Cambridge Journal of Mathematics
Volume 12, Number 2, 357–415, 2024

The conjecture of Birch and Swinnerton-Dyer for certain elliptic curves with complex multiplication

Ashay Burungale[*] and Matthias Flach

Dedicated to John H. Coates

Let E/F be an elliptic curve over a number field F with complex multiplication by the ring of integers in an imaginary quadratic field K. We give a complete proof of the conjecture of Birch and Swinnerton-Dyer for E/F, as well as its equivariant refinement formulated by Gross [39], under the assumption that $L(E/F,1) \neq 0$ and that $F(E_{tors})/K$ is abelian. We also prove analogous results for CM abelian varieties A/K.

AMS 2000 subject classifications: Primary 11G40; secondary 11G15, 11R23.
Keywords and phrases: Elliptic curves, Birch and Swinnerton-Dyer Conjecture, Complex multiplication.

1. Introduction

Let E/F be an elliptic curve over a number field F with complex multiplication by the ring of integers in an imaginary quadratic field K and such that $F(E_{tors})/K$ is abelian. It is well known that the conjecture of Birch and

arXiv: 2206.09874

[*] Partially supported by the NSF grants DMS 2303864 and 2302064.

Swinnerton-Dyer for this class of elliptic curves, as well as its K-equivariant refinement formulated by Gross [39], is amenable to the Iwasawa theory of the field K. Indeed, this principle has its origin in the seminal work of Coates and Wiles [18] which led to the finiteness of $E(F)$ if $L(E/F,1) \neq 0$. About a decade later Rubin [66] showed the finiteness of $Ш(E/F)$ if $L(E/F,1) \neq 0$. This remarkable work, partly motivated by the ideas of Thaine [81], gave the very first proof of finiteness of the Tate-Shafarevich group of an abelian variety over a number field. Subsequently, as a consequence of his proof of the Iwasawa main conjecture for K, Rubin [68] proved the $\mathfrak{p}$-primary part of Gross' conjecture assuming $F = K$, $L(E/F,1) \neq 0$ and $\mathfrak{p} \nmid |\mathcal{O}_K^\times|$. He also indicated that for general F his arguments give a proof of the $\mathfrak{p}$-primary part of Gross' conjecture if $L(E/F,1) \neq 0$ and

$$\mathfrak{p} \nmid |\mathcal{O}_K^\times| \cdot [F:K] \cdot \mathrm{disc}(F/K).$$

The purpose of this paper is to eliminate these restrictions on the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and give a complete proof of Gross' conjecture if $L(E/F,1) \neq 0$. The main result is Theorem 1.1 below. Our approach is based on the principle of the equivariant Tamagawa number conjecture: zeta elements generate equivariant determinants of certain étale cohomology groups. The key ingredients of the proof are the two variable Iwasawa main conjecture for K due to Johnson-Leung and Kings [44] (based on the Euler system of elliptic units) and Kato's reciprocity law [48, Prop. 15.9] (we use Kato's formulation but the case we need goes back to Wiles [86] and Coates/Wiles [19]). Our arguments also give the L-equivariant Birch and Swinnerton-Dyer conjecture for abelian varieties A/K with complex multiplication by a CM field L if $L(A/K,1) \neq 0$ which we record in Theorem 1.2. In particular this proves a conjecture of Buhler and Gross [3, Conj. 12.3].

We first introduce some notation. For archimedean places v of F we have the K-bilinear integration pairings

$$H_1(E(F_v),\mathbb{Q}) \times H^0(E,\Omega_{E/F}) \otimes_F F_v \to F_v; \quad (\gamma,\omega) \mapsto \int_\gamma \omega \tag{1}$$

which jointly induce a $K_\mathbb{R}$-linear period isomorphism

$$\prod_{v\mid\infty} H_1(E(F_v),\mathbb{Q})_\mathbb{R} \cong \mathrm{Hom}_F(H^0(E,\Omega_{E/F}),F)_\mathbb{R}. \tag{2}$$

For each $v \mid \infty$ the period lattice $H_1(E(F_v),\mathbb{Z})$ is an invertible $\mathcal{O}_K$-module. If $\mathcal{E}/\mathcal{O}_F$ denotes the Néron model of E then $H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F})$ is an invertible $\mathcal{O}_F$-module and a projective $\mathcal{O}_K$-module of rank $d = [F:K]$, hence so is $\mathrm{Hom}_{\mathcal{O}_F}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F}),\mathcal{O}_F)$. It follows that there is an invertible $\mathcal{O}_K$-submodule $\mathfrak{a}\subset K_{\mathbb{R}}$ so that

$$\bigotimes_{v|\infty} H_1(E(F_v),\mathbb{Z})=\mathfrak{a}\cdot\det_{\mathcal{O}_K}\mathrm{Hom}_{\mathcal{O}_F}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F}),\mathcal{O}_F)$$

under the determinant over $K_{\mathbb{R}}$ of the isomorphism (2). We may write

$$\mathfrak{a}=\Omega\cdot\mathfrak{a}(\Omega)$$

for some period

$$\Omega\in K_{\mathbb{R}}^{\times}\cong\mathbb{C}^{\times}$$

and fractional $\mathcal{O}_K$-ideal $\mathfrak{a}(\Omega)\subseteq K$. Denote the order ideal of a finite $\mathcal{O}_K$-module A by $|A|_K$ and the cardinality of a finite abelian group A by $|A|$. Let Φ_v be the component group of the Néron model of E/F at the prime v.

Theorem 1.1. *Let E/F be an elliptic curve over a number field F with CM by $\mathcal{O}_K$ for an imaginary quadratic field K and such that $F(E_{tors})/K$ is abelian. Let $\psi:\mathbb{A}_F^{\times}/F^{\times}\to\mathbb{C}^{\times}$ be the Hecke character associated to E/F and assume that $L(\overline{\psi},1)\neq 0$. Then $E(F)$ and $Ш(E/F)$ are finite $\mathcal{O}_K$-modules,*

$$\frac{L(\overline{\psi},1)}{\Omega}\in K^{\times}$$

and

$$\frac{L(\overline{\psi},1)}{\Omega}=\frac{|Ш(E/F)|_K}{|E(F)|}\cdot\prod_v|\Phi_v|_K\cdot\mathfrak{a}(\Omega)$$

in the group of fractional $\mathcal{O}_K$-ideals.

Remark 1. As pointed out by Gross, not only the ideal $|E(F)|$ but also the ideal $|Ш(E/F)|_K$ is generated by a rational integer [39, Prop. 3.7]. The ideals $|\Phi_v|_K$ are equal to either (1), (2) or $\mathfrak{p}$ with $\mathfrak{p}^2=(2)$ or $\mathfrak{p}^2=(3)$ [39, Prop. 4.5].

Restricting scalars from $K_{\mathbb{R}}$ to $\mathbb{R}$ in the period isomorphism (2) and taking determinants over $\mathbb{Z}$ of the natural lattices in both sides, we find that there exists $\Omega(E)\in\mathbb{R}^{\times}$ such that

$$\bigotimes_{v|\infty}\det_{\mathbb{Z}}H_1(E(F_v),\mathbb{Z})=\Omega(E)\cdot\det_{\mathbb{Z}}\mathrm{Hom}_{\mathcal{O}_F}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F}),\mathcal{O}_F).$$

Moreover, we have

$$\Omega(E)\cdot\mathbb{Z}=N_{K/\mathbb{Q}}\mathfrak{a}=\mathfrak{a}\overline{\mathfrak{a}}=\Omega\overline{\Omega}\cdot\mathfrak{a}(\Omega)\overline{\mathfrak{a}(\Omega)}. \tag{3}$$

Corollary 1 (BSD for E/F)**.** *Under the assumptions of Theorem 1.1 the groups $E(F)$ and $Ш(E/F)$ are finite and*

$$\frac{L(E/F,1)}{\Omega(E)}=\frac{|Ш(E/F)|}{|E(F)|^2}\cdot\prod_v|\Phi_v|$$

Proof. This follows from the identity [73, Thm. 7.42]

$$L(E/F,s)=L(\overline{\psi},s)\overline{L(\overline{\psi},s)}=L(\overline{\psi},s)L(\psi,s)$$

the fact that $N_{K/\mathbb{Q}}(|A|_K)=|A|$ for any finite $\mathcal{O}_K$-module A, and (3). □

Any elliptic curve E/K with CM by $\mathcal{O}_K$ for which $L(E/K,1)\neq 0$ satisfies the assumptions of Theorem 1.1 and Corollary 1. In this case the class number of K is 1. More generally, for primes $q\equiv 3 \mod 4$ and $K=\mathbb{Q}(\sqrt{-q})$ the class number of K is odd and elliptic curves E/H where $F=H$ is the Hilbert class field have been much studied in, for example [37, 63, 58, 3]. One finds in these references many examples which satisfy the assumption $L(E/H,1)\neq 0$ of Theorem 1.1 (see also Corollary 4).

Remark 2. For elements $\omega\in H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F})$ and $\gamma_v\in H_1(E(F_v),\mathbb{Z})$ we may define periods

$$\Omega_v:=\Omega(\gamma_v,\omega):=\int_{\gamma_v}\omega$$

in terms of which Ω and $\Omega(E)$ can be expressed as follows. First, there are fractional $\mathcal{O}_K$-ideals $\mathfrak{a}(\gamma_v)$ and $\mathfrak{a}(\omega)$ such that

$$H_1(E(F_v),\mathbb{Z})=\mathfrak{a}(\gamma_v)\cdot\gamma_v$$

and

$$\det_{\mathcal{O}_K}H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F})=\mathfrak{a}(\omega)\cdot\det_{\mathcal{O}_K}(\mathcal{O}_F\cdot\omega).$$

The trace map $\mathcal{O}_F\xrightarrow{\mathrm{Tr}}\mathcal{O}_K$ induces an isomorphism

$$\mathrm{Hom}_{\mathcal{O}_F}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F}),\mathcal{O}_F)\cong\mathrm{Hom}_{\mathcal{O}_K}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F})\otimes_{\mathcal{O}_F}\mathcal{D}_{F/K}^{-1},\mathcal{O}_K)$$

where $\mathcal{D}_{F/K}^{-1}$ is the inverse different, an invertible $\mathcal{O}_F$-module. Assume for simplicity that $\mathcal{D}_{F/K}^{-1}$ is a free $\mathcal{O}_K$-module and let $\beta_1,\dots,\beta_d$ be a basis. Then if we define

$$\Omega:=\det\left(\int_{\gamma_v}\omega\otimes\beta_k\right)_{v,k}$$

we have

$$\mathfrak{a}(\Omega) = \mathfrak{a}(\omega) \cdot \prod_{v|\infty} \mathfrak{a}(\gamma_v).$$

Let e_v be the indecomposable idempotents in

$$\mathcal{D}_{F/K}^{-1} \otimes_{\mathcal{O}_K} K_{\mathbb{R}} \cong \mathcal{O}_F \otimes_{\mathcal{O}_K} K_{\mathbb{R}} \cong \prod_{v|\infty} F_v$$

and express the β_k as a linear combination of the e_v. Then the base change matrix has determinant

$$\det(\beta_{k,v})_{v,k} = \left(\sqrt{D_{F/K}}\right)^{-1}$$

where $D_{F/K} \in \mathcal{O}_K$ generates the relative discriminant ideal of the extension F/K (and depends on the choice of β_k by a factor in $(\mathcal{O}_K^\times)^2$ so that the $\mathcal{O}_K$-ideal generated by $\sqrt{D_{F/K}}$ is well defined). So we find

$$\Omega = \left(\sqrt{D_{F/K}}\right)^{-1} \cdot \det\left(\int_{\gamma_v} \omega \otimes e_{v'}\right)_{v,v'} = \left(\sqrt{D_{F/K}}\right)^{-1} \cdot \prod_{v|\infty} \Omega_v.$$

Denoting by $D_{L/\mathbb{Q}} \in \mathbb{Z}$ the discriminant of a number field L we have

$$|D_{F/\mathbb{Q}}| = N_{K/\mathbb{Q}} D_{F/K} \cdot |D_{K/\mathbb{Q}}|^{[F:K]} = D_{F/K}\overline{D_{F/K}} \cdot |D_{K/\mathbb{Q}}|^{[F:K]}$$

and therefore

$$\begin{aligned}\mathbb{Z} \cdot \Omega(E) &= \mathfrak{a}(\omega)\overline{\mathfrak{a}(\omega)} \cdot \left(\sqrt{N_{K/\mathbb{Q}} D_{F/K}}\right)^{-1} \cdot \prod_{v|\infty} \Omega_v \overline{\Omega}_v \cdot \mathfrak{a}(\gamma_v)\overline{\mathfrak{a}(\gamma_v)} \\ &= \mathfrak{a}(\omega)\overline{\mathfrak{a}(\omega)} \cdot \left(\sqrt{|D_{F/\mathbb{Q}}|}\right)^{-1} \cdot \prod_{v|\infty} \sqrt{|D_{K/\mathbb{Q}}|} \cdot \Omega_v \overline{\Omega}_v \cdot \mathfrak{a}(\gamma_v)\overline{\mathfrak{a}(\gamma_v)} \\ &= \frac{1}{I_\omega} \cdot \left(\sqrt{|D_{F/\mathbb{Q}}|}\right)^{-1} \cdot \prod_{v|\infty} \mathrm{vol}_\omega(E(F_v))\end{aligned}$$

where

$$I_\omega := (\mathfrak{a}(\omega)\overline{\mathfrak{a}(\omega)})^{-1} = [H^0(\mathcal{E}, \Omega_{\mathcal{E}/\mathcal{O}_F}) : \mathcal{O}_F \cdot \omega] \in \mathbb{Z}$$

and the Haar measure on $E(F_v)$ is induced by the volume form

$$2dx \wedge dy = idz \wedge d\bar{z}$$

after identifying the cotangent space of E/F_v with $F_v \simeq \mathbb{C}$ via the basis ω. This last form of the period term $\Omega(E)$ in the conjecture of Birch and Swinnerton-Dyer for abelian varieties over number fields can be found, for example, in [28, L3, Ex. 6.4] (see also [34, Lemma 18]) and continues to hold without our assumption of the existence of a basis β_i. However, in the above computation there will then be yet another corrective fractional $\mathcal{O}_K$-ideal $\mathfrak{a}(\beta_i)$ contributing to $\mathfrak{a}(\Omega)$.

Corollary 2 (BSD for E/F^+)**.** *Under the assumptions of Theorem 1.1 assume in addition that E is defined over a subfield $F^+ \subset F$ which is the fixed field of an involution of F inducing complex conjugation on K. Then the groups $E(F^+)$ and $\text{Ш}(E/F^+)$ are finite and*

$$\frac{L(E/F^+,1)}{\Omega(E^+)} = \frac{|\text{Ш}(E/F^+)|}{|E(F^+)|^2} \cdot \prod_v |\Phi_v^+|$$

where Φ_v^+ is the component group of the Néron model of E/F^+ at the prime v.

Proof. If F/F^+ is a quadratic extension of number fields and E/F^+ an elliptic curve then there is an isogeny of abelian surfaces over F^+

$$A := Res_{F^+}^F(E/F) \sim E \times E_\epsilon$$

where E_ϵ is the twist of E by the quadratic character ϵ attached to F/F^+. In our case E_ϵ is isogenous to E (see [56, Thm. 3]), hence an isogeny

$$A \sim E \times E.$$

We have isomorphisms $\text{Ш}(E/F) \simeq \text{Ш}(A/F^+)$, $E(F) \simeq A(F^+)$ and the BSD formula for E/F is equivalent to the BSD formula for A/F^+ [56, Thm. 1]. By isogeny invariance of BSD we deduce the BSD formula for $(E \times E)/F^+$ (as well as finiteness of $\text{Ш}((E \times E)/F^+)$ and $(E \times E)(F^+)$). Since all terms in the BSD formula for $(E \times E)/F^+$ are simply the squares of the corresponding terms in the BSD formula for E/F^+ we deduce the BSD formula for E/F^+ by taking square roots (see also [56, Cor. to Thm. 3] for this entire argument). □

Any CM elliptic curve $E/\mathbb{Q}$ with $L(E/\mathbb{Q},1) \neq 0$ satisfies the assumptions of Corollary 2. In particular we obtain the following.

Corollary 3. *The Birch and Swinnerton-Dyer conjecture is true for congruent number elliptic curves*

$$E^{(n)} : ny^2 = x^3 - x$$

for a density one subset of positive square-free integers $n \equiv 1, 2, 3 \mod 8$.

Proof. By [9] we have $L(E^{(n)}/\mathbb{Q}, 1) \neq 0$ for a density one subset of positive square-free integers $n \equiv 1, 2, 3 \mod 8$ (see also [8]). □

Remark 3. Let $E/\mathbb{Q}$ be a CM elliptic curve and $\{E^{(n)}\}_n$ the family of its quadratic twists over $\mathbb{Q}$. Then Corollary 2 in combination with [60, Thm. 3] implies that the distribution of orders of Tate-Shafarevich groups $\{Ш(E^{(n)}/\mathbb{Q})\}_n$ in the quadratic twist subfamily with analytic rank zero is as in [60, Thm. 3].

The following application was suggested to us by B. Gross, to whom we are grateful.

Corollary 4. *Let* $p \equiv 7 \mod 8$ *be a prime,* $K = \mathbb{Q}(\sqrt{-p})$ *and* h *the class number of* K*. Let* $F = K(j)$ *denote the Hilbert class field of* K *for*

$$j = j((1 + \sqrt{-p})/2)$$

and $F^+ = \mathbb{Q}(j)$*. Let* $A(p)/F^+$ *be the elliptic curve with CM by* $\mathcal{O}_K$ *over* F *with Weierstrass equation*

$$y^2 = x^3 + \frac{mp}{2^3 3}x - \frac{np^2}{2^5 3^3}$$

where m *and* n *are unique real numbers such that*

$$m^3 = j, \ -n^2 p = j - 1728 \text{ and } \operatorname{sgn}(n) = (\frac{2}{p}).$$

Then

$$|Ш(A(p)/F^+)| = \left(\frac{1}{2^{h-1}} \cdot \frac{\prod_{\varphi \in \hat{\mathrm{Cl}}_K} \sum_{C \in \mathrm{Cl}_K} \varphi(C)t(C)}{\prod_{C \in \mathrm{Cl}_K} t(C)}\right)^2$$

where $\hat{\mathrm{Cl}}_K$ *denotes the character group of* Cl_K *and* t *the modular function as in [62, p. 562].*

Proof. By [63] we have $L(A(p)/F^+, 1) \neq 0$. So the assertion follows from Corollary 2 and [62, Thm. 8.2]. □

Remark 4. The elliptic curves $A(p)$ were introduced by Gross in the late 70's [37, 38, 39, 40] which continue to be instrumental.

Corollary 5. *Let E/F' be an elliptic curve as in either Corollary 1 or Corollary 2 so that F' is either F or F^+. Let X/F' be a principal homogeneous space of E/F' and $\mathcal{X} \to \operatorname{Spec}(\mathcal{O}_{F'})$ a proper regular model of X. Then $\operatorname{Br}(\mathcal{X})$ is finite and the special value conjecture [33, Conj. 5.12] for $\zeta(\mathcal{X}, s)$ at $s = 1$ holds true. More precisely, if the Zeta function $\zeta(\mathcal{X}, s)$ is factored as in [34, Eq. (4)]*

$$\zeta(\mathcal{X}, s) = \frac{\zeta_{F'}(s)\zeta_{F'}(s-1)}{\zeta(H^1, s)}$$

then

$$\operatorname{ord}_{s=1} \zeta(H^1, s) = \operatorname{rank}_{\mathbb{Z}} \operatorname{Pic}^0(\mathcal{X})$$

and

$$\zeta^*(H^1, 1) = \frac{\# \operatorname{Br}(\overline{\mathcal{X}}) \cdot \delta^2 \cdot \Omega(\mathcal{X}) \cdot R(\mathcal{X})}{(\#(\operatorname{Pic}^0(\mathcal{X})_{tor} / \operatorname{Pic}(\mathcal{O}_{F'})))^2} \cdot \prod_{v \text{ real}} \frac{\#\Phi_v}{\delta_v^2}$$

where $\operatorname{Pic}^0(\mathcal{X})$ is the kernel of the degree map on $\operatorname{Pic}(\mathcal{X})$, $R(\mathcal{X})$ is the regulator of the Arakelov intersection pairing on $\operatorname{Pic}^0(\mathcal{X})$, $\Omega(\mathcal{X})$ is the determinant of the period isomorphism between the finitely generated abelian groups $H^1(\mathcal{X}(\mathbb{C}), 2\pi i \cdot \mathbb{Z})^{G_\mathbb{R}}$ and $H^1(\mathcal{X}, \mathcal{O}_\mathcal{X})$ and

$$\operatorname{Br}(\overline{\mathcal{X}}) = \ker \left(\operatorname{Br}(\mathcal{X}) \to \bigoplus_{v \text{ real}} \operatorname{Br}(X_{F'_v}) \right).$$

The integer δ is the index of X, i.e. the g.c.d. of the degrees of all closed points, $\Phi_v = E(F'_v)/E(F'_v)^0$ is the group of components, and δ_v is the index of $X_{F'_v}$ over F'_v.

Proof. By [34, Thm. 6.1] the BSD formula for E/F' is equivalent to the special value conjecture [34, Eq. (6)] for $\zeta^*(H^1, 1)$. Since E has genus 1 the equality $\delta'_v = \delta_v$ of period and index for real v in [34, Eq. (6)] follows from the proof of [34, Lemma 9]. □

Remark 5. In the situation of Corollary 2 the extension $F/\mathbb{Q}$ is Galois since $\operatorname{Aut}(F)$ contains the involution σ in addition to $\operatorname{Gal}(F/K)$ so that $\# \operatorname{Aut}(F) = [F : \mathbb{Q}]$. The number r_1 of real places of F^+ is the number of fixed points of the action of σ on the set of archimedean places of F. If one chooses $\sigma \in \operatorname{Aut}(F)$ as the restriction of complex conjugation with respect to a particular complex embedding there is at least one fixed point, and the total number of fixed points of σ coincides with the number of fixed points of the conjugation action of $\operatorname{Gal}(K/\mathbb{Q})$ on $\operatorname{Gal}(F/K)$. Hence the signature

(r_1, r_2) of the field F^+ in Corollary 2 either satisfies $r_1 = 0$ or $r_1 \mid 2r_2$. One can construct examples of fields F^+ for any (r_1, r_2) with $r_1 \mid 2r_2$: choose

$$\mathrm{Gal}(F/K) \simeq \mathbb{Z}/r_1'\mathbb{Z} \times \mathbb{Z}/((r_1 + 2r_2)/r_1')\mathbb{Z}$$

with $\mathrm{Gal}(K/\mathbb{Q})$ acting trivially on the first factor and by -1 on the second. Here $r_1' = r_1$ if r_1 is odd and $r_1' = r_1/2$ if r_1 is even. To construct examples of Corollaries 2 and 5 one may take E/F with $j(E) \in \mathbb{Q}$ but one also needs non-vanishing results for $L(\overline{\psi}, 1)$.

Theorem 1.2. *Let A/K be a CM abelian variety with $\mathrm{End}_K(A) \simeq \mathcal{O}_L$ for some CM field L with $[L : \mathbb{Q}] = 2\dim(A)$. Let φ be its Serre-Tate character and assume*

$$L(\bar{\varphi}, 1) \neq 0.$$

Let $\Omega \in L_{\mathbb{R}}^\times$ and $\mathfrak{a}(\Omega)$ be the period and fractional $\mathcal{O}_L$-ideal defined in Def. 1 in Section 2. Then $Ш(A/K)$ and $A(K)$ are finite, $\frac{L(\bar{\varphi},1)}{\Omega} \in L^\times$ and

$$\frac{L(\bar{\varphi}, 1)}{\Omega} = \frac{|Ш(A/K)|_L}{|A(K)|_L|^tA(K)|_L} \cdot \prod_v |\Phi_v|_L \cdot \mathfrak{a}(\Omega)$$

in the group of fractional ideals of L.

Apart from being a special case of the equivariant Tamagawa number conjecture [5] this L-equivariant Birch and Swinnerton-Dyer conjecture was also formulated by Buhler and Gross [3, Conj. 12.3] in the special case where $A = \mathrm{Res}_{H/K} E$ for E/H a CM elliptic curve over the Hilbert class field and $[H : K]$ odd. We will explicate the connection to [3, Conj. 12.3] in Prop. 4.2 in Section 4.4.

Corollary 6 (BSD for A/K). *Under the assumptions of Thm. 1.2 we have*

$$\frac{L(A/K, 1)}{\Omega(A)} = \frac{|Ш(A/K)|}{|A(K)| \cdot |^tA(K)|} \cdot \prod_v |\Phi_v|$$

where the period $\Omega(A)$ is defined for example in [34, Lemma 18].

Proof. This follows by taking the norm from L to $\mathbb{Q}$ of the identity in Thm. 1.2. □

Corollary 7 (BSD for $A/\mathbb{Q}$). *In the situation of Thm. 1.2 assume in addition that A is defined over $\mathbb{Q}$. Then we have*

$$\frac{L(A/\mathbb{Q}, 1)}{\Omega(A^+)} = \frac{|Ш(A/\mathbb{Q})|}{|A(\mathbb{Q})| \cdot |^tA(\mathbb{Q})|} \cdot \prod_v |\Phi_v^+|$$

where the period $\Omega(A^+)$ is the period of [34, Lemma 18] for $A/\mathbb{Q}$.

Proof. This follows as in the proof of Cor. 2. □

Corollary 8. *Let f be an elliptic newform of weight 2, level N and arbitrary character, and let A_f be the isogeny factor of the Jacobian of $X_1(N)$ associated to f by Eichler-Shimura. If f has CM and $L(A_f, 1) \neq 0$ then the Birch and Swinnerton-Dyer conjecture holds for A_f.*

Proof. Let K be the CM field of f and $L_0 := \mathrm{End}_{\mathbb{Q}}(A_f)_{\mathbb{Q}}$ the field generated by the Hecke eigenvalues of f [61, Cor. 4.2]. Then the base change $A_{f,K}$ of A_f to K is either simple with $\mathrm{End}_K(A_{f,K})_{\mathbb{Q}} \simeq L := L_0K$ or $A_{f,K} \sim A_1 \times A_2$ with $\mathrm{End}_K(A_i)_{\mathbb{Q}} \simeq L := L_0$. By isogeny invariance of BSD we can assume that $A_{f,K}$ has multiplications by the maximal order in either case. Then BSD holds for $A_{f,K}$ by Cor. 6 and follows for A_f as in Cor. 2. □

Remarks on the proof. The proof of Theorem 1.1 is naturally situated in the framework of the equivariant Tamagawa number conjecture. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and p the rational prime below. The proof begins with a reduction of Theorem 1.1 to the existence of an equivariant zeta element for E/F, i.e. a basis z of the $\mathcal{O}_K$-equivariant determinant of the p-adic étale cohomology of E/F which also encodes the L-value $L(E/F, 1)$ (Prop. 2.3). By a descent of the Iwasawa main conjecture for K [44], such a basis z is constructed via elliptic units (Subsections 4.3 and 4.5) whose link to $L(E/F, 1)$ is given by an explicit reciprocity law (Subsection 3.4). The main conjecture [44] expresses the determinant of Iwasawa cohomology of K in terms of elliptic units as pioneered by Kato [46, 47]. Our descent of the main conjecture is formulated in terms of perfect complexes and is uniform for any prime $\mathfrak{p}$. It first leads to the finiteness of $E(F)$ and $Ш(E/F)_{\mathfrak{p}^\infty}$ (offering another proof of results of [18, 66]) and then to z.

The above approach to the $\mathfrak{p}$-primary part of Gross' conjecture and the BSD formula differs from that of Rubin [68]. The calculus of determinants of perfect complexes does not appear in [68]. The descent [68, §11] involves classical Iwasawa modules and is more involved for primes p non-split in K [68, pp. 61–66].

Remarks on the related work. The CM elliptic curve $X_0(49)$ has analytic rank 0 and it was the first elliptic curve for which the full BSD conjecture was proved [37, 66, §22]. (See also the discussion in [40, p. 17].) Since Rubin's fundamental work [68], the $\mathfrak{p}$-primary part of the BSD formula for CM elliptic curves with analytic rank 0 and primes $\mathfrak{p}$ such that

$$\mathfrak{p} \| |\mathcal{O}_K^\times| \cdot [F : K] \cdot \mathrm{disc}(F/K)$$

has been much studied, especially the case of CM elliptic curves over $\mathbb{Q}$ and the prime $p = 2$. This includes the extensive work of Coates [20, 21, 24, 26, 17, 25, 23], Kezuka [49, 50, 53, 51, 52], Tian [55, 82, 83, 12, 13, 84], Tian-Yuan-Zhang [85], Zhao [89, 90, 91, 92], as well as [69, 36, 59, 32, 10, 16, 43, 87, 64, 11, 74]. The prior work was the original impetus for our study. Note that Coates-Kezuka-Li-Tian [23] prove the 2-part of the BSD formula for CM elliptic curves with ordinary reduction at 2. Some of the prior work concerns specific families of CM curves, for instance Tian [83] and Tian-Yuan-Zhang [85] prove seminal results for congruent number elliptic curves (which led to Smith's work [77, 78, 79, 80]). The proofs employ various tools such as the Euler system of elliptic units, explicit Waldspurger formula and congruences between modular forms. Yet, prior to Corollary 2, the p-part of the BSD formula for CM elliptic curves over $\mathbb{Q}$ with analytic rank 0 and $p||\mathcal{O}_K^\times|$ remained open in general.

For some complementary results towards the BSD conjecture over the last decade the reader may refer to [76, 75, 45, 88, 7, 6].

Our approach to the BSD formula seems amenable to other situations. In future work we plan to consider the case of CM elliptic curves with analytic rank 1.

2. Preliminary reductions

In this section we reduce the proof of Thm. 1.1, resp. Thm. 1.2, to the existence of a basis of the determinant of global Galois cohomology of the Tate module with certain properties, see Prop. 2.3, resp. Prop. 2.2. Such a basis will then be provided by the combination of Kato's reciprocity law with the Iwasawa main conjecture in the next section. We present the initial reduction step in the slightly more general context of an abelian variety which is not necessarily CM. This initial reduction step is in principle well known [47, Ch. I. 2.3] and has an analogue for any motive over a number field (see for example [4, p. 85/86]).

Let A/F be an abelian variety over a number field F with dual abelian variety ${}^tA/F$ and denote by $\mathcal{A}/\mathcal{O}_F$, resp. ${}^t\mathcal{A}/\mathcal{O}_F$, the Néron model of A, resp. ${}^tA$. Let L be a number field so that there is given an embedding

$$\mathcal{O}_L \to \mathrm{End}_F(A).$$

This induces an embedding $\mathcal{O}_L \to \mathrm{End}_F({}^tA)$ by functoriality. We fix a prime number p and define

$$L_p := L \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \prod_{\mathfrak{p}|p} L_{\mathfrak{p}}; \quad \mathcal{O}_{L_p} := \mathcal{O}_L \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \prod_{\mathfrak{p}|p} \mathcal{O}_{L_{\mathfrak{p}}}$$

and

$$T := T_p({}^tA) \simeq H^1(A_{\bar{F}}, \mathbb{Z}_p(1)); \quad V := V_p({}^tA) := T_p({}^tA) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

where $T_p({}^tA)$ is the p-adic Tate module of ${}^tA$. Let S be a finite set of places of F containing all archimedean places, all places above p and all places of bad reduction. Then we may view T as a smooth sheaf of $\mathcal{O}_{L_p}$-modules on $\mathrm{Spec}(\mathcal{O}_{F,S})_{et}$ and we denote by $R\Gamma(\mathcal{O}_{F,S}, T)$ its étale cohomology. For each prime $v \mid p$ of F let

$$H^1(F_v, V) \xrightarrow{\exp_v^*} D^0_{dR}(V) \simeq H^0(A_{F_v}, \Omega_{A_{F_v}/F_v})$$

be the dual exponential map of the $\mathrm{Gal}(\bar{F}_v/F_v)$ -representation V [47, Ch. II, Thm. 1.4.1]. For any prime v of F denote by

$$P_v({}^tA/F, t) = \det_{L_l}(1 - \mathrm{Fr}_v^{-1} \cdot t | H^1({}^tA_{\bar{F}}, \mathbb{Q}_l)^{I_v}) \in \mathcal{O}_L[t]$$

the Euler factor of the L-equivariant Hasse-Weil L-function of ${}^tA/F$ (which is independent of the auxiliary prime $v \nmid l$) and let Φ_v be the component group of $\mathcal{A}$ at v. Denote by $|M|_{L_p}$ the part of the order ideal of a finite $\mathcal{O}_L$-module M supported in $\{\mathfrak{p} \mid p\}$.

Proposition 2.1. *With the notation just introduced the following hold.*

a) If $A(F)$ and $Ш(A/F)_{p^\infty}$ are finite then the composite map

$$H^1(\mathcal{O}_{F,S}, V) \to \prod_{v|p} H^1(F_v, V) \xrightarrow{\prod_{v|p} \exp_v^*} \prod_{v|p} H^0(A_{F_v}, \Omega_{A_{F_v}/F_v})$$

is an isomorphism, and $H^i(\mathcal{O}_{F,S}, V) = 0$ for $i \neq 1$. We obtain an induced isomorphism

$$\iota : \det_{L_p}^{-1} R\Gamma(\mathcal{O}_{F,S}, V) \simeq \det_{L_p} H^1(\mathcal{O}_{F,S}, V) \simeq \det_{L_p} H^0(A, \Omega_{A/F}) \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

b) Assume in addition that F has no real embedding or that $p > 2$. Then $R\Gamma(\mathcal{O}_{F,S}, T)$ is a perfect complex of $\mathcal{O}_{L_p}$-modules and

$$\begin{aligned} &\iota\left(\det^{-1}_{\mathcal{O}_{L_p}} R\Gamma(\mathcal{O}_{F,S}, T)\right) \\ &\quad = \frac{|Ш(A/F)|_{L_p}}{|A(F)|_{L_p} |{}^tA(F)|_{L_p}} \cdot \prod_v |\Phi_v|_{L_p} \cdot \prod_{v \in S} P_v({}^tA/F, Nv^{-1}) \cdot \Upsilon_p \end{aligned}$$

where $\Upsilon_p := \Upsilon \otimes_{\mathcal{O}_L} \mathcal{O}_{L_p}$,

$$\Upsilon := \det_{\mathcal{O}_L}\left(H^0(\mathcal{A}, \Omega_{\mathcal{A}/\mathcal{O}_F}) \otimes_{\mathcal{O}_F} \mathcal{D}_{F/\mathbb{Q}}^{-1}\right)$$

and $\mathcal{D}_{F/\mathbb{Q}}^{-1}$ *is the inverse different of the extension* $F/\mathbb{Q}$*.*

Proof. Consider the following diagram of complexes of $\mathcal{O}_{L_p}$-modules with exact rows and columns

$$\begin{tikzcd}
R\Gamma_c(\mathcal{O}_{F,S}, T) \arrow[r] \arrow[d, equal] & R\Gamma_f(F,T) \arrow[r] \arrow[d] & \bigoplus_{v\in S} R\Gamma_f(F_v, T) \arrow[d, "\oplus_v \alpha_v"] \\
R\Gamma_c(\mathcal{O}_{F,S}, T) \arrow[r] & R\Gamma(\mathcal{O}_{F,S}, T) \arrow[r] \arrow[d, "\beta"] & \bigoplus_{v\in S} R\Gamma(F_v, T) \arrow[d] \\
 & \bigoplus_{v\in S} R\Gamma_{/f}(F_v, T) \arrow[r, equal] & \bigoplus_{v\in S} R\Gamma_{/f}(F_v, T).
\end{tikzcd} \tag{4}$$

Here, following [2] we define

$$R\Gamma_f(F_v, T) = \begin{cases} {}^tA(F_v)^\wedge[-1] & v \nmid \infty \\ \tau^{\leq 1} R\Gamma(F_v, T) & v \mid \infty \end{cases}$$

where for any abelian group M we denote by

$$M^\wedge := \varprojlim_{\nu} M/p^\nu \tag{5}$$

its (underived) p-adic completion. Since $H^0(F_v, T) = 0$ for $v \nmid \infty$ there is a map of complexes

$$\alpha_v : {}^tA(F_v)^\wedge[-1] \xrightarrow{\tilde{\alpha}_v} H^1(F_v, T)[-1] \to R\Gamma(F_v, T)$$

where $\tilde{\alpha}_v$ is the inverse limit of the connecting homomorphisms

$${}^tA(F_v)/p^\nu \to H^1(F_v, {}^tA_{p^\nu})$$

induced by the Kummer sequence. The complex $R\Gamma_{/f}(F_v, T)$ is defined as the mapping cone of α_v and the complex $R\Gamma_f(F, T)$ as the mapping fibre of β.

Lemma 1. *We have*

$$H^i_f(F,T)\simeq\begin{cases} {}^tA(F)^\wedge & i=1\\ Ш({}^tA/F)^\wedge\oplus\mathrm{Hom}_{\mathbb{Z}_p}(A(F)^\wedge,\mathbb{Z}_p) & i=2\\ \mathrm{Hom}_{\mathbb{Z}_p}(A(F)^\wedge_{tor},\mathbb{Q}_p/\mathbb{Z}_p) & i=3\\ 0 & i\neq 1,2,3\end{cases}$$

Proof. First note that $R\Gamma_{/f}(F_v,T)$ is concentrated in degrees $1,2$ for $v\nmid\infty$ and there is an isomorphism

$$H^i(\mathcal{O}_{F,S},T)\simeq\bigoplus_{v\text{ real}}H^i(F_v,T)\simeq\bigoplus_{v\text{ real}}H^i_{/f}(F_v,T)$$

for $i\geq 3$ by [57, Prop. II.2.9, Thm. I.4.10]. It follows that $R\Gamma_f(F,T)$ is concentrated in degrees $0\leq i\leq 3$. The long exact sequence associated to the middle column in (4) gives

$$H^0_f(F,T)=H^0(\mathcal{O}_{F,S},T)=0$$

and

$$H^1_f(F,T)=\ker\left(H^1(\mathcal{O}_{F,S},T)\to\bigoplus_{v\in S}\frac{H^1(F_v,T)}{{}^tA(F_v)^\wedge}\right).$$

Recall that the classical Selmer group $\mathrm{Sel}(F,{}^tA_{p^\nu})$ can be defined as

$$\mathrm{Sel}(F,{}^tA_{p^\nu})=\ker\left(H^1(\mathcal{O}_{F,S},{}^tA_{p^\nu})\to\bigoplus_{v\in S}\frac{H^1(F_v,{}^tA_{p^\nu})}{{}^tA(F_v)/p^\nu}\right)$$

since the image of ${}^tA(F_v)/p^\nu$ in $H^1(F_v,{}^tA_{p^\nu})$ coincides with the unramified classes for $v\notin S$. Taking the inverse limit over ν in the short exact sequence

$$0\to{}^tA(F)/p^\nu\to\mathrm{Sel}(F,{}^tA_{p^\nu})\to Ш({}^tA/F)_{p^\nu}\to 0$$

and using finiteness of $Ш({}^tA/F)_{p^\infty}$ we find

$${}^tA(F)^\wedge\simeq\varprojlim_\nu\mathrm{Sel}(F,{}^tA_{p^\nu})\simeq H^1_f(F,T).$$

The long exact sequence associated to the top row in (4) gives an exact sequence

$$\bigoplus_{v\in S}H^1_f(F_v,T)\to H^2_c(\mathcal{O}_{F,S},T)\to H^2_f(F,T)\to 0$$

and an isomorphism

$$H^3_c(\mathcal{O}_{F,S},T)\simeq H^3_f(F,T).$$

Using Artin-Verdier duality [57, Cor. II.3.3] and the fact that our $R\Gamma_c$ agrees with that of loc. cit. (formed with Tate cohomology at the infinite places) in degrees ≥ 2 we find an exact sequence

$$0\to H^2_f(F,T)^*\to H^1(\mathcal{O}_{F,S},A_{p^\infty})\to\bigoplus_{v\in S}\frac{H^1(F_v,A_{p^\infty})}{A(F_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p}$$

and an isomorphism

$$H^3_f(F,T)^*\simeq H^0(\mathcal{O}_{F,S},A_{p^\infty}).$$

Here we use the definition

$$M^*:=\mathrm{Hom}_{\mathbb{Z}_p}(M,\mathbb{Q}_p/\mathbb{Z}_p),$$

the isomorphism of $\pi_1(\mathrm{Spec}(\mathcal{O}_{F,S}))$-modules

$$T^*(1)\simeq A_{p^\infty} \tag{6}$$

and the fact that the orthogonal complement of ${}^tA(F_v)^\wedge$ under the perfect pairing

$$H^1(F_v,T)\times H^1(F_v,A_{p^\infty})\to H^2(F_v,\mathbb{Q}_p/\mathbb{Z}_p(1))\simeq\mathbb{Q}_p/\mathbb{Z}_p$$

is $A(F_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p$ [57, Cor. I.3.4, Rem. I.3.5]. Hence we obtain an isomorphism

$$H^2_f(F,T)^*\simeq\mathrm{Sel}(F,A_{p^\infty}).$$

Dualizing again we find an exact sequence

$$0\to Ш(A/F)^*_{p^\infty}\to H^2_f(F,T)\to(A(F)^\wedge\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p)^*\to 0$$

and an isomorphism

$$H^3_f(F,T)\simeq(A(F)^\wedge_{tor})^*.$$

By [57, Thm. I.6.13] if $Ш(A/F)_{p^\infty}$ is finite there is a non-degenerate pairing

$$Ш({}^tA/F)^\wedge\times Ш(A/F)_{p^\infty}\to\mathbb{Q}_p/\mathbb{Z}_p$$

and for any $\mathbb{Z}_p$-module M there is an isomorphism

$$\begin{aligned} & \operatorname{Hom}_{\mathbb{Z}_p}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \\ \simeq & \operatorname{Hom}_{\mathbb{Z}_p}(M, \operatorname{Hom}_{\mathbb{Z}_p}(\mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p)) \\ \simeq & \operatorname{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p). \end{aligned} \tag{7}$$

Hence we find an exact sequence

$$0 \to Ш({}^tA/F)^\wedge \to H^2_f(F,T) \to \operatorname{Hom}_{\mathbb{Z}_p}(A(F)^\wedge, \mathbb{Z}_p) \to 0$$

concluding the proof of Lemma 1. □

Lemma 2. *We have*

$$H^i_{/f}(F_v,T) = \begin{cases} \operatorname{Hom}_{\mathbb{Z}_p}(A(F_v)^\wedge, \mathbb{Z}_p) & i=1, v \mid p \\ \operatorname{Hom}_{\mathbb{Z}_p}(A(F_v)^\wedge_{tor}, \mathbb{Q}_p/\mathbb{Z}_p) & i=2, v \nmid \infty \\ H^i(F_v,T) & i \geq 3, v \mid \infty \\ 0 & \textit{else.} \end{cases}$$

In particular, for $v \nmid \infty$ there is a quasi-isomorphism of complexes of $\mathcal{O}_{L_p}$-modules

$$R\Gamma_{/f}(F_v,T)[1] \simeq R\operatorname{Hom}_{\mathbb{Z}_p}(A(F_v)^\wedge, \mathbb{Z}_p). \tag{8}$$

Proof. The Kummer sequence

$$0 \to {}^tA(F_v)^\wedge \to H^1(F_v,T) \to \varprojlim_\nu H^1(F_v, {}^tA)_{p^\nu} \to 0$$

together with duality for abelian varieties over local fields [57, Cor. I.3.4] and (7)

$$\varprojlim_\nu H^1(F_v, {}^tA)_{p^\nu} \simeq \left(\varinjlim_\nu A(F_v)/p^\nu \right)^* \simeq \operatorname{Hom}_{\mathbb{Z}_p}(A(F_v)^\wedge, \mathbb{Z}_p)$$

give the Lemma for $i=1$. Note that these groups vanish unless $v \mid p$. The statement for $i=2$ follows from (6) and Tate local duality [57, Cor. I.2.3]

$$H^2_{/f}(F_v,T) \simeq H^2(F_v,T) \simeq H^0(F_v, A_{p^\infty})^* \simeq \left(A(F_v)^\wedge_{tor}\right)^*.$$

The statement for $i \geq 3$ is just the definition of $R\Gamma_{/f}(F_v,T)$. Note here that $H^i(F_v,T)=0$ for $i=2$ and $v \mid \infty$ and for $i \geq 3$ and $v \nmid \infty$. The isomorphism

(8) can be proved either via a version of Tate duality in the derived category, or by direct inspection since $\mathrm{Hom}_{\mathbb{Z}_p}(A(F_v)^\wedge_{tor}, \mathbb{Q}_p/\mathbb{Z}_p) \simeq \mathrm{Ext}^1_{\mathbb{Z}_p}(A(F_v)^\wedge, \mathbb{Z}_p)$, and since any bounded complex of $\mathcal{O}_{L_p}$-modules is quasi-isomorphic to the sum of its cohomology groups (placed in their respective degrees). □

For $v \mid p$ the dual exponential map

$$H^1_{/f}(F_v, V_p({}^tA)) \xrightarrow{\exp_v^*} H^0(A_{F_v}, \Omega_{A_{F_v}/F_v}) \tag{9}$$

is an isomorphism since its dual [47, Ch. II, Thm. 1.4.1]

$$\mathrm{Lie}(A_{F_v}) \xrightarrow{\exp_v} H^1_f(F_v, V_p(A)) \simeq A(F_v)^\wedge \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is an isomorphism. This is because the inverse $\log_v$ of $\exp_v$ (the formal group logarithm) induces an isomorphism

$$\log_v : \hat{\mathcal{A}}(\mathfrak{m}_v^n) \xrightarrow{\sim} \mathfrak{m}_v^n \mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}}) \tag{10}$$

for large enough n and

$$(\mathfrak{m}_v^n \mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}})) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \mathrm{Lie}(A_{F_v}); \quad \hat{\mathcal{A}}(\mathfrak{m}_v^n) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = A(F_v)^\wedge \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Here $\mathfrak{m}_v$ is the maximal ideal of $\mathcal{O}_{F_v}$ and $\hat{\mathcal{A}}$ is the formal completion of $\mathcal{A}_{\mathcal{O}_{F_v}}$ at the identity section. If now $A(F)$ and $Ш(A/F)_{p^\infty}$ are both finite then so are ${}^tA(F)$ and $Ш({}^tA/F)_{p^\infty}$ and it follows from Lemmas 1 and 2 that

$$R\Gamma_f(F, V) \simeq 0; \quad R\Gamma_{/f}(F_v, V) \simeq \begin{cases} H^1_{/f}(F_v, V)[-1] & v \mid p \\ 0 & \text{else.} \end{cases}$$

The middle vertical exact triangle in (4) then implies part a) of Prop. 2.1.

Lemma 3. *For $v \mid p$ let ι_v be the isomorphism*

$$\iota_v : \det{}^{-1}_{L_p} R\Gamma_{/f}(F_v, V) \simeq \det{}_{L_p} H^1_{/f}(F_v, V) \simeq \det{}_{L_p} H^0(A_{F_v}, \Omega_{A_{F_v}/F_v})$$

induced by the dual exponential map (9). For $v \nmid p\infty$ let

$$\iota_v : \det{}^{-1}_{L_p} R\Gamma_{/f}(F_v, V) \simeq L_p$$

be the isomorphism arising from acyclicity of $R\Gamma_{/f}(F_v, V)$. Then

$$\iota_v\left(\det{}^{-1}_{\mathcal{O}_{L_p}} R\Gamma_{/f}(F_v,T)\right) = |{}^t\Phi_v|_{L_p}\cdot P_v({}^tA/F, Nv^{-1})\cdot\Upsilon_v \tag{11}$$

where

$$\Upsilon_v := \begin{cases}\det_{\mathcal{O}_{L_p}}\left(H^0(\mathcal{A}_{\mathcal{O}_{F_v}},\Omega_{\mathcal{A}_{\mathcal{O}_{F_v}}/\mathcal{O}_{F_v}})\otimes_{\mathcal{O}_{F_v}}\mathcal{D}^{-1}_{F_v/\mathbb{Q}_p}\right) & v\mid p\\ \mathcal{O}_{L_p} & v\nmid p\end{cases}$$

and $\mathcal{D}^{-1}_{F_v/\mathbb{Q}_p}$ is the inverse different of the extension $F_v/\mathbb{Q}_p$.

Proof. Let $\mathcal{A}^0/\mathcal{O}_F$ be the open sub-group scheme of $\mathcal{A}/\mathcal{O}_F$ so that $\mathcal{A}^0_{\kappa_v}$ is the connected component of the identity of $\mathcal{A}_{\kappa_v}$ for each residue field κ_v of $\mathcal{O}_F$. We have a filtration of the group $A(F_v)=\mathcal{A}(\mathcal{O}_{F_v})$ given by exact sequences of $\mathcal{O}_L$-modules

$$0\to\mathcal{A}^0(\mathcal{O}_{F_v})\to A(F_v)\to\Phi_v\to 0$$

and

$$0\to\hat{\mathcal{A}}(\mathfrak{m}_v)\to\mathcal{A}^0(\mathcal{O}_{F_v})\to\mathcal{A}^0(\kappa_v)\to 0.$$

Since all these groups have bounded p-primary torsion, the p-adic completion functor (5) is exact and we obtain exact sequences of $\mathcal{O}_{L_p}$-modules

$$0\to\mathcal{A}^0(\mathcal{O}_{F_v})^\wedge\to A(F_v)^\wedge\to\Phi_v^\wedge\to 0 \tag{12}$$

and

$$0\to\hat{\mathcal{A}}(\mathfrak{m}_v)^\wedge\to\mathcal{A}^0(\mathcal{O}_{F_v})^\wedge\to\mathcal{A}^0(\kappa_v)^\wedge\to 0. \tag{13}$$

Lemma 4. *For any finite place v of F and any prime p there is an identity of fractional $\mathcal{O}_{L_p}$-ideals*

$$\frac{|\mathcal{A}^0(\kappa_v)^\wedge|_{L_p}}{|\operatorname{Lie}(\mathcal{A}_{\kappa_v})^\wedge|_{L_p}} = P_v({}^tA/F, Nv^{-1}). \tag{14}$$

Proof. The smooth, connected commutative group scheme $\mathcal{A}^0_{\kappa_v}$ over the perfect field κ_v has a filtration, preserved by any endomorphism,

$$0\to U\to\mathcal{A}^0_{\kappa_v}\to B\to 0 \tag{15}$$

where U is unipotent (and smooth and connected) and B is semiabelian (combine Chevalley's theorem [27] with [41, XVII Thm. 7.2.1]). We claim that

$$\frac{|U(\kappa_v)^\wedge|_{L_p}}{|\operatorname{Lie}(U)^\wedge|_{L_p}} = 1. \tag{16}$$

The group scheme U has a filtration with successive quotients $\mathbb{G}_a$ [41, XVII, Prop. 4.1.1]. The Lie algebra functor being exact for smooth group schemes, there is a corresponding filtration of $\operatorname{Lie}(U)$. Since $H^1(G_{\kappa_v}, U') = 0$ for any connected group scheme U'/κ_v there is also a corresponding filtration of $U(\kappa_v)$ with successive quotients $\mathbb{G}_a(\kappa_v) = \kappa_v$. So for $v \nmid p$ we have $U(\kappa_v)^\wedge = \operatorname{Lie}(U)^\wedge = 0$ and (16) holds. Since p annihilates $\mathbb{G}_a$ for $v \mid p$ some power p^ν annihilates U, and the action of $\mathcal{O}_L$ on U factors through the finite semilocal ring $\mathcal{O}_L/p^\nu$. The indecomposable idempotents $e_1, \dots, e_r$ of $\mathcal{O}_L/p^\nu$ act by algebraic endomorphisms on U, so have closed image e_iU and

$$U \simeq e_1U \times \cdots \times e_rU.$$

To prove (16) it suffices to show

$$\operatorname{length}_{e_i\mathcal{O}_L/p^\nu}(e_iU(\kappa_v)) = \operatorname{length}_{e_i\mathcal{O}_L/p^\nu}(\operatorname{Lie}(e_iU))$$

for $i = 1, \dots, r$. This follows from the fact that e_iU is itself unipotent, smooth, connected, hence has a filtration with subquotients $\mathbb{G}_a$ and $\mathbb{G}_a(\kappa_v) \simeq \kappa_v \simeq \operatorname{Lie}(\mathbb{G}_a)$.

By similar reasoning the filtration (15) induces corresponding filtrations on $\operatorname{Lie}(\mathcal{A}^0_{\kappa_v}) \simeq \operatorname{Lie}(\mathcal{A}_{\kappa_v})$ and on $\mathcal{A}^0(\kappa_v)$. It therefore suffices to show

$$\frac{|B(\kappa_v)^\wedge|_{L_p}}{|\operatorname{Lie}(B)^\wedge|_{L_p}} = P_v({}^tA/F, Nv^{-1}). \tag{17}$$

For $v \nmid p$ we have

$$\begin{aligned} P_v({}^tA/F, Nv^{-1}) &= \det_{L_p}(1 - \mathrm{Fr}_v^{-1} \cdot Nv^{-1} | H^1({}^tA_{\bar{F}}, \mathbb{Q}_p)^{I_v}) \\ &= \det_{L_p}(1 - \mathrm{Fr}_v^{-1} | H^1({}^tA_{\bar{F}}, \mathbb{Q}_p(1))^{I_v}) \\ &= \det_{L_p}(1 - \mathrm{Fr}_v^{-1} | V_p(A)^{I_v}) \\ &= \det_{L_p}(1 - \mathrm{Fr}_v^{-1} | V_p(B)) \end{aligned}$$

where the last identity is [42, IX, Prop. 2.2.5]. Moreover $\operatorname{Lie}(B)^\wedge = 0$ and

Fr_v acts invertibly on $T_p(B)$. The exact sequence[1] of $\mathcal{O}_{L_p}$-modules

$$0 \to T_p(B) \xrightarrow{\mathrm{Fr}_v - 1} T_p(B) \to B(\kappa_v)^\wedge \to 0$$

then shows that

$$|B(\kappa_v)^\wedge|_{L_p} = \det_{L_p}(\mathrm{Fr}_v - 1|V_p(B)) \sim_{\mathcal{O}_{L_p}^\times} \det_{L_p}(1 - \mathrm{Fr}_v^{-1}|V_p(B))$$

verifying (17).

For $v \mid p$ let $D(B)$ be the covariant Dieudonné module of the p-divisible group $B[p^\infty]$ associated to B/κ_v [15, Thm. 4.33]. This is a free $W(\kappa_v)$-module so that

$$\begin{aligned}
&P_v({}^tA/F, Nv^{-1})\\
=&\det_{L_p\otimes W(\kappa_v)}(1 - \mathrm{Fr}_v^{-1}|D(B)_{\mathbb{Q}})\\
=&\det_{L_p\otimes W(\kappa_v)}(\mathrm{Fr}_v - 1|D(B)_{\mathbb{Q}}) \cdot \det_{L_p\otimes W(\kappa_v)}(\mathrm{Fr}_v|D(B)_{\mathbb{Q}})^{-1}\\
=&\det_{L_p\otimes W(\kappa_v)}(V^{[\kappa_v:\mathbb{F}_p]} - 1|D(B)_{\mathbb{Q}}) \cdot \det_{L_p\otimes W(\kappa_v)}(V^{[\kappa_v:\mathbb{F}_p]}|D(B)_{\mathbb{Q}})^{-1}
\end{aligned}$$

where V denotes the Verschiebung on $D(B)$ and the last identity is [15, Rem. 10.25].

Lemma 5. *There is an exact sequence of $\mathcal{O}_{L_p} \otimes W(\kappa_v)$-modules*

$$0 \to D(B) \xrightarrow{V^{[\kappa_v:\mathbb{F}_p]}-1} D(B) \to B(\kappa_v)^\wedge \otimes_{\mathbb{Z}_p} W(\kappa_v) \to 0$$

[1] It arises as follows. The snake lemma applied to

$$\begin{tikzcd}
0 \arrow[r] & B(\kappa_v) \arrow[r] \arrow[d, "p^n"] & B(\overline{\kappa}_v) \arrow[r, "\mathrm{Fr}_v - 1"] \arrow[d, "p^n"] & B(\overline{\kappa}_v) \arrow[r] \arrow[d, "p^n"] & 0 \\
0 \arrow[r] & B(\kappa_v) \arrow[r] & B(\overline{\kappa}_v) \arrow[r, "\mathrm{Fr}_v - 1"] & B(\overline{\kappa}_v) \arrow[r] & 0
\end{tikzcd} \tag{18}$$

gives an exact sequence of finite $\mathcal{O}_{L_p}$-modules

$$0 \to B(\kappa_v)[p^n] \to B(\overline{\kappa}_v)[p^n] \xrightarrow{\mathrm{Fr}_v - 1} B(\overline{\kappa}_v)[p^n] \to B(\kappa_v)/p^n \to 0$$

to which one applies the projective limit over n (an exact functor in this case).

Proof. The kernel of the isogeny $B[p^\infty] \xrightarrow{\mathrm{Fr}_v - 1} B[p^\infty]$ of p-divisible groups over κ_v is the constant finite flat group scheme over κ_v associated to the finite abelian p-group $B(\kappa_v)[p^\infty] \simeq B(\kappa_v)^\wedge$. The covariant Dieudonné module $D(B(\kappa_v)^\wedge) \simeq B(\kappa_v)^\wedge \otimes_{\mathbb{Z}_p} W(\kappa_v)$ of $B(\kappa_v)^\wedge$ sits in an exact sequence

$$0 \to B(\kappa_v)^\wedge \otimes_{\mathbb{Z}_p} W(\kappa_v) \to D(B) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\mathrm{Fr}_v - 1} D(B) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

by [15, Prop. 4.53 (ii)]. Multiplication by p^n gives a diagram analogous to (18) and one proceeds as in the case $v \nmid p$. The identity $\mathrm{Fr}_v = V^{[\kappa_v:\mathbb{F}_p]}$ is again [15, Rem. 10.25]. □

Lemma 5 shows that

$$\begin{aligned} &\det_{L_p \otimes W(\kappa_v)}(V^{[\kappa_v:\mathbb{F}_p]} - 1 | D(B)_{\mathbb{Q}}) \\ =&|B(\kappa_v)^\wedge \otimes_{\mathbb{Z}_p} W(\kappa_v)|_{\mathcal{O}_{L_p} \otimes W(\kappa_v)} = |B(\kappa_v)^\wedge|_{\mathcal{O}_{L_p}}. \end{aligned}$$

Similarly, the exact sequence of $\mathcal{O}_{L_p}$-modules [15, Thm. 4.33 (3)]

$$0 \to D(B) \xrightarrow{V} D(B) \to \mathrm{Lie}(B) \to 0$$

shows

$$\det_{L_p \otimes W(\kappa_v)}(V^{[\kappa_v:\mathbb{F}_p]} | D(B)_{\mathbb{Q}}) \sim_{(\mathcal{O}_{L_p} \otimes W(\kappa_v))^\times} \det_{L_p}(V | D(B)_{\mathbb{Q}}) = |\,\mathrm{Lie}(B)|_{\mathcal{O}_{L_p}}$$

proving (17). □

For a perfect complex of $\mathbb{Z}_p$-modules put

$$M^\dagger := R\,\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p).$$

If M is a finite $\mathcal{O}_{L_p}$-module we have

$$\det_{\mathcal{O}_{L_p}}(M^\dagger) = \det_{\mathcal{O}_{L_p}}(M^*[-1]) = |M^*|_{L_p} \cdot \mathcal{O}_{L_p} \subset \det_{L_p}(0) = L_p.$$

For $v \mid p$ the isomorphism (10) together with the isomorphisms

$$\hat{\mathcal{A}}(\mathfrak{m}_v^i)/\hat{\mathcal{A}}(\mathfrak{m}_v^{i+1}) \xrightarrow{\sim} \mathfrak{m}_v^i \mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}})/\mathfrak{m}_v^{i+1}\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}})$$

for $i = 1, \ldots, n-1$ give an equality

(19) $$\iota_v\left(\det_{\mathcal{O}_{L_p}}(\hat{\mathcal{A}}(\mathfrak{m}_v))\right)$$

$$
\begin{aligned}
&= \iota_v\left(\det_{\mathcal{O}_{L_p}}(\mathfrak{m}_v\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}}))\right)\\
&= \iota_v\left(\det_{\mathcal{O}_{L_p}}(\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}}))\right)\cdot|\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}})\otimes_{\mathcal{O}_{F_v}}\kappa_v|_{L_p}^{-1}\\
&= \iota_v\left(\det_{\mathcal{O}_{L_p}}(\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}}))\right)\cdot|\,\mathrm{Lie}(\mathcal{A}_{\kappa_v})|_{L_p}^{-1}\\
&\overset{(14)}{=} \iota_v\left(\det_{\mathcal{O}_{L_p}}(\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}}))\right)\cdot|\mathcal{A}^0(\kappa_v)^\wedge|_{L_p}^{-1}\cdot P_v({}^tA/F,Nv^{-1}).
\end{aligned}
$$

For $v\nmid p$ we have $\hat{\mathcal{A}}(\mathfrak{m}_v)^\wedge=0$. Hence

$$
\begin{aligned}
&\iota_v\left(\det^{-1}_{\mathcal{O}_{L_p}}R\Gamma_{/f}(F_v,T)\right)\\
\overset{(8)}{=}&\iota_v\left(\det_{\mathcal{O}_{L_p}}(A(F_v)^{\wedge,\dagger})\right)\\
\overset{(12)}{=}&\iota_v\left(\det_{\mathcal{O}_{L_p}}(\mathcal{A}^0(\mathcal{O}_{F_v})^{\wedge,\dagger})\right)\cdot|\Phi_v^{\wedge,*}|_{L_p}\\
\overset{(13)}{=}&\iota_v\left(\det_{\mathcal{O}_{L_p}}(\hat{\mathcal{A}}(\mathfrak{m}_v)^{\wedge,\dagger})\right)\cdot|\mathcal{A}^0(\kappa_v)^{\wedge,*}|_{L_p}\cdot|\Phi_v^{\wedge,*}|_{L_p}\\
\overset{(19)}{=}&\begin{cases}\iota_v\left(\det_{\mathcal{O}_{L_p}}(\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}})^{\dagger})\right)\cdot P_v({}^tA/F,Nv^{-1})\cdot|{}^t\Phi_v|_{L_p} & v\mid p\\ P_v({}^tA/F,Nv^{-1})\cdot|{}^t\Phi_v|_{L_p} & v\nmid p.\end{cases}
\end{aligned}
$$

Here we have used the perfect perfect pairing of finite groups [42, IX, 1.3.1]

$$
{}^t\Phi_v\times\Phi_v\to\mathbb{Q}/\mathbb{Z}. \tag{20}
$$

The proof of Lemma 3 is now completed by the following isomorphisms

$$
\begin{aligned}
\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}})^{\dagger}&\simeq\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}})\otimes_{\mathcal{O}_{F_v}}\mathcal{O}_{F_v},\mathbb{Z}_p)\\
&\simeq\mathrm{Hom}_{\mathcal{O}_{F_v}}(\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}}),\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{O}_{F_v},\mathbb{Z}_p))\\
&\simeq\mathrm{Hom}_{\mathcal{O}_{F_v}}(\mathrm{Lie}(\mathcal{A}_{\mathcal{O}_{F_v}}),\mathcal{O}_{F_v})\otimes_{\mathcal{O}_{F_v}}\mathcal{D}^{-1}_{F_v/\mathbb{Q}_p}\\
&\simeq H^0(\mathcal{A}_{\mathcal{O}_{F_v}},\Omega_{\mathcal{A}_{\mathcal{O}_{F_v}}/\mathcal{O}_{F_v}})\otimes_{\mathcal{O}_{F_v}}\mathcal{D}^{-1}_{F_v/\mathbb{Q}_p}.
\end{aligned}
$$

□

We complete the proof of part b) of Prop. 2.1. The middle vertical exact triangle in (4) and Lemmas 1 and 3 give

$$
\begin{aligned}
&\iota\left(\det^{-1}_{\mathcal{O}_{L_p}}R\Gamma(\mathcal{O}_{F,S},T)\right)\\
=&\iota\left(\det^{-1}_{\mathcal{O}_{L_p}}R\Gamma_f(F,T)\otimes\bigotimes_{v\in S}\det^{-1}_{\mathcal{O}_{L_p}}R\Gamma_{/f}(F_v,T)\right)
\end{aligned}
$$

$$=\frac{|\text{Ш}({}^tA/F)|_{L_p}}{|A(F)|_{L_p}|{}^tA(F)|_{L_p}}\cdot\prod_v|{}^t\Phi_v|_{L_p}\cdot\prod_{v\in S}P_v({}^tA/F,Nv^{-1})\cdot\Upsilon_p$$

using the isomorphism

$$\begin{aligned}H^0(\mathcal{A},\Omega_{\mathcal{A}/\mathcal{O}_F})\otimes_{\mathcal{O}_F}\mathcal{D}_{F/\mathbb{Q}}^{-1}\otimes_{\mathbb{Z}}\mathbb{Z}_p &\simeq\prod_{v|p}H^0(\mathcal{A},\Omega_{\mathcal{A}/\mathcal{O}_F})\otimes_{\mathcal{O}_F}\mathcal{D}_{F/\mathbb{Q}}^{-1}\otimes_{\mathcal{O}_F}\mathcal{O}_{F_v}\\ &\simeq\prod_{v|p}H^0(\mathcal{A}_{\mathcal{O}_{F_v}},\Omega_{\mathcal{A}_{\mathcal{O}_{F_v}}/\mathcal{O}_{F_v}})\otimes_{\mathcal{O}_{F_v}}\mathcal{D}_{F_v/\mathbb{Q}_p}^{-1}.\end{aligned}$$

Since $\text{Ш}({}^tA/F)$ and $\text{Ш}(A/F)$, resp. ${}^t\Phi_v$ and Φ_v, are dual finite abelian groups with dual $\mathcal{O}_L$-action we have in fact

$$|\text{Ш}({}^tA/F)|_{L_p}=|\text{Ш}(A/F)|_{L_p};\quad|{}^t\Phi_v|_{L_p}=|\Phi_v|_{L_p}$$

concluding the proof of b). □

For an abelian variety A/F with multiplications by $\mathcal{O}_L\to\text{End}_F(A)$ and each place $v\mid\infty$ of F consider the $\mathbb{Q}$-bilinear L-balanced integration pairing

$$H_1(A(F_v),\mathbb{Q})\times H^0(A,\Omega_{A/F})\otimes_F F_v\to F_v\xrightarrow{\text{tr}_{F_v/\mathbb{R}}}\mathbb{R};\quad(\gamma,\omega)\mapsto\text{tr}_{F_v/\mathbb{R}}\int_\gamma\omega$$

which induces $L_{\mathbb{R}}$-linear isomorphisms

$$\text{per}_v:H^0(A,\Omega_{A/F})\otimes_F F_v\xrightarrow{\sim}\text{Hom}_{\mathbb{Q}}(H_1(A(F_v),\mathbb{Q}),\mathbb{R})\xrightarrow{\sim}H^1(A(F_v),\mathbb{R}).$$

These isomorphisms combine to give a $L_{\mathbb{R}}$-linear (Deligne) period isomorphism

$$\text{per}_A:H^0(A,\Omega_{A/F})_{\mathbb{R}}\simeq\prod_{v|\infty}H^1(A(F_v),\mathbb{R}).\tag{21}$$

Definition 1. *For the invertible $\mathcal{O}_L$-module*

$$\Upsilon:=\det_{\mathcal{O}_L}\left(H^0(\mathcal{A},\Omega_{\mathcal{A}/\mathcal{O}_F})\otimes_{\mathcal{O}_F}\mathcal{D}_{F/\mathbb{Q}}^{-1}\right)$$

introduced in Prop. 2.1 choose a period $\Omega\in L_{\mathbb{R}}^\times$ and a fractional $\mathcal{O}_L$-ideal $\mathfrak{a}(\Omega)\subset L$ so that

$$\det_{L_{\mathbb{R}}}(\text{per}_A)(\Upsilon)=\Omega\cdot\mathfrak{a}(\Omega)\cdot\det_{\mathcal{O}_L}\left(\prod_{v|\infty}H^1(A(F_v),\mathbb{Z})\right)\tag{22}$$

under the determinant of the period isomorphism (21).

Let A/F be a CM abelian variety together with an isomorphism

$$\mu : \mathcal{O}_L \simeq \mathrm{End}_F(A)$$

for a CM field L with $[L : \mathbb{Q}] = 2\dim(A)$. To the CM abelian variety A/F is attached a Serre-Tate character [71, Thm. 10]

$$\varphi : \mathbb{A}_F^\times \to L^\times, \quad \varphi|_{F^\times} = F^\times \xrightarrow{t} L^\times$$

from which a Hecke character

$$\varphi_\tau : \mathbb{A}_F^\times/F^\times \xrightarrow{\varphi\cdot(t_{\mathbb{R}}^{-1}\cdot p_\infty)} L_{\mathbb{R}}^\times \xrightarrow{\tau} \mathbb{C}^\times \tag{23}$$

is deduced for each $\tau \in \mathrm{Hom}(L, \mathbb{C})$. Here p_∞ is the projection to $F_{\mathbb{R}}^\times$ and t is an algebraic homomorphism determined by the CM-type of A/F. We have the $L_{\mathbb{C}}$-valued L-function

$$L(\varphi, s) := (L(\varphi_\tau, s))_\tau \in \prod_\tau \mathbb{C} \simeq L_{\mathbb{C}}$$

which takes values in $L_{\mathbb{R}}$ for real s. If

$$\mu' : \mathcal{O}_L \simeq \mathrm{End}_F({}^tA)$$

denotes the isomorphism functorially induced by μ then a polarization $p : A \to {}^tA$ induces an isomorphism

$$(A, \rho \circ \mu) \simeq ({}^tA, \mu')$$

of abelian varieties with CM by L (up to isogeny). Here ρ denotes the Rosati involution associated to p. Since ρ induces complex conjugation on L the Serre-Tate character of $({}^tA, \mu')$ is $\bar{\varphi}$.

Proposition 2.2. *Let A/F be a CM abelian variety so that*

$$\mathcal{O}_L \xrightarrow{\sim} \mathrm{End}_F(A)$$

for a CM field L with $[L : \mathbb{Q}] = 2\dim(A)$ and assume

$$L(\bar{\varphi}, 1) \neq 0.$$

Let p be any prime number, $T = T_p({}^tA)$, $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and S a finite set of places of F containing $\{v \mid p\infty\}$ and all places of bad reduction. Assume that $Ш(A/F)_{p^\infty}$ and $A(F)$ are finite and let

$$\iota : \det_{L_p}^{-1} R\Gamma(\mathcal{O}_{F,S}, V) \simeq \det_{L_p} H^1(\mathcal{O}_{F,S}, V) \simeq \det_{L_p} H^0(A, \Omega_{A/F}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$$

be the isomorphism of Prop. 2.1. Assume there exists

$$z \in \det_{L_p} H^1(\mathcal{O}_{F,S}, V)$$

and a fractional $\mathcal{O}_L$-ideal $\mathfrak{a}(z)$ prime to p with the following properties

a) $\mathcal{O}_{L_p} \cdot z = \det_{\mathcal{O}_{L_p}}^{-1} R\Gamma(\mathcal{O}_{F,S}, T)$
b) $\iota(z) \in \det_L H^0(A, \Omega_{A/F}) \subset \det_{L_p} \left(H^0(A, \Omega_{A/F}) \otimes_{\mathbb{Q}} \mathbb{Q}_p\right)$
c) $\mathcal{O}_L \cdot \det_{L_{\mathbb{R}}}(\mathrm{per}_A)(\iota(z)) = L_S(\bar{\varphi}, 1) \cdot \mathfrak{a}(z) \cdot \det_{\mathcal{O}_L}\Big(\prod_{v\mid\infty} H^1(A(F_v), \mathbb{Z})\Big)$

Then $\frac{L(\bar{\varphi},1)}{\Omega} \in L^\times$ and

$$\frac{L(\bar{\varphi}, 1)}{\Omega} = \frac{|Ш(A/F)|_{L_p}}{|A(F)|_{L_p} |{}^tA(F)|_{L_p}} \cdot \prod_v |\Phi_v|_{L_p} \cdot \mathfrak{a}(\Omega)$$

in the group of fractional $\mathcal{O}_L$-ideals supported in $\{\mathfrak{p} \mid p\}$.

Proof. First note that

$$\begin{aligned} P_v({}^tA/F, t) &= \det_{L_l}(1 - \mathrm{Fr}_v^{-1} \cdot t | H^1({}^tA_{\bar{F}}, \mathbb{Q}_l)^{I_v}) \\ &= \det_{L_l}(1 - \mathrm{Fr}_v \cdot t | V_l({}^tA)_{I_v}) \\ &= 1 - \overline{\varphi(v)} \cdot t \end{aligned}$$

and the L-equivariant L-function of ${}^tA/F$ agrees with $L(\bar{\varphi}, s)$. Also note that F is totally imaginary (since the action of $\mathcal{O}_L$ is defined over F) and hence Prop. 2.1 applies for all primes p. By Prop. 2.1 and a) we have

$$\begin{aligned} \mathcal{O}_{L_p} \cdot \iota(z) &= \iota\left(\det_{\mathcal{O}_{L_p}}^{-1} R\Gamma(\mathcal{O}_{F,S}, T)\right) \\ &= \frac{|Ш(A/F)|_{L_p}}{|A(F)|_{L_p} |{}^tA(F)|_{L_p}} \cdot \prod_v |\Phi_v|_{L_p} \cdot \prod_{v\in S} P_v({}^tA/F, Nv^{-1}) \cdot \Upsilon_p \\ &= \frac{|Ш(A/F)|_{L_p}}{|A(F)|_{L_p} |{}^tA(F)|_{L_p}} \cdot \prod_v |\Phi_v|_{L_p} \cdot \prod_{v\in S} \left(1 - \frac{\overline{\varphi(v)}}{Nv}\right) \cdot \Upsilon_p \end{aligned}$$

and by the definition (22) of Ω and $\mathfrak{a}(\Omega)$ we have

$$\mathcal{O}_{L_p}\cdot\det_{L_{\mathbb{R}}}(\mathrm{per}_{\mathrm{A}})(\iota(z))=\frac{|\text{Ш}(A/F)|_{L_p}}{|A(F)|_{L_p}|{}^tA(F)|_{L_p}}\cdot\prod_v|\Phi_v|_{L_p}\cdot\prod_{v\in S}\left(1-\frac{\overline{\varphi(v)}}{Nv}\right)$$
$$\cdot\,\Omega\cdot\mathfrak{a}(\Omega)\cdot\det_{\mathcal{O}_L}\left(\prod_{v|\infty}H^1(A(F_v),\mathbb{Z})\right).$$

Comparing this identity with c) we find

$$L_S(\bar{\varphi},1)=\frac{|\text{Ш}(A/F)|_{L_p}}{|A(F)|_{L_p}|{}^tA(F)|_{L_p}}\cdot\prod_v|\Phi_v|_{L_p}\cdot\prod_{v\in S}\left(1-\frac{\overline{\varphi(v)}}{Nv}\right)\cdot\Omega\cdot\mathfrak{a}(\Omega)$$

up to a fractional $\mathcal{O}_L$-ideal $\mathfrak{a}(z)$ prime to p. This is the statement of Proposition 2.2. □

Let now E/F be an elliptic curve over a number field F with complex multiplication by $\mathcal{O}_K$ for an imaginary quadratic field K. The period $\Omega\in K_{\mathbb{R}}^\times$ and the fractional ideal $\mathfrak{a}(\Omega)\subseteq K$ defined in the introduction satisfy

$$\bigotimes_{v|\infty}H_1(E(F_v),\mathbb{Z})=\Omega\cdot\mathfrak{a}(\Omega)\cdot\det_{\mathcal{O}_K}\mathrm{Hom}_{\mathcal{O}_F}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F}),\mathcal{O}_F)$$

under the determinant over $K_{\mathbb{R}}$ of the isomorphism

$$\prod_{v|\infty}H_1(E(F_v),\mathbb{Q})_{\mathbb{R}}\cong\mathrm{Hom}_F(H^0(E,\Omega_{E/F}),F)_{\mathbb{R}}$$

which is the $\mathbb{R}$-dual of per_E defined in (21). Since

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Z}}(H^1(E(F_v),\mathbb{Z}),\mathbb{Z})&\simeq H_1(E(F_v),\mathbb{Z})\\ \mathrm{Hom}_{\mathbb{Z}}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F})\otimes_{\mathcal{O}_F}\mathcal{D}_{F/\mathbb{Q}}^{-1},\mathbb{Z})&\simeq\mathrm{Hom}_{\mathcal{O}_F}(H^0(\mathcal{E},\Omega_{\mathcal{E}/\mathcal{O}_F}),\mathcal{O}_F)\end{aligned}$$

the quantities Ω and $\mathfrak{a}(\Omega)$ defined in the introduction coincide with the period and ideal defined in Def. 1.

Proposition 2.3. *Let E/F be an elliptic curve with CM by $\mathcal{O}_K$ and associated Serre-Tate character $\psi:\mathbb{A}_F^\times\to K^\times$. Assume that*

$$L(\bar{\psi},1)\neq 0.$$

Let p be any prime number, $T = T_p({}^tE)$, $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and S a finite set of places of F containing $\{v \mid p\infty\}$ and all places of bad reduction. Assume that $\text{Ш}(E/F)_{p^\infty}$ and $E(F)$ are finite and let

$$\iota : \det_{K_p}^{-1} R\Gamma(\mathcal{O}_{F,S}, V) \simeq \det_{K_p} H^1(\mathcal{O}_{F,S}, V) \simeq \det_{K_p}(H^0(E, \Omega_{E/F}) \otimes_{\mathbb{Q}} \mathbb{Q}_p)$$

be the isomorphism of Prop. 2.1. Assume there exists

$$z \in \det_{K_p} H^1(\mathcal{O}_{F,S}, V)$$

and a fractional $\mathcal{O}_K$-ideal $\mathfrak{a}(z)$ prime to p with the following properties

a) $\mathcal{O}_{K_p} \cdot z = \det_{\mathcal{O}_{K_p}}^{-1} R\Gamma(\mathcal{O}_{F,S}, T)$

b) $\iota(z) \in \det_K H^0(E, \Omega_{E/F}) \subset \det_{K_p}\big(H^0(E, \Omega_{E/F}) \otimes_{\mathbb{Q}} \mathbb{Q}_p\big)$

c) $\mathcal{O}_K \cdot \det_{K_\mathbb{R}}(\mathrm{per}_E)(\iota(z)) = L_S(\bar{\psi}, 1) \cdot \mathfrak{a}(z) \cdot \det_{\mathcal{O}_K}\Big(\prod_{v \mid \infty} H^1(E(F_v), \mathbb{Z})\Big)$

Then $\frac{L(\bar{\psi},1)}{\Omega} \in K^\times$ and

$$\frac{L(\bar{\psi}, 1)}{\Omega} = \frac{|\text{Ш}(E/F)|_{K_p}}{|E(F)|} \cdot \prod_v |\Phi_v|_{K_p} \cdot \mathfrak{a}(\Omega)$$

in the group of fractional $\mathcal{O}_K$-ideals supported in $\{\mathfrak{p} \mid p\}$.

Proof. This is the special case of Prop. 2.2 where $A/F = E/F$ is an elliptic curve and $L = K$, noting that

$$|E(F)|_K \cdot |{}^tE(F)|_K = |E(F)|_K \cdot \overline{|E(F)|}_K = |E(F)|. \qquad \square$$

3. Kato's reciprocity law

In this section we recall some definitions and results of [48, §15] for which we need to introduce quite a bit of notation. Let K be an imaginary quadratic field and fix an embedding $K \subset \mathbb{C}$. We identify $\bar{K} = \bar{\mathbb{Q}}$ with the algebraic closure of K in $\mathbb{C}$.

3.1. Iwasawa modules

For any ideal $\mathfrak{f}$ of $\mathcal{O}_K$ we denote by

$$K(\mathfrak{f}) \subseteq \bar{K}$$

the ray class field of conductor $\mathfrak{f}$. For any prime number p and ideal $\mathfrak{f}$ of $\mathcal{O}_K$ we set

$$K(p^\infty\mathfrak{f}) = \bigcup_n K(p^n\mathfrak{f}); \qquad G_{p^\infty\mathfrak{f}} := \mathrm{Gal}(K(p^\infty\mathfrak{f})/K).$$

Then

$$G_{p^\infty\mathfrak{f}} \cong \Gamma \times \Delta; \quad \Gamma \simeq \mathbb{Z}_p \times \mathbb{Z}_p \tag{24}$$

where $\Delta := G_{p^\infty\mathfrak{f}}^{tor}$ is a finite abelian group. Put

$$\Lambda := \mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty\mathfrak{f})/K)]] \simeq \mathbb{Z}_p[\Delta][[T_1, T_2]].$$

Consider the complex of Λ-modules

$$R\Gamma_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) := \varprojlim_{K'} R\Gamma(\mathcal{O}_{K'}[\frac{1}{p}], \mathbb{Z}_p(1))$$

where K' runs through the finite extensions of K contained in $K(p^\infty\mathfrak{f})$. According to [48, 15.6] the cohomology groups of $H^i_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1))$ are finitely generated Λ-modules and vanish for $i \neq 1, 2$.

3.2. Elliptic units

In [48, 15.5] there is defined an elliptic unit

$$_{\mathfrak{a}}z_{\mathfrak{f}} \in \mathcal{O}_{K(\mathfrak{f})}[1/\mathfrak{f}]^\times \tag{25}$$

for ideals $\mathfrak{a}, \mathfrak{f}$ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f})^\times$ is injective and $(\mathfrak{a}, 6\mathfrak{f}) = 1$. If $\mathfrak{f}$ is not a power of a prime ideal then $_{\mathfrak{a}}z_{\mathfrak{f}} \in \mathcal{O}_{K(\mathfrak{f})}^\times$. The units $_{\mathfrak{a}}z_{\mathfrak{f}}$ are norm compatible; in particular for any prime number p, any $n \geq 1$ and any nonzero ideal $\mathfrak{f}$ (such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/p^n\mathfrak{f})^\times$ is injective) one has

$$N_{K(p^{n+1}\mathfrak{f})/K(p^n\mathfrak{f})}({}_{\mathfrak{a}}z_{p^{n+1}\mathfrak{f}}) = {}_{\mathfrak{a}}z_{p^n\mathfrak{f}}.$$

Denoting by $(\mathfrak{a}, F/K) \in \mathrm{Gal}(F/K)$ the Artin symbol, we have in particular an element

$$\sigma_{\mathfrak{a}} := (\mathfrak{a}, K(p^\infty\mathfrak{f})/K) \in G_{p^\infty\mathfrak{f}} \subset \Lambda^\times.$$

Define

$$z_{p^\infty\mathfrak{f}} := (N\mathfrak{a} - \sigma_{\mathfrak{a}})^{-1} \, ({}_{\mathfrak{a}}z_{p^n\mathfrak{f}})_{n\geq 1}$$

$$\in \left(\varprojlim_{K'} \mathcal{O}_{K'}[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \right) \otimes_\Lambda Q(\Lambda) \simeq H^1_{p^\infty \mathfrak{f}}(\mathbb{Z}_p(1)) \otimes_\Lambda Q(\Lambda)$$

which is independent of $\mathfrak{a}$.

3.3. Hecke characters

Let

$$\varphi : \mathbb{A}_K^\times \to L^\times$$

be an algebraic Hecke character of K with values in the number field L and of infinity type $(-1, 0)$. Following [48, 15.8] we recall the definition of the motivic structure associated to φ. This consists of rank one L-vector spaces $V_L(\varphi)$ and $S(\varphi)$, a continuous $L_\mathfrak{p}$-linear $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$-representation $V_{L_\mathfrak{p}}(\varphi)$ for each place $\mathfrak{p} \mid p$ of L together with a (Deligne) period isomorphism

$$\mathrm{per}_\tau : S(\varphi) \otimes_{L,\tau} \mathbb{C} \xrightarrow{\simeq} V_L(\varphi) \otimes_{L,\tau} \mathbb{C}$$

for each embedding $\tau : L \to \mathbb{C}$ and comparison isomorphisms

$$V_{L_\mathfrak{p}}(\varphi) \simeq V_L(\varphi) \otimes_L L_\mathfrak{p} \tag{26}$$

as well as p-adic (Deligne) period isomorphisms

$$D^1_{dR}(K_p, V_{L_\mathfrak{p}}(\varphi)) \simeq S(\varphi) \otimes_L L_\mathfrak{p} \tag{27}$$

for each $\mathfrak{p} \mid p$.

Let $\mathfrak{f}$ be a multiple of the conductor of φ such that $\mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{f})^\times$ is injective, and let $E = (E, \alpha)$ be the canonical CM-pair over $K(\mathfrak{f})$ in the sense of [48, (15.3.1)], i.e. $E/K(\mathfrak{f})$ is an elliptic curve with CM by $\mathcal{O}_K$ and $\alpha \in E(K(\mathfrak{f}))$ is a torsion point with annihilator $\mathfrak{f}$. As explained in [48, (15.3.3)] if $\mathfrak{a}$ is an ideal prime to $\mathfrak{f}$ with Artin symbol $\sigma = (\mathfrak{a}, K(\mathfrak{f})/K) \in \mathrm{Gal}(K(\mathfrak{f})/K)$ there is a canonical isomorphism

$$\eta_\mathfrak{a} : (E/E[\mathfrak{a}], \alpha \bmod E[\mathfrak{a}]) \simeq (E^{(\sigma)}, \sigma(\alpha)).$$

We denote by $\eta_\mathfrak{a}^*$ the map induced on cohomology by the composite isogeny $E \to E/E[\mathfrak{a}] \xrightarrow{\eta_\mathfrak{a}} E^{(\sigma)}$. We then define

$$\begin{aligned} V_L(\varphi) &:= H^1(E(\mathbb{C}), \mathbb{Q}) \otimes_K L \\ S(\varphi) &:= (H^0(E, \Omega_{E/K(\mathfrak{f})}) \otimes_K L)^{\mathrm{Gal}(K(\mathfrak{f})/K)} \end{aligned}$$

where $\sigma \in \mathrm{Gal}(K(\mathfrak{f})/K)$ acts as the composite

$$H^0(E, \Omega_{E/K(\mathfrak{f})}) \underset{K}{\otimes} L \xrightarrow{\sigma\otimes 1} H^0(E^{(\sigma)}, \Omega_{E^{(\sigma)}/K(\mathfrak{f})}) \underset{K}{\otimes} L$$
$$\xrightarrow[\simeq]{\varphi(\mathfrak{a})^{-1}\eta_{\mathfrak{a}}^*} H^0(E, \Omega_{E/K(\mathfrak{f})}) \underset{K}{\otimes} L.$$

For each place $\mathsf{p} \mid p$ of L we define a $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$-representation

$$V_{L_{\mathsf{p}}}(\varphi) := H^1_{et}(E \otimes_{K(\mathfrak{f})} \bar{\mathbb{Q}}, \mathbb{Q}_p) \otimes_{K_p} L_{\mathsf{p}}$$

where $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$ acts via

$$V_{L_{\mathsf{p}}}(\varphi) = H^1_{et}(E \otimes_{K(\mathfrak{f})} \bar{\mathbb{Q}}, \mathbb{Q}_p) \underset{K_p}{\otimes} L_{\mathsf{p}} \xrightarrow{\sigma} H^1_{et}(E^{(\sigma)} \otimes_{K(\mathfrak{f})} \bar{\mathbb{Q}}, \mathbb{Q}_p) \underset{K_p}{\otimes} L_{\mathsf{p}}$$
$$\xrightarrow{\varphi(\mathfrak{a})^{-1}\eta_{\mathfrak{a}}^*} V_{L_{\mathsf{p}}}(\varphi).$$

Here $\mathfrak{a}$ an ideal such that $\sigma|_{K(\mathfrak{f})} = (\mathfrak{a}, K(\mathfrak{f})/K)$. The isomorphism (27) is induced by the p-adic period isomorphism for $E/K(\mathfrak{f})$ [48, (15.8.1)] and the isomorphism per_τ is induced by the period isomorphism (21) for $E/K(\mathfrak{f})$.

Remark 6. In the construction of the motivic structure the role of a torsion point $\alpha \in E(K(\mathfrak{f}))$ is to fix the isomorphism $\eta_{\mathfrak{a}} : E/E[\mathfrak{a}] \simeq E^{(\sigma_{\mathfrak{a}})}$. It induces the isogeny $E \to E/E[\mathfrak{a}] \xrightarrow{\eta_{\mathfrak{a}}} E^{(\sigma_{\mathfrak{a}})}$ which is the only way $\eta_{\mathfrak{a}}$ enters into the construction. Note that the isogeny $E \to E^{(\sigma_{\mathfrak{a}})}$ is uniquely determined.

3.4. The reciprocity law

We state Kato's reciprocity law and then deduce its consequences for an elliptic curve E/F as in Thm. 1.1.

Proposition 3.1. *Let φ be an algebraic Hecke character of K with values in the number field L and of infinity type $(-1, 0)$. For an embedding $\tau : L \to \mathbb{C}$ let*

$$\varphi_\tau : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$$

be the Hecke character deduced from φ as in (23). Let $\mathsf{p} \mid p$ be any prime ideal of $\mathcal{O}_L$, $\mathfrak{f}$ a multiple of the conductor of φ and $\gamma \in V_L(\varphi)$. Then the image $z_{p^\infty\mathfrak{f}}(\gamma)'$ of $z_{p^\infty\mathfrak{f}}$ under

$$H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \xrightarrow{\gamma} H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \otimes V_{L_{\mathsf{p}}}(\varphi) \simeq H^1_{p^\infty\mathfrak{f}}(V_{L_{\mathsf{p}}}(\varphi)(1))$$
$$\to H^1(\mathcal{O}_K[\frac{1}{p}], V_{L_{\mathsf{p}}}(\varphi)(1)) \xrightarrow{\exp^*} D^1_{dR}(K_p, V_{L_{\mathsf{p}}}(\varphi)) \simeq S(\varphi) \otimes_L L_{\mathsf{p}}$$

is an element of $S(\varphi)$. *Moreover*

$$\mathrm{per}_\tau(z_{p^\infty\mathfrak{f}}(\gamma)') = L_{p\mathfrak{f}}(\bar{\varphi}_\tau, 1)\cdot\gamma.$$

Proof. This is the special case of [48, Prop. 15.9] where φ has infinity type $(-1, 0)$ and where $K' = K$. □

Remark 7. Prop. 3.1 includes Deligne's period conjecture [29] for the algebraic Hecke character $\bar{\varphi}$. If b is an L-basis of $S(\varphi)$ and

$$\Omega = \Omega(b, \gamma) = (\Omega_\tau) \in L_{\mathbb{R}}^\times$$

is such $\mathrm{per}_\tau(b) = \Omega_\tau \cdot \gamma$ for all τ then

$$\frac{L_{p\mathfrak{f}}(\bar{\varphi}, 1)}{\Omega} \in L \subseteq L_{\mathbb{R}}.$$

In particular, if $L_{p\mathfrak{f}}(\bar{\varphi}_{\tau_0}, 1) \neq 0$ for one τ_0 then

$$L_{p\mathfrak{f}}(\bar{\varphi}_\tau, 1) \neq 0$$

for all $\tau \in \mathrm{Hom}(L, \mathbb{C})$. Deligne's period conjecture in the situation of Prop. 3.1 was proven in [35] and is known for all algebraic Hecke characters of all number fields (see [70, Ch. II, Thm. 2.1] and references therein. The proof for non-CM base fields was recently completed in [54]).

Recall the following proposition from [35, Thm. 4.1]

Proposition 3.2. *Let* E/F *be an elliptic curve over a number field* F *with complex multiplication by the ring of integers in an imaginary quadratic field* K. *Then* $K \subseteq F$ *and the following are equivalent*

a) $F(E_{tors})/K$ *is an abelian extension of* K.
b) *The abelian variety* $B := \mathrm{Res}_{F/K} E$ *has complex multiplication over* K *in the sense that*

$$L := \mathrm{End}_K(B) \otimes \mathbb{Q} \simeq L_1 \times \cdots \times L_r$$

where $L_1, \ldots, L_r$ *are CM fields containing* K *such that*

$$[L : K] = \sum_{i=1}^{r} [L_i : K] = [F : K](= \dim B).$$

c) *The extension F/K is abelian and there exists an algebraic Hecke character η of K so that*

$$\psi = \eta \circ N_{F/K}$$

where ψ is the algebraic Hecke character of F associated to E/F.

To the CM abelian variety B/K is attached a L-valued Serre-Tate character [71, Thm. 10]

$$\varphi = (\varphi_1, \dots, \varphi_r) : \mathbb{A}_K^\times \to L^\times, \quad \varphi|_{K^\times} = K^\times \xrightarrow{i} L^\times$$

where φ_j is the Serre-Tate character of the simple isogeny factor B_j of B with endomorphism algebra L_j. Here i is the inclusion.

Proposition 3.3. *In the situation of Prop. 3.2 there are isomorphisms of free rank one L-modules*

$$V_L(\varphi) := V_{L_1}(\varphi_1) \times \cdots \times V_{L_r}(\varphi_r) \simeq H^1(B(\mathbb{C}), \mathbb{Q})$$
$$S(\varphi) := S(\varphi_1) \times \cdots \times S(\varphi_r) \simeq H^0(B, \Omega_{B/K})$$

so that the diagram of free rank one $L_\mathbb{R}$-modules

$$\begin{tikzcd}
\prod\limits_{\tau\in\mathrm{Hom}_K(L,\mathbb{C})} S(\varphi)\otimes_{L,\tau}\mathbb{C} \arrow[r, "\simeq"] \arrow[d, "\prod_\tau \mathrm{per}_\tau"'] & S(\varphi)_\mathbb{R} \arrow[r, "\simeq"] & H^0(B,\Omega_{B/K})_\mathbb{R} \arrow[d, "\mathrm{per}_B"] \\
\prod\limits_{\tau\in\mathrm{Hom}_K(L,\mathbb{C})} V_L(\varphi)\otimes_{L,\tau}\mathbb{C} \arrow[r, "\simeq"] & V_L(\varphi)_\mathbb{R} \arrow[r, "\simeq"] & H^1(B(\mathbb{C}),\mathbb{Q})_\mathbb{R}
\end{tikzcd}$$

commutes where per_B *was defined in (21). Moreover, for each prime number p there is a* $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$*-equivariant isomorphism of free rank one L_p-modules*

$$V_p(\varphi) := \prod_{\mathfrak{p}|p} V_{L_{1,\mathfrak{p}}}(\varphi_1) \times \cdots \times \prod_{\mathfrak{p}|p} V_{L_{r,\mathfrak{p}}}(\varphi_r) \simeq H^1_{et}(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Q}_p)$$

compatible with (26) and the Artin comparison isomorphism for B. Finally, the p-adic (Deligne) period isomorphism for B is compatible with (27).

Proof. The following is based on the construction of B/K via Galois descent. Put $G = \mathrm{Gal}(F/K)$ and define an abelian variety

$$\tilde{B} = \prod_{\sigma'\in G} E^{(\sigma')}$$

for $E^{(\sigma')}$ the Galois conjugate. An element $\sigma \in G$ induces an isomorphism $E^{(\sigma')} \simeq E^{(\sigma\circ\sigma')}$ which leads to

$$\phi_\sigma : \tilde{B} \simeq \tilde{B}^{(\sigma)}.$$

Note that $(\tilde{B}, (\phi_\sigma)_{\sigma\in G})$ is an effective descent datum, B/K being the descent. One has

$$\mathrm{End}_F(\tilde{B})^G = \prod_{\sigma'\in G} \mathrm{Hom}_F(E, E^{(\sigma')})$$

and accordingly Prop. 3.2 b) gives a partition of G by the indices $\{1, ..., r\}$. Let G_i denote the subset of elements associated to an index i. For each i define an abelian variety

$$\tilde{B}_i = \prod_{\tau\in G_i} E^{(\tau)}. \tag{28}$$

The descent datum on $\tilde{B}$ induces a datum on $\tilde{B}_i$, let B_i/K denote the descent. Note that there is an isogeny

$$B \to \prod_{i=1}^{r} B_i \tag{29}$$

over K. The main theorem of complex multiplication leads to the following description of the descent datum on $\tilde{B}_i$. Let $\mathcal{O}_i \subset L_i$ denote the endomorphism ring of B_i. For $\sigma \in G$ pick $s_\sigma \in \mathbb{A}_{K,f}^\times$ with $\mathrm{rec}_K(s_\sigma) = \sigma$ where

$$\mathrm{rec}_K : \mathbb{A}_K^\times/K^\times \simeq \mathrm{Gal}(K^{ab}/K) \twoheadrightarrow G$$

is the Artin map normalized so that uniformizers map to lifts of the the arithmetic Frobenius. By the main theorem of complex multiplication [14, Thm. A.2.7] there is a unique L_i-linear isomorphism of abelian varieties

$$\theta_{\sigma,s_\sigma} : \tilde{B}_i \otimes_{\mathcal{O}_i} I_{s_\sigma} \simeq \tilde{B}_i^{(\sigma)}$$

for I_{s_σ} the principal fractional $\mathcal{O}_i$-ideal generated by $\varphi_i(s_\sigma)^{-1} \in L_i^\times$. The composite

$$c(\sigma) : \tilde{B}_i \overset{\varphi_i(s_\sigma)^{-1}}{\simeq} \tilde{B}_i \otimes_{\mathcal{O}_i} I_{s_\sigma} \overset{\theta_{\sigma,s_\sigma}}{\simeq} \tilde{B}_i^{(\sigma)} \tag{30}$$

is an L_i-linear F-isomorphism. For varying σ the isomorphisms $c(\sigma) : \tilde{B}_i \simeq \tilde{B}_i^{(\sigma)}$ induce an $\mathcal{O}_i$-linear descent datum on $\tilde{B}_i$ with respect to G, which is compatible with the preceding datum [14, A.3.4] (see also [72, p. 513]).

Note that the motivic structure associated to a Hecke character φ as in Section 3.3 may be defined via a CM pair (E', α') where E'/F' is an elliptic curve as in Prop. 3.2 and $\alpha' \in E'(\tilde{F}')$ is a torsion point with annihilator $\mathfrak{f}$ a multiple of the conductor of φ and $\tilde{F}'/K$ an abelian extension containing F'. The resulting motivic structure is independent of the choice [48, p. 257]. In light of Remark 6 the elliptic curve E'/F' along with the isogeny $E' \to E'^{\sigma_{\mathfrak{a}}}$ for $\sigma_{\mathfrak{a}} \in \mathrm{Gal}(F'/K)$ give rise to the motivic structure. In the following we may thus consider an elliptic curve $E^{(\tau)}/F$ as above for $\tau \in G_i$. By definition

$$H^1(B_i(\mathbb{C}), \mathbb{Q}) = H^1(\tilde{B}_i(\mathbb{C}), \mathbb{Q}) \simeq H^1(E^{(\tau)}(\mathbb{C}), \mathbb{Q}) \otimes_K L_i = V_{L_i}(\varphi_i). \tag{31}$$

As for the de Rham realisation $S(\varphi_i)$ first note

$$H^0(\tilde{B}_i, \Omega_{\tilde{B}_i/F}) \simeq H^0(E^{(\tau)}, \Omega_{E^{(\tau)}/F}) \otimes_K L_i$$

since the endomorphism ring of $\tilde{B}_i$ is an order in L_i and (28). In light of the construction of B_i/K observe $H^0(B_i, \Omega_{B_i/K})$ is the fixed part of the $\mathrm{Gal}(F/K)$-action on $H^0(\tilde{B}_i, \Omega_{\tilde{B}_i/F})$ arising from the descent datum (30). From the above description the action coincides with the $\mathrm{Gal}(F/K)$-action on $H^0(E^{(\tau)}, \Omega_{E^{(\tau)}/F}) \otimes_K L_i$ as in Section 3.3. Hence one has

$$H^0(B_i, \Omega_{B_i/K}) \simeq S(\varphi_i). \tag{32}$$

In the same vein the construction induces an isomorphism of $L_{i,\mathfrak{p}}[G_K]$-modules

$$H^1_{et}(B_i \otimes_K \bar{K}_w, \mathbb{Q}_p) \otimes_{L_i \otimes \mathbb{Q}_p} L_{i,\mathfrak{p}} \simeq V_{L_{i,\mathfrak{p}}}(\varphi_i). \tag{33}$$

Under the isomorphisms (31), (32) and (33) note that the period maps per_τ and (27) as in Section 3.3 correspond to the period maps

$$\mathrm{per}_{\mathrm{B_i}} : H^0(B_i, \Omega_{B_i/K}) \to H^1(B_i(\mathbb{C}), \mathbb{C})$$

and

$$D_{dR}(L_i \otimes \mathbb{Q}_p, H^1_{et}(B_i \otimes_K \bar{K}_v, \mathbb{Q}_p) \otimes_{L_i \otimes \mathbb{Q}_p} L_{i,\mathfrak{p}}) \simeq H^1_{dR}(B_i/K_v) \otimes_{L_i \otimes \mathbb{Q}_p} L_{i,\mathfrak{p}}$$

respectively. In view of the isogeny (29) the proof concludes. □

Corollary 9. *In the situation of Prop. 3.2 let p be any prime number, $\mathfrak{f}$ a multiple of the conductor of B and $\gamma \in H^1(B(\mathbb{C}),\mathbb{Q})$. Then the image $z_{p^\infty\mathfrak{f}}(\gamma)'$ of $z_{p^\infty\mathfrak{f}}$ under*

$$\begin{aligned} &H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \xrightarrow{\gamma} H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \otimes H^1_{et}(B\otimes_K\bar{\mathbb{Q}},\mathbb{Q}_p) \simeq H^1_{p^\infty\mathfrak{f}}(V_p({}^tB)) \\ \to &H^1(\mathcal{O}_K[\frac{1}{p}],V_p({}^tB)) \xrightarrow{\exp^*} H^0(B_{K_p},\Omega_{B_{K_p}/K_p}) \end{aligned}$$

is an element $H^0(B,\Omega_{B/K})$. Moreover, if $\gamma_1,\dots,\gamma_d$ is a K-basis of $H^1(B(\mathbb{C}),\mathbb{Q})$ then

$$\det_{K_\mathbb{R}}(\mathrm{per}_B)\left(z_{p^\infty\mathfrak{f}}(\gamma_1)'\wedge\cdots\wedge z_{p^\infty\mathfrak{f}}(\gamma_d)'\right) = L_{p\mathfrak{f}}(\bar{\psi},1)\cdot(\gamma_1\wedge\cdots\wedge\gamma_d). \tag{34}$$

Proof. The first statement is clear from Prop. 3.1 for $\varphi_1,\dots,\varphi_r$. Since $\gamma\mapsto z_{p^\infty\mathfrak{f}}(\gamma)$ is K-linear, and its scalar extension $K_\mathbb{R}$-linear, it suffices to show (34) for a particular $K_\mathbb{R}$-basis $\{\gamma_i\}$ of $H^1(B(\mathbb{C}),\mathbb{Q})_\mathbb{R}$ in order to deduce it for all. Taking $\{\gamma_i\}=\{\gamma_\tau\}$ where γ_τ is a $K_\mathbb{R}=\mathbb{C}$-basis of $V_L(\varphi)\otimes_{L,\tau}\mathbb{C}$ Prop. 3.1 gives the equality

$$\det_{K_\mathbb{R}}(\mathrm{per}_B)(z_{p^\infty\mathfrak{f}}(\gamma_1)\wedge\cdots\wedge z_{p^\infty\mathfrak{f}}(\gamma_d)) = \prod_{\tau\in\mathrm{Hom}_K(L,\mathbb{C})} L_{p\mathfrak{f}}(\bar{\varphi}_\tau,1)\cdot(\gamma_1\wedge\cdots\wedge\gamma_d).$$

It remains to recall the identity of L-functions [35, Eq. (5.0), Lemma (4.8)(iii)]

$$L_{p\mathfrak{f}}(\bar{\psi}_\iota,s) = \prod_{\tau|_K=\iota} L_{p\mathfrak{f}}(\bar{\varphi}_\tau,s) \tag{35}$$

where $\iota: K\to\mathbb{C}$ is the embedding fixed above. One can view the left hand side as the K-equivariant L-function of ${}^tE/F$ or, since

$$V_p({}^tB) = \mathrm{Ind}_{G_F}^{G_K} V_p({}^tE),$$

as the K-equivariant L-function of ${}^tB = \mathrm{Res}_{F/K}{}^tE$ over K. On the other hand, the tuple

$$(L_{p\mathfrak{f}}(\bar{\varphi}_\tau,s))_\tau \in \prod_{\tau|_K=\iota}\mathbb{C}\simeq L_\mathbb{R}$$

can be viewed as the L-equivariant L-function of ${}^tB/K$. The identity (35) then amounts to the fact that the norm from $L_\mathbb{R}$ to $K_\mathbb{R}$ of the L-equivariant L-function is the K-equivariant L-function. □

4. The Iwasawa main conjecture

In Section 4.1 we recall the exact notation for the Euler system of elliptic units used in [44] and match it with the notation already introduced in Section 3.2 (which is identical to Kato's notation in [48]). In Section 4.2 we recall the "Λ-main conjecture" of [44] associated to an arbitrary prime number p and finite order character χ of G_K. In Section 4.3 we compute the image of the basis given by the main conjecture in the determinant of Galois cohomology of the Galois representation associated to a Hecke character. This will allow us to complete the proof of Thm. 1.2, resp. Thm. 1.1, in Section 4.4, resp. 4.5.

4.1. Twisted Elliptic Units

We use the notation of Sections 3.1 and 3.2. Let $\mathcal{O}$ be the ring of integers in a finite extension of $\mathbb{Q}_p$ and

$$G_K \to G_{p^\infty\mathfrak{f}} \xrightarrow{\chi} \mathcal{O}^\times$$

a finite order character of conductor $\mathfrak{f}_\chi \mid \mathfrak{f}$. Following [44, Def. 1.1] we denote by $\mathcal{O}(\chi)$ the free rank one $\mathcal{O}$-module on which $G_{p^\infty\mathfrak{f}}$ acts via χ^{-1} and following [44, Def. 4.2] we define

$$\Lambda(\chi) := \mathcal{O}(\chi) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[[\Gamma]]. \tag{36}$$

Then $\Lambda(\chi)$ is a free, rank one module over

$$\Lambda_{\mathcal{O}} := \mathcal{O}[[\Gamma]] \simeq \mathcal{O}[[T_1, T_2]]$$

with a continuous $\Lambda_{\mathcal{O}}$-linear $G_{p^\infty\mathfrak{f}}$-action.

For nonzero ideals $\mathfrak{a}, \mathfrak{m}$ of $\mathcal{O}_K$, prime number p and $r \geq 1$ so that $(\mathfrak{a}, 6p\mathfrak{m}) = 1$ and $\mathcal{O}_K^\times \to (\mathcal{O}_K/p^r)^\times$ is injective, define [44, Def. 3.2]

$${}_{\mathfrak{a}}\zeta_{\mathfrak{m}} := N_{K(p^r\mathfrak{m})/K(\mathfrak{m})}({}_{\mathfrak{a}}z_{p^r\mathfrak{m}}).$$

Note that ${}_{\mathfrak{a}}\zeta_{\mathfrak{m}}$ depends on p (in addition to $\mathfrak{a}$ and $\mathfrak{m}$) but not on r. For an $\mathcal{O}$-basis $t(\chi)$ of $\mathcal{O}(\chi)$ define [44, Def. 3.5]

$${}_{\mathfrak{a}}\zeta_{\mathfrak{m}}(\chi) := \mathrm{Tr}_{K(\mathfrak{f}_\chi\mathfrak{m})/K(\mathfrak{m})}({}_{\mathfrak{a}}\zeta_{\mathfrak{f}_\chi\mathfrak{m}} \otimes t(\chi)) \in H^1(\mathcal{O}_{K(\mathfrak{m})}[\frac{1}{p}], \mathcal{O}(\chi)(1)).$$

Here $\mathcal{O}(\chi)$ denotes the p-adic étale sheaf $j_*\mathcal{O}(\chi)$ where

$$j : \operatorname{Spec}\mathcal{O}_{K(\mathfrak{m})}[\frac{1}{p\mathfrak{f}}] \to \operatorname{Spec}\mathcal{O}_{K(\mathfrak{m})}[\frac{1}{p}]$$

is an open embedding and the Galois module $\mathcal{O}(\chi)$ is viewed as a local system on $\operatorname{Spec}\mathcal{O}_{K(\mathfrak{m})}[\frac{1}{p\mathfrak{f}}]$. For any field $K \subseteq F \subseteq K(\mathfrak{m})$ define

$${}_{\mathfrak{a}}\zeta_F(\chi) := \operatorname{Tr}_{K(\mathfrak{m})/F}({}_{\mathfrak{a}}\zeta_{\mathfrak{m}}(\chi)).$$

Denote by K_n/K the fixed field of the kernel of $G_{p^\infty\mathfrak{f}} \to \Gamma \to \Gamma/\Gamma^{p^n}$ and define [44, 5.2]

$${}_{\mathfrak{a}}\zeta(\chi) := \varprojlim_n {}_{\mathfrak{a}}\zeta_{K_n}(\chi) \in H^1(\mathcal{O}_K[\frac{1}{p}], \Lambda(\chi)(1))$$

and

$$\zeta(\chi) := (N\mathfrak{a} - \sigma_{\mathfrak{a}})^{-1}{}_{\mathfrak{a}}\zeta(\chi) \in H^1(\mathcal{O}_K[\frac{1}{p}], \Lambda(\chi)(1)) \otimes_{\Lambda_{\mathcal{O}}} Q(\Lambda_{\mathcal{O}}).$$

From Section 3.2 recall the norm compatible system

$${}_{\mathfrak{a}}z_{p^\infty\mathfrak{f}} := ({}_{\mathfrak{a}}z_{p^n\mathfrak{f}})_{n\geq 1} \in \varprojlim_{K'} \mathcal{O}_{K'}[\frac{1}{p}]^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq H^1(\mathcal{O}_K[\frac{1}{p}], \Lambda(1)).$$

Lemma 6. *For $\mathfrak{f}_\chi \mid \mathfrak{f}$ the image of ${}_{\mathfrak{a}}z_{p^\infty\mathfrak{f}}$ under the map*

$$H^1(\mathcal{O}_K[\frac{1}{p}], \Lambda(1)) \to H^1(\mathcal{O}_K[\frac{1}{p}], \Lambda(\chi)(1)) \tag{37}$$

induced by (36) coincides with

$$\prod_{\mathfrak{l}|\mathfrak{f}, \mathfrak{l}\nmid p} (1 - \chi(\mathfrak{l}) \operatorname{Fr}_{\mathfrak{l}}^{-1}) \cdot {}_{\mathfrak{a}}\zeta(\chi).$$

Similarly, the image of $z_{p^\infty\mathfrak{f}}$ coincides with $\prod_{\mathfrak{l}|\mathfrak{f}, \mathfrak{l}\nmid p}(1 - \chi(\mathfrak{l}) \operatorname{Fr}_{\mathfrak{l}}^{-1}) \cdot \zeta(\chi)$.

Proof. By definition

$$\begin{aligned} {}_{\mathfrak{a}}\zeta_{K_n}(\chi) &= \operatorname{Tr}_{K(\mathfrak{f}_\chi p^n)/K_n}({}_{\mathfrak{a}}\zeta_{\mathfrak{f}_\chi p^n}(\chi)) \\ &= \operatorname{Tr}_{K(\mathfrak{f}_\chi p^{r+n})/K_n}({}_{\mathfrak{a}}z_{\mathfrak{f}_\chi p^{r+n}} \otimes t(\chi)) \end{aligned}$$

for an integer r with $\mathcal{O}_K^\times \to (\mathcal{O}_K/p^r)^\times$ injective. So the image of ${}_{\mathfrak{a}}z_{p^\infty\mathfrak{f}_\chi}$ under (37) coincides with ${}_{\mathfrak{a}}\zeta(\chi)$. Note that (37) factors through the map

$$H^1(\mathcal{O}_K[\frac{1}{p}],\Lambda_{\mathfrak{f}}(1)) \to H^1(\mathcal{O}_K[\frac{1}{p}],\Lambda_{\mathfrak{f}_\chi}(1))$$

induced by the projection $G_{p^\infty\mathfrak{f}} \twoheadrightarrow G_{p^\infty\mathfrak{f}_\chi}$ where $\Lambda_{\mathfrak{g}} := \mathbb{Z}_p[[\mathrm{Gal}(K(p^\infty\mathfrak{g})/K)]]$ for an ideal $\mathfrak{g}\subset\mathcal{O}_K$. It coincides with the norm map

$$N_{K(\mathfrak{f}p^\infty)/K(\mathfrak{f}_\chi p^\infty)} : \varprojlim_{K'\subset K(\mathfrak{f}p^\infty)} \mathcal{O}_{K'}[\frac{1}{p}]^\times\otimes_{\mathbb{Z}}\mathbb{Z}_p \to \varprojlim_{K'\subset K(\mathfrak{f}_\chi p^\infty)} \mathcal{O}_{K'}[\frac{1}{p}]^\times\otimes_{\mathbb{Z}}\mathbb{Z}_p.$$

Recall the Euler system norm relation [44, Prop. 3.3 (2)]

$$N_{K(\mathfrak{f}p^\infty)/K(\mathfrak{f}_\chi p^\infty)}({}_{\mathfrak{a}}z_{\mathfrak{f}p^\infty}) = \prod_{\mathfrak{l}|\mathfrak{f},\mathfrak{l}\nmid p\mathfrak{f}_\chi}(1-\mathrm{Fr}_{\mathfrak{l}}^{-1})\cdot {}_{\mathfrak{a}}z_{\mathfrak{f}_\chi p^\infty}$$

and observe that $\chi(\mathrm{Fr}_{\mathfrak{l}}^{-1})=\chi(\mathfrak{l})^{-1}\in\mathcal{O}$ acts on $\Lambda(\chi)$ via $\chi(\mathfrak{l})$. Noting that $\chi(\mathfrak{l})=0$ for $\mathfrak{l}\mid\mathfrak{f}_\chi$ the proof concludes. □

4.2. The main conjecture

We shall also denote by $z_{p^\infty\mathfrak{f}}$ the image of $z_{p^\infty\mathfrak{f}}$ under the composition of (37) with the restriction map

$$H^1(\mathcal{O}_K[\frac{1}{p}],\Lambda(\chi)(1))\otimes_{\Lambda_{\mathcal{O}}}Q(\Lambda_{\mathcal{O}}) \to H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))\otimes_{\Lambda_{\mathcal{O}}}Q(\Lambda_{\mathcal{O}})$$

induced by the open immersion j.

Theorem 4.1. *For $\mathfrak{f}_\chi\,|\,\mathfrak{f}$ there is an equality of invertible $\Lambda_{\mathcal{O}}$-submodules*

$$\Lambda_{\mathcal{O}}\cdot z_{p^\infty\mathfrak{f}} = \det\nolimits^{-1}_{\Lambda_{\mathcal{O}}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))$$

of $\det^{-1}_{\Lambda_{\mathcal{O}}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))\otimes_{\Lambda_{\mathcal{O}}}Q(\Lambda_{\mathcal{O}})$.

Proof. By [44, Cor. 5.3] there is an equality of invertible $\Lambda_{\mathcal{O}}$-submodules

$$\Lambda_{\mathcal{O}}\cdot\prod_{\mathfrak{l}|\mathfrak{f},\mathfrak{l}\nmid p}(1-\chi(\mathfrak{l})\,\mathrm{Fr}_{\mathfrak{l}}^{-1})\cdot\zeta(\chi) = \det\nolimits^{-1}_{\Lambda_{\mathcal{O}}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))$$

of $\det^{-1}_{\Lambda_{\mathcal{O}}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))\otimes_{\Lambda_{\mathcal{O}}}Q(\Lambda_{\mathcal{O}})$. Together with Lemma 6 this gives the result. □

Remark 8. For primes $p \nmid |\mathcal{O}_K^\times| \cdot |G_{p^\infty\mathfrak{f}}^{tor}|$ the above main conjecture is equivalent Rubin's main conjecture [67, 68] (see [44, §5.5]).

4.3. Descent to Galois representation of Hecke characters

Let φ be an algebraic Hecke character of K of infinity type $(-1,0)$ and with values in the number field L. For a prime number p and place $\mathfrak{p} \mid p$ of L let $V_{L_\mathfrak{p}}(\varphi)$ be the continuous $L_\mathfrak{p}$-linear G_K-representation associated to φ as in Section 3.3. Choose a free, rank one G_K-invariant $\mathcal{O} := \mathcal{O}_{L_\mathfrak{p}}$-submodule

$$T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi) \subset V_{L_\mathfrak{p}}(\varphi)$$

and let

$$\rho : G_{p^\infty\mathfrak{f}} \to \mathcal{O}^\times$$

denote the character giving the action of G_K on $T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi)$. Here $\mathfrak{f}$ is any multiple of the conductor $\mathfrak{f}_\varphi$ of φ. Choose a decomposition (24), i.e. a splitting $G_{p^\infty\mathfrak{f}} \to \Delta$ of the inclusion $\Delta := G_{p^\infty\mathfrak{f}}^{tor} \subseteq G_{p^\infty\mathfrak{f}}$ and define a finite order character χ as the composite

$$\chi : G_{p^\infty\mathfrak{f}} \to \Delta \xrightarrow{\rho^{-1}|_\Delta} \mathcal{O}^\times .$$

Lemma 7. *For primes $v \nmid p$ of K we have*

$$(\mathfrak{f}_\chi)_v = (\mathfrak{f}_\varphi)_v \ \ (= (\mathfrak{f}_\rho)_v) .$$

Proof. For $v \nmid p$ the image of the inertia subgroup I_v in $G_{p^\infty\mathfrak{f}}$ is finite, hence lies in Δ. By the definition of χ we have $\chi|_{I_v} = \rho^{-1}|_{I_v}$ and hence $(\mathfrak{f}_\chi)_v = (\mathfrak{f}_{\rho^{-1}})_v = (\mathfrak{f}_\rho)_v$. □

Remark 9. For $v \mid p$ the conductor of χ depends on the choice of a decomposition (24) and might differ from $(\mathfrak{f}_\varphi)_v$ (in either direction).

The following Lemma is a pared down generalization of [31, Lemma 5.7] from a one-variable to a two-variable Iwasawa algebra. Lemma 5.7 in [31] computes the descent of a basis of the determinant of a perfect complex over a one-variable Iwasawa algebra. It might be possible to formulate a descent Lemma over a two-variable Iwasawa algebra in similar generality but we found it too confusing to do so for the simple application that we need.

Lemma 8. *Let R be a two-dimensional regular local ring with fraction field F and residue field k, Δ a perfect complex of R-modules and $\mathcal{L} \in H^1(\Delta)$ an element such that the following hold.*

1) $H^1(\Delta)$ is R-torsion free and of R-rank one, $H^2(\Delta)$ is R-torsion and $H^i(\Delta) = 0$ for $i \neq 1, 2$.

2) There is an equality of invertible R-submodules

$$R \cdot \mathcal{L} = \det_R^{-1} \Delta$$

of

$$H^1(\Delta) \otimes_R F \simeq \det_R^{-1}(\Delta) \otimes_R F.$$

3) The image $\bar{\mathcal{L}}$ of $\mathcal{L}$ under the natural map $H^1(\Delta) \to H^1(\Delta \otimes_R^{\mathbb{L}} k)$ is nonzero.

4) $H^0(\Delta \otimes_R^{\mathbb{L}} k) = 0$.

Then $H^i(\Delta \otimes_R^{\mathbb{L}} k) = 0$ for $i \neq 1$, $\dim_k H^1(\Delta \otimes_R^{\mathbb{L}} k) = 1$ and the image of $\mathcal{L} \otimes 1$ under the isomorphism

$$(\det_R^{-1} \Delta) \otimes_R k \simeq \det_k^{-1}(\Delta \otimes_R^{\mathbb{L}} k) \simeq H^1(\Delta \otimes_R^{\mathbb{L}} k)$$

coincides with $\bar{\mathcal{L}}$.

Proof. Let $a, b \in R$ be a system of parameters so that $k \simeq R/(a, b)$. The short exact sequences

$$0 \to H^i(\Delta) \otimes_R R/a \to H^i(\Delta \otimes_R^{\mathbb{L}} R/a) \to H^{i+1}(\Delta)_a \to 0$$

and the fact that $H^1(\Delta)$ is torsion free show that $H^i(\Delta \otimes_R^{\mathbb{L}} R/a) = 0$ for $i \neq 1, 2$. The map in 3) factors

$$H^1(\Delta) \to H^1(\Delta) \otimes_R R/a \to H^1(\Delta \otimes_R^{\mathbb{L}} k)$$

and hence the image $\mathcal{L}_a$ of $\mathcal{L}$ in $H^1(\Delta) \otimes_R R/a$ is nonzero. By Nakayama's Lemma for the discrete valuation ring $R_{(a)}$ and the fact that $H^1(\Delta)_{(a)}$ is $R_{(a)}$-torsion free and of $R_{(a)}$-rank one the element $\mathcal{L}$ is a basis of $H^1(\Delta)_{(a)}$. From 2) we find $H^2(\Delta)_{(a)} = 0$ and hence that $H^1(\Delta \otimes_R^{\mathbb{L}} R/a)_{(a)}$ has $R_{(a)}/a$-rank one.

We now have the perfect complex $\Delta' := \Delta \otimes_R^{\mathbb{L}} R/a$ over the discrete valuation ring $R' := R/a$ with uniformizer b and fraction field $F' = R_{(a)}/a$, cohomologically concentrated in degrees $1, 2$, such that $H^2(\Delta')$ is R'-torsion and $H^1(\Delta')$ is of rank one and R'-torsion free. This last claim follows from the isomorphism

$$H^0(\Delta \otimes_R^{\mathbb{L}} k) \simeq H^0(\Delta' \otimes_{R'}^{\mathbb{L}} R'/b) \simeq H^1(\Delta')_b$$

and assumption 4). By assumption 3) the image of $\mathcal{L}_a \in H^1(\Delta')$ under

$$H^1(\Delta') \to H^1(\Delta') \otimes_{R'} R'/b \to H^1(\Delta' \otimes^{\mathbb{L}}_{R'} R'/b) \simeq H^1(\Delta \otimes^{\mathbb{L}}_{R} k)$$

is nonzero, hence by Nakayama's Lemma $\mathcal{L}_a$ is an R'-basis of $H^1(\Delta')$ (as we already know that $H^1(\Delta')$ is free of rank one). From 2) we know that $\mathcal{L} \otimes 1$ is an R'-basis of

$$(\det{}_R^{-1}\Delta) \otimes_R R' \simeq \det{}_{R'}^{-1}(\Delta') \simeq H^1(\Delta') \otimes_{R'} \det{}_{R'}^{-1} H^2(\Delta')$$

and the image of $\mathcal{L} \otimes 1$ in

$$(38) \qquad (\det{}_R^{-1}\Delta) \otimes_R F' \simeq \det{}_{F'}^{-1}(H^1(\Delta)_{(a)}/a) \simeq H^1(\Delta') \otimes_{R'} F'$$

coincides with $\mathcal{L}_a$. It follows that the R'-order ideal of the torsion module $H^2(\Delta')$ equals R and hence that $H^2(\Delta') = 0$. We deduce that

$$0 = H^2(\Delta') \otimes_{R'} R'/b \simeq H^2(\Delta' \otimes^{\mathbb{L}}_{R'} R'/b) \simeq H^2(\Delta \otimes^{\mathbb{L}}_{R} k).$$

Since $\mathcal{L}_a$ is an R'-basis of

$$H^1(\Delta') \simeq \det{}_{R'}^{-1}(\Delta')$$

the image $\bar{\mathcal{L}}$ of $\mathcal{L}_a$ in

$$H^1(\Delta \otimes^{\mathbb{L}}_{R} k) \xleftarrow{\simeq} H^1(\Delta') \otimes_{R'} R'/b \simeq \det{}_{R'}^{-1}(\Delta') \otimes_{R'} R'/b \simeq \det{}_{R}^{-1}(\Delta) \otimes_R k$$

is a k-basis. But $\bar{\mathcal{L}}$ is also the image of $\mathcal{L} \otimes 1 \in \det_R^{-1}(\Delta) \otimes_R k$ as we saw in (38). This concludes the proof. □

Remark 10. It follows from the proof of Lemma 8 that $H^2(\Delta) = 0$ and $H^1(\Delta)$ is free with basis $\mathcal{L}$ under the assumptions of Lemma 8.

Proposition 4.1. *Let $\gamma \in V_L(\varphi)$ be such that its image in $V_{L_\mathfrak{p}}(\varphi)$ is an $\mathcal{O}$-basis of $T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi)$ and let $\mathfrak{f}$ be a multiple of $\mathfrak{f}_\varphi$. Let $z_{p^\infty\mathfrak{f}}(\gamma)$ be the image of $z_{p^\infty\mathfrak{f}}$ under*

$$\begin{aligned} &H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \xrightarrow{\gamma} H^1_{p^\infty\mathfrak{f}}(\mathbb{Z}_p(1)) \otimes V_{L_\mathfrak{p}}(\varphi) \simeq H^1_{p^\infty\mathfrak{f}}(V_{L_\mathfrak{p}}(\varphi)(1)) \\ \to &H^1(\mathcal{O}_K[\frac{1}{p}], V_{L_\mathfrak{p}}(\varphi)(1)) \to H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_{L_\mathfrak{p}}(\varphi)(1)) \end{aligned}$$

and assume that $L_{p\mathfrak{f}}(\bar{\varphi},1)\neq 0$. *Then there is an equality of invertible* $\mathcal{O}$-*submodules*

$$\mathcal{O}\cdot z_{p^\infty\mathfrak{f}}(\gamma)=\det\nolimits_{\mathcal{O}}^{-1}R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi)(1))$$

of

$$\begin{aligned}\det\nolimits_{L_\mathfrak{p}}^{-1}R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],V_{L_\mathfrak{p}}(\varphi)(1))&\simeq\det\nolimits_{L_\mathfrak{p}}H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],V_{L_\mathfrak{p}}(\varphi)(1))\\&\simeq H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],V_{L_\mathfrak{p}}(\varphi)(1)).\end{aligned}$$

Moreover, the Selmer group

$$\mathrm{Sel}(K,T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi)(1))$$

is finite.

Proof. The character $\chi\rho$ is trivial on Δ, hence induces a character $\chi\rho:\Gamma\to\mathcal{O}^\times$ and a ring homomorphism $\chi\rho:\mathbb{Z}_p[[\Gamma]]\to\mathcal{O}$. We obtain an induced ring homomorphism

$$\kappa:=\mathrm{id}\otimes\chi\rho:\Lambda_{\mathcal{O}}\simeq\mathcal{O}\otimes_{\mathbb{Z}_p}\mathbb{Z}_p[[\Gamma]]\to\mathcal{O}$$

so that there is an $\mathcal{O}$-linear isomorphism of $G_{p^\infty\mathfrak{f}}$-modules

$$\Lambda(\chi)\otimes_{\Lambda_{\mathcal{O}},\kappa}\mathcal{O}\simeq T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi).$$

This induces an isomorphism of invertible $\mathcal{O}$-modules

$$\begin{aligned}&\left(\det\nolimits_{\Lambda_{\mathcal{O}}}^{-1}R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))\right)\otimes_{\Lambda_{\mathcal{O}},\kappa}\mathcal{O}\\ \simeq&\det\nolimits_{\mathcal{O}}^{-1}\left(R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))\otimes^{\mathbb{L}}_{\Lambda_{\mathcal{O}},\kappa}\mathcal{O}\right)\\ \simeq&\det\nolimits_{\mathcal{O}}^{-1}\left(R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1)\otimes_{\Lambda_{\mathcal{O}},\kappa}\mathcal{O})\right)\\ \simeq&\det\nolimits_{\mathcal{O}}^{-1}R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi)(1)).\end{aligned}\tag{39}$$

We apply Lemma 8 in the following situation. Denote by $\mathfrak{q}$ the kernel of κ and set

$$R:=\Lambda_{\mathcal{O},\mathfrak{q}};\quad\Delta:=R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}],\Lambda(\chi)(1))_{\mathfrak{q}};\quad\mathcal{L}:=z_{p^\infty\mathfrak{f}}.$$

Then we have

$$k \simeq L_{\mathfrak{p}}; \quad \Delta \otimes^{\mathbb{L}}_{R} k \simeq R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_{\mathcal{O}_{L_{\mathfrak{p}}}}(\varphi)(1)); \quad \bar{\mathcal{L}} = z_{p^\infty \mathfrak{f}}(\gamma).$$

For assumption 1) of Lemma 8 we refer to [48, §15], assumption 2) is the $\mathfrak{q}$-localization of Theorem 4.1, assumption 3) follows from $L_{p\mathfrak{f}}(\bar{\varphi}, 1) \neq 0$ and Prop. 3.1 and assumption 4)

$$H^0(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_{L_{\mathfrak{p}}}(\varphi)(1)) = 0$$

holds since the G_K-action on $V_{L_{\mathfrak{p}}}(\varphi)(1)$ is nontrivial. Lemma 8 implies that the image of $z_{p^\infty \mathfrak{f}} \otimes 1$ in

$$\det{}^{-1}_{L_{\mathfrak{p}}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_{\mathcal{O}_{L_{\mathfrak{p}}}}(\varphi)(1)) \simeq H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_{L_{\mathfrak{p}}}(\varphi)(1))$$

under the isomorphisms in (39) coincides with $z_{p^\infty \mathfrak{f}}(\gamma)$. On the other hand it follows from Theorem 4.1 that $z_{p^\infty \mathfrak{f}} \otimes 1$ is an $\mathcal{O}$-basis of the invertible $\mathcal{O}$-module (39). This proves the first part of Prop. 4.1.

Lemma 8 also includes the vanishing of $H^2(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_{L_{\mathfrak{p}}}(\varphi)(1))$ and the fact that

$$\dim_{L_{\mathfrak{p}}} H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_{L_{\mathfrak{p}}}(\varphi)(1)) = 1.$$

Prop. 3.1 then implies that the map in Prop. 2.1a) is nonzero and hence an isomorphism. The central vertical triangle in (4) shows that

$$R\Gamma_f(K, V_{L_{\mathfrak{p}}}(\varphi)(1)) = 0.$$

By Lemma 1 we have $\mathrm{Sel}(K, T_{\mathcal{O}_{L_{\mathfrak{p}}}}(\varphi)(1))_{\mathbb{Q}_p} \simeq H^1_f(K, V_{L_{\mathfrak{p}}}(\varphi)(1)) = 0.$ □

Remark 11. In the situation of Prop. 4.1 the finiteness of the Mordell-Weil group is due to Coates and Wiles [18], Arthaud [1] and Rubin [65]. For $L = K$ the finiteness of the Tate-Shafarevich group is due to Rubin [66] and his approach likely generalizes. The above complementary approach via Lemma 8 is essentially based on the arguments in [48, §15].

4.4. Proof of Theorem 1.2

We have $K \subseteq \mathrm{End}_L H^0(A, \Omega_{A/K}) = L$ and the CM type of A is induced from K. Since $\varphi(\alpha) = \alpha$ for $\alpha \equiv 1 \mod \mathfrak{f}_\varphi$ the character $\varphi \circ N_{F/K}$ of the idèle group of $F := K(\mathfrak{f}_\varphi)$ takes values in K, hence arises from an elliptic curve E/F with CM by $\mathcal{O}_K$. By [35, (4.4), (4.8)] and our assumption that A/K is simple, A is an isogeny factor of $B := \operatorname{Res}_{F/K} E$. An argument as in the proof of Prop. 3.3 shows that the motivic structure associated to φ in section 3.3 is isomorphic to the rational structure $H^1(A)$. We then verify the assumptions of Prop. 2.2 for all primes p. We may choose

$$T_{\mathcal{O}_{L_\mathfrak{p}}}(\varphi)(1) \simeq H^1(A_{\bar{K}}, \mathbb{Z}_p(1)) \simeq T_p({}^tA)$$

and hence the finiteness of $\text{Ш}(A/K)_{p^\infty}$ and of $A(K)$ follow from Prop. 4.1. The element $z := z_{p^\infty\mathfrak{f}}(\gamma)$ of Prop. 4.1 satisfies the assumptions of Prop. 2.2. Indeed, assumption a) follows from Prop. 4.1 and assumptions b) and c) follow from Prop. 3.1 if we choose γ to be an L-basis of $H^1(A(\mathbb{C}), \mathbb{Q})$ which is also a $\mathcal{O}_{L_p}$-basis of $H^1(A(\mathbb{C}), \mathbb{Z}_p)$. The finiteness of $\text{Ш}(A/K)$ then follows from the global formula for its cardinality given by Thm. 1.2. This concludes the proof of Thm. 1.2.

We next specialize Thm. 1.2 to the situation considered in [3]. Let $q \equiv 3 \mod 4$ be a prime number and set $K = \mathbb{Q}(\sqrt{-q})$. Let H be the Hilbert class field of K and E/H an elliptic curve with j-invariant $j(\mathcal{O}_K)$ whose Hecke character is fixed by all $\sigma \in G := \operatorname{Gal}(H/K)$. Set

$$B = \operatorname{Res}_{H/K} E; \quad L = \operatorname{End}_K(B)_\mathbb{Q}.$$

It was shown in [37, Thm. 15.2.5] that L is a CM field. Let φ be the Serre-Tate character of B/K.

Proposition 4.2. *Assume $L(\bar{\varphi}, 1) \neq 0$ and $\operatorname{End}_K(B) = \mathcal{O}_L$. Then Conjecture (12.3) of [3] holds true for B/K.*

Proof. The main work in this proof consists in matching the period of Def. 1 to that defined in [3]. The field $\mathbb{Q}(j(\mathcal{O}_K))$ has a unique real embedding as the class number $h = [H : K]$ is odd (see Remark 5). Together with our given embedding $K \subseteq \mathbb{C}$ this gives a distinguished embedding $\iota : K(j(\mathcal{O}_K)) = H \subseteq \mathbb{C}$. Following [3, (10.2)] define γ and ω, uniquely up to $\mathcal{O}_K^\times$, by

$$H_1(E^\iota(\mathbb{C}), \mathbb{Z}) = \mathcal{O}_K \cdot \gamma; \quad H^0(\mathcal{E}, \Omega_{\mathcal{E}/\mathcal{O}_H}) = \mathcal{O}_H \cdot \omega$$

and put

$$\Omega_\iota := \int_\gamma \iota(\omega) \in \mathbb{C}^\times/\mathcal{O}_K^\times.$$

For $\sigma \in G$ we have isomorphisms of $\mathcal{O}_K$-modules

$$\text{(40)} \quad \operatorname{Hom}_H(E^\sigma, E) \otimes_{\mathcal{O}_K} H_1(E^{\iota\sigma}(\mathbb{C}), \mathbb{Z}) \simeq H_1(E^\iota(\mathbb{C}), \mathbb{Z}); \quad f \otimes \delta \mapsto f_*\delta.$$

Indeed this can be checked locally at each prime p and for any p there exists an isogeny $f : E^\sigma \to E$ of degree prime to p. Since

$$\text{(41)} \qquad \mathcal{O}_L = \operatorname{End}_K(B) = \bigoplus_{\sigma \in G} \operatorname{Hom}_H(E^\sigma, E) \cdot \sigma$$

by [37, (15.1.5)] we see that

$$H_1(B(\mathbb{C}), \mathbb{Z}) \simeq \bigoplus_{\sigma \in G} H_1(E^{\iota\sigma}(\mathbb{C}), \mathbb{Z}) = \mathcal{O}_L \cdot \gamma$$

is free of rank one over $\mathcal{O}_L$ (see also [3, proof of Prop. 10.12]).

The period $\Omega \in L_{\mathbb{R}}^\times$ and fractional $\mathcal{O}_L$-ideal $\mathfrak{a}(\Omega)$ of Def. 1 for B/K satisfy

$$H^0(\mathcal{B}, \Omega_{\mathcal{B}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} \mathcal{D}_{K/\mathbb{Q}}^{-1} = \Omega \cdot \mathfrak{a}(\Omega) \cdot \operatorname{Hom}_{\mathbb{Z}}(H_1(B(\mathbb{C}), \mathbb{Z}), \mathbb{Z})$$

under the Deligne period isomorphism per_B, or equivalently

$$\begin{aligned} H^0(\mathcal{B}, \Omega_{\mathcal{B}/\mathcal{O}_K}) &= \Omega \cdot \mathfrak{a}(\Omega) \cdot \operatorname{Hom}_{\mathbb{Z}}(H_1(B(\mathbb{C}), \mathbb{Z}), \mathbb{Z}) \otimes_{\mathcal{O}_K} \mathcal{D}_{K/\mathbb{Q}} \\ &= \Omega \cdot \mathfrak{a}(\Omega) \cdot \operatorname{Hom}_{\mathcal{O}_K}(H_1(B(\mathbb{C}), \mathbb{Z}), \mathcal{O}_K) \end{aligned}$$

under the $K_{\mathbb{R}} = \mathbb{C}$-valued integration pairing. Define

$$\text{(42)} \qquad \gamma^* \in \operatorname{Hom}_{\mathcal{O}_K}(H_1(B(\mathbb{C}), \mathbb{Z}), \mathcal{O}_K)$$

by

$$\gamma^*(\delta) = \begin{cases} c & \text{if } \delta = c\gamma \in H_1(E^\iota(\mathbb{C}), \mathbb{Z}) \text{ with } c \in \mathcal{O}_K \\ 0 & \text{if } \delta \in H_1(E^{\iota\sigma}(\mathbb{C}), \mathbb{Z}) \text{ with } \sigma \neq 1. \end{cases}$$

Again by (40) and (41) the element γ^* is a $\mathcal{O}_L$-basis of (42). However, $H^0(\mathcal{B}, \Omega_{\mathcal{B}/\mathcal{O}_K})$ need not be free over $\mathcal{O}_L$. Following [3] let $M = LH$ be the composite field, an extension of degree h^2 of K. Since H/K is unramified we have $\mathcal{O}_M \simeq \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_H$. There is an isomorphism of $\mathcal{O}_M$-modules

$$\text{(43)} \quad H^0(\mathcal{B}, \Omega_{\mathcal{B}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} \mathcal{O}_H \simeq H^0(\mathcal{B}_{\mathcal{O}_H}, \Omega_{\mathcal{B}_{\mathcal{O}_H}/\mathcal{O}_H}) \simeq \bigoplus_{\sigma \in G} H^0(\mathcal{E}^\sigma, \Omega_{\mathcal{E}^\sigma/\mathcal{O}_H})$$

and we have isomorphisms of $\mathcal{O}_K$-modules

$$\mathrm{Hom}_H(E^\sigma, E) \otimes_{\mathcal{O}_K} H^0(\mathcal{E}, \Omega_{\mathcal{E}/\mathcal{O}_H}) \simeq H^0(\mathcal{E}^\sigma, \Omega_{\mathcal{E}^\sigma/\mathcal{O}_H}); \quad f \otimes \eta \mapsto f^*\eta.$$

Again this can be checked locally at each prime p. From (41) we see that (43) is free of rank one over $\mathcal{O}_M$ with basis ω. Extending scalars from $\mathcal{O}_K$ to $\mathcal{O}_H$ we then have an identity of free, rank one $\mathcal{O}_M$-modules

$$H^0(\mathcal{B}, \Omega_{\mathcal{B}/\mathcal{O}_K}) \otimes_{\mathcal{O}_K} \mathcal{O}_H = \Omega \cdot \mathfrak{a}(\Omega) \cdot \mathrm{Hom}_{\mathcal{O}_H}(H_1(B(\mathbb{C}), \mathbb{Z}) \otimes_{\mathcal{O}_K} \mathcal{O}_H, \mathcal{O}_H)$$

under an $H_{\mathbb{R}}$-valued integration pairing per_{B_H}. Since

$$\int_\delta \omega = 0$$

for $\delta \in H_1(E^{\iota\sigma}(\mathbb{C}), \mathbb{Z}),\ \sigma \neq 1$ we have

$$\mathrm{per}_{B_{H_\iota}}(\omega) = \Omega_\iota \cdot \gamma^*$$

where $\Omega_\iota \in K_{\mathbb{R}}^\times \subset L_{\mathbb{R}}^\times \simeq M_\iota^\times$ with $M_\iota = M \otimes_{H,\iota} \mathbb{C}$. We obtain an identity of invertible $\mathcal{O}_M$-submodules of M_ι

$$\mathcal{O}_M \cdot \Omega_\iota = \Omega \cdot \mathfrak{a}(\Omega) \otimes_{\mathcal{O}_L} \mathcal{O}_M.$$

The element $\Omega \in L_{\mathbb{R}}^\times$ is the period of some K-rational differential on B, for example we can take

$$\omega_B := \sum_{\sigma \in G} \omega^\sigma \in H^0(\mathcal{B}, \Omega_{\mathcal{B}/\mathcal{O}_K}).$$

In order to compute $\mathfrak{a}(\Omega)$ recall that by [3, (10.8)] there exist units $u_\sigma \in \mathcal{O}_M^\times$ for each $\sigma \in G$ such that

$$u_\sigma \cdot \omega^\sigma = \omega; \quad u_{\sigma\tau} = u_\sigma^\tau \cdot u_\tau.$$

Indeed, the differential ω^σ is an $\mathcal{O}_H$-basis of $H^0(\mathcal{E}^\sigma, \Omega_{\mathcal{E}^\sigma/\mathcal{O}_H})$ and an $\mathcal{O}_M$-basis of (43), by the same reasoning as used above for ω. We have

$$\omega_B = \sum_{\sigma \in G} \omega^\sigma = \left(\sum_{\sigma \in G} u_\sigma^{-1}\right) \cdot \omega =: v^{-1} \cdot \omega$$

with $v \in M^\times$ and

$$\Omega = v^{-1} \cdot \Omega_\iota. \tag{44}$$

Since $(v^\tau) = (u_\tau^{-1} v) = (v)$ for $\tau \in G$ and M/L is unramified the principal $\mathcal{O}_M$-ideal (v) descends to a fractional $\mathcal{O}_L$-ideal $\mathfrak{a}(\Omega)$. By [3, Prop. 11.1] there is an element $m \in M$ so that

$$\frac{L(\bar{\varphi}^\alpha, 1)}{\Omega_\iota} = m^\alpha \quad \forall \alpha \in \mathrm{Hom}_{H,\iota}(M, \mathbb{C}) = \mathrm{Hom}_{K,\iota}(L, \mathbb{C})$$

and such that the $\mathcal{O}_M$-ideal (m) is G-invariant, hence descends to a fractional $\mathcal{O}_L$-ideal $\mathfrak{m}_B$. Conjecture (12.3) of [3] states that

$$\mathfrak{m}_B = \mathfrak{g}_{\text{Ш}} \cdot \prod_v \mathfrak{g}_v / \mathfrak{g}_{tor}^{1+c} \tag{45}$$

where

$$\mathfrak{g}_{\text{Ш}} := |\text{Ш}(B/K)|_L; \quad \mathfrak{g}_{tor} := |B(K)|_L; \quad \mathfrak{g}_v := |\Phi_v|_L$$

and c denotes the complex conjugation of L. On the other hand Theorem 1.2 states that

$$t := \frac{L(\bar{\varphi}, 1)}{\Omega} \in L^\times; \quad (t) = \mathfrak{g}_{\text{Ш}} \cdot \prod_v \mathfrak{g}_v / \mathfrak{g}_{tor}^{1+c} \cdot \mathfrak{a}(\Omega). \tag{46}$$

By (44) we have $t = mv$ and $(t) = \mathfrak{m}_B \cdot \mathfrak{a}(\Omega)$ and hence we find that (45) and (46) are equivalent. □

Remark 12. By [58] the assumption $L(\bar{\varphi}, 1) \neq 0$ holds if $q \equiv 7 \mod 8$ and $E = A(q)$ is the curve of conductor $(\sqrt{-q})$ studied in [37]. The condition $\mathrm{End}_K(B) = \mathcal{O}_L$ may or may not hold. In [3, Sec.3] examples are given for both maximal and non-maximal $\mathrm{End}_K(B)$.

4.5. Proof of Theorem 1.1

The proof of Theorem 1.1 amounts to the conjunction of Theorem 1.2 for all characters $\varphi_1, \ldots, \varphi_r$ in Prop. 3.2, restriction of coefficients from L to K, and isogeny invariance of the K-equivariant BSD conjecture. We present these arguments in the following sequence of Lemmas. From now on the notation of Prop. 3.2 will be in effect. In particular L denotes the semisimple algebra

$$L = L_1 \times \cdots \times L_r$$

with maximal order

$$\mathcal{O}_L := \mathcal{O}_{L_1} \times \cdots \times \mathcal{O}_{L_r}.$$

For the Serre-Tate character $\bar{\varphi} = (\bar{\varphi}_1, \dots, \bar{\varphi}_r)$ of ${}^tB$ we denote by

$$L(\bar{\varphi}, s) := ((L(\bar{\varphi}_\tau, s))_\tau \in \prod_{\tau \in \mathrm{Hom}(L,\mathbb{C})} \mathbb{C} \simeq L_{\mathbb{C}}$$

its $L_{\mathbb{C}}$-valued L-function. For any prime number p define a free, rank one G_K-invariant $\mathcal{O}_{L_p}$-submodule

$$T_p(\varphi) := \prod_{\mathfrak{p}|p} T_{\mathcal{O}_{L_{1,\mathfrak{p}}}}(\varphi_1) \times \cdots \times \prod_{\mathfrak{p}|p} T_{\mathcal{O}_{L_{r,\mathfrak{p}}}}(\varphi_r) \subseteq V_p(\varphi)$$

of $V_p(\varphi)$ introduced in Prop. 3.3.

Lemma 9. *Let $\gamma \in V_L(\varphi)$ be such that its image in $V_p(\varphi)$ is a $\mathcal{O}_{L_p}$-basis of $T_p(\varphi)$ and let $\mathfrak{f}$ be a multiple of the conductor $\mathfrak{f}_B$ of B/K. Let $z_{p^\infty \mathfrak{f}}(\gamma)$ be the image of $z_{p^\infty \mathfrak{f}}$ in $H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_p(\varphi)(1))$ and assume that $L(\bar{\varphi}, 1) \neq 0$. Then there is an equality of invertible $\mathcal{O}_{L_p}$-submodules*

$$\mathcal{O}_{L_p} \cdot z_{p^\infty \mathfrak{f}}(\gamma) = \mathrm{det}^{-1}_{\mathcal{O}_{L_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p(\varphi)(1))$$

of

$$\mathrm{det}^{-1}_{L_p} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_p(\varphi)(1)) \simeq \mathrm{det}_{L_p} H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_p(\varphi)(1)).$$

Proof. This is immediate by combining Prop. 4.1 for $\varphi = \varphi_1, \dots, \varphi_r$ and all primes $\mathfrak{p} \mid p$ of the fields L_i. □

Lemma 10. *Let $\gamma_1, \dots, \gamma_d$ be a K-basis of $V_L(\varphi)$ whose image in $V_p(\varphi)$ is a $\mathcal{O}_{K_p}$-basis of $T_p(\varphi)$ and let $\mathfrak{f}$ be a multiple of $\mathfrak{f}_B$. Assume that $L(\bar{\varphi}, 1) \neq 0$. Then there is an equality of invertible $\mathcal{O}_{K_p}$-submodules*

$$\mathcal{O}_{K_p} \cdot z_{p^\infty \mathfrak{f}}(\gamma_1) \wedge \cdots \wedge z_{p^\infty \mathfrak{f}}(\gamma_d) = \mathrm{det}^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p(\varphi)(1))$$

of

$$\mathrm{det}^{-1}_{K_p} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_p(\varphi)(1)) \simeq \mathrm{det}_{K_p} H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_p(\varphi)(1)).$$

Proof. Since the map $\gamma \mapsto z_{p^\infty\mathfrak{f}}(\gamma)$ is K-linear it suffices to prove Lemma 10 for one particular basis $\{\gamma_i\}$ satisfying its condition. Choosing $\gamma_i = b_i \cdot \gamma$ where b_i is a K-basis of L which is also an $\mathcal{O}_{K_p}$-basis of $\mathcal{O}_{L_p}$ and γ is as in Lemma 9 we deduce Lemma 10 immediately from Lemma 9. □

By Prop. 3.3 there is an isomorphism of G_K-representations

$$V_p(\varphi) \simeq H^1_{et}(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Q}_p)$$

over K_p. The following is an analogue of Lemma 10 where the G_K-stable $\mathcal{O}_{K_p}$-lattice $T_p(\varphi)$ has been replaced by the G_K-stable $\mathcal{O}_{K_p}$-lattice $H^1(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Z}_p)$. Also recall the isomorphism $H^1(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Z}_p)(1) \simeq T_p({}^tB)$.

Lemma 11. *Let $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_d$ be a K-basis of $V_L(\varphi) \simeq H^1(B(\mathbb{C}), \mathbb{Q})$ whose image in $V_p(\varphi) \simeq H^1_{et}(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Q}_p)$ is a $\mathcal{O}_{K_p}$-basis of $H^1(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Z}_p)$ and let $\mathfrak{f}$ be a multiple of $\mathfrak{f}_B$. Assume that $L(\bar{\varphi}, 1) \neq 0$. Then there is an equality of invertible $\mathcal{O}_{K_p}$-submodules*

$$\mathcal{O}_{K_p} \cdot z_{p^\infty\mathfrak{f}}(\tilde{\gamma}_1) \wedge \cdots \wedge z_{p^\infty\mathfrak{f}}(\tilde{\gamma}_d) = \det{}^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p({}^tB))$$

of

$$\det{}^{-1}_{K_p} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_p({}^tB)) \simeq \det{}_{K_p} H^1(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], V_p({}^tB)).$$

Proof. The order $\mathrm{End}_K(B)$ is contained in the maximal order $\mathcal{O}_L$. By choosing $T_p(\varphi)$ to be the $\mathcal{O}_{L_p}$-span of $H^1(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Z}_p)$ inside $V_p(\varphi) \simeq H^1_{et}(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Q}_p)$ we can assume that $H^1(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Z}_p)$ is contained in $T_p(\varphi)$. Define a finite $\mathcal{O}_{K_p}[G_K]$-module M by the exact sequence

$$0 \to H^1(B \otimes_K \bar{\mathbb{Q}}, \mathbb{Z}_p)(1) \simeq T_p({}^tB) \to T_p(\varphi)(1) \to M \to 0. \tag{47}$$

This sequence induces an exact triangle in the derived category of $\mathcal{O}_{K_p}$-modules

$$R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p({}^tB)) \to R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p(\varphi)(1)) \to R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], M) \to$$

and an isomorphism of invertible $\mathcal{O}_{K_p}$-modules

$$\det{}^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p(\varphi)(1)) \simeq \det{}^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p({}^tB)) \tag{48}$$

$$\otimes_{\mathcal{O}_{K_p}} \det^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], M).$$

The complex $R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], M)$ has finite cohomology groups and there is an equality of invertible $\mathcal{O}_{K_p}$-submodules

$$\det^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], M) = \prod_i |H^i(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], M)|_{K_p}^{(-1)^i} = |M|_{K_p}^{-1} \tag{49}$$

of

$$\left(\det^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], M)\right) \otimes_{\mathcal{O}_{K_p}} K_p \simeq K_p.$$

Here $|N|_{K_p}$ denotes the order ideal of a finite $\mathcal{O}_{K_p}$-module N and the last identity in (49) is Tate's formula for the Euler characteristic [57, Thm. I.5.1], or rather its equivariant generalization [30, Thm. 5.1]. If now $\gamma_1, \dots, \gamma_d$ is a basis as in Lemma 10 we deduce from Lemma 10, (48) and (49)

$$\mathcal{O}_{K_p} \cdot z_{p^\infty\mathfrak{f}}(\gamma_1) \wedge \cdots \wedge z_{p^\infty\mathfrak{f}}(\gamma_d) = \det^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p({}^tB)) \cdot |M|_{K_p}^{-1}. \tag{50}$$

On the other hand, if $\tilde{\gamma}_1, \dots, \tilde{\gamma}_d$ is a basis as in Lemma 11 the exact sequence (47) shows that

$$\mathcal{O}_{K_p} \cdot \tilde{\gamma}_1 \wedge \cdots \wedge \tilde{\gamma}_d = |M|_{K_p} \cdot \gamma_1 \wedge \cdots \wedge \gamma_d$$

and K-linearity of $\gamma \mapsto z_{p^\infty\mathfrak{f}}(\gamma)$ gives

$$\mathcal{O}_{K_p} \cdot z_{p^\infty\mathfrak{f}}(\tilde{\gamma}_1) \wedge \cdots \wedge z_{p^\infty\mathfrak{f}}(\tilde{\gamma}_d) = |M|_{K_p} \cdot z_{p^\infty\mathfrak{f}}(\gamma_1) \wedge \cdots \wedge z_{p^\infty\mathfrak{f}}(\gamma_d).$$

Comparing this last identity with (50) gives Lemma 11. □

Since

$$T_p({}^tB) \simeq \operatorname{Ind}_{G_F}^{G_K} T_p({}^tE)$$

Shapiro's Lemma gives a canonical isomorphism

$$R\Gamma(\mathcal{O}_K[\frac{1}{p\mathfrak{f}}], T_p({}^tB)) \simeq R\Gamma(\mathcal{O}_F[\frac{1}{p\mathfrak{f}}], T_p({}^tE)).$$

Furthermore there are canonical isomorphisms

$$H^0(B, \Omega_{B/K}) \simeq H^0(E, \Omega_{E/F})$$

and

$$H^1(B(\mathbb{C}),\mathbb{Z}) \simeq H^1(E(\mathbb{C}\otimes_K F),\mathbb{Z}) \simeq \prod_{v|\infty} H^1(E(F_v),\mathbb{Z}).$$

Lemma 11 and Corollary 9 can therefore be rewritten in terms of E/F as follows.

Lemma 12. *Let E/F be an elliptic curve as in Theorem 1.1, in particular assume that $L(\bar{\psi},1)\neq 0$. Let $\tilde{\gamma}_1,\dots,\tilde{\gamma}_d$ be a K-basis of $H^1(E(\mathbb{C}),\mathbb{Q})$ whose image in $H^1_{et}(E\otimes_K\bar{\mathbb{Q}},\mathbb{Q}_p)$ is a $\mathcal{O}_{K_p}$-basis of $H^1(E\otimes_K\bar{\mathbb{Q}},\mathbb{Z}_p)$ and let $\mathfrak{f}$ be a multiple of $\mathfrak{f}_B = N_{F/K}\mathfrak{f}_E\cdot D_{F/K}$. Put*

$$z := z_{p^\infty\mathfrak{f}}(\tilde{\gamma}_1)\wedge\cdots\wedge z_{p^\infty\mathfrak{f}}(\tilde{\gamma}_d)\in \det_{K_p} H^1(\mathcal{O}_F[\frac{1}{p\mathfrak{f}}],V_p({}^tE)).$$

Then there is an equality of invertible $\mathcal{O}_{K_p}$-submodules

$$\mathcal{O}_{K_p}\cdot z = \det^{-1}_{\mathcal{O}_{K_p}} R\Gamma(\mathcal{O}_F[\frac{1}{p\mathfrak{f}}],T_p({}^tE))$$

of

$$\det^{-1}_{K_p} R\Gamma(\mathcal{O}_F[\frac{1}{p\mathfrak{f}}],V_p({}^tE)) \simeq \det_{K_p} H^1(\mathcal{O}_F[\frac{1}{p\mathfrak{f}}],V_p({}^tE)).$$

Moreover

$$z' := \det_{K_p}(\exp^*)(z)\in \det_{K_p} H^0(E_{F_p},\Omega_{E_{F_p}/F_p})$$

is an element of $\det_K H^0(E,\Omega_{E/F})$ such that

$$\det_{K_\mathbb{R}}(\mathrm{per})\left(z'\right) = L_{p\mathfrak{f}}(\bar{\psi},1)\cdot\mathfrak{a}(z)\cdot\det_{\mathcal{O}_K}\left(\prod_{v|\infty} H^1(E(F_v),\mathbb{Z})\right)$$

where $\mathfrak{a}(z)$ is a fractional $\mathcal{O}_K$-ideal prime to p.

Proof. This is immediate from Lemma 11 and Corollary 9. Note that the assumption

$$\mathcal{O}_{K_p}\cdot\tilde{\gamma}_1\wedge\cdots\wedge\tilde{\gamma}_d = \det_{\mathcal{O}_{K_p}} H^1(B\otimes_K\bar{\mathbb{Q}},\mathbb{Z}_p)$$

on the basis $\tilde{\gamma}_i$ translates into the fact that

$$\mathcal{O}_K\cdot\tilde{\gamma}_1\wedge\cdots\wedge\tilde{\gamma}_d = \mathfrak{a}(z)\cdot\det_{\mathcal{O}_K}\left(\prod_{v|\infty} H^1(E(F_v),\mathbb{Z})\right)$$

for some fractional $\mathcal{O}_K$-ideal $\mathfrak{a}(z)$ prime to p. □

Proof of Theorem 1.1. It suffices to produce an element z as in Prop. 2.3 for all prime numbers p. The content of Lemma 12 is precisely that the element z satisfies the assumptions of Prop. 2.3 for $S = \{v \mid p\mathfrak{f}\}$. Since it was shown in Prop. 4.1 that the p-primary part of $\text{Ш}(E/F)$ (and of $E(F)$) is finite for any prime p, the finiteness of $\text{Ш}(E/F)$ follows from the global formula for its cardinality given by Prop. 2.3. This concludes the proof of Theorem 1.1. □

Acknowledgements

We would like to thank Benedict Gross, Shinichi Kobayashi, Karl Rubin, Chris Skinner, Ye Tian and Shou-Wu Zhang for helpful comments, discussions and encouragement. We are grateful to the referee for valuable suggestions.

We were looking forward to send a copy of this article to John Coates for comments when we received the sudden news of his passing. In a sad and strange coincidence of events it is now entirely fitting to dedicate this article to his memory. John not only initiated this particular field of study some 45 years ago [22] but he also kept constantly moving it forward over the years with his characteristic passion and energy, being an inspiration to many generations of mathematicians.

References

[1] N. Arthaud, On Birch and Swinnerton-Dyer's conjecture for elliptic curves with complex multiplication. I, Compositio Math. 37 (1978), no. 2, 209–232. MR0504632

[2] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives, Progr. Math., 86 Birkhäuser Boston, Inc., Boston, MA, 1990, 333–400. MR1086888

[3] J. Buhler and B. Gross, Arithmetic on elliptic curves with complex multiplication. II, Invent. Math. 79 (1985), no. 1, 11–29. MR0774527

[4] D. Burns and M. Flach, Motivic L-functions and Galois module structures, Math. Ann. 305 (1996), no. 1, 65–102. MR1386106

[5] D. Burns and M. Flach, Tamagawa numbers for motives with (non-commutative) coefficients, Doc. Math. 6 (2001), 501–570. MR1884523

[6] A. Burungale, C. Skinner and Y. Tian, The Birch and Swinnerton-Dyer conjecture: a brief survey, Proc. Sympos. Pure Math., 104 American Mathematical Society, Providence, RI, 2021, 11–29. MR4337415

[7] A. Burungale and Y. Tian, p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin, Invent. Math. 220 (2020), no. 1, 211–253. MR4071412

[8] A. Burungale and Y. Tian, The even parity Goldfeld conjecture: congruent number elliptic curves, J. Number Theory 230 (2022), 161–195, MR4327953

[9] A. Burungale and Y. Tian, A rank zero p-converse to a theorem of Gross-Zagier, Kolyvagin and Rubin, preprint, 2019.

[10] L. Cai, Y. Chen and Y. Liu, Heegner points on modular curves, Trans. Amer. Math. Soc. 370 (2018), no. 5, 3721–3743. MR3766864

[11] L. Cai, C. Li and S. Zhai, On the 2-part of the Birch and Swinnerton-Dyer conjecture for quadratic twists of elliptic curves, J. Lond. Math. Soc. (2) 101 (2020), no. 2, 714–734. MR4093972

[12] L. Cai, J. Shu and Y. Tian, Explicit Gross-Zagier and Waldspurger formulae, Algebra Number Theory 8 (2014), no. 10, 2523–2572. MR3298547

[13] L. Cai, J. Shu and Y. Tian, Cube sum problem and an explicit Gross-Zagier formula, Amer. J. Math. 139 (2017), no. 3, 785–816. MR3650233

[14] C.-L. Chai, B. Conrad and F. Oort, Complex multiplication and lifting problems, Math. Surveys Monogr., 195 American Mathematical Society, Providence, RI, 2014, x+387 pp. MR3137398

[15] C.-L. Chai and F. Oort, Moduli of abelian varieties and p-divisible groups, Clay Math. Proc., 8 American Mathematical Society, Providence, RI, 2009, 441–536. MR2498069

[16] J. Choi, On the 2-adic valuations of central L-values of elliptic curves, J. Number Theory 204 (2019), 405–422. MR3991426

[17] J. Choi and J. Coates, Iwasawa theory of quadratic twists of $X_0(49)$, Acta Math. Sin. (Engl. Ser.) 34 (2018), no. 1, 19–28. MR3735830

[18] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39 (1977), no. 3, 223–251. MR0463176

[19] J. Coates and A. Wiles, On p-adic L-functions and elliptic units, J. Austral. Math. Soc. Ser. A 26 (1978), no. 1, 1–25. MR0510581

[20] J. Coates, Elliptic curves with complex multiplication and Iwasawa theory, Bull. London Math. Soc. 23 (1991), no. 4, 321–350. MR1125859

[21] J. Coates, Lectures on the Birch-Swinnerton-Dyer conjecture, ICCM Not. 1 (2013), no. 2, 29–46. MR3310602

[22] J. Coates, Memories of Kenkichi Iwasawa, Adv. Stud. Pure Math., 86 Mathematical Society of Japan, Tokyo, 2020, i–viii. MR4385073

[23] J. Coates, Y. Kezuka, Y. Li and Y. Tian, On the Birch-Swinnerton-Dyer conjecture for certain elliptic curves with complex multiplication, in preparation, 2023.

[24] J. Coates, M. Kim, Z. Liang and C. Zhao, On the 2-part of the Birch–Swinnerton-Dyer conjecture for elliptic curves with complex multiplication, Münster J. Math. 7 (2014), no. 1, 83–103. MR3271240

[25] J. Coates, J. Li and Y. Li, Classical Iwasawa theory and infinite descent on a family of abelian varieties, Selecta Math. (N.S.) 27 (2021), no. 2, Paper No. 28, 36 pp. MR4247928

[26] J. Coates, Y. Li, Y. Tian and S. Zhai, Quadratic twists of elliptic curves, Proc. Lond. Math. Soc. (3) 110 (2015), no. 2, 357–394. MR3335282

[27] B. Conard, A modern proof of Chevalley's theorem on algebraic groups, J. Ramanujan Math. Soc. 17 (2002), no. 1, 1–18. MR1906417

[28] B. Conrad, Seminar notes on the Birch and Swinnerton-Dyer conjecture, 2015, link.

[29] P. Deligne, Valeurs de fonctions L et périodes d'intégrales, Proc. Sympos. Pure Math., XXXIII American Mathematical Society, Providence, RI, 1979, pp. 313–346. MR0546622

[30] M. Flach, Euler characteristics in relative K-groups, Bull. London Math. Soc. 32 (2000), no. 3, 272–284. MR1750171

[31] M. Flach, The equivariant Tamagawa number conjecture: a survey, Contemp. Math., 358 American Mathematical Society, Providence, RI, 2004, 79–125. MR2088713

[32] M. Flach, Iwasawa theory and motivic L-functions, Pure Appl. Math. Q. 5 (2009), no. 1, 255–294. MR2520461

[33] M. Flach and B. Morin, Weil-étale cohomology and zeta-values of proper regular arithmetic schemes, Doc. Math. 23 (2018), 1425–1560. MR3874942

[34] M. Flach and D. Siebel, Special values of the zeta function of an arithmetic surface, J. Inst. Math. Jussieu 21 (2022), no. 6, 2043–2091. MR4515288

[35] C. Goldstein and N. Schappacher, Séries d'Eisenstein et fonctions L de courbes elliptiques à multiplication complexe, J. Reine Angew. Math. 327 (1981), 184–218. MR0631315

[36] C. Gonzalez-Avilés, On the conjecture of Birch and Swinnerton-Dyer, Trans. Amer. Math. Soc. 349 (1997), no. 10, 4181–4200. MR1390036

[37] B. Gross, Arithmetic on elliptic curves with complex multiplication, Lecture Notes in Math., 776 Springer, Berlin, 1980, iii+95 pp. MR0563921

[38] B. Gross, Minimal models for elliptic curves with complex multiplication, Compositio Math. 45 (1982), no. 2, 155–164. MR0651979

[39] B. Gross, On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication, Progr. Math., 26 Birkhäuser, Boston, MA, 1982, pp. 219–236. MR0685298

[40] B. Gross, On Hecke's decomposition of the regular differentials on the modular curve of prime level, Res. Math. Sci. 5 (2018), no. 1, Paper No. 1, 19 pp. MR3749283

[41] A. Grothendieck and M. Demazure, Schémas en groupes. III: Structure des schémas en groupes réductifs, Lecture Notes in Math., Vol. 153 Springer-Verlag, Berlin-New York, 1970. viii+529 pp. MR0274460

[42] A. Grothendieck, M. Raynaud and D. S. Rim, Groupes de monodromie en géométrie algébrique. I, Lecture Notes in Mathematics, Vol. 288, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Springer-Verlag, 1972, viii+523. MR0354656

[43] Y. Hu, J. Shu and H. Yin, An explicit Gross-Zagier formula related to the Sylvester conjecture, Trans. Amer. Math. Soc. 372 (2019), no. 10, 6905–6925. MR4024542

[44] J. Johnson-Leung and G. Kings, On the equivariant main conjecture for imaginary quadratic fields, J. Reine Angew. Math. 653 (2011), 75–114. MR2794626

[45] D. Jetchev, C. Skinner and X. Wan, The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one, Camb. J. Math. 5 (2017), no. 3, 369–434. MR3684675

[46] K. Kato, Iwasawa theory and p-adic Hodge theory, Kodai Math. J. 16 (1993), no. 1, 1–31. MR1207986

[47] K. Kato, Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. I, Lecture Notes in Math., 1553 Springer-Verlag, Berlin, 1993, 50–163. MR1338860

[48] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Astérisque(2004), no. 295, ix, 117–290. MR2104361

[49] Y. Kezuka, On the p-part of the Birch–Swinnerton-Dyer conjecture for elliptic curves with complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$, Math. Proc. Cambridge Philos. Soc. 164 (2018), no. 1, 67–98. MR3733239

[50] Y. Kezuka, On the main conjecture of Iwasawa theory for certain non-cyclotomic $\mathbb{Z}_p$-extensions, J. Lond. Math. Soc. (2) 100 (2019), no. 1, 107–136. MR3999684

[51] Y. Kezuka, Tamagawa number divisibility of central L-values of twists of the Fermat elliptic curve, J. Théor. Nombres Bordeaux 33 (2021), no. 3, 945–970. MR4402385

[52] Y. Keuzka, On central L-values and the growth of the 3-part of the Tate-Shafarevich group, Int. J. Number Theory 19 (2023), no. 4, 785–802. MR4555385

[53] Y. Kezuka and Y. Li, A classical family of elliptic curves having rank one and the 2-primary part of their Tate-Shafarevich group non-trivial, Doc. Math. 25 (2020), 2115–2147. MR4198839

[54] H.-U. Kufner, Deligne's conjecture on critical values of L-functions for Hecke characters, talk at the Oberwolfach workshop 2326 "Algebraische Zahlentheorie" June 26–30, 2023.

[55] D. Li and Y. Tian, On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D : y^2 = x^3 - D^2x$, Acta Math. Sin. (Engl. Ser.) 16 (2000), no. 2, 229–236. MR1778704

[56] J. S. Milne, On the arithmetic of abelian varieties, Invent. Math. 17 (1972), 177–190. MR0330174

[57] J. S. Milne, Arithmetic duality theorems, Perspect. Math., 1 Academic Press, Inc., Boston, MA, 1986, x+421 pp. MR0881804

[58] H. Montgomery and D. Rohrlich, On the L-functions of canonical Hecke

characters of imaginary quadratic fields. II, Duke Math. J. 49 (1982), no. 4, 937–942. MR0683009

[59] D. Qiu and X. Zhang, Elliptic curves with CM by $\sqrt{-3}$ and 3-adic valuations of their L-series, Manuscripta Math. 108 (2002), no. 3, 385–397. MR1918084

[60] M. Radziwiłłand K. Soundararjan, Moments and distribution of central L-values of quadratic twists of elliptic curves, Invent. Math. 202 (2015), no. 3, 1029–1068. MR3425386

[61] K. Ribet, Twists of modular forms and endomorphisms of abelian varieties, Math. Ann. 253 (1980), no. 1, 43–62. MR0594532

[62] F. Rodríguez Villegas, On the square root of special values of certain L-series, Invent. Math. 106 (1991), no. 3, 549–573. MR1134483

[63] D. Rohrlich, On the L-functions of canonical Hecke characters of imaginary quadratic fields, Duke Math. J. 47 (1980), no. 3, 547–557. MR0587165

[64] E. Rosu, Central values of L-functions of cubic twists, Math. Ann. 378 (2020), no. 3–4, 1327–1370. MR4163529

[65] K. Rubin, Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 64 (1981), no. 3, 455–470. MR0632985

[66] K. Rubin, Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. Math. 89 (1987), no. 3, 527–559. MR0903383

[67] K. Rubin, On the main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. Math. 93 (1988), no. 3, 701–713. MR0952288

[68] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields Invent. Math. 103 (1991), no. 1, 25–68. MR1079839

[69] K. Rubin, More "main conjectures" for imaginary quadratic fields, CRM Proc. Lecture Notes, 4 American Mathematical Society, Providence, RI, 1994, 23–28. MR1260952

[70] N. Schappacher, Periods of Hecke characters, Lecture Notes in Math., 1301 Springer-Verlag, Berlin, 1988, xvi+160 pp. MR0935127

[71] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. (2) 88 (1968), 492–517. MR0236190

[72] G. Shimura, On the zeta-function of an abelian variety with complex multiplication, Ann. of Math. (2) 94 (1971), 504–533. MR0288089

[73] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Kanô Memorial Lectures, No. 1, Publ. Math. Soc. Japan, No. 11, Iwanami Shoten Publishers, TokyoPrinceton University Press, Princeton, NJ, 1971, xiv+267 pp. MR0314766

[74] J. Shu and S. Zhai, Generalized Birch lemma and the 2-part of the Birch and Swinnerton-Dyer conjecture for certain elliptic curves, J. Reine Angew. Math. 775 (2021), 117–143. MR4265185

[75] C. Skinner, A converse to a theorem of Gross, Zagier, and Kolyvagin, Ann. of Math. (2) 191 (2020), no. 2, 329–354. MR4076627

[76] C. Skinner and E. Urban, The Iwasawa main conjectures for GL_2, Invent. Math. 195 (2014), no. 1, 1–277. MR3148103

[77] A. Smith, The congruent numbers have positive natural density, preprint, arXiv:1603.08479, 2016.

[78] A. Smith, 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture, preprint, arXiv:1702.02325, 2017.

[79] A. Smith, The distribution of ℓ^∞-Selmer groups in degree ℓ twist families I, preprint, arXiv:2207.05674, 2022.

[80] A. Smith, The distribution of ℓ^∞-Selmer groups in degree ℓ twist families II, preprint, arXiv:2207.05143, 2022.

[81] F. Thaine, On the ideal class groups of real abelian number fields, Ann. of Math. (2) 128 (1988), no. 1, 1–18. MR0951505

[82] Y. Tian, Congruent numbers with many prime factors, Proc. Natl. Acad. Sci. USA 109 (2012), no. 52, 21256–21258. MR3023667

[83] Y. Tian, Congruent numbers and Heegner points, Camb. J. Math. 2 (2014), no. 1, 117–161. MR3272014

[84] Y. Tian, The congruent number problem and elliptic curves, Proceedings of the International Congress of Mathematicians, 2022.

[85] Y. Tian, X. Yuan and S.-W. Zhang, Genus periods, genus points and congruent number problem, Asian J. Math. 21 (2017), no. 4, 721–773. MR3691853

[86] A. Wiles, Higher explicit reciprocity laws, Ann. of Math. (2) 107 (1978), no. 2, 235–254. MR0480442

[87] S. Zhai, On the weak forms of the 2-part of Birch and Swinnerton-Dyer conjecture, Math. Proc. Cambridge Philos. Soc. 168 (2020), no. 1, 197–209. MR4043826

[88] W. Zhang, Selmer groups and the indivisibility of Heegner points, Camb. J. Math. 2 (2014), no. 2, 191–253. MR3295917

[89] C. Zhao, A criterion for elliptic curves with lowest 2-power in $L(1)$, Math. Proc. Cambridge Philos. Soc. 121 (1997), no. 3, 385–400. MR1434649

[90] C. Zhao, A criterion for elliptic curves with second lowest 2-power in $L(1)$, Math. Proc. Cambridge Philos. Soc. 131 (2001), no. 3, 385–404. MR1866384

[91] C. Zhao, A criterion for elliptic curves with lowest 2-power in $L(1)$. II, Math. Proc. Cambridge Philos. Soc. 134 (2003), no. 3, 407–420. MR1981208

[92] C. Zhao, A criterion for elliptic curves with second lowest 2-power in $L(1)$. II, Acta Math. Sin. (Engl. Ser.) 21 (2005), no. 5, 961–976. MR2176306

Ashay Burungale
Dept. of Mathematics 258
California Institute of Technology
Pasadena, CA 91125
The University of Texas at Austin
Austin, TX 78712
USA
E-mail address: ashayburungale@gmail.com
URL: https://sites.google.com/view/ashayk/home

Matthias Flach
Dept. of Mathematics 253-37
California Institute of Technology
Pasadena, CA 91125
USA
E-mail address: flach@caltech.edu
URL: http://www.math.caltech.edu/people/flach.html

Received July 30, 2022