restriction map*

$$H^1(D_{\infty,\mathfrak{q}}, W_{\mathfrak{p}^*}) \rightarrow H^1(K_{\infty,\mathfrak{q}}, W_{\mathfrak{p}^*})$$

is finite.

Proof. The kernel of the restriction map is isomorphic to

$$H^0(K_{\infty,\mathfrak{q}}, W_{\mathfrak{p}^*})/IH^0(K_{\infty,\mathfrak{q}}, W_{\mathfrak{p}^*})$$

by the inflation-restriction sequence and [25] Lemma B.2.8. The finiteness follows from Lemma 2.3.3 and local duality. □

Lemma 2.4.11. *The semi-local restriction map*

$$\bigoplus_{w|\mathfrak{f}} H^1(D_{\infty,w}, W_{\mathfrak{p}^*}) \rightarrow \bigoplus_{w|\mathfrak{f}} H^1(K_{\infty,w}, W_{\mathfrak{p}^*}).$$

is injective.

Proof. This is [17] II.7, Lemme 13 (or [4], proof of Lemma IV.3.5), together with the isomorphism

$$H^1(L, W_{\mathfrak{p}^*}) \cong H^1(L, E)[\mathfrak{p}^{*\infty}]$$

for any algebraic extension L/K_w (it suffices to prove this isomorphism for finite extensions, where it is a consequence of the Kummer sequence and the fact that $E(L)$ has a finite index pro-ℓ subgroup, where $\ell \neq p$ is the residue characteristic of w). □

We will need the following slight generalization of the control theorems of Mazur and Perrin-Riou.

Proposition 2.4.12. *The dual to the restriction map*

$$\mathrm{Sel}_{\mathrm{rel}}(D_\infty, W_{\mathfrak{p}^*}) \rightarrow \mathrm{Sel}_{\mathrm{rel}}(K_\infty, W_{\mathfrak{p}^*})[I] \tag{2.7}$$

is an isomorphism of $\Lambda(D_\infty)$*-modules*

$$X^*_{\mathrm{rel}}(K_\infty)/IX^*_{\mathrm{rel}}(K_\infty) \rightarrow X^*_{\mathrm{rel}}(D_\infty).$$

The analogous maps for X^* *and* X^*_{str} *are surjective with finite cokernel.*

Proof. Let S be the set of places of K consisting of the archimedean place and the primes dividing $p\mathfrak{f}$, and denote by K_S/K the maximal extension of K unramified outside S. By Lemma 1.1.2 $H^0(K_S/K_\infty, W_{\mathfrak{p}^*}) = 0$, and so the inflation-restriction sequence shows that the restriction map

$$H^1(K_S/D_\infty, W_{\mathfrak{p}^*}) \rightarrow H^1(K_S/K_\infty, W_{\mathfrak{p}^*})[I]$$

is an isomorphism. As in the proof of Lemma 1.1.5, for w a prime of D_∞ not lying above a prime of S the local condition $H^1_f(D_{\infty,w}, W_{\mathfrak{p}^*})$ is equal to the unramified condition, and similarly for K_∞. From the definition of the relaxed Selmer group, we have the commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_{\mathrm{rel}}(D_\infty, W_{\mathfrak{p}^*}) \arrow[r] \arrow[d] & H^1(K_S/D_\infty, W_{\mathfrak{p}^*}) \arrow[r] \arrow[d] & \bigoplus H^1(D_{\infty,w}, W_{\mathfrak{p}^*}) \arrow[d] \\
0 \arrow[r] & \mathrm{Sel}_{\mathrm{rel}}(K_\infty, W_{\mathfrak{p}^*})[I] \arrow[r] & H^1(K_S/K_\infty, W_{\mathfrak{p}^*})[I] \arrow[r] & \bigoplus H^1(K_{\infty,w}, W_{\mathfrak{p}^*})
\end{tikzcd}$$

where the direct sums are over places $w|\mathfrak{f}$. In particular, since the middle vertical arrow is an isomorphism, the restriction map (2.7) is injective, and to bound the cokernel of this map it suffices to bound the kernel of the right vertical arrow in the diagram above. This kernel is trivial by Lemma 2.4.11. This completes the proof for the relaxed Selmer groups.

In order to prove the result for the true Selmer groups, we replace the top and bottom rows of the commutative diagram above with the exact sequence (1.6) applied with $F = D_\infty$ and $F = K_\infty$, respectively. Again by the snake lemma, it then suffices to bound the kernel of restriction

$$H^1(D_{\infty,\mathfrak{p}}, W_{\mathfrak{p}^*}) \rightarrow H^1(K_{\infty,\mathfrak{p}}, W_{\mathfrak{p}^*}),$$

and this is the content of Lemma 2.4.10. Similarly, one deduces the result for the strict Selmer group from the result for the true Selmer group by using the exact sequence (1.4), together with another application of Lemma 2.4.10. ☐

Definition 2.4.13. We define the *descent defect* $\mathfrak{D} \subset \Lambda(D_\infty)$ by

$$\mathfrak{D} = \mathrm{char}_{\Lambda(D_\infty)}(X^*_{\mathrm{str}}(K_\infty)[I]).$$

Corollary 2.4.14. *The descent defect $\mathfrak{D}$ is nonzero, and we have the equality of ideals in $\Lambda(D_\infty)$*

$$\mathrm{char}_{\Lambda(D_\infty)}(X^*_{\mathrm{str}}(D_\infty)) = \mathrm{char}_{\Lambda(K_\infty)}(X^*_{\mathrm{str}}(K_\infty)) \cdot \mathfrak{D}$$

If $W = 1$ then

$$\mathrm{char}_{\Lambda(D_\infty)}(X^*(D_\infty)) = \mathrm{char}_{\Lambda(K_\infty)}(X^*(K_\infty)).$$

Proof. By Proposition 2.4.4 $X^*_{\mathrm{str}}(D_\infty)$ is a torsion $\Lambda(D_\infty)$-module, and so by Proposition 2.4.12, the same is true of $X^*_{\mathrm{str}}(K_\infty)/IX^*_{\mathrm{str}}(K_\infty)$. The claim now follows from [21] Lemma 6.2 (i).

When $W = 1$, $X^*(D_\infty)$ is a torsion module and the proof is identical, except that now [21] Lemma 6.2 (i) and Proposition 2.4.9 above show that $X^*(K_\infty)[I] = 0$. ☐

Recall from Propositions 2.4.3 and 2.4.4 that $Z(D_\infty)$ is a torsion $\Lambda(D_\infty)$-module. The following proposition gives the other half of the descent from K_∞ to D_∞.

Proposition 2.4.15. *The natural maps of $\Lambda(D_\infty)$-modules*

$$\begin{array}{rcl} \mathcal{S}_{\mathrm{rel}}(K_\infty, T_\mathfrak{p})/I\mathcal{S}_{\mathrm{rel}}(K_\infty, T_\mathfrak{p}) & \to & \mathcal{S}_{\mathrm{rel}}(D_\infty, T_\mathfrak{p}) \\ Z(K_\infty)/IZ(K_\infty) & \to & Z(D_\infty) \end{array}$$

are injective, and their cokernels have characteristic ideal $\mathfrak{D}$. The same holds with Z replaced by $Z_\mathfrak{a}$ for any ideal $\mathfrak{a}$ prime to $p\mathfrak{f}$.

Proof. Let $L \subset K_\infty$ be finite over K. As always, let S the set of places of K consisting of the archimedean place and the primes dividing $p\mathfrak{f}$. Let K_S/K be the maximal extension of K unramified outside S. From the Poitou-Tate nine-term exact sequence we extract the exact sequence

$$0 \to X^*_{\mathrm{str}}(L) \to H^2(K_S/L, T_\mathfrak{p}) \to \bigoplus_{v \in S} H^0(L_v, W_{\mathfrak{p}^*})^\vee,$$

(for example, by taking $B_v = 0$ in [19] Proposition 4.1). Passing to the limit as L varies and taking I-torsion gives

$$0 \to X^*_{\mathrm{str}}(K_\infty)[I] \to H^2(K_S/K, T_\mathfrak{p} \otimes \Lambda(K_\infty))[I] \to \bigoplus_{v \mid p\mathfrak{f}} H^0(K_{\infty,v}, W_{\mathfrak{p}^*})^\vee[I],$$

where we have used Shapiro's lemma to identify

$$H^2(K_S/K, T_\mathfrak{p} \otimes \Lambda(K_\infty)) \cong \varprojlim H^2(K_S/L, T_\mathfrak{p}).$$

The final term in the exact sequence is the Pontryagin dual of

$$\begin{aligned} &\bigoplus_{v \mid p\mathfrak{f}} H^0(K_{\infty,v}, W_{\mathfrak{p}^*})/(\gamma - 1) \bigoplus_{v \mid p\mathfrak{f}} H^0(K_{\infty,v}, W_{\mathfrak{p}^*}) \\ &\qquad \cong \bigoplus_{v \mid p\mathfrak{f}} H^1(K_{\infty,v}/D_{\infty,v}, H^0(K_{\infty,v}, W_{\mathfrak{p}^*})), \end{aligned}$$

which is the kernel of restriction

$$\bigoplus_{v|p\mathfrak{f}} H^1(D_{\infty,v}, W_{\mathfrak{p}^*}) \;\to\; \bigoplus_{v|p\mathfrak{f}} H^1(K_{\infty,v}, W_{\mathfrak{p}^*}).$$

Lemmas 2.4.10 and 2.4.11 (for $v|p$ and $v|\mathfrak{f}$, respectively) show that this kernel is finite. By Corollary 2.4.14 we conclude that $H^2(K_S/K, T_{\mathfrak{p}} \otimes \Lambda(K_\infty))[I]$ is a torsion $\Lambda(D_\infty)$-module with characteristic ideal equal to $\mathfrak{D}$.

From the $\mathrm{Gal}(K_S/K)$-cohomology of

$$0 \;\to\; T_{\mathfrak{p}} \otimes \Lambda(K_\infty) \;\xrightarrow{\gamma-1}\; T_{\mathfrak{p}} \otimes \Lambda(K_\infty) \;\to\; T_{\mathfrak{p}} \otimes \Lambda(D_\infty) \;\to\; 0$$

we deduce that the map

$$H^1(K_S/K, T_{\mathfrak{p}} \otimes \Lambda(K_\infty)) \otimes_{\Lambda(K_\infty)} \Lambda(D_\infty) \;\to\; H^1(K_S/K, T_{\mathfrak{p}} \otimes \Lambda(D_\infty))$$

is injective with torsion cokernel of characteristic ideal $\mathfrak{D}$. Again using Shapiro's lemma, together with Lemma 1.1.5, we see that the map

$$\mathcal{S}_{\mathrm{rel}}(K_\infty, T_{\mathfrak{p}})/I\mathcal{S}_{\mathrm{rel}}(K_\infty, T_{\mathfrak{p}}) \;\to\; \mathcal{S}_{\mathrm{rel}}(D_\infty, T_{\mathfrak{p}})$$

is injective with cokernel of characteristic ideal $\mathfrak{D}$. The map

$$\mathcal{C}(K_\infty)/I\mathcal{C}(K_\infty) \;\to\; \mathcal{C}(D_\infty)$$

is visibly surjective, since this merely asserts that the twisted elliptic units are universal norms in the cyclotomic direction. The snake lemma now proves the claim. ☐

Proposition 2.4.16. *We have the equality of characteristic ideals*

$$\mathrm{char}(X^*_{\mathrm{str}}(D_\infty)) = \mathrm{char}(Z(D_\infty)).$$

Proof. Let $\mathfrak{a}$ be an ideal of K prime to $p\mathfrak{f}$. Using the fact that I is principal, the snake lemma gives the exactness of

$$\mathcal{S}_{\mathrm{rel}}(K_\infty, T_{\mathfrak{p}})[I] \;\to\; Z_{\mathfrak{a}}(K_\infty)[I] \;\to\; \mathcal{C}_{\mathfrak{a}}(K_\infty)/I\mathcal{C}_{\mathfrak{a}}(K_\infty).$$

The leftmost term is trivial by Lemma 1.1.9, and the term on the right is isomorphic to $\Lambda(D_\infty)$, since $\mathcal{C}_{\mathfrak{a}}(K_\infty)$ is free of rank one over $\Lambda(K_\infty)$. Therefore $Z_{\mathfrak{a}}(K_\infty)[I]$ is a torsion-free $\Lambda(D_\infty)$-module. On the other hand, the quotient $Z_{\mathfrak{a}}(K_\infty)/IZ_{\mathfrak{a}}(K_\infty)$ is a torsion $\Lambda(D_\infty)$-module (by Propositions 2.4.4 and 2.4.15), and so [21] Lemma 6.2 (i) tells us that $Z(K_\infty)[I]$ is a torsion $\Lambda(D_\infty)$-module. We conclude that $Z_{\mathfrak{a}}(K_\infty)[I] = 0$. Now by [21] Lemma 6.2 (ii),

$$\mathrm{char}_{\Lambda(K_\infty)}(Z_{\mathfrak{a}}(K_\infty)) \cdot \Lambda(D_\infty) = \mathrm{char}_{\Lambda(D_\infty)}(Z_{\mathfrak{a}}(K_\infty)/IZ_{\mathfrak{a}}(K_\infty)).$$

Applying Proposition 2.4.15 gives

$$\mathrm{char}_{\Lambda(K_\infty)}(Z_{\mathfrak{a}}(K_\infty)) \cdot \mathfrak{D} = \mathrm{char}_{\Lambda(D_\infty)}(Z_{\mathfrak{a}}(D_\infty)).$$

Now let $\mathfrak{a}$ vary and apply Theorem 2.4.7 and Proposition 2.4.14 to get

$$\begin{aligned}\mathrm{char}_{\Lambda(D_\infty)}(X^*_{\mathrm{str}}(D_\infty)) &= \mathrm{char}_{\Lambda(K_\infty)}(X^*_{\mathrm{str}}(K_\infty)) \cdot \mathfrak{D} \\ &= \mathrm{char}_{\Lambda(K_\infty)}(Z(K_\infty)) \cdot \mathfrak{D}\end{aligned}$$

proving the claim. ☐

Theorem 2.4.17.

(1) *If $W = 1$, then*
  (a) $\mathcal{S}(D_\infty, T_{\mathfrak{p}}) = 0$,
  (b) $X^*(D_\infty)$ *is a torsion* $\Lambda(D_\infty)$*-module,*

(c) *the ideal of* $\Lambda_{\mathrm{R}}(D_\infty)$ *generated by* $\mathrm{char}(X^*(D_\infty))$ *is equal to the ideal generated by the* p*-adic* L*-function* $\mu_{\mathfrak{p}^*}(D_\infty, \psi_{\mathfrak{p}^*})$. *If* p *does not divide* $[K(\mathfrak{f}) : K]$ *the same holds with* R *replaced by* R_0.

(2) *If* $W = -1$, *then*

(a) $\mathcal{S}(D_\infty, T_{\mathfrak{p}})$ *is a torsion-free* $\Lambda(D_\infty)$*-module of rank one,*

(b) $X^*(D_\infty)$ *has rank one,*

(c) $\mathrm{char}\big(X^*_{\mathrm{str}}(D_\infty)\big) = \mathrm{char}\big(\mathcal{S}(D_\infty, T_{\mathfrak{p}})/\mathcal{C}(D_\infty)\big)$.

Proof. The first two claims of (1) and (2) all follow from Lemma 1.1.9, Theorem 1.2.2, and Proposition 2.4.4. When $W = 1$ the determination of the characteristic ideal follows from Propositions 2.3.4 and 2.4.16, using the exact sequence

$$0 \to Z(D_\infty) \to \mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}})/\mathrm{loc}_{\mathfrak{p}^*}\mathcal{C}(D_\infty) \to X^*(D_\infty) \to X^*_{\mathrm{str}}(D_\infty) \to 0.$$

When $W = -1$ the claim follows from the final statement of Proposition 2.4.4 and from Proposition 2.4.16. □

Remark 2.4.18. The case $W = 1$ can be deduced more directly from the first equality of Theorem 2.4.7 and the second part of Corollary 2.4.14 (which requires Proposition 2.4.9), by using Lemma 2.3.3, the local analogue of Proposition 2.4.15. This avoids the application of the Euler system machinery directly over D_∞ (Proposition 2.4.4) needed to prove Proposition 2.4.15, or, more precisely, to prove the nontriviality of $\mathfrak{D}$. When $W = -1$, the ideals appearing in the first equality of Theorem 2.4.7 have trivial image in $\Lambda(D_\infty)$, so one seems to have no recourse but to prove some form of Proposition 2.4.15.

3. The p-adic height pairing

Throughout this section we assume $W = -1$ and we set

$$\Delta = \mathrm{Gal}(D_\infty/K) \qquad \Gamma = \mathrm{Gal}(C_\infty/K).$$

We will frequently identify $\Gamma \cong \mathrm{Gal}(K_\infty/D_\infty)$. For any nonnegative integer n, let $\Delta_n = \Delta/\Delta^{p^n}$ and similarly for Γ. Let $\mathcal{I}$ be the kernel of the natural projection $\Lambda(C_\infty) \to \Lambda(K)$ and set $\mathcal{J} = \mathcal{I}/\mathcal{I}^2$. Many authors use some choice of "logarithm" $\lambda : \Gamma \to \mathbf{Z}_p$ to define the p-adic height pairing. Following the fashion of the day, we instead take

$$\lambda : \Gamma \to \mathcal{J}$$

to be the isomorphism $\gamma \mapsto \gamma - 1$, and so obtain a $\mathcal{J}$-valued height pairing.

3.1. **The linear term.** Choose a generator $\gamma \in \Gamma$ and fix some integral ideal $\mathfrak{a} \subset \mathcal{O}_K$ prime to $\mathfrak{f}p$. For every $K \subset L \subset K_\infty$ we set

$$c_{\mathfrak{a}}(L) = \varprojlim c_{\mathfrak{a}}(L'),$$

where $c_{\mathfrak{a}}$ is the Euler system of Proposition 2.3.1 and the limit is taken over all subfields $L' \subset L$ finite over K. We may identify

$$\Lambda(K_\infty)_{\mathrm{R}_0} \cong \Lambda(D_\infty)_{\mathrm{R}_0}[[\Gamma]]$$

and expand $\mu_{\mathfrak{p}^*}(K_\infty, \psi_{\mathfrak{p}^*}, \mathfrak{a})$ as a power series in $\gamma - 1$,

$$\mu_{\mathfrak{p}^*}(K_\infty, \psi_{\mathfrak{p}^*}, \mathfrak{a}) = \mathcal{L}_{\mathfrak{a},0} + \mathcal{L}_{\mathfrak{a},1}(\gamma - 1) + \mathcal{L}_{\mathfrak{a},2}(\gamma - 1)^2 + \cdots .$$

Similarly we may expand

$$\mu_{\mathfrak{p}^*}(K_\infty, \psi_{\mathfrak{p}^*}) = \mathcal{L}_0 + \mathcal{L}_1(\gamma - 1) + \mathcal{L}_2(\gamma - 1)^2 + \cdots .$$

By Corollary 2.1.5 and the assumption that $W = -1$, we have

$$\mathcal{L}_0 = \mu_{\mathfrak{p}^*}(D_\infty, \psi_{\mathfrak{p}^*}) = 0.$$

It follows that also $\mathcal{L}_{\mathfrak{a},0} = 0$. By Proposition 2.3.4 the image of $c_{\mathfrak{a}}(D_\infty)$ in $\mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}})$ is trivial, and so by Proposition 1.1.7, $c_{\mathfrak{a}}(D_\infty) \in \mathcal{S}(D_\infty, T_{\mathfrak{p}})$.

Lemma 3.1.1. *Set $F_n = D_n C_\infty$. For every n there is a unique element*

$$\beta_n \in \mathcal{H}^1(F_{n,\mathfrak{p}^*}, T_{\mathfrak{p}})_{\mathrm{R}}$$

such that

$$(\gamma - 1)\beta_n = \mathrm{loc}_{\mathfrak{p}^*}\big(c_{\mathfrak{a}}(F_n)\big).$$

Let α_n be the image of β_n in $\mathcal{H}^1(D_{n,\mathfrak{p}^*}, T_{\mathfrak{p}})_{\mathrm{R}}$. The elements α_n are norm-compatible and they define an element $\alpha_\infty \in \mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}})_{\mathrm{R}}$. The Coleman map of Proposition 2.3.4 identifies

$$\mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}})_{\mathrm{R}} \cong \Lambda(D_\infty)_{\mathrm{R}}$$

and takes α_∞ to $\mathcal{L}_{\mathfrak{a},1}$.

Proof. This is immediate from Proposition 2.3.4, the fact that $\mathcal{L}_{\mathfrak{a},0} = 0$, and the definition of $\mathcal{L}_{\mathfrak{a},1}$. □

Tate local duality defines a pairing

$$\langle\ ,\ \rangle_n : \mathcal{H}^1(D_{n,\mathfrak{p}^*}, T_{\mathfrak{p}}) \times \mathcal{H}^1(D_{n,\mathfrak{p}^*}, T_{\mathfrak{p}^*}) \ \to\ \mathbf{Z}_p$$

whose kernel on either side is the $\mathbf{Z}_p$-torsion submodule, and the induced pairing on the quotients by the torsion submodules is perfect.

The height pairing of the following theorem has been studied by many authors, including Mazur-Tate, Nekovář, Perrin-Riou, and Schneider. The fourth property of the pairing, the height formula, is due to Rubin, and plays a crucial role in what follows.

Theorem 3.1.2. *For every nonnegative integer n there is a canonical (up to sign) p-adic height pairing*

$$h_n : \mathrm{Sel}(D_n, T_{\mathfrak{p}}) \times \mathrm{Sel}(D_n, T_{\mathfrak{p}^*}) \ \to\ \mathbf{Q}_p \otimes \mathcal{J}$$

satisfying the following properties

(1) *there is a positive integer k, independent of n, such that h_n takes values in $p^{-k}\mathbf{Z}_p \otimes \mathcal{J}$*

(2) *if $a \in \mathrm{Sel}(D_n, T_{\mathfrak{p}})$, $b \in \mathrm{Sel}(D_n, T_{\mathfrak{p}^*})$, and $\sigma \in \Delta_n$, then*

$$h_n(a^\sigma, b^\sigma) = h_n(a, b)$$

(3) *if $a_n \in \mathrm{Sel}(D_n, T_{\mathfrak{p}})$, $b_{n+1} \in \mathrm{Sel}(D_{n+1}, T_{\mathfrak{p}^*})$, and* res *and* cor *are the restriction and corestriction maps relative to D_{n+1}/D_n, then*

$$h_{n+1}(\mathrm{res}(a_n), b_{n+1}) = h_n(a_n, \mathrm{cor}(b_{n+1}))$$

(4) *(height formula) for every $b \in \mathrm{Sel}(D_n, T_{\mathfrak{p}^*})$, we have (up to sign)*

$$h_n\big(c_{\mathfrak{a}}(D_n), b\big) = \langle \alpha_n, \mathrm{loc}_{\mathfrak{p}^*}(b)\rangle_n \otimes (\gamma - 1).$$

Proof. This will be proved in the next section. □

Define the $\Lambda(D_\infty)$-adic Tate pairing

$$\langle\ ,\ \rangle_\infty : \mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_\mathfrak{p})_{\mathrm{R}} \otimes_{\Lambda(D_\infty)_{\mathrm{R}}} \mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}^*})^\iota_{\mathrm{R}} \cong \Lambda(D_\infty)_{\mathrm{R}}$$

by

$$\langle a_\infty, b_\infty\rangle_\infty = \varprojlim \sum_{\sigma\in\Delta_n} \langle a_n^\sigma, b_n\rangle_n \cdot \sigma^{-1}$$

and define the $\Lambda(D_\infty)$-adic height pairing

$$h_\infty : \mathcal{S}(D_\infty, T_\mathfrak{p})_{\mathrm{R}} \otimes_{\Lambda(D_\infty)_{\mathrm{R}}} \mathcal{S}(D_\infty, T_{\mathfrak{p}^*})^\iota_{\mathrm{R}} \ \rightarrow\ \Lambda(D_\infty)_{\mathrm{R}} \otimes_{\mathbf{Z}_p} \mathcal{J}$$

similarly. The element $\alpha_\infty \in \mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_\mathfrak{p})$ satisfies

$$h_\infty(c_\mathfrak{a}(D_\infty), b_\infty) = \langle \alpha_\infty, \mathrm{loc}_{\mathfrak{p}^*}(b_\infty)\rangle_\infty \otimes (\gamma - 1) \tag{3.1}$$

for every $b_\infty \in \mathcal{S}(D_\infty, T_{\mathfrak{p}^*})$.

Definition 3.1.3. Define the *anticyclotomic regulator*, $\mathcal{R}$, to be the characteristic ideal of the cokernel of h_∞.

Define $\mathcal{R}(\mathcal{C}_\mathfrak{a})$ to be the characteristic ideal of the cokernel of

$$h_\infty|_{\mathcal{C}_\mathfrak{a}} : \mathcal{C}_\mathfrak{a} \otimes_{\Lambda(D_\infty)_{\mathrm{R}}} \mathcal{S}(D_\infty, T_{\mathfrak{p}^*})^\iota \ \rightarrow\ \Lambda(D_\infty)_{\mathrm{R}} \otimes_{\mathbf{Z}_p} \mathcal{J},$$

and let η be the ideal

$$\eta = \mathrm{char}\big(\mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}^*})/\mathrm{loc}_{\mathfrak{p}^*}(\mathcal{S}(D_\infty, T_{\mathfrak{p}^*}))\big).$$

From Proposition 2.4.4 and the results of Section 1.2 we have that $\mathcal{S}_{\mathrm{str}}(D_\infty, T_{\mathfrak{p}^*})$ is trivial. The exactness of (1.5) then shows that $\eta \neq 0$.

Proposition 3.1.4. *There is an equality of ideals in* $\Lambda(D_\infty)_{\mathrm{R}}$

$$\begin{aligned} \mathcal{R}\cdot \mathrm{char}\big(\mathcal{S}(D_\infty, T_\mathfrak{p})/\mathcal{C}_\mathfrak{a}\big) &= \mathcal{R}(\mathcal{C}_\mathfrak{a}) \\ &= (\mathcal{L}_{\mathfrak{a},1})\cdot \eta^\iota. \end{aligned}$$

Proof. The first equality is clear. The height formula (3.1) implies that the image of $h_\infty|_{\mathcal{C}_\mathfrak{a}}$ is equal to

$$\langle \alpha_\infty, \mathrm{loc}_{\mathfrak{p}^*}(\mathcal{S}(D_\infty, T_{\mathfrak{p}^*})_{\mathrm{R}})^\iota\rangle_\infty \otimes \mathcal{J} \subset \Lambda(D_\infty)_{\mathrm{R}} \otimes_{\mathbf{Z}_p} \mathcal{J}$$

The second equality now follows from Lemma 3.1.1 and the fact that the $\Lambda(D_\infty)$-adic Tate pairing is an isomorphism. □

Theorem 3.1.5. *Let $\mathcal{X}$ denote the ideal of $\Lambda(D_\infty)_{\mathrm{R}}$ generated by the characteristic ideal of the $\Lambda(D_\infty)$-torsion submodule of $X^*(D_\infty)$. Then we have the equality of ideals*

$$\mathcal{R}\cdot\mathcal{X} = (\mathcal{L}_1).$$

Proof. If we replace $\mathfrak{p}$ by $\mathfrak{p}^*$ and take $F = D_\infty$ in the second pair of exact sequences of Proposition 1.1.7, we obtain the exact sequence

$$0 \ \rightarrow\ \mathcal{H}^1(D_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}^*})/\mathrm{loc}_{\mathfrak{p}^*}(\mathcal{S}(D_\infty, T_{\mathfrak{p}^*})) \ \rightarrow\ X_{\mathrm{rel}}(D_\infty) \ \rightarrow\ X(D_\infty) \ \rightarrow\ 0.$$

Taking $\Lambda(D_\infty)$-torsion and applying Lemma 1.2.1 and Theorem 1.2.2 we obtain

$$\mathrm{char}\big(X^*_{\mathrm{str}}(D_\infty)\big) = \eta^\iota\cdot\mathcal{X}.$$

Letting $\mathfrak{a}$ vary in Proposition 3.1.4, the claim follows from Theorem 2.4.17 (2), part (c). □

3.2. **The height formula.** In this section we sketch Perrin-Riou's construction of the p-adic height pairing

$$h_n : \mathrm{Sel}(D_n, T_{\mathfrak{p}}) \times \mathrm{Sel}(D_n, T_{\mathfrak{p}^*}) \rightarrow \mathbf{Q}_p \otimes \mathcal{J}$$

of Theorem 3.1.2, as well Rubin's proof of the height formula. Our exposition closely follows that of [23], to which we refer the reader for details.

For every $0 \leq k \leq \infty$, let $L_k = D_n C_k$.

Lemma 3.2.1. *Fix a place v of D_n and some extension of it to L_∞. The submodule of $H^1_f(D_{n,v}, T_{\mathfrak{p}})$ defined by*

$$H^1_f(D_{n,v}, T_{\mathfrak{p}})^{\mathrm{univ}} = \bigcap_k \mathrm{cor}\ H^1_f(L_{k,v}, T_{\mathfrak{p}})$$

has finite index, and the index is bounded as v and n vary.

Proof. First assume that v divides $\mathfrak{p}^*$, so that $H^1_f(D_{n,v}, T_{\mathfrak{p}})$ is the torsion submodule of $H^1(D_{n,v}, T_{\mathfrak{p}})$, which is in turn isomorphic to $H^0(D_{n,v}, W_{\mathfrak{p}})$. It clearly suffices to show that this is bounded as n varies. But $K_v(W_{\mathfrak{p}})$ is unramfied, and $D_{\infty,v}$ is a ramified $\mathbf{Z}_p$-extension of K_v, so this is clear.

From now on suppose that v does not divide $\mathfrak{p}^*$, so that

$$H^1_f(L_{k,v}, T_{\mathfrak{p}}) = H^1(L_{k,v}, T_{\mathfrak{p}}).$$

By local duality, it suffices to bound the kernel of restriction

$$H^1(D_{n,v}, W_{\mathfrak{p}^*}) \rightarrow H^1(L_{\infty,v}, W_{\mathfrak{p}^*}),$$

which is $H^1(L_{\infty,v}/D_{n,v}, M)$, where $M = E(L_{\infty,v})[\mathfrak{p}^{*\infty}]$.

If v does not divide $\mathfrak{p}$ then $L_{\infty,v}$ is the unique unramified $\mathbf{Z}_p$-extension of K_v (in particular it does not vary with n). If E does not have any $\mathfrak{p}^*$-torsion defined over K_v, then $K_v(E[\mathfrak{p}^*])/K_v$ is a nontrivial extension of degree dividing $p-1$, so E has no $\mathfrak{p}^*$-torsion defined over any p-extension of K_v, and so $M = 0$. Assume $E[\mathfrak{p}^*]$ is defined over K_v, and that E has good reduction at v. Then $K_v(E[\mathfrak{p}^{*\infty}]) = L_{\infty,v}$ and so $M = W_{\mathfrak{p}^*}$ is p-divisible. If γ is a generator of $\mathrm{Gal}(L_{\infty,v}/D_{n,v})$ then

$$H^1(L_{\infty,v}/D_{n,v}, M) \cong M/(\gamma - 1)M.$$

Since γ acts as a scalar $\neq 1$ on M, this group is trivial. If E has bad reduction at v then M is finite by the criterion of Néron-Ogg-Shafarevich, and the order of M does not vary with n (since $L_{\infty,v}$ does not vary).

Now assume that v divides $\mathfrak{p}$. The extension of K_v generated by $E[\mathfrak{p}^{*\infty}]$ is unramified, and since $K_v^{\mathrm{unr}} \cap L_{\infty,v}$ is a finite extension of K_v, M is finite. If γ generates $\mathrm{Gal}(L_{\infty,v}/D_{n,v})$ then using the exactness of

$$0 \rightarrow M^{\gamma=1} \rightarrow M \xrightarrow{\gamma-1} M \rightarrow M/(\gamma-1)M \rightarrow 0$$

we see that the order of $H^1(L_{\infty,v}/D_{n,v}, M)$ is equal to the order of

$$M^{\gamma=1} = E(D_{n,v})[\mathfrak{p}^{*\infty}].$$

Since $D_{\infty,v}$ is a ramified $\mathbf{Z}_p$-extension of K_v, this order is bounded as n varies. $\square$

Fix $a \in \mathrm{Sel}(D_n, T_{\mathfrak{p}})$ and $b \in \mathrm{Sel}(D_n, T_{\mathfrak{p}^*})$. In view of the above lemma, it suffices to define the height pairing of a and b under the assumption that both are everywhere locally contained in $H^1_f(D_{n,v}, T_{\mathfrak{p}})^{\mathrm{univ}}$. Viewing b as an element of the larger group $H^1(D_n, T_{\mathfrak{p}^*})$, b defines an extension of Galois modules

$$0 \to T_{\mathfrak{p}^*} \to M_b^* \to \mathbf{Z}_p \to 0,$$

and taking $\mathbf{Z}_p(1)$-duals we obtain an exact sequence

$$0 \to \mathbf{Z}_p(1) \to M_b \to T_{\mathfrak{p}} \to 0. \tag{3.2}$$

If L/D_n is any finite extension, we may consider the global and local Galois cohomology

$$\begin{tikzcd} H^1(L,\mathbf{Z}_p(1)) \arrow[r] \arrow[d] & H^1(L,M_b) \arrow[r, "\pi_L"] \arrow[d] & H^1(L,T_{\mathfrak{p}}) \arrow[r, "\delta_L"] \arrow[d] & H^2(L,\mathbf{Z}_p(1)) \arrow[d] \\ H^1(L_w,\mathbf{Z}_p(1)) \arrow[r] & H^1(L_w,M_b) \arrow[r, "\pi_{L_w}"] & H^1(L_w,T_{\mathfrak{p}}) \arrow[r, "\delta_{L_w}"] & H^2(L_w,\mathbf{Z}_p(1)). \end{tikzcd}$$

Lemma 3.2.2. *Let L be a finite Galois extension of D_n and suppose $a' \in H^1(L, T_{\mathfrak{p}})$ satisfies $\mathrm{cor}(a') = a$. Then a' is in the image of π_L. For every place w of L, $H^1_f(L_w, T_{\mathfrak{p}})$ is contained in the image of π_{L_w}*

Proof. Let res be the restriction map from D_n to L. The connecting homomorphism δ_L is given (up to sign) by $\cup\mathrm{res}(b)$. If w is any place of L and v is the place of D_n below it,

$$\mathrm{loc}_w(\delta(a')) = \mathrm{loc}_w(a' \cup \mathrm{res}(b)) = \mathrm{loc}_v(a \cup b) = 0,$$

since a and b are everywhere locally orthogonal under the Tate pairing. Thus $\delta_L(a')$ is everywhere locally trivial, and by a fundamental fact of class field theory it is globally trivial. The proof of the second claim is similar. $\square$

Class field theory gives a homomorphism

$$\rho : \mathbf{A}_{D_n}^\times \to \mathrm{Gal}(D_n C_\infty / D_n) \cong \Gamma \xrightarrow{\lambda} \mathcal{J}$$

and we factor $\rho = \sum_v \rho_v$, the sum over all places of D_n. By local Kummer theory we may view ρ_v as a map

$$\rho_v : H^1(D_{n,v}, \mathbf{Z}_p(1)) \to \mathcal{J},$$

which can also be described as follows: the homomorphism

$$\mathrm{Gal}(D_n C_\infty / D_n) \cong \Gamma \xrightarrow{\lambda} \mathcal{J}$$

defines a class $\lambda \in H^1(D_n, \mathcal{J})$ (we always regard $\mathcal{J}$ as having trivial Galois action), and cup product with $\mathrm{loc}_v(\lambda)$ defines a map

$$H^1(D_{n,v}, \mathbf{Z}_p(1)) \to H^2(D_{n,v}, \mathcal{J}(1)) \cong \mathcal{J}$$

which agrees (up to sign) with ρ_v.

Taking $L = D_n$ and $a' = a$ in Lemma 3.2.2, we may choose some $y^{\mathrm{glob}} \in H^1(D_n, M_b)$ with $\pi_{D_n}(y^{\mathrm{glob}}) = a$. Fix a place v of D_n and an extension of v to L_∞, and for every k choose $y_{k,v} \in H^1_f(L_{k,v}, T_{\mathfrak{p}})$ which corestricts to $\mathrm{loc}_v(a)$. By Lemma 3.2.2 we may choose some $y'_{k,v} \in H^1(L_{k,v}, M_b)$ such that $\pi_{L_{k,v}}(y'_{k,v}) = y_{k,v}$. Let $\mathrm{cor}(y'_{k,v})$ be the image of $y'_{k,v}$ in $H^1(D_{n,v}, M_b)$. Then $\mathrm{loc}_v(y^{\mathrm{glob}}) - \mathrm{cor}(y'_{k,v})$ comes from some $w_{k,v} \in H^1(D_{n,v}, \mathbf{Z}_p(1))$, and we define

$$h_n(a, b) = \lim_{k\to\infty} \sum_v \rho_v(w_{k,v})$$

This limit exists and is independent of all choices made.

We now sketch the proof of the height formula. Suppose that $a = c_{\mathfrak{a}}(D_n)$, and set $a_k = c_{\mathfrak{a}}(L_k)$,

$$a_\infty = \lim_{\leftarrow} a_k \in \lim_{\leftarrow} \mathrm{Sel}_{\mathrm{rel}}(L_k, T_{\mathfrak{p}}).$$

By Lemma 3.2.2 there is a sequence $z_k \in H^1(L_k, M_b)$ with $\pi_{L_k}(z_k) = a_k$. Working semi-locally above $\mathfrak{q} = \mathfrak{p}$ or $\mathfrak{p}^*$, we have defined in the preceeding paragraph a sequence $y'_{k,\mathfrak{q}} \in H^1(L_{k,\mathfrak{q}}, M_b)$ which lifts $y_{k,\mathfrak{q}}$. The image of

$$t_{k,\mathfrak{q}} = \mathrm{loc}_{\mathfrak{q}}(z_k) - y'_{k,\mathfrak{q}} \in H^1(L_{k,\mathfrak{q}}, M_b)$$

in $H^1(D_{n,\mathfrak{q}}, M_b)$ comes from some $s_{k,\mathfrak{q}} \in H^1(D_{n,\mathfrak{q}}, \mathbf{Z}_p(1))$.

Proposition 3.2.3. *With notation as above*

$$h_n(a,b) = \lim_{k\to\infty} [\rho_{\mathfrak{p}}(s_{k,\mathfrak{p}}) + \rho_{\mathfrak{p}^*}(s_{k,\mathfrak{p}^*})].$$

Proof. This is Proposition 5.3 of [23]. □

Define $H_{k,\mathfrak{q}}$ by the exactness of

$$0 \to H_{k,\mathfrak{q}} \to H^1(L_{k,\mathfrak{q}}, T_{\mathfrak{p}}) \xrightarrow{\mathrm{cor}} H^1(D_{n,\mathfrak{q}}, T_{\mathfrak{p}}).$$

In [23] Section 4, one finds the definition of a derivative operator

$$\mathrm{Der}_{k,\mathfrak{q}} : H_{k,\mathfrak{q}} \to H^1(D_{n,\mathfrak{q}}, T_{\mathfrak{p}}/p^k T_{\mathfrak{p}}) \otimes \mathcal{J}.$$

From the definition of $t_{k,\mathfrak{q}}$, it is immediate that $\pi_{L_{k,\mathfrak{q}}}(t_{k,\mathfrak{q}}) \in H_{k,\mathfrak{q}}$. We set

$$t'_{k,\mathfrak{q}} = \mathrm{Der}_{k,\mathfrak{q}}(\pi_{L_{k,\mathfrak{q}}}(t_{k,\mathfrak{q}})) \in H^1(D_{n,\mathfrak{q}}, T_{\mathfrak{p}}/p^k T_{\mathfrak{p}}) \otimes \mathcal{J}.$$

Proposition 4.3 of [23] then reads

$$\lambda \cup s_{k,\mathfrak{q}} = \delta_{D_{n,\mathfrak{q}}}(t'_{k,\mathfrak{q}}) \in H^2(D_{n,\mathfrak{q}}, (\mathbf{Z}/p^k\mathbf{Z})(1)) \otimes \mathcal{J}$$

and so up to sign

$$\begin{aligned} \rho_{\mathfrak{q}}(s_{k,\mathfrak{q}}) &\equiv \mathrm{inv}_{\mathfrak{q}}(\delta_{D_{n,\mathfrak{q}}}(t'_{k,\mathfrak{q}})) \pmod{p^k} \\ &= \mathrm{inv}_{\mathfrak{q}}(t'_{k,\mathfrak{q}} \cup \mathrm{loc}_{\mathfrak{q}}(b)) \end{aligned} \tag{3.3}$$

where $\mathrm{inv}_{\mathfrak{q}}$ is the semi-local invariant

$$H^2(D_{n,\mathfrak{q}}, (\mathbf{Z}/p^k\mathbf{Z})(1)) \otimes \mathcal{J} \to \mathcal{J}/p^k\mathcal{J}.$$

From the definition of $\mathrm{Sel}(D_n, T_{\mathfrak{p}^*})$, we see that $\mathrm{loc}_{\mathfrak{p}}(b)$ is a torsion element. If $p^\ell \mathrm{loc}_{\mathfrak{p}}(b) = 0$ then (3.3) implies that $\rho_{\mathfrak{p}}(s_{k,\mathfrak{p}})$ is divisible by $p^{k-\ell}$. Letting $k \to \infty$, we have $\rho_{\mathfrak{p}}(s_{k,\mathfrak{p}}) \to 0$, leaving

$$h_n(a,b) = \lim_{k\to\infty} \rho_{\mathfrak{p}^*}(s_{k,\mathfrak{p}^*}). \tag{3.4}$$

Lemma 3.2.4. *Suppose $d_k \in H_{k,\mathfrak{p}^*}$ is such that $d_k \cup z = \mathrm{loc}_{\mathfrak{p}^*}(a_k) \cup z$ for every $z \in H^1_f(L_{k,\mathfrak{p}^*}, T_{\mathfrak{p}^*})$. Then for any sequence $x_k \in H^1_f(L_{k,\mathfrak{p}^*}, T_{\mathfrak{p}^*})$ such that the image of x_k in $H^1_f(D_{n,\mathfrak{p}^*}, T_{\mathfrak{p}^*})$ is constant,*

$$\lim_{k\to\infty} \mathrm{inv}_{\mathfrak{p}^*}(\mathrm{Der}_{k,\mathfrak{p}^*}(d_k) \cup x_0) = \lim_{k\to\infty} \sum_{\sigma\in\Gamma_k} \langle \mathrm{loc}_{\mathfrak{p}^*}(a_k), \sigma\cdot x_k\rangle_{L_k,\mathfrak{p}^*} \otimes \lambda(\sigma)$$

where λ is viewed as a character $\Gamma_k \to \mathcal{J}/p^k\mathcal{J}$.

Proof. This is Lemma 5.1 of [23]. □

Recall that Lemma 3.1.1 provides, for some choice of generator $\gamma \in \Gamma$, a $\beta \in \mathcal{H}^1(L_{\infty,\mathfrak{p}^*}, T_{\mathfrak{p}})$ such that

$$(\gamma - 1)\beta = \mathrm{loc}_{\mathfrak{p}^*}(a_\infty).$$

Let α be the image of β in $H^1(D_{n,\mathfrak{p}^*}, T_{\mathfrak{p}})$. Write

$$\beta = \varprojlim \beta_k \in \varprojlim H^1(L_{k,\mathfrak{p}^*}, T_{\mathfrak{p}})$$

so that $\beta_0 = \alpha$. Fix some sequence $x_k \in H^1_f(L_{k,\mathfrak{p}^*}, T_{\mathfrak{p}^*})$ lifting $\mathrm{loc}_{\mathfrak{p}^*}(b)$. Applying Lemma 3.2.4 with $d_k = \pi_{L_{k,\mathfrak{p}^*}}(t_{k,\mathfrak{p}^*})$ and comparing with (3.3) and (3.4) gives

$$\begin{aligned}
h_n(a,b) &= \lim_{k\to\infty} \rho_{\mathfrak{p}^*}(s_{k,\mathfrak{p}^*}) \\
&= \lim_{k\to\infty} \sum_{\sigma\in\Gamma_k} \langle \mathrm{loc}_{\mathfrak{p}^*}(a_k), x_k^\sigma\rangle_{L_k,\mathfrak{p}^*} \otimes \lambda(\sigma) \\
&= \lim_{k\to\infty} \sum_{\sigma\in\Gamma_k} \langle (\gamma-1)\beta_k, \sigma\cdot x_k\rangle_{L_k,\mathfrak{p}^*} \otimes \lambda(\sigma) \\
&= \lim_{k\to\infty} \sum_{i=1}^{p^k-1} \langle (\gamma-1)\beta_k, i\gamma^i\cdot x_k\rangle_{L_k,\mathfrak{p}^*} \otimes (\gamma-1) \\
&= \lim_{k\to\infty} \langle \beta_k, \mathrm{Norm}_{\Gamma_k} x_k\rangle_{L_k,\mathfrak{p}^*} \otimes (\gamma-1) \\
&= \langle \alpha, \mathrm{loc}_{\mathfrak{p}^*}(b)\rangle_{D_n,\mathfrak{p}^*} \otimes (\gamma-1).
\end{aligned}$$

This completes the proof of the height formula.

Appendix A. Proof of Theorem B
by Karl Rubin

In this appendix we prove Theorem B of the introduction. Essentially what we need to prove is that the anticyclotomic regulator $\mathcal{R}$ of Definition 3.1.3 is nonzero. The key tool is Theorem A.1 of Bertrand below, which says that on a CM elliptic curve the $\mathfrak{p}$-adic height of a point of infinite order is nonzero. This is much weaker than saying that the p-adic height is nondegenerate, but it suffices for our purposes.

We assume throughout this appendix that the sign in the functional equation of $L(E/\mathbf{Q}, s)$ is -1.

We need to consider a slightly more general version of p-adic heights than appears in the main text. If F is a finite extension of K in K_∞, then there is a p-adic height pairing

$$h_F : \mathrm{Sel}(F, T_{\mathfrak{p}}) \otimes \mathrm{Sel}(F, T_{\mathfrak{p}^*}) \to \mathrm{Gal}(K_\infty/F) \otimes \mathbf{Q}_p.$$

We are interested in three specializations of this pairing. Namely,

$$\begin{aligned}
h_{F,\mathrm{cycl}} &: \mathrm{Sel}(F, T_{\mathfrak{p}}) \otimes \mathrm{Sel}(F, T_{\mathfrak{p}^*}) \to \mathrm{Gal}(FC_\infty/F) \otimes \mathbf{Q}_p, \\
h_{F,\mathrm{anti}} &: \mathrm{Sel}(F, T_{\mathfrak{p}}) \otimes \mathrm{Sel}(F, T_{\mathfrak{p}^*}) \to \mathrm{Gal}(FD_\infty/F) \otimes \mathbf{Q}_p, \\
h_{F,\mathfrak{p}} &: \mathrm{Sel}(F, T_{\mathfrak{p}}) \otimes \mathrm{Sel}(F, T_{\mathfrak{p}^*}) \to \mathrm{Gal}(FL_\infty/F) \otimes \mathbf{Q}_p
\end{aligned}$$

where L_∞ is the unique $\mathbf{Z}_p$-extension of K which is unramified outside of $\mathfrak{p}$, are defined by restricting the image of h_F to the appropriate group. If $P \in E(F)$, we will write $h_F(P) = h_F(a,b)$ where a is the image of P in $\mathrm{Sel}(F, T_{\mathfrak{p}})$ and b is the image of P in $\mathrm{Sel}(F, T_{\mathfrak{p}^*})$.

The p-adic height pairing h_n of Theorem 3.1.2 is the composition of $h_{D_n,\mathrm{cycl}}$ with the isomorphism $\mathrm{Gal}(D_nC_\infty/D_n) \cong \mathrm{Gal}(C_\infty/K) \cong \mathcal{J}$.

Theorem A.1 (Bertrand [2]). *Suppose F is a number field and $P \in E(F)$ is a point of infinite order. Then the $\mathfrak{p}$-adic height $h_{F,\mathfrak{p}}(P)$ is nonzero.*

Lemma A.2. *Suppose $a \in \mathrm{Sel}(F, T_{\mathfrak{p}})$ and $b \in \mathrm{Sel}(F, T_{\mathfrak{p}^*})$. If two of $h_{F,\mathrm{cycl}}(a,b)$, $h_{F,\mathrm{anti}}(a,b)$, $h_{F,\mathfrak{p}}(a,b)$ are zero, then so is the third.*

Proof. Since $\mathrm{Gal}(K_\infty/F) \cong \mathbf{Z}_p^2$, the projections $\mathrm{Gal}(K_\infty/F) \to \mathrm{Gal}(FC_\infty/F)$, $\mathrm{Gal}(K_\infty/F) \to \mathrm{Gal}(FD_\infty/F)$, and $\mathrm{Gal}(K_\infty/F) \to \mathrm{Gal}(FL_\infty/F)$ are linearly dependent. It follows that each of the three heights is a linear combination of the other two. □

Definition A.3. For every n define a submodule of $\mathrm{Sel}(D_n, T_{\mathfrak{p}})$, the *universal norms*, by

$$\mathrm{Sel}(D_n, T_{\mathfrak{p}})^{\mathrm{univ}} = \bigcap_{m>n} \mathrm{cor}_{D_m/D_n} \mathrm{Sel}(D_m, T_{\mathfrak{p}}).$$

Define $\mathrm{Sel}(D_n, T_{\mathfrak{p}^*})^{\mathrm{univ}}$ similarly.

Lemma A.4. *For every n we have*

$$h_{D_n,\mathrm{anti}}(\mathrm{Sel}(D_n, T_{\mathfrak{p}})^{\mathrm{univ}} \otimes \mathrm{Sel}(D_n, T_{\mathfrak{p}^*})^{\mathrm{univ}}) = 0.$$

Proof. This is a basic property of the p-adic height (see for example Proposition 4.5.2 of [16]). □

Proposition A.5. *The natural maps*

$$X(D_\infty) \otimes \Lambda(D_n) \to X(D_n)$$

have kernel and cokernel which are finite and bounded independently of n.

Proof. This is the standard "Control Theorem", see for example [11]. □

Recall that $\Delta_n = \mathrm{Gal}(D_n/K)$.

Lemma A.6. *For every n, $\mathrm{Sel}(D_n, T_{\mathfrak{p}})^{\mathrm{univ}} \otimes \mathbf{Q}_p$ and $\mathrm{Sel}(D_n, T_{\mathfrak{p}^*})^{\mathrm{univ}} \otimes \mathbf{Q}_p$ are free of rank one over $\mathbf{Q}_p[\Delta_n]$.*

Proof. This is proved in exactly the same way as Theorem 4.2 of [13] (which proves a stronger statement about universal norms in Mordell-Weil groups, assuming that all relevant Tate-Shafarevich groups are finite), using Theorem 2.4.17. For completeness we give a proof here.

The exact sequence $0 \to E[\mathfrak{p}^k] \to W_{\mathfrak{p}} \to W_{\mathfrak{p}} \to 0$ and the fact that $E(D_n) \cap E[\mathfrak{p}] = 0$ show that $\mathrm{Sel}(D_n, E[\mathfrak{p}^k]) = \mathrm{Sel}(D_n, W_{\mathfrak{p}})[\mathfrak{p}^k]$ for every k. This and the Control Theorem (Proposition A.5) give us maps

$$\begin{aligned}\mathrm{Sel}(D_n, T_{\mathfrak{p}}) &= \varprojlim_k \mathrm{Sel}(D_n, E[\mathfrak{p}^k]) = \varprojlim_k \mathrm{Hom}(\mathrm{Sel}(D_n, E[\mathfrak{p}^k])^\wedge, \mathbf{Z}/p^k\mathbf{Z}) \\ &= \varprojlim_k \mathrm{Hom}(X(D_n), \mathbf{Z}/p^k\mathbf{Z}) = \mathrm{Hom}(X(D_n), \mathbf{Z}_p) \\ &= \mathrm{Hom}_{\Lambda(D_n)}(X(D_n), \Lambda(D_n)) \to \mathrm{Hom}_{\Lambda(D_\infty)}(X(D_\infty), \Lambda(D_n))\end{aligned}$$

with finite kernel and cokernel bounded independently of n. This gives the bottom row, and passing to the inverse limit over n gives the top row, of the commutative diagram with horizontal isomorphisms

$$\begin{array}{ccc} \mathcal{S}(D_\infty, T_\mathfrak{p}) \otimes \mathbf{Q}_p & \xrightarrow{\sim} & \mathrm{Hom}_{\Lambda(D_\infty)}(X(D_\infty), \Lambda(D_\infty)) \otimes \mathbf{Q}_p \\ \downarrow & & \downarrow \\ \mathrm{Sel}(D_n, T_\mathfrak{p}) \otimes \mathbf{Q}_p & \xrightarrow{\sim} & \mathrm{Hom}_{\Lambda(D_\infty)}(X(D_\infty), \Lambda(D_n)) \otimes \mathbf{Q}_p \end{array}$$

By Theorem 2.4.17, the upper modules are free of rank one over $\Lambda(D_\infty) \otimes \mathbf{Q}_p$. The kernel of the right-hand vertical map is $I_n \mathrm{Hom}_{\Lambda(D_\infty)}(X(D_\infty), \Lambda(D_\infty)) \otimes \mathbf{Q}_p$ where I_n is the kernel of the map $\Lambda(D_\infty) \to \Lambda(D_n)$, and so the kernel of the left-hand vertical map is $I_n \mathcal{S}(D_\infty, T_\mathfrak{p}) \otimes \mathbf{Q}_p$. Hence the image of the left-hand vertical map is free of rank one over $\mathbf{Q}_p[\Delta_n]$. But that image is precisely $\mathrm{Sel}(D_n, T_\mathfrak{p})^{\mathrm{univ}} \otimes \mathbf{Q}_p$.

The proof for $\mathrm{Sel}(D_n, T_{\mathfrak{p}^*})^{\mathrm{univ}} \otimes \mathbf{Q}_p$ is the same. □

Proposition A.7. *If the anticyclotomic regulator $\mathcal{R}$ is zero, then the p-adic height pairing h_n is identically zero on* $\mathrm{Sel}(D_n, T_\mathfrak{p})^{\mathrm{univ}} \otimes \mathrm{Sel}(D_n, T_{\mathfrak{p}^*})^{\mathrm{univ}}$.

Proof. Suppose $n \geq 0$, $\mathbf{a} = (a_n) \in \mathcal{S}(D_\infty, T_\mathfrak{p})$ and $\mathbf{b} = (b_n) \in \mathcal{S}(D_\infty, T_\mathfrak{p}^*)$. Recall that $\Delta_n = \mathrm{Gal}(D_n/K)$. Using property (3) of Theorem 3.1.2 and the definition of h_∞, we see that projecting $h_\infty(\mathbf{a}, \mathbf{b})$ to $\mathbf{Z}_p[\Delta_n] \otimes \mathcal{J}$ gives $\sum_{\sigma \in \Delta_n} h_n(a_n^\sigma, b_n)\sigma^{-1}$.

Now suppose $v_n \in \mathrm{Sel}(D_n, T_\mathfrak{p})^{\mathrm{univ}}$ and $v_n^* \in \mathrm{Sel}(D_n, T_{\mathfrak{p}^*})^{\mathrm{univ}}$. Since v_n and v_n^* are universal norms we can choose $\mathbf{a} = (a_n) \in \mathcal{S}(D_\infty, T_\mathfrak{p})$ and $\mathbf{b} = (b_n) \in \mathcal{S}(D_\infty, T_\mathfrak{p}^*)$ with $a_n = v_n$ and $b_n = v_n^*$. If $\mathcal{R} = 0$, then $h_\infty(\mathbf{a}, \mathbf{b}) = 0$, and projecting to $\mathbf{Z}_p[\Delta_n] \otimes \mathcal{J}$ shows that $h_n(v_n, v_n^*) = 0$. □

Proposition A.8. *If n is sufficiently large then there are points $P \in E(D_n)$ of infinite order such that the image of P in* $\mathrm{Sel}(D_n, T_\mathfrak{p})$ *lies in* $\mathrm{Sel}(D_n, T_\mathfrak{p})^{\mathrm{univ}}$ *and the image of P in* $\mathrm{Sel}(D_n, T_{\mathfrak{p}^*})$ *lies in* $\mathrm{Sel}(D_n, T_{\mathfrak{p}^*})^{\mathrm{univ}}$*. I.e., there are D_n-rational points of infinite order which are universal norms in the Selmer group.*

Proof. Let ψ denote the Hecke character of K attached to E, so that $L(E/\mathbf{Q}, s) = L(\psi, s)$. Fix an integer n.

Choose a character χ of Δ_n of order p^n (any two such characters are conjugate under $G_\mathbf{Q}$, so the choice will not matter). The Hecke L-function $L(\psi\chi, s)$ is the L-function of a modular form f_χ on $\Gamma_0(Np^{2n})$, where N is the conductor of E. Let A_n denote the simple factor over $\mathbf{Q}$ of the Jacobian $J_0(Np^{2n})$ corresponding to f_χ. Comparing L-functions we see that there is an isogeny of abelian varieties over K

$$A_n \times \mathrm{Res}_{D_{n-1}/K} E \sim \mathrm{Res}_{D_n/K} E$$

where Res stands for the restriction of scalars. Passing to Mordell-Weil groups we get

$$(A_n(K) \otimes \mathbf{Q}) \times (E(D_{n-1}) \otimes \mathbf{Q}) \cong E(D_n) \otimes \mathbf{Q},$$

and therefore, if γ is a topological generator of Δ_∞,

$$A_n(K) \otimes \mathbf{Q} \cong (1 - \gamma^{p^{n-1}}) E(D_n) \otimes \mathbf{Q}. \tag{A.1}$$

It follows from our assumption about the sign in the functional equation of $L(E/\mathbf{Q}, s)$ that $L(\psi\rho, 1) = 0$ for every character ρ of finite order of Δ_∞. By a theorem of Rohrlich [20], there are only finitely many characters ρ of Δ_∞ such that the derivative $L'(\psi\rho, 1) = 0$. Suppose now that n is large enough so that

(a) $L'(\psi\chi, 1) \neq 0$,

(b) $\mathrm{char}(X(D_\infty)_{\mathrm{tor}})$ is relatively prime to $(\gamma^{p^n} - 1)/(\gamma^{p^{n-1}} - 1)$.

Since $L'(\psi\chi,1)\neq 0$, the theorem of Gross and Zagier [7] shows that

$$\text{(A.2)}\qquad \mathrm{rank}_{\mathbf{Z}} A_n(\mathbf{Q}) \geq \dim\, A_n = p^n - p^{n-1}.$$

On the other hand, using (A.1) and the Control Theorem (Proposition A.5) we get

$$\begin{aligned}\text{(A.3)}\quad \mathrm{rank}_{\mathbf{Z}} A_n(\mathbf{Q}) &\leq \mathrm{rank}_{\mathbf{Z}_p}(1-\gamma^{p^{n-1}})X(D_n)\\ &= \mathrm{rank}_{\mathbf{Z}_p}(1-\gamma^{p^{n-1}})X(D_\infty)/(1-\gamma^{p^n})X(D_\infty)\end{aligned}$$

Since $X(D_\infty)$ has $\Lambda(D_\infty)$-rank one (Theorem 2.4.17(2)), we conclude from condition (b) on n that

$$\mathrm{rank}_{\mathbf{Z}_p}(1-\gamma^{p^{n-1}})X(D_\infty)/(1-\gamma^{p^n})X(D_\infty) = p^n - p^{n-1}.$$

It follows that we must have equality in (A.2) and (A.3), and

$$\dim_{\mathbf{Q}_p}(1-\gamma^{p^{n-1}})\mathrm{Sel}(D_n,T_{\mathfrak{p}})\otimes\mathbf{Q}_p = \mathrm{rank}_{\mathbf{Z}_p}(1-\gamma^{p^{n-1}})X(D_n) = p^n - p^{n-1}.$$

Since $(1-\gamma^{p^{n-1}})\mathbf{Q}_p[\Delta_n]$ is a simple $\mathbf{Q}_p[\Delta_n]$-module it follows that

$$(1-\gamma^{p^{n-1}})\mathrm{Sel}(D_n,T_{\mathfrak{p}})\otimes\mathbf{Q}_p \cong (1-\gamma^{p^{n-1}})\mathbf{Q}_p[\Delta_n]$$

By Lemma A.6 we now see that

$$(1-\gamma^{p^{n-1}})\mathrm{Sel}(D_n,T_{\mathfrak{p}})^{\mathrm{univ}}\otimes\mathbf{Q}_p = (1-\gamma^{p^{n-1}})\mathrm{Sel}(D_n,T_{\mathfrak{p}})\otimes\mathbf{Q}_p.$$

In particular if P is any point of infinite order in $(1-\gamma^{p^{n-1}})E(D_n)$ (and we know that such points exist by (A.1)) then some multiple of the image of P in $\mathrm{Sel}(D_n,T_{\mathfrak{p}})$ lies in $\mathrm{Sel}(D_n,T_{\mathfrak{p}})^{\mathrm{univ}}$. In exactly the same way some multiple of the image of P in $\mathrm{Sel}(D_n,T_{\mathfrak{p}^*})$ lies in $\mathrm{Sel}(D_n,T_{\mathfrak{p}^*})^{\mathrm{univ}}$, and the proposition is proved. □

Proof of Theorem B. Using Proposition A.8, find an n and a point of infinite order $P\in E(D_n)$ whose images in $\mathrm{Sel}(D_n,T_{\mathfrak{p}})$ and $\mathrm{Sel}(D_n,T_{\mathfrak{p}^*})$ are universal norms.

By Bertrand's Theorem A.1, we have $h_{D_n,\mathfrak{p}}(P)\neq 0$. By Lemma A.4 we have $h_{D_n,\mathrm{anti}}(P)=0$, and therefore by Lemma A.2 we have that $h_{D_n,\mathrm{cycl}}(P)$ (and hence $h_n(P)$) is nonzero.

It now follows from Proposition A.7 that the anticyclotomic regulator $\mathcal{R}$ is nonzero, and so by Theorem 3.1.5 the leading term $\mathcal{L}_1$ is nonzero. This is Theorem B. □

Remark A.9. In the notation of Proposition A.8, the abelian variety A_n is isogenous to its twist by the quadratic character of $K/\mathbf{Q}$, and so there are isomorphisms

$$A_n(K)\otimes\mathbf{Q}\cong(\mathrm{Res}_{K/\mathbf{Q}}A_n)(\mathbf{Q})\otimes\mathbf{Q}\cong(A_n\times A_n)(\mathbf{Q})\otimes\mathbf{Q}.$$

Thus

$$\begin{aligned} p^n - p^{n-1} &= \frac{1}{2}\,\mathrm{rank}_{\mathbf{Z}} A_n(K)\\ &= \mathrm{rank}_{\mathcal{O}_K} E(D_n) - \mathrm{rank}_{\mathcal{O}_K} E(D_{n-1})\end{aligned}$$

for $n\gg 0$. This implies that there is a constant c such that

$$\mathrm{rank}_{\mathcal{O}_K} E(D_n) = p^n + c$$

for $n\gg 0$. The same asymptotic formula holds for the corank of the $\mathfrak{p}$-primary Selmer group (by Theorem 2.4.17 and Proposition A.5), and so the $\mathcal{O}_{\mathfrak{p}}$-corank of of $\text{Ш}(E/D_n)_{\mathfrak{p}^\infty}$ is bounded as n varies.

References

[1] T. Arnold. Anticyclotomic main conjectures for CM modular forms. Preprint. 2005.

[2] D. Bertrand. Propriétés arithmétiques de fonctions thêta à plusieurs variables. In: Number theory, Noordwijkerhout 1983, *Lecture Notes in Math.* **1068** Springer: Berlin (1984) 17–22.

[3] J. Coates. Infinite descent on elliptic curves with complex multiplication, in *Arithmetic and Geometry, Vol. I,* 107–137, Progr. Math., 35, Birkhuser. (1983).

[4] E. de Shalit. *Iwasawa Theory of Elliptic Curves with Complex Multiplication.* Academic Press, (1987).

[5] R. Greenberg. On the structure of certain Galois groups. *Invent. Math.* 47 (1978) 85–99.

[6] R. Greenberg. On the Birch and Swinnerton-Dyer conjecture. *Invent. Math.* 72 (1983) 241–265.

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

[8] B. Howard. The Iwasawa theoretic Gross-Zagier theorem. *Comp. Math.* 141, No. 4 (2005), 811–846.

[9] S. Lang. *Algebraic Number Theory*, Second Edition, Springer Verlag, (1994).

[10] J. Martinet. Character theory and Artin L-functions. In: *Algebraic Number Fields*, A. Fröhlich (ed.), Academic Press, (1977) 1–88.

[11] B. Mazur, Rational points of abelian varieties with values in towers of number fields. *Invent. Math.* **18** (1972) 183–266.

[12] B. Mazur. Modular curves and arithmetic. In: *Proceedings of the International Congress of Mathematicians (Warsaw, 1983)*, PWN, Warsaw (1984) 195–237.

[13] B. Mazur, K. Rubin, Studying the growth of Mordell-Weil. In: *Documenta math.* Extra Volume: Kazuya Kato's Fiftieth Birthday (2003) 585–607.

[14] B. Mazur and K. Rubin. Kolyvagin Systems. *Memoirs of the AMS,* **168**, (2004).

[15] B. Mazur and K. Rubin. Elliptic curves and class field theory. In: *Proceedings of the International Congress of Mathematicians (Beijing, 2002).*

[16] B. Mazur, J. Tate, Canonical height pairings via biextensions. In: Arithmetic and geometry, Vol. I, *Progr. Math.* **35** Birkhuser: Boston (1983) 195–237.

[17] B. Perrin-Riou. Arithmétique des courbes elliptiques et théorie d'Iwasawa. *Bull. Soc. Math. France, Memoires*, N.S. 17 (1984).

[18] B. Perrin-Riou. Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner. *Bull. Soc. math. France*, 115 (1987) 399-456.

[19] B. Perrin-Riou. Théorie d'Iwasawa et hauteurs p-adiques. *Invent. Math.* 109 (1992) 137–185.

[20] D. Rohrlich. On L-functions of elliptic curves and anticyclotomic towers. *Invent. Math.,* 75 (1984) 383–408.

[21] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.* 103 (1991) 25–68.

[22] K. Rubin. p-adic L-functions and rational points on elliptic curves with complex multiplication. *Invent. Math.* 107 (1992) 323-350.

[23] K. Rubin. Abelian varieties, p-adic heights and derivatives. In *Algebra and Number Theory.* Walter de Gruyter and Co. (1994) 247–266.

[24] K. Rubin. Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-dyer. In *Arithmetic Theory of Elliptic Curves (Cetraro, 1997)*, number 1716 in Lecture Notes in Math., pages 167–234. Springer, (1999).

[25] K. Rubin. *Euler Systems.* Princeton University Press, (2000).

[26] A. Weil. *Automorphic Forms and Dirichlet Series*, Lecture Notes in Math. No. 189, Springer, (1971).

[27] R. Yager. On two variable p-adic L-functions. *Ann. Math.* 115 (1982) 411–449.

Department of Mathematics, University of California, Santa Barbara, CA, 93106
E-mail address: agboola@math.ucsb.edu

Department of Mathematics, Harvard University, Cambridge, MA, 02138
Current address: Department of Mathematics, Boston College, Chestnut Hill, MA 02467
E-mail address: howardbe@bc.edu

Department of Mathematics, Stanford University, Stanford, CA 94305
Current address: Department of Mathematics, UC Irvine, Irvine, CA 92697
E-mail address: krubin@math.uci.edu