On the refined 'Birch–Swinnerton-Dyer type' conjectures of Mazur and Tate

Dominik Bullach Matthew H. L. Honnor

We prove a substantial part of conjectures of Mazur and Tate that refine the conjecture of Birch and Swinnerton-Dyer. Our approach, which also leads to some results even finer than the predictions of Mazur and Tate, is via the 'rank-zero component' of the relevant case of the equivariant Tamagawa Number conjecture .

1. Introduction

1.1. Refined conjectures of 'Birch–Swinnerton-Dyer type'

The conjectures of Birch and Swinnerton-Dyer, originating from [BSD65] and developed into their final form by Tate in [Tat95], connect arithmetic invariants of an elliptic curve E defined over $\mathbb{Q}$ with the order of vanishing and the leading term of its Hasse–Weil L-series at $s = 1$. These arithmetic invariants include the rank, as an abelian group, of the group of $\mathbb{Q}$-rational points $E(\mathbb{Q})$ of E and the cardinality of the, conjecturally finite, Tate–Shafarevich group $Ш_{E/\mathbb{Q}}$ of E. For a more detailed introduction, and further reading, the reader may for example consult the survey articles [BST21b; Gro11; SD67; Tat95; Wil06; Zha14].

In the 1980s Mazur and Tate formulated refinements of this conjecture that relate a certain group-ring-valued element θ_K^{MT}, which is constructed from modular symbols and interpolates the values of twisted Hasse–Weil L-series, to Galois-equivariant invariants of the base change of E to an abelian number field K. In particular, the element θ_K^{MT} is expected to encode precise information about the Galois module structure of $E(K)$ and $Ш_{E/K}$.

It is convenient to subdivide the predictions of Mazur and Tate into three separate statements that we will refer to as as their 'order of vanishing', 'weak main conjecture', and 'leading term' component. Each of these components has been very influential and has inspired a range of similar conjectures in a variety of different contexts. This includes the analogue for Heegner points formulated by Darmon [Dar92] and extended by Bertolini and Darmon [BD94], conjectures in the setting of the multiplicative group such as the 'integral Gross–Stark conjecture' (from [Gro88]) and its refinements and generalisations due to Tate [Tat04], Darmon [Dar95], Sano [San14], and Mazur–Rubin [MR16], as well as an analogue for the Rankin–Selberg convolution of two modular forms formulated by Cauchi and Lei [CL22]. Generalisations to modular forms of higher weight have moreover been studied by Ota [Ota23], Kim [Kim23], and Emerton–Pollack–Weston [EPW25]. Kurihara [Kur02, Conj. 0.3] has also formulated a 'strong main conjecture' as a strengthening of the 'weak main conjecture' of Mazur and Tate, and results towards this are due to Kurihara [Kur02], Pollack [Pol05], and Kim–Kurihara [KK21].

To describe the conjectures of Mazur and Tate in more detail, we set $G = G_K \coloneqq \mathrm{Gal}(K/\mathbb{Q})$ and let $\mathcal{R}$ be a ring with the property that $\mathcal{R}[G]$ contains θ_K^{MT}. Work of Stevens [Ste89] shows that one can often take $\mathcal{R} = \mathbb{Z}$ in practice[1], and a self-contained discussion of this integrality question is given in Appendix A.

Write $I_{\mathcal{R},G}$ for the augmentation ideal of $\mathcal{R}[G]$ and $S(E/K)$ for the 'integral Selmer group' defined by Mazur and Tate in [MT87, § 1.7]. If $Ш_{E/K}$ is finite, then $S(E/K)$ is a finitely generated $\mathbb{Z}[G]$-module with the property that, for every prime number p, the 'p-component'

[1] Recent numerical computations of Llerena-Córdova [LC24] suggest that one should however always choose $\mathcal{R}$ big enough such that $|E(K)_{\mathrm{tor}}| \in \mathcal{R}^\times$ in order for the conjectures of Mazur and Tate to be valid.

$S(E/K) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ identifies with the Pontryagin dual $\mathrm{Sel}_{p,E/K}^{\vee}$ of the classical p-primary Selmer group $\mathrm{Sel}_{p,E/K}$ which fits into the fundamental exact sequence (cf., for example, [Sil09, § X.4])

$$0 \longrightarrow (Ш_{E/K}[p^{\infty}])^{\vee} \longrightarrow \mathrm{Sel}_{p,E/K}^{\vee} \longrightarrow \mathrm{Hom}_{\mathbb{Z}_p}(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_p, \mathbb{Z}_p) \longrightarrow 0. \tag{1}$$

We also write $r \coloneqq \mathrm{rk}_{\mathbb{Z}}(E(\mathbb{Q}))$ for the rank of E and $\mathrm{sp}(m_K)$ for the number of primes dividing the conductor m_K of K at which E has split-multiplicative reduction.

(1.1) Conjecture (Mazur–Tate)**.** *The following claims are valid.*

(a) ('order of vanishing', [MT87, Conj. 4]) $\theta_K^{\mathrm{MT}} \in I_{\mathcal{R},G}^{r+\mathrm{sp}(m_K)}$

(b) ('weak main conjecture', [MT87, Conj. 3]) $\theta_K^{\mathrm{MT}} \in \mathrm{Fitt}^0_{\mathcal{R}[G]}(S(E/K) \otimes_{\mathbb{Z}} \mathcal{R})$

This conjecture holds for a fixed ring $\mathcal{R}$ if and only if its 'p-part', namely the conjecture for $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_p$, holds for every prime number p. In this article, we will focus on the p-parts of Conjecture (1.1) for prime numbers p that satisfy the following mild hypothesis, which, for any given pair (E, K), is known to be valid for all but finitely many prime numbers p (see Remarks (1.3) and (2.11) for more details). In the statement we write $\widetilde{E}$ for the reduction of E modulo p.

(1.2) Hypothesis. Assume $p > 3$ is a prime number with the following properties:

(i) The image of the Galois representation $\rho_{E,p}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{T}_p E) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ attached to E contains $\mathrm{SL}_2(\mathbb{Z}_p)$.

(ii) At least one of the following conditions is satisfied:
  (a) K contains no primitive p-th root of unity.
  (b) E has potentially good reduction at p and $\widetilde{E}(\mathbb{F}_p)$ contains no point of order p.

(iii) If E has additive reduction at p, then p is unramified in K.

In particular, p is allowed to be an 'anomalous' prime (in the terminology used by Mazur [Maz72]) if Hypothesis (1.2) (ii) (a) is valid.

(1.3) Remark. If E does not have CM, then Serre has proved in [Ser72] that $\rho_{E,p}$ is surjective for all but finitely many prime numbers p, and asked if in fact $\rho_{E,p}$ is always surjective when $p > 37$. It is conjectured that surjectivity is implied by $p \notin \{2, 3, 5, 11, 13, 17, 37\}$ and the following is known in this direction.

- Zywina has proved in [Zyw22, Thm. 1.10] that a prime that fails surjectivity is bounded from above by $\max\{37, N\}$, where N denotes the conductor of E.
- If E is a semi-stable elliptic curve and $p \geq 11$, then $\rho_{E,p}$ is surjective by a result of Mazur [Maz78, Thm. 4].
- Zywina has proved in [Zyw22, Thm. 1.5] that if $\rho_{E,p}$ is not surjective (with $p > 13$) and $\ell \neq p$ is a prime at which E does not have potentially good reduction, then $\ell \equiv \pm 1 \bmod p$ and p divides the Tamagawa number Tam_ℓ at ℓ.

To state our first main result, we set $r_p \coloneqq \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Sel}_{p,E/K}^{\vee})$ and write $\#\colon \mathbb{Z}_p[G] \to \mathbb{Z}_p[G]$ for the involution that sends $\sigma \in G$ to σ^{-1}.

(1.4) Theorem. *Fix an abelian number field K of conductor m. If the pair (K, p) satisfies Hypothesis (1.2), then the following claims are valid.*

(a) $\theta_K^{\mathrm{MT}} \in I_{\mathbb{Z}_p,G}^{r_p+\mathrm{sp}(m)+2c^{(p)}(K)}$ *with the integer $c^{(p)}(K) \geq 0$ defined in Remark (1.5) (c) below.*

(b) $\theta_K^{\mathrm{MT},\#} \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(\mathrm{Sel}_{p,E/K}^{\vee})$.

(1.5) Remark. (a) The adornment # in Theorem (1.4) (b) can often be removed. To explain this, we write $D(m) \coloneqq \gcd(m, N)$ and $\delta(m) \coloneqq \gcd(D(m), \frac{N}{D(m)})$. If $\delta(m) = 1$,

which is automatically satisfied if E is semistable, then θ_K^{MT} satisfies a 'functional equation' (stated in Remark (2.5)) that implies that θ_K^{MT} and $\theta_K^{\mathrm{MT},\#}$ only differ by a unit in $\mathbb{Z}[G]$. In this case, therefore, Theorem (1.4) (b) also shows that θ_K^{MT} belongs to $\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(\mathrm{Sel}^\vee_{p,E/K})$. However, the ideals generated by θ_K^{MT} and $\theta_K^{\mathrm{MT},\#}$ may not be equal if $\delta(m) > 1$ and the authors would like to thank Juan-Pablo Llerena-Córdova for providing them with numerical examples where they are indeed different.

(b) The perhaps surprising appearance of the factor 2 in Theorem (1.4) (a) can be motivated conceptually as follows. Write $\mathrm{ord}(\theta_K^{\mathrm{MT}})$ for the largest non-negative integer n such that θ_K^{MT} belongs to $I^n_{\mathbb{Z}_p,G}$. By an observation of Mazur and Tate [MT87, (1.6.4)], the known validity of the parity conjecture [DD10] then combines with the functional equation for θ_K^{MT} to imply, if p is odd, that $\mathrm{ord}(\theta_K^{\mathrm{MT}}) \equiv r_p \mod 2$.

(c) To define the integer $c^{(p)}(K)$ that appears in the statement of Theorem (1.4) (a), we set $a_\ell := \ell + 1 - |\widetilde{E}(\mathbb{F}_\ell)|$ for every prime number ℓ. We also define $\mathbf{1}_N(\ell) = 1$ if $\ell \nmid N$ and $\mathbf{1}_N(\ell) = 0$ otherwise. We then let $f^{(p)}_{\ell,K/\mathbb{Q}}$ denote prime-to-p part of the residue degree of ℓ in $K/\mathbb{Q}$ and define the set (see also Lemma (4.8) for an alternative characterisation)

$$C^{(p)}_\times(K) := \{\ell : \ell \not\equiv \zeta(a_\ell - \mathbf{1}_N(\ell)\zeta) \mod p \text{ for all } \zeta \in \overline{\mathbb{Q}_p}^\times \text{ with } \zeta^{f^{(p)}_{\ell,K/\mathbb{Q}}} = 1\}|$$

as well the subsets

$$C^{(p)}_2(K) := \{\ell \nmid N : \ell \neq p, \ell \in C^{(p)}_\times(K), a_\ell = 1, \ell \mid m, \ell^2 \nmid m\}$$
$$C^{(p)}_0(m) := \{\ell \mid N : \ell \neq p, a_\ell = 0, \ell^2 \mid m\}$$

as well as their cardinalities $c^{(p)}_2(K) := |C^{(p)}_2(K)|$ and $c^{(p)}_0(m) := |C^{(p)}_0(m)|$. Given this, we may then define

$$c^{(p)}(K) := c^{(p)}_2(K) + c^{(p)}_0(m).$$

To the knowledge of the authors, Theorem (1.4) (a) is the first general result that combines the contributions from both the rank of $\mathrm{Sel}^\vee_{p,E/\mathbb{Q}}$ and the presence of trivial zeros. That a refinement of Conjecture (1.1) (a) of this shape may hold was first suggested by Ota, who proved in [Ota23, Thm. 1.1] that $\theta_K^{\mathrm{MT}} \in I^{\min\{r_p,p\}}_{\mathbb{Z}_p,G}$ if one assumes Hypothesis (1.2) (i) and certain local conditions at p and at primes ℓ that divide the conductors of K or E. If all split-multiplicative primes ℓ dividing m belong to $C^{(p)}_\times(K)$ and p is big enough, then this also easily implies $\theta_K^{\mathrm{MT}} \in I^{r_p+\mathrm{sp}(m)+c^{(p)}_2(K)}_{\mathbb{Z}_p,G}$ (cf. [Ota18, Cor. 6.3]).
Using entirely different methods, Bergunde and Gehrmann [BG17] have also proved that θ_K^{MT} belongs to $I^{\mathrm{sp}(m)}_{\mathcal{R},G}$ if K is a real abelian field (which settles Conjecture (1.1) (a) in this case, if $r = 0$).
As for Conjecture (1.1) (b), the following results have previously been obtained assuming Hypothesis (1.2) (i) and a slight strengthening of (1.2) (ii) (b), where p is also assumed to be of good reduction for E.

- If one also assumes the vanishing of a relevant μ-invariant and that p does not divide the product of Tamagawa numbers $\mathrm{Tam}(E) := \prod_{\ell|N}(E(\mathbb{Q}_\ell) : E_0(\mathbb{Q}_\ell))$, then Kurihara has proved that the image of θ_K^{MT} in $\mathbb{Z}_p[G_K]$ belongs to the annihilator of a relevant Selmer group for every finite abelian p-extension $K/\mathbb{Q}$ of conductor m coprime to pN (see [Kur14, Rk. 1.2.6]) and to $\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(\mathrm{Sel}^\vee_{p,E/K})$ if E has good ordinary reduction at p, the prime p is tamely ramified in K, and suitable additional assumptions are satisfied (see [Kur03, Thm. 10.]).
- Results of Kataoka (see [Kat21, Thm. 1.8] and [Kat22, Thm. 1.6]) combine to imply the p-part of the 'weak main conjecture' [MT87, Conj. 3] holds if E has good reduction at every $\ell \mid pm$ and one assumes certain further local conditions such as the vanishing of $H^0(\mathbb{Q}(\zeta_{mp^\infty}) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell, E[p^\infty])$ for every $\ell \mid pm$.

If K is a subfield of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, then the result of Theorem (1.4) (b) has previously been proved by Emerton–Pollack–Weston [EPW25]. (We note that the main result of loc. cit. also involves the involution #.)

To state the leading term conjecture of Mazur and Tate, we denote the Tate multiplicative period of E at a prime ℓ of split-multiplicative reduction by $q_{E,\ell} \in \mathbb{Q}_\ell^\times$, and write $\mathrm{Tam}_\ell := \mathrm{ord}_\ell(q_{E,\ell})$ for the Tamagawa number of E at ℓ. We also fix an abelian number field L with Galois group $G_L := \mathrm{Gal}(L/\mathbb{Q})$, write $\mathcal{D}_L^{(\ell)} \subseteq G_L$ for the decomposition group at ℓ, and let $\mathrm{rec}_\ell \colon \mathbb{Q}_\ell^\times \to \mathcal{D}_L^{(\ell)} \subseteq G_L$ denote the associated local reciprocity map.

(1.6) Conjecture ('leading term', [MT87, Conj. 6])**.** *Suppose the conductor m' of L is a product of primes at which E has split-multiplicative reduction. Then one has*

$$\theta_L^{\mathrm{MT}} \equiv \theta_{\mathbb{Q}}^{\mathrm{MT}} \cdot \prod\nolimits_{\ell \mid m'} \big(\mathrm{Tam}_\ell^{-1} \cdot (\mathrm{rec}_\ell(q_{E,\ell}) - 1)\big) \mod I_{\mathcal{R},G_L}^{\mathrm{sp}(m')+1}.$$

The approach of Mazur and Tate is directly motivated by the earlier 'p-adic Birch–Swinnerton-Dyer conjecture' of Mazur–Tate–Teitelbaum (from [MTT86]) and by experimental evidence (see [MT87, § 3.2] and, more recently, the articles of Portillo-Bobadilla [PB19] and Llerena-Córdova [LC24]). Indeed, if $m' = \ell^n$ for some split-multiplicative prime ℓ, then the 'ℓ-part' (so $\mathcal{R} = \mathbb{Z}_\ell$) of Conjecture (1.6) is a special case of the Mazur–Tate–Teitelbaum conjecture and therefore follows from the result of Greenberg and Stevens [GS93] if $\ell \geq 5$ (see also [Kob06]). Note that, due to its Iwasawa-theoretic nature, this approach only sees the 'ℓ-part' of Conjecture (1.6) (hence concerns the component on which ℓ is wildly ramified) and so misses much of the finer aspects of these congruences. The only theoretical evidence in an ℓ-tamely ramified setting (still assuming $m' = \ell^n$) that has hitherto been available in the literature is the result of de Shalit in [Sha95] that applies to elliptic curves of prime conductor ℓ and is proved via an extension of the strategy of Greenberg and Stevens (see also recent work of Lecouturier [Lec23] in this direction).

For a natural number m we let F_m denote the m-th cyclotomic field and write $\theta_m^{\mathrm{MT}} := \theta_{F_m}^{\mathrm{MT}}$. We also let $\mathrm{Sp}(m)$ denote the set of prime numbers dividing m at which E has split-multiplicative reduction.

Our second main result is a refinement of Conjecture (1.6) and reads as follows.

(1.7) Theorem. *Let L be an abelian number field of conductor m' and fix a prime number p such that the pair (L,p) satisfies Hypothesis (1.2). Let K be a subfield of L and take $S' \subseteq \mathrm{Sp}(m')$ to be a subset of primes which split completely in K. Set $M' := m' \prod_{\ell \in S'} \ell^{-\mathrm{ord}_\ell(m')}$, and suppose that all primes ℓ dividing M' satisfy $\ell \in C_\times^{(p)}(L)$.*

Then θ_L^{MT} belongs to $\mathfrak{A} := (\prod_{\ell \in S'} I_{\mathbb{Z}_p,\mathcal{D}_L^{(\ell)}})\mathbb{Z}_p[G_L]$ and one has

$$\theta_L^{\mathrm{MT}} \equiv \pi_{F_{M'}/K}(\theta_{F_{M'}}^{\mathrm{MT}}) \cdot \prod\nolimits_{\ell \in S'} \big(\mathrm{Tam}_\ell^{-1} \cdot (\mathrm{rec}_\ell(q_{E,\ell}) - 1)\big) \mod I_{\mathbb{Z}_p,H}\mathfrak{A}$$

with $H := \mathrm{Gal}(L/K)$ and $F_{M'} := \mathbb{Q}(\zeta_{M'})$ the M'-th cyclotomic field.

(1.8) Remark. (a) Using the 'norm relations' in Proposition (2.4), one can explicitly compute the element $\pi_{F_{M'}/K}(\theta_{F_{M'}}^{\mathrm{MT}})$ that appears in Theorem (1.4) (c) as a linear combination of the elements θ_F^{MT} with F ranging over a suitable set of subfields of K. If the conductor m of K and M'/m are coprime, then one may in fact take this set to be simply $\{K\}$.

(b) If $E(\mathbb{Q})$ has positive rank $r > 0$, then the result of Theorem (1.7) is trivial (by Theorem (1.4) (a)). In any such case, Mazur and Tate predict in [MT87, Conj. 4] a finer congruence for θ_K^{MT} modulo $I_{\mathcal{R},G}^{r+\mathrm{sp}(m)+1}$. If $r = 1$ and $\mathrm{sp}(m) = 0$, results towards this conjecture have recently been obtained by Burns, Kurihara, and Sano in [BKS25]. We expect that their approach can be combined with ours in order to prove the 'p-part' of the full congruence modulo $I_{\mathbb{Z}_p,G}^{r+\mathrm{sp}(m)+1}$, for primes p as in Theorem (1.4), up to a unit in $\mathbb{Z}_p^\times$ if the Birch–Swinnerton-Dyer conjecture holds for E and without ambiguity if

E validates the 'generalised Perrin-Riou conjecture' from [BKS25]. In the generality of Hypothesis (1.2), a result of this kind would require an extension of the comparison of height pairings carried out by Burns and Macías Castillo in [BMC24, Thm. 10.3].

To end the discussion of our main results, we summarise some of the consequences towards the 'p-parts' of the conjectures of Mazur and Tate (that is, the statements of the conjectures after extending scalars from $\mathcal{R}$ to $\mathcal{R} \otimes_{\mathbb{Z}} \mathbb{Z}_p$) in their original formulations from [MT87] in the following corollary. This result is obtained by taking K to be the maximal real subfield F_m^+ of the m-th cyclotomic field F_m in Theorem (1.4) (and taking note of Remark (1.5) (a)), and $K = \mathbb{Q}$ and $L = F_{m'}^+$ with m' a product of split-multiplicative primes in Theorem (1.7). Note that, in these cases, condition (ii) (a) in Hypothesis (1.2) is always satisfied and, if E is a semistable non-CM elliptic curve, then Hypothesis (1.2) (i) is satisfied by Remark (1.3) and Hypothesis (1.2) is empty.

(1.9) Corollary. *If $p \geq 11$ is a prime number and E is a semistable elliptic curve without CM, then the following claims are valid.*

(a) The 'p-part' of the 'order-of-vanishing component' of [MT87, Conj. 4], and hence also the 'weak vanishing conjecture' [MT87, Conj. 1], holds.

(b) The 'p-part' of the 'weak main conjecture' [MT87, Conj. 3] holds.

(c) The 'p-part' of the 'leading term conjecture' [MT87, Conj. 6] holds.

1.2. Overview of proof strategy

The approach we adopt in this article is motivated by the 'Tamagawa Number Conjecture' of Bloch and Kato [BK90], which, when specialised appropriately, is well-known to recover the Birch–Swinnerton-Dyer conjecture (see [Kin11; Ven07; BF24] for details). Since the Mazur–Tate conjectures are themselves an equivariant refinement of the conjecture of Birch–Swinnerton-Dyer, it is natural to view them within the framework of the equivariant refinement of the Tamagawa Number Conjecture. This refinement, formulated independently by Fontaine–Perrin-Riou [FPR94] and Kato [Kat93] in the commutative setting and later generalised to motives with non-commutative coefficients by Burns and Flach [BF01], is commonly referred to as the 'equivariant Tamagawa Number Conjecture' (eTNC). While results in [BMC24; BKS25] suggest there should exist a link between the eTNC and the Mazur–Tate conjectures, the full nature of this connection has hitherto remained unclear.

In this article, we establish a precise link between the relevant case of the eTNC and the conjectures of Mazur and Tate that sheds new light onto their relationship. With 'one inclusion' in the eTNC at a prime satisfying Hypothesis (1.2) recently proved in work of Burns and the first author [BB25] via an enhancement of the general theory of Euler systems and Kato's Euler system (from [Kat04]), this new connection leads directly to Theorems (1.4) and (1.7).

To explain this strategy in a little more detail, we write $z^{\mathrm{Kato}} = (z_m^{\mathrm{Kato}})_{m \in \mathbb{N}}$ for the collection of cohomology classes constructed by Kato in [Kat04] (and adapted to our needs in Theorem (2.8)). Here each class z_m^{Kato} belongs to $H^1(\mathcal{O}_{F_m}[1/Nmp], \mathrm{T}_p E)$ and is linked to the values of the twisted Hasse–Weil L-series at $s = 1$ via Kato's explicit reciprocity law. This reciprocity law can be reformulated (cf. Theorem (2.10)) in such a way that there is a suitable local cohomology class Q_m in $\bigoplus_{v|p} H^1(F_{m,v}, \mathrm{V}_p E)$ with the property that

$$\mathcal{P}_m(z_m^{\mathrm{Kato}}, Q_m) = \theta_m^{\mathrm{MT}}.$$

Here $\mathcal{P}_m(\cdot, \cdot)$ is induced by the cup product pairing on $\bigoplus_{v|p} H^1(F_{m,v}, \mathrm{V}_p E)$ (see § 2.2 for a precise definition).

The local class Q_m has been given a very explicit description by Otsuki in [Ots09] (by building on earlier work of Kurihara [Kur02]) that, amongst other things, enables us to control the denominators of Q_m under condition (1.2) (ii). More precisely, we use Honda theory to construct

a suitable analogue of the 'Artin–Hasse exponential' and show that Q_m can be decomposed as the value of this exponential times the inverses of the relevant Euler factors $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)$, and certain elements $\nu_m^{(\ell)}$ of $\mathbb{Z}_p[G_m]$. The elements $\nu_m^{(\ell)}$ each encode the contribution of a prime $\ell \neq p$ towards Otsuki's construction and are amenable to explicit calculations. In the case of a split-multiplicative prime ℓ, they are also given a cohomological interpretation in § 5 in the following way. For big enough m, one can define a canonical map

$$\vartheta_m^{(\ell)} \colon \mathrm{Det}_{\mathbb{Z}_p[G_m]}\left(\bigoplus\nolimits_{v|\ell} \mathrm{R}\Gamma(F_{m,v}, \mathbb{Z}_p(1))\right)^{-1} \to \mathbb{Q}_p[G_m]$$

such that $\nu_m^{(\ell)}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}$ belongs to the image of this map. This approach is very much in the spirit of the eTNC since its relevant component implies that a similarly defined map,

$$\Theta_m \colon \mathrm{Det}_{\mathbb{Z}_p[G_m]}(\mathrm{R}\Gamma(\mathcal{O}_{F_m}[1/Nmp], \mathrm{T}_pE))^{-1} \to H^1(\mathcal{O}_{F_m}[1/Nmp], \mathrm{V}_pE),$$

sends a $\mathbb{Z}_p[G_m]$-basis of $\mathrm{Det}_{\mathbb{Z}_p[G_m]}(\mathrm{R}\Gamma(\mathcal{O}_{F_m}[1/Nmp], \mathrm{T}_pE))^{-1}$ to z_m^{Kato}. In this direction, the equivariant theory of Euler systems, initiated by Burns, Sakamoto, and Sano in [BSS25] and extended by Burns and the first author in [BB25], can be used to prove that z_m^{Kato} belongs to the image of Θ_m if Hypothesis (1.2) is valid.

To make this latter statement more explicit, one would ideally replace the étale cohomology complex $\mathrm{R}\Gamma(\mathcal{O}_{F_m}[1/Nmp], \mathrm{T}_pE)$ with the 'finite-support cohomology' complex of Bloch and Kato, the cohomology groups of which are classical objects such as $\mathrm{Sel}_{p,E/K}^\vee$. This is also the strategy used in [Kin11; Ven07; BF24] to relate the Tamagawa Number Conjecture with the Birch–Swinnerton-Dyer conjecture. However, a significant obstacle arises when attempting to extend these arguments to the equivariant setting: The finite-support cohomology complex is rarely perfect as a complex of $\mathbb{Z}_p[G_m]$-modules, making it unavailable for equivariant computations. To overcome this, we carefully construct certain auxiliary Selmer complexes in § 4 that are perfect and sufficiently approximate the finite-support cohomology complex. By applying purely algebraic results of the nature proved by Burns and Sano in [BS21, App.] and extended in Appendix B, one may then prove rather generally that one has the inclusion

$$\prod\nolimits_{\ell|m}(\nu_m^{(\ell)}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell))^{\#} \cdot \mathcal{P}_m(\Theta_m(a), Q_m) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G_m]}(\mathrm{Sel}_{p,E/F_m}^\vee) \tag{2}$$

for every $a \in \mathrm{Det}_{\mathbb{Z}_p[G_m]}(\mathrm{R}\Gamma(\mathcal{O}_{F_m}[1/Nmp], \mathrm{T}_pE))^{-1}$. This, when combined with the aforementioned result on the eTNC, then directly leads to Theorem (1.4) (b).

To prove Theorems (1.1) (a) and (1.6), we 'combine' the maps Θ_m and $\vartheta_m^{(\ell)}$. That is to say, we define a certain Nekovář–Selmer complex $\mathrm{SC}_m^\bullet$ with the local condition at a split-multiplicative prime ℓ given by $\bigoplus_{v|\ell}\mathrm{R}\Gamma(F_{m,v}, \mathbb{Z}_p(1))$ such that the left hand side of (2) belongs to the image of a certain map

$$\mathrm{Det}_{\mathbb{Z}_p[G_m]}(\mathrm{SC}_m^\bullet)^{-1} \to \mathbb{Z}_p[G_m].$$

In the context of Iwasawa theory, Nekovář has previously observed in [Nek06, § 0.10] that a complex of this kind detects the presence of trivial zeroes.

Theorem (1.7) is then obtained via a calculation of 'Bockstein morphisms' attached to the complex $\mathrm{SC}_m^\bullet$. These calculations are in many ways parallel to those previously performed in the context of the multiplicative group by Burns [Bur07, § 10] and Burns–Kurihara–Sano [BKS16, § 5]. The definition of Bockstein morphisms is directly inspired by the 'algebraic height pairings' introduced by Nekovář in [Nek06, § 11], and we discuss their general formalism in § B.3.

It might be worth noting that, to date, the authors have found such a cohomological interpretation of $\nu_m^{(\ell)}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}$ only for primes ℓ which are of split-multiplicative reduction for E. In the absence of a similar interpretation for the remaining primes ℓ dividing Nmp, we have to impose the condition $\ell - a_\ell + \mathbf{1}_N(\ell) \not\equiv 0 \mod p$ in Theorem (1.7) in order to ensure the associated Euler factors are invertible in $\mathbb{Z}_p[G_m]$. It would therefore be highly desirable to find a uniform cohomological intepretation of the constructions made by Otsuki in [Ots09], likely within the framework of Kato's 'local ε-constant conjecture' [Kat; FK06] (see also Remark (5.3) in this direction).

1.3. General notation

For the convenience of the reader, we collect some general notation that we use throughout the article.

Algebra Given an abelian group A, we write $A_{\mathrm{tor}} \coloneqq \bigcup_{n\in\mathbb{N}} A[n]$ for its torsion subgroup, and $A_{\mathrm{tf}} \coloneqq A/A_{\mathrm{tor}}$ for its torsionfree quotient. For any ring R, we then write $R[A] \coloneqq \bigoplus_{a\in A} R$ for the group ring of A over R and denote by $x^{\#}$ the image of an element $x \in R[A]$ under the involution $\#\colon R[A] \to R[A]$ that is defined by R-linear extension of the rule $a \mapsto a^{-1}$ for all $a \in A$. If M is an $R[A]$-module, then $M^{\#}$ will denote M with A-action given by $a\cdot m \coloneqq a^{\#}\cdot m$. The completed group ring of A is denoted as $R[\![A]\!] \coloneqq \varprojlim_{U\subseteq A} R[A/U]$ with U ranging over all finite-index subgroups of A. Given a subgroup U of A, we write $I_R(U) \coloneqq \ker\{R[\![U]\!] \to R\}$ for its absolute and $I_{R,U} \coloneqq I_R(U)R[\![A]\!] = \ker\{R[\![A]\!] \to R[\![A/U]\!]\}$ for its relative augmentation ideal. (If the coefficient ring is clear from context, then we suppress the subscript R.)

We write $M^\vee \coloneqq \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ for the Pontryagin dual of a $\mathbb{Z}$-module M. If M is a $\mathbb{Z}[A]$-module, this is endowed with the contragredient A-action. Similarly, the R-linear dual $\mathrm{Hom}_R(M, R)$ of an $R[A]$-module is given the contragredient action. If A is a finite group, then one has the isomorphism

$$\mathrm{Hom}_R(M,R)^{\#} \xrightarrow{\simeq} \mathrm{Hom}_{R[A]}(M, R[A]), \quad f \mapsto \big\{m \mapsto \sum\nolimits_{a\in A} f(am)a^{-1}\big\}. \tag{3}$$

Furthermore, for a fixed prime p (that will always be clear from context), we let $\widehat{A} \coloneqq \varprojlim_{n\in\mathbb{N}}(A/p^nA)$ (or $A^\wedge$ where notationally more convenient) denote the p-adic completion of A. The p-primary component of A is denoted $A[p^\infty] \coloneqq \bigcup_{n\in\mathbb{N}} A[p^n]$.

For any ring commtuative ring R, we write $D(R)$ for the derived category of R-modules. The right-derived functor of a functor $\mathcal{F}$ is denoted $\mathrm{R}\mathcal{F}$. For example, we write $\mathrm{RHom}_R(-,R)$ and $\mathrm{R}\Gamma(R,-) \coloneqq \mathrm{R}\Gamma_{\text{ét}}(\mathrm{Spec}\, R, -)$. Left-derived tensor products are denoted $\otimes^{\mathbb{L}}$. We will use the determinant functor $\mathrm{Det}_R(-)$ of Knudsen–Mumford [KM76] (see also § B.1).

Arithmetic Fix an algebraic closure $\overline{\mathbb{Q}}$ along with an embedding $\iota\colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. For every natural number $m \in \mathbb{N} \coloneqq \mathbb{Z}_{>0}$ we then set $\zeta_m \coloneqq \iota^{-1}(e^{2\pi i/m})$. We also write $F_m \coloneqq \mathbb{Q}(\zeta_m)$ for the m-th cyclotomic field, set $G_m \coloneqq \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$, and recall that one has an isomorphism

$$(\mathbb{Z}/m\mathbb{Z})^\times \to G_m, \quad a \mapsto \sigma_a$$

with σ_a defined by sending ζ_m to ζ_m^a. For every prime number ℓ, we also write Frob_ℓ for a lift of the (arithmetic) Frobenius automorphism at ℓ to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

For every finite Galois extension K of $\mathbb{Q}$ we set $G_K \coloneqq \mathrm{Gal}(K/\mathbb{Q})$ and we say K is an 'abelian number field' if G_K is abelian. Given another finite Galois extension L of $\mathbb{Q}$ that contains K, we then write $\pi_{L/K}\colon \mathbb{C}[G_L] \to \mathbb{C}[G_K]$ for the natural epimorphism induced by the restriction map $G_L \to G_K$.

Let E be an an elliptic curve E defined over $\mathbb{Q}$ and of conductor $N = N_E$, which will be fixed throughout the article. We also fix a global minimal Weierstraß equation for E and write ω_E for the corresponding Néron differential. We will often regard E as an elliptic curve over a finite extension F of $\mathbb{Q}_\ell$ for some prime number ℓ, and write $\widehat{E}$ for the formal group of E (usually with respect to ω_E). The formal logarithm and formal exponential map of $\widehat{E}$ are denoted as $\log_{\widehat{E}}$ and $\exp_{\widehat{E}}$, respectively. The reduction of E modulo the maximal ideal of F (with respect to a Weierstraß equation that is minimal over F) will be written as $\widetilde{E}$. We also write $E_0(F)$ and $E_1(F)$ for the subgroups of $E(F)$ comprising points that, over the residue field $\mathbb{F}$ of F, reduce to a non-singular point and to the identity of $\widetilde{E}(\mathbb{F})$, respectively. We also use the semi-local variants $E_i(K_\ell) \coloneqq \bigoplus_{v|\ell} E_i(K_v)$ for $i \in \{\varnothing, 0, 1\}$ if K is a number field and ℓ a prime number.

For a prime number p, assumed to be odd in this article, we denote the p-adic Tate modules of E as

$$\mathrm{T}_pE \coloneqq \varprojlim_{n\in\mathbb{N}} E[p^n] \quad \text{and} \quad \mathrm{V}_pE \coloneqq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \mathrm{T}_pE.$$

These are endowed with a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Given an abelian field K, we often also write $T_{K/\mathbb{Q}}$ for the induced representation $\mathrm{Ind}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}^{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}(\mathrm{T}_pE) = (\mathrm{T}_pE)\otimes_{\mathbb{Z}_p}\mathbb{Z}_p[G]$ on which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts by $\sigma\cdot(a\otimes b) \coloneqq (\sigma a)\otimes(\overline{\sigma}^{-1}b)$. Here $\overline{\sigma}$ is the image of $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in G. We let $\mathbf{1}_S(x)$ denote the indicator function of a set S. If S is the set of prime numbers not dividing an integer N, we write simply $\mathbf{1}_N(x)$.

2. Local points and Mazur–Tate elements

In this section we define the modular elements of Mazur and Tate, and relate them to Kato's Euler system. To do this, we follow the approach of Kurihara [Kur02], as further developed by Kobayashi [Kob03; Kob06] and Otsuki [Ots09], to construct useful local points. After some preliminaries, the main result of this section is stated as Theorem (2.10).

2.1. Modular symbols

Fix a minimal Weierstrass model of E over $\mathbb{Z}$ and write ω_E for the corresponding Néron differential. We also fix generators γ^+ and γ^- of the subgroups $H_1(E(\mathbb{C}),\mathbb{Z})^+$ and $H_1(E(\mathbb{C}),\mathbb{Z})^-$ of $H_1(E(\mathbb{C}),\mathbb{Z})$ on which complex conjugation acts by $+1$ and -1, respectively. Write $c_\infty\in\{1,2\}$ for the number of connected components of $E(\mathbb{R})$, and define periods of E by setting

$$\Omega^+ = \Omega^+_{\omega,\gamma} \coloneqq \int_{E(\mathbb{R})} |\,\omega_E\,| = c_\infty\cdot\int_{\gamma^+}\omega_E \quad\text{and}\quad \Omega^- = \Omega^-_{\omega,\gamma} \coloneqq c_\infty\int_{\gamma^-}\omega_E.$$

We assume γ^+ and γ^- are chosen in such a way that $\Omega^+>0$ and $\Omega^-\in i\mathbb{R}_{>0}$.

(2.1) Remark. Artin formalism suggests that the above normalisation of periods, which is consistent with [WW22], is best suited to the study of special values of L-series. We note, however, that our convention slightly differs from that chosen by Mazur and Tate in [MT87]. To be more precise, Mazur and Tate use the periods $\frac{1}{2}\Omega^+$ and $\frac{c_\infty}{2}\Omega^-$. Since the difference only concerns a possible factor of 2, this will be irrelevant to our main results.

By the modularity theorem [BCDT01] there is a normalised newform f of weight 2 associated to the isogeny class of E, which we use to define the map

$$\lambda_f\colon\mathbb{Q}\to\mathbb{C},\quad a\mapsto 2\pi\int_0^\infty f(a+i\tau)\mathrm{d}\tau.$$

In addition, we define maps $[\cdot]_E^+\colon\mathbb{Q}\to\mathbb{R}$ and $[\cdot]_E^-\colon\mathbb{Q}\to\mathbb{R}$ by means of

$$\lambda_f(a) = [a]_E^+\Omega^+ + [a]_E^-\Omega^- \quad\text{for all } a\in\mathbb{Q}.$$

(2.2) Definition. *For every abelian number field K of conductor $m=m_K$, we define the 'Mazur–Tate element'*

$$\theta_K^{\mathrm{MT}} \coloneqq \pi_{F_m/K}\Big(\sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}([\tfrac{a}{m}]_E^+ + [\tfrac{a}{m}]_E^-)\sigma_a\Big) \quad\in\mathbb{R}[G_K].$$

If $K=F_m$, then we abbreviate this to $\theta_m^{\mathrm{MT}} \coloneqq \theta_{F_m}^{\mathrm{MT}}$.

(2.3) Remark. (a) The Manin–Drinfeld theorem [Man72; Dri73] implies that the modular symbols $[\cdot]^\pm$ are rational-valued, hence θ_K^{MT} belongs to $\mathbb{Q}[G_K]$. In addition, the Mazur–Tate elements have nice integrality properties which are discussed in detail in Appendix A.

(b) Write F_m^+ for the maximal real subfield of F_m. Then $\frac{1}{2}\theta_{F_m^+}^{\mathrm{MT}}$ coincides with the 'modular element' defined by Mazur and Tate in [MT87, (1.2)]. This follows from the fact that $\lambda(\frac{-a}{m}) = \overline{\lambda(\frac{a}{m})}$, (cf. [WW22, Lem. 5]).

(c) Birch's formula (see [MTT86, (8.6)]) implies that, for every primitive Dirichlet character χ of conductor m, the Mazur–Tate element is related to L-values via the interpolation property

$$\chi(\theta_m^{\mathrm{MT}}) = \frac{G(\chi)\cdot L(E,\chi^{-1},1)}{\Omega^{\epsilon(\chi)}}$$

with the (primitive) 'Gauss sum' $G(\chi) \coloneqq \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(\sigma_a)e^{2\pi ia/m} \in \mathbb{C}$ and $\epsilon(\chi) = +$ if χ is even and $\epsilon(\chi) = -$ if χ is odd.

The Mazur–Tate elements satisfy the following norm relations.

(2.4) Proposition (Mazur–Tate)**.** *For every $m \in \mathbb{N}$ and prime number ℓ one has that*

$$\pi_{m\ell/m}(\theta_{m\ell}^{\mathrm{MT}}) = \begin{cases} (a_\ell - \mathbf{1}_N(\ell)\sigma_\ell^{-1} - \sigma_\ell)\cdot\theta_m^{\mathrm{MT}} & \text{if } \ell \nmid m, \\ a_\ell\theta_m^{\mathrm{MT}} - \mathbf{1}_N(\ell)\mathrm{N}_{F_m/F_{m/\ell}}\theta_{m/\ell}^{\mathrm{MT}} & \text{if } \ell \mid m. \end{cases}$$

Proof. This follows from [MTT86, (4.2)], see also [MT87, (1.3) on p. 717]. □

(2.5) Remark. Write $D(m) \coloneqq \gcd(m, N)$. If $\gcd(D(m), \frac{N}{D(m)}) = 1$, then the Mazur–Tate elements satisfy the 'functional equation' (see [MT87, (1.6.2)])

$$\theta_m^{\mathrm{MT}} = \epsilon_f \cdot \sigma_{-Q}^{-1} \cdot (\theta_m^{\mathrm{MT}})^{\#},$$

where $Q \coloneqq N/D(m)$ and $\epsilon_f \in \{\pm 1\}$. In this case, therefore, θ_m^{MT} and $(\theta_m^{\mathrm{MT}})^{\#}$ generate the same $\mathbb{Z}[G_m]$-submodule of $\mathbb{Q}[G_m]$. The proof of this functional equation follows from the corresponding result for modular symbols (see [MTT86, § 6 Prop.]), and is given, in the case m and N are coprime in [Ota18, Prop. 5.16]. The proof for general m and N is identical.

2.2. Local Tate duality

For every finite place v of K we write $E(K_v)^\wedge \coloneqq \varprojlim_{n\in\mathbb{N}}(E(K_v)/p^nE(K_v))$ for the p-adic completion of the group of K_v-rational points $E(K_v)$ of E. We denote the local Kummer map as $\kappa^{(v)}\colon E(K_v)^\wedge \hookrightarrow H^1(K_v, \mathrm{T}_pE)$ and, for every prime number ℓ, denote its semilocal variant as $\kappa^{(\ell)}\colon \bigoplus_{v|\ell} E(K_v)^\wedge \hookrightarrow H^1(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})$. Following Bloch and Kato [BK90], we define local spaces

$$H^1_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \coloneqq \mathrm{im}(\kappa^{(\ell)}) \quad \text{and} \quad H^1_{/f}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \coloneqq \mathrm{coker}(\kappa^{(\ell)}).$$

Recall that the Weil pairing induces a canonical isomorphism $(\mathrm{T}_pE)^*(1) \cong \mathrm{T}_pE$ and hence a cup product pairing

$$H^1(K_v, \mathrm{T}_pE) \times H^1(K_v, \mathrm{T}_pE) \cong H^1(K_v, \mathrm{T}_pE) \times H^1(K_v, (\mathrm{T}_pE)^*(1)) \xrightarrow{\cup} H^2(K_v, \mathbb{Z}_p(1)) \cong \mathbb{Z}_p$$

for every p-adic place v of K. Taking the sum over all p-adic places of K then gives a pairing

$$H^1(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \times H^1(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \to \bigoplus\nolimits_{v|p} \mathbb{Z}_p \xrightarrow{\mathrm{Trace}} \mathbb{Z}_p. \tag{4}$$

By [BK90, Prop. 3.8] the space $H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ is self-orthogonal under (4) and so it induces a pairing

$$(\cdot,\cdot)_{E/K}\colon H^1_{/f}(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \times H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \to \mathbb{Z}_p. \tag{5}$$

In particular, every $Q = (Q_v)_{v|p}$ in $H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}}) = \bigoplus_{v|p}\mathrm{im}(\kappa^{(v)})$ gives rise to a map

$$\mathcal{P}_K(\cdot, Q)\colon H^1(K, \mathrm{T}_pE) \to \mathbb{Z}_p[G], \quad a \mapsto \sum\nolimits_{\sigma\in G} (\mathrm{loc}^{(p)}_{/f}(\sigma a), Q)_{E/K}\sigma^{-1}, \tag{6}$$

where, as before, $G = \mathrm{Gal}(K/\mathbb{Q})$ and $\mathrm{loc}^{(p)}_{/f} \coloneqq \oplus_{v|p}\mathrm{loc}^{(v)}_{/f}$ with $\mathrm{loc}^{(v)}_{/f}$ the composite of the restriction map $\mathrm{loc}^{(v)}\colon H^1(K, \mathrm{T}_pE) \to H^1(K_v, \mathrm{T}_pE)$ and the projection onto $H^1_{/f}(K_v, \mathrm{T}_pE)$.

(2.6) Remark. Write $V_{K/\mathbb{Q}} \coloneqq T_{K/\mathbb{Q}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. We note that the pairing $(\cdot,\cdot)_{E/K}$ can be linearly extended to a pairing on $H^1_{/f}(\mathbb{Q}_p, V_{K/\mathbb{Q}}) \times H^1_f(\mathbb{Q}_p, V_{K/\mathbb{Q}})$. As a consequence, for every $Q \in H^1_f(\mathbb{Q}_p, V_{K/\mathbb{Q}})$ we also obtain a map $H^1(K, \mathrm{V}_p E) \to \mathbb{Q}_p[G]$ that we denote by $\mathcal{P}_K(\cdot, Q)$ as well. Since the target of (6) is $\mathbb{Z}_p$-torsion free, it factors through the natural map $H^1(K, \mathrm{T}_p E) \to H^1(K, \mathrm{V}_p E)$ and so we feel this slight abuse of notation is not unjustified.

Write

$$\exp^*_{K_v} \colon H^1_{/f}(K_v, \mathrm{V}_p E) \xrightarrow{\simeq} \mathrm{Fil}^0 D_{\mathrm{dR}, K_v}(\mathrm{V}_p E) \tag{7}$$

for the 'dual exponential map' that is defined by Kato in [Kat93, Ch. II, § 1.2.4] and define the composite map

$$\exp^*_{\omega_E} \colon \bigoplus\nolimits_{v|p} H^1_{/f}(K_v, \mathrm{V}_p E) \xrightarrow{\oplus_{v|p} \exp^*_{K_v}} \bigoplus\nolimits_{v|p} \mathrm{Fil}^0 D_{\mathrm{dR}, K_v}(\mathrm{V}_p E) \xrightarrow{\simeq} (\mathbb{Q}_p \otimes_{\mathbb{Q}} K) \otimes_{\mathbb{Q}} H^0(E, \Omega^1_{E/\mathbb{Q}}) \xrightarrow{\omega_E \mapsto 1} \mathbb{Q}_p \otimes_{\mathbb{Q}} K,$$

where the second arrow is the comparison isomorphism of p-adic Hodge theory. The following result then records the basic properties of the pairing $\mathcal{P}(\cdot,\cdot)$.

(2.7) Lemma. *Fix $Q = (Q_v)_{v|p} \in H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ and let $a \in H^1(\mathcal{O}_{K,S}, \mathrm{T}_p E)$.*

(a) Assume that p is unramified in K if E has additive reduction at p. Then one has

$$\mathcal{P}_K(a, Q) = \sum\nolimits_{\sigma \in G_K} \mathrm{Tr}_{(\mathbb{Q}_p \otimes_{\mathbb{Q}} K)/\mathbb{Q}_p}\big((\log_{\widehat{E}}(Q_v))_{v|p} \cdot (\exp^*_{\omega_E} \circ \mathrm{loc}^{(p)}_{/f})(\sigma a)\big)\sigma^{-1}. \tag{8}$$

(b) For every $x \in \mathbb{Z}_p[G]$ one has $x \cdot \mathcal{P}_K(a, Q) = \mathcal{P}_K(x \cdot a, Q) = \mathcal{P}_K(a, x^{\#} \cdot Q)$.

(c) If L is a subfield of K and $H \coloneqq \mathrm{Gal}(K/L)$, then in $\mathbb{Z}_p[G_L]$ one has

$$\pi_{K/L}\big(\mathcal{P}_K(a, Q)\big) = \mathcal{P}_L(\mathrm{cores}_{K/L}(a), \mathrm{Tr}_{K/L}(Q)).$$

In particular, if a is fixed by H, then $\mathcal{P}_K(a, Q) = \mathcal{P}_L(a, \mathrm{Tr}_{K/L}(Q)) \cdot \mathrm{N}_H$ in $\mathbb{Z}_p[G_K]$.

Proof. In light of Remark (2.6), we may verify claim (a) after extending scalars to $\mathbb{Q}_p$. The assumed validity of Hypothesis (1.2) (iii) moreover implies that our fixed minimal Weierstraß equation (over $\mathbb{Q}$) is still minimal over K_v for every $v \mid p$, and hence that ω_E is a Néron differential for E/K_v. Given this, the key point is then that, by [BK90, Ex. 3.11], one has the commutative diagram

$$\begin{array}{ccccc} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_{/f}(\mathbb{Q}_p, T_{K/\mathbb{Q}}) & & \xrightarrow{\qquad\qquad\exp^*_{\omega_E}\qquad\qquad} & & \mathbb{Q}_p \otimes_{\mathbb{Q}} K \\ \simeq\downarrow & & & & \simeq\downarrow \\ (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}}))^* & \xrightarrow{\simeq} & \bigoplus\nolimits_{v|p} (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \widehat{E}(K_v))^* & \xrightarrow{\exp^*_{\widehat{E}}} & (\mathbb{Q}_p \otimes_{\mathbb{Q}} K)^*. \end{array}$$

Here the vertical isomorphism on the left is induced by the fact that the pairing $(\cdot,\cdot)_{E/K}$ is perfect after extending scalars to $\mathbb{Q}_p$ (by [BK90, Prop. 3.8]), and the vertical isomorphism on the right is the map $\mathbb{Q}_p \otimes_{\mathbb{Q}} K \to (\mathbb{Q}_p \otimes_{\mathbb{Q}} K)^*$ that sends $a \mapsto \{\alpha \mapsto \mathrm{Tr}_{(\mathbb{Q}_p \otimes_{\mathbb{Q}} K)/\mathbb{Q}_p}(a\alpha)\}$ (and so is induced by the trace pairing). Finally, the map $\exp^*_{\widehat{E}}$ is induced by the duals of the exponential maps $\exp_{\widehat{E}}$ of the formal groups $\widehat{E}$ of E/K_v (associated to ω_E).
Now, the commutativity of the diagram implies $(x, \exp_{\widehat{E}}(\alpha))_{E/K} = \mathrm{Tr}_{(\mathbb{Q}_p \otimes_{\mathbb{Q}} K)/\mathbb{Q}_p}(\alpha \exp^*_{\omega_E}(x))$ for all $x \in H^1_{/f}(\mathbb{Q}_p, V_{K/\mathbb{Q}})$ and $\alpha \in \mathbb{Q}_p \otimes_{\mathbb{Q}} K$. Claim (a) then follows upon substituting $\alpha = \log_{\widehat{E}}(Q)$.
Claims (b) and (c), in turn, are verified by means of direct calculations (cf. [Ots09, Lem. 3.5]). □

2.3. Kato's Euler system

Recall that, for every prime number ℓ, the 'Euler factor' at $\ell \neq p$ is defined as

$$\mathrm{Eul}_\ell(X) \coloneqq \det_{\mathbb{Q}_p}(1 - \mathrm{Frob}_\ell^{-1} X \mid (\mathrm{V}_p E)^{\mathcal{I}_\ell}) \quad \in \mathbb{Q}_p[X],$$

where $\mathcal{I}_\ell \subseteq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denotes a choice of inertia subgroup at ℓ. Explicitly, one has (see, for example, [Kin11, Ex. 1.26])

$$\mathrm{Eul}_\ell(X) = 1 - a_\ell \ell^{-1} X + \mathbf{1}_N(\ell)\ell^{-1}X^2.$$

For any integer n, we let S_n denote the set of prime divisors of n. We also write $S_{n\infty} \coloneqq S_n \cup \{\infty\}$ and set

$$S(K) \coloneqq S_{pNm\infty}$$

with $m \coloneqq m_K$ the conductor of K and $N \coloneqq N_E$ the conductor of E.

(2.8) Theorem (Kato)**.** *Let $\mathscr{F}$ denote the set of finite abelian extensions of $\mathbb{Q}$. Then there exists a collection of elements*

$$z^{\mathrm{Kato}} \coloneqq (z_K^{\mathrm{Kato}})_{K\in\mathscr{F}} \in \prod\nolimits_{K\in\mathscr{F}} H^1(\mathcal{O}_{K,S(K)}, \mathrm{V}_p E)$$

with the following properties.

(a) If $L, K \in \mathscr{F}$ with $K \subseteq L$, then one has

$$\mathrm{Cores}_{L/K}(z_L^{\mathrm{Kato}}) = \big(\prod\nolimits_{\ell\in S(L)\setminus S(K)} \mathrm{Eul}_\ell(\mathrm{Frob}_\ell^{-1})\big)\cdot z_K^{\mathrm{Kato}},$$

where $\mathrm{Cores}_{L/K}\colon H^1(L, \mathrm{V}_pE) \to H^1(K, \mathrm{V}_pE)$ denotes the corestriction map.

(b) Set

$$y_K^{\mathrm{Kato}} \coloneqq \big(\prod\nolimits_{\ell\in S_N\setminus S_{pm_K}} \mathrm{Eul}_\ell(\mathrm{Frob}_\ell^{-1})\big)^{-1}\cdot z_K^{\mathrm{Kato}}.$$

If $E[p]$ is irreducible as an $\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module and $E(K)$ contains no point of order p, then $c_\infty y_K^{\mathrm{Kato}}$ (and hence also $c_\infty z_K^{\mathrm{Kato}}$) belongs to $H^1(\mathcal{O}_{K,S(K)}, \mathrm{T}_pE)$.

(c) One has the equality

$$(\oplus_{v|p} \exp^*_{K_v})(z_K^{\mathrm{Kato}}) = \big(\sum\nolimits_{\chi\in\widehat{G_K}} \frac{L_{S(K)}(E,\chi^{-1},1)}{\Omega^{\mathrm{sgn}(\chi)}} e_\chi\big)\otimes\omega_E$$

in $\bigoplus_{v|p}\mathrm{Fil}^0_{\mathrm{dR},K_v}(\mathrm{V}_pE) \cong \mathbb{Q}_p\otimes_{\mathbb{Q}} H^0(E,\Omega^1_{E/K}) = (\mathbb{Q}_p\otimes_{\mathbb{Q}} K)\otimes_{\mathbb{Q}} H^0(E,\Omega^1_{E/\mathbb{Q}})$.

Proof. The elements z_K^{Kato} are defined by slightly modifying the elements ${}_{c,d}z_m^{(p)}(f,1,1,\xi,S(K))$ constructed by Kato in [Kat04, (8.1.3)]. The integrality property in claim (b) is proved by the argument of [Kat04, p. 12.6] (following Delbourgo [Del08, App. A], see also [Kat21, Thm. 6.1]) and the 'explicit reciprocity law' in claim (c) follows from [Kat04, Thm. 9.7 and 12.5]. □

(2.9) Remark. Suppose the Galois representation $\rho_{E,p}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{T}_pE) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ contains $\mathrm{SL}_2(\mathbb{Z}_p)$. Then $E[p]$ is an irreducible $\mathbb{F}_p[G_{\mathbb{Q}}]$-module and $E(K)$ has no non-trivial point of order p for all finite abelian extensions K of $\mathbb{Q}$.

We now explain the link between Kato's Euler system, as normalised in Theorem (2.8), and the Mazur–Tate elements θ_K^{MT}.

To prepare for the statement of our result in this direction we define, for $a \in \mathbb{N}$, an automorphism $\tilde{\sigma}_a$ of $\mathbb{Z}[\zeta_m]$ as follows. Set $m_2 \coloneqq \prod_{\ell|a}\ell^{\mathrm{ord}_\ell(m)}$ and $m_1 \coloneqq m/m_2$ so that we have a decomposition $m = m_1m_2$. We then take $\tilde{\sigma}_a$ to be the image of σ_a under the splitting map $G_{m_1} \hookrightarrow G_{m_1}\times G_{m_2} \cong G_m$ that sends $g \mapsto (g, \mathrm{id}_{F_{m_2}})$. In particular, $\tilde{\sigma}_a$ agrees with σ_a if a is coprime with m, and is the identity map if $m \mid a$ (more generally, if and only if $m_1 = 1$).

The main result of this section is as follows.

(2.10) Theorem. *Let m be a natural number coprime to p and fix $n \in \mathbb{Z}_{\geq 0}$. If E has additive reduction at p, then we take $n = 0$. We also write τ for the p-adic Teichmüller character (regarded as a character $G_{mp^n} \to \mathbb{Z}_p^\times$). Then there exists*

$$\mathfrak{k}_{mp^n} \in \mathbb{Q}_p\otimes_{\mathbb{Z}_p} E_1(F_{mp^n,p}) \coloneqq \mathbb{Q}_p\otimes_{\mathbb{Z}_p}\bigoplus\nolimits_{v|p} E_1(F_{mp^n,v})$$

and, for every prime number $\ell \mid m$, an element $\nu_{mp^n}^{(\ell)} \in \mathbb{Z}_p[G_{mp^n}]$ with the following properties.

(a) One has

$$\Big(\prod\nolimits_{\ell\mid m}\mathrm{Eul}_\ell(\tilde\sigma_\ell)^{-1}\cdot\nu^{(\ell)}_{mp^n}\Big)^{\#}\cdot\mathcal{P}_{F_{mp^n}}(y^{\mathrm{Kato}}_{mp^n},\mathfrak{k}_{mp^n})=\theta^{\mathrm{MT}}_{mp^n}.$$

(b) The element $(1-e_\tau)\mathfrak{k}_{mp^n}$ *belongs to (the image of)* $E_1(F_{mp^n,p})+(p\mathrm{Eul}_p(\sigma_p))^{-1}E_1(F_{m,p})$. *If* p *is not a multiplicative prime and* $a_p\not\equiv 1 \mod p$, *then also* $\mathfrak{k}_{mp^n}$ *belongs to* $E_1(F_{mp^n,p})$.

(c) One has the following equalities in $\mathbb{Q}_p\otimes_{\mathbb{Z}_p}E_1(F_{mp^n,p})$.

(i) $\mathrm{Tr}_{mp^{n+1}/mp^n}(\mathfrak{k}_{mp^{n+1}})=\begin{cases}a_p\mathfrak{k}_{mp^n}-\mathbf{1}_N(p)\mathfrak{k}_{mp^{n-1}} & \text{if } n\geq 1,\\ (a_p-\mathbf{1}_N(p)\sigma_p-\sigma_p^{-1})\mathfrak{k}_m & \text{if } n=0.\end{cases}$

(ii) For every prime number $\ell\neq p$, *one has* $\mathrm{Tr}_{\ell mp^n/mp^n}(\mathfrak{k}_{\ell mp^n})=\begin{cases}\ell\mathfrak{k}_{mp^n} & \text{if } \ell\mid m,\\ -\sigma_\ell^{-1}\mathfrak{k}_{mp^n} & \text{if } \ell\nmid m.\end{cases}$

(d) Write $\mathcal{D}^{(\ell)}_{mp^n}\subseteq G_{mp^n}$ *for the decomposition group of* ℓ. *If any of the following hold:*

- $a_\ell=2$, $\ell\nmid N$ *and* $\ell^2\nmid m$,
- $a_\ell=1$ *and* $\ell\mid N$,
- $a_\ell=0$, $\ell\mid N$ *and* $\ell^2\mid m$,

then $\nu^{(\ell)}_{mp^n}$ *belongs to* $I_{\mathcal{D}^{(\ell)}_{mp^n}}\coloneqq\ker\{\mathbb{Z}_p[G_{mp^n}]\to\mathbb{Z}_p[G_{mp^n}/\mathcal{D}^{(\ell)}_{mp^n}]\}$. *Furthermore, one has the following congruence modulo* $I^2_{\mathcal{D}^{(\ell)}_{mp^n}}$,

$$\nu^{(\ell)}_{mp^n}\equiv\begin{cases}0 & \text{if } a_\ell=2,\ell\nmid N \text{ and } \ell^2\nmid m,\\ \ell^{-(\mathrm{ord}_\ell(m)-1)}(1-\tilde\sigma_\ell) & \text{if } a_\ell=1 \text{ and } \ell\mid N,\\ 0 & \text{if } a_\ell=0,\ell\mid N \text{ and } \ell^2\mid m.\end{cases}$$

(e) Each $\nu^{(\ell)}_{mp^n}$ *belongs to the ideal of* $\mathbb{Z}_p[G_{mp^n}]$ *that is generated by* $\mathrm{Eul}_\ell(\tilde\sigma_\ell)$ *and* $\mathrm{N}_{\mathcal{I}^{(\ell)}_{mp^n}}$, *with* $\mathcal{I}^{(\ell)}_{mp^n}\subseteq\mathcal{D}^{(\ell)}_{mp^n}$ *the inertia subgroup at* ℓ.

The proof of this result is given in § 2.5.3 after a number of preparations. To end this section, we comment on the hypothesis $a_p\not\equiv 1 \mod p$ that appears in claim (b) of Theorem (2.10).

(2.11) Remark. Primes p of good reduction for which $\widetilde{E}(\mathbb{F}_p)$ contains a point of order p (or, equivalently, for which $a_p\coloneqq p+1-|\widetilde{E}(\mathbb{F}_p)|$ is congruent to $1 \mod p$) are called 'anomalous' by Mazur in [Maz72]. Hasse's bound implies that one has $a_p=1$ for any anomalous prime $p\geq 7$, and this combines with a result of Serre [Ser81] to show that the set of anomalous primes is of density zero. It is not known whether an elliptic curve can have infinitely many anomalous primes (although Mazur has conjectured this to be possible and it would follow from conjectures of Hardy–Littlewood, see [Qin16], and Lang–Trotter [LT76]). Given any set of prime numbers $\mathcal{P}$, one can however construct an elliptic curve $E/\mathbb{Q}$ such that every prime in $\mathcal{P}$ is anomalous for E (see [Maz72, Lem. 8.19]).
If $E(\mathbb{Q})$ contains a torsion point, then the set of anomalous primes for E is either empty, consists of a single element, or else is contained in $\{2,3,5\}$ (see [Maz72, Lem. 8.18]). For example, if $E(\mathbb{Q})$ contains a point of prime-order $\ell\neq p$ and E has good reduction at $p>5$, then $a_p\not\equiv 1 \mod p$.

2.4. Otsuki's elements

In this section we first recall important definitions and results from Otsuki's article [Ots09], and then further develop certain aspects of Otsuki's theory. This will be crucial to the proof of Theorem (2.10).

2.4.1. Review of Otsuki theory

For every natural number $a \in \mathbb{N}$, we will use the $\mathbb{Q}$-algebra homomorphism

$$\hat{\sigma}_a \colon \mathbb{Q}[X] \to \mathbb{Q}[X], \quad \hat{\sigma}_a(X) \coloneqq X^a.$$

(2.12) Lemma ([Ots09, Prop. 1.3])**.** *The following claims are valid for every $m \in \mathbb{N}$ and prime number ℓ.*

(a) $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)$ *defines an invertible* $\mathbb{Q}$*-algebra endomorphism of* $\mathbb{Q}[X]/(X^m-1)$*. In particular, there is a unique well-defined element* $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1} \in \mathrm{End}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}[X]/(X^m-1))$*.*

(b) If $\ell \nmid m$*, then* $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)$ *defines an invertible* $\mathbb{Q}$*-algebra endomorphism of* $\mathbb{Q}[X]/(\Phi_m)$ *with* Φ_m *the* m*-th cyclotomic polynomial. In other words,* $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}$ *induces a well-defined element of* $\mathrm{End}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}[X]/(\Phi_m))$*.*

Proof. To prove claim (a), it suffices to show that $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)$ defines an injective endomorphism of the finite-dimensional $\mathbb{Q}$-vector space $\mathbb{Q}[X]/(X^m-1)$ and this is verified in [Ots09, Prop. 1.3]. As for claim (b), it follows from the fact that $\hat{\sigma}_\ell$ preserves the ideal (Φ_m) if $\ell \nmid m$ that $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)$ does the same. Since we know $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)$ to be injective by claim (a), this shows that $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)$ restricts to an automorphism of the $\mathbb{Q}$-subvector space $(\Phi_m)/(X^m-1)$ of $\mathbb{Q}[X]/(X^m-1)$. As a consequence, $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}$ preserves $(\Phi_m)/(X^m-1)$. This shows that $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)$ and $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}$ both descend to elements of $\mathrm{End}_{\mathbb{Q}\text{-alg}}(\mathbb{Q}[X]/(\Phi_m))$, as required to prove claim (b). □

The endomorphism $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}$ introduced above is rather inexplicit but does satisfy a certain inductive relation that will be useful in computations. To state this relation, we shall use certain constructions, themselves based on [Kur02, § 2.2], that are made by Otsuki in [Ots09] and which we now recall. For a prime divisor ℓ of m and integer $i \in \mathbb{Z}_{\geq 0}$ we inductively define elements $c_i^{(\ell)} \in \mathbb{Z}[1/\ell]$ as follows. Set $c_0^{(\ell)} \coloneqq 0$, $c_1^{(\ell)} \coloneqq 1$ and, for $i \geq 2$,

$$c_{i+1}^{(\ell)} \coloneqq \frac{a_\ell}{\ell} c_i^{(\ell)} - \frac{\mathbf{1}_N(\ell)}{\ell} c_{i-1}^{(\ell)}. \tag{9}$$

For $i \in \mathbb{Z}_{\geq 0}$ we also define a polynomial $\widetilde{F}_\ell^{(i)}(X) \in \mathbb{Z}[1/\ell][X]$ by

$$\widetilde{F}_\ell^{(i)}(X) \coloneqq c_{i+1}^{(\ell)} - \frac{\mathbf{1}_N(\ell)}{\ell} c_i^{(\ell)} X.$$

By induction on $j \in \mathbb{N}$, one then proves the key relation

$$\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1} = \sum_{i=0}^{j-1} c_{i+1}^{(l)} \hat{\sigma}_\ell^i + \widetilde{F}_\ell^{(j)}(\hat{\sigma}_\ell) \mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1} \hat{\sigma}_\ell^j, \tag{10}$$

(see [Ots09, Lem. 2.6] for details).

2.4.2. The definition of Otsuki's elements

In this section we discuss the canonical local elements defined by Otsuki in [Ots09, Def. 2.4].

(2.13) Definition. *For every natural number m, we define*

$$x_m \coloneqq \Big(\big(\textstyle\prod_{\ell \mid mp} \mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1} \big)(X) \Big)(\zeta_m) \in F_m.$$

(2.14) Remark. Our definition of x_m differs slightly from that of Otsuki in [Ots09]. To be precise, if we write x_m^{Otsuki} for the element denoted as x'_m in [Ots09, Def. 2.4], then

$$x_m = \begin{cases} x_m^{\mathrm{Otsuki}} & \text{if } p \mid m, \\ \mathrm{Eul}_p(\sigma_p)^{-1} x_m^{\mathrm{Otsuki}} & \text{if } p \nmid m. \end{cases}$$

In the remainder of this section, we will make the element x_m more explicit. To do this, it is convenient to introduce some further notation. For every prime number ℓ and integers $0 \leq j \leq n$, we set $e^{(\ell)}_{n,0} := \ell^{-(n-1)}\mathrm{N}_{F_{\ell^n}/\mathbb{Q}}$ and $e^{(\ell)}_{n,j} := \ell^{-(n-j)}\mathrm{N}_{F_{\ell^n}/F_{\ell^j}}$. If $m' \in \mathbb{N}$ is coprime with ℓ, then one has

$$\zeta_{m'\ell^j} = \omega^{(\ell)}_{n,j} \cdot \sum_{i=0}^{n} \zeta_{m'\ell^i} \quad \text{with} \quad \omega^{(\ell)}_{n,j} := \begin{cases} (e^{(\ell)}_{n,j} - e^{(\ell)}_{n,j-1}) & \text{if } j \geq 2, \\ e^{(\ell)}_{n,1} & \text{if } j = 1, \\ -\tilde{\sigma}_\ell e^{(\ell)}_{n,0} & \text{if } j = 0. \end{cases} \tag{11}$$

Here $\omega^{(\ell)}_{n,j}$ is considered to be an element of $\mathbb{Z}_p[G_{m'\ell^n}]$ via the splitting $G_{m'\ell^n} \cong G_{m'} \times G_{\ell^n}$ induced by the relevant restriction maps. We may then define an element of $\mathbb{Z}[1/\ell][G_{\ell^n}][X]$ by

$$\lambda^{(\ell)}_n(X) := \mathrm{Eul}_\ell(X)\Big(\sum_{i=0}^{n-1} c^{(l)}_{i+1}\omega^{(\ell)}_{n,n-i}\Big) - \widetilde{F}^{(n)}_\ell(X)Xe^{(\ell)}_{n,0}.$$

(2.15) Lemma. *For every prime number $\ell \neq p$ and natural number n the polynomial $\lambda^{(\ell)}_n(X)$ has the property that, for every $m' \in \mathbb{N}$ with $\ell \nmid m'$, one has the following equality in $F_{\ell^n m'}$.*

$$\big(\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}(X)\big)(\zeta_{m'\ell^n}) = \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \lambda^{(\ell)}_n(\tilde{\sigma}_\ell) \cdot \sum_{i=0}^{n} \zeta_{m'\ell^i}.$$

Proof. We first make the useful observation that one has

$$\big((\widetilde{F}^{(n)}_\ell(\hat{\sigma}_\ell)\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}\hat{\sigma}^n_\ell)(X)\big)(\zeta_{m'\ell^n}) = \widetilde{F}^{(n)}_\ell(\sigma_\ell)\mathrm{Eul}_\ell(\sigma_\ell)^{-1} \cdot \zeta_{m'}. \tag{12}$$

To justify this, we note that $\hat{\sigma}^n_\ell(X) = X^{\ell^n}$ belongs to the image of the map $\mathbb{Q}[X]/(X^{m'}-1) \to \mathbb{Q}[X]/(X^{\ell^n m'}-1)$ that is defined by sending $X \mapsto X^{\ell^n}$. From the commutative diagram

$$\begin{array}{ccc} \mathbb{Q}[X]/(X^{m'}-1) & \xrightarrow{X \mapsto X^{\ell^n}} & \mathbb{Q}[X]/(X^{\ell^n m'}-1) \\ \downarrow{\scriptstyle X \mapsto \zeta_{m'}} & & \downarrow{\scriptstyle X \mapsto \zeta_{\ell^n m'}} \\ \mathbb{Q}[\zeta_{m'}] & \xrightarrow{\zeta_{m'} \mapsto \zeta_{m'}} & \mathbb{Q}[\zeta_{\ell^n m'}] \end{array}$$

we therefore see that is suffices to compute $(\widetilde{F}^{(n)}_\ell(\hat{\sigma}_\ell)\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1})(X)$ evaluated at $X = \zeta_{m'}$. By Lemma (2.12) (b) the endomorphism $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}$ of $\mathbb{Q}[X]/(X^{m'}-1)$ descends to $\mathbb{Q}[X]/(\Phi_{m'})$ (and corresponds with multiplication by $\mathrm{Eul}_\ell(\sigma_\ell)^{-1}$ under the isomorphism $\mathbb{Q}[X]/(\Phi_{m'}) \cong \mathbb{Q}[\zeta_{m'}]$ that sends $X \mapsto \zeta_{m'}$), so this computation can be done in $\mathbb{Q}[\zeta_{m'}]$ and leads to the claimed equality (12).
Now, (12) combines with the relation (10) to imply that one has

$$\begin{aligned} \big(\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}(X)\big)(\zeta_{m'\ell^n}) &= \big(\sum_{i=0}^{n-1} c^{(l)}_{i+1}\hat{\sigma}^i_\ell(X) + (\widetilde{F}^{(n)}_\ell(\hat{\sigma}_\ell)\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}\hat{\sigma}^n_\ell)(X)\big)(\zeta_{m'\ell^n}) \\ &= \big(\sum_{i=0}^{n-1} c^{(l)}_{i+1}\zeta_{m'\ell^{n-i}}\big) + \big(\widetilde{F}^{(n)}_\ell(\tilde{\sigma}_\ell)\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\zeta_{m'}\big) \\ &= \big(\sum_{i=0}^{n-1} c^{(l)}_{i+1}\omega^{(\ell)}_{n,n-i} + \widetilde{F}^{(n)}_\ell(\tilde{\sigma}_\ell)\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\omega^{(\ell)}_{n,0}\big) \cdot \sum_{i=0}^{n} \zeta_{m'\ell^i} \\ &= \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \lambda^{(\ell)}_n(\tilde{\sigma}_\ell) \cdot \sum_{i=0}^{n} \zeta_{m'\ell^i}, \end{aligned}$$

as claimed. □

For every natural number $m \in \mathbb{N}$ and prime divisor $\ell \neq p$ of m, we define

$$\nu^{(\ell)}_m := \lambda^{(l)}_{\mathrm{ord}_\ell(m)}(\tilde{\sigma}_\ell) \in \mathbb{Z}_p[G_m].$$

The following result, in which we write $m_0 \coloneqq \prod_{\ell|m} \ell$ for the 'squarefree radical' of an integer m, describes the contribution to the definition of x_m of the factors $\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1}$ for $\ell \neq p$ in terms of the elements $\nu_m^{(\ell)}$.

(2.16) Proposition. *Let m be a natural number coprime to p. For every integer $n \geq 0$ one has*

$$x_{mp^n} = \big(\prod_{\ell|m} \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \nu_{mp^n}^{(\ell)}\big) \cdot \sum_{m_0|d|m} (\mathrm{Eul}_p(\hat{\sigma}_p)^{-1}(X))(\zeta_{dp^n}).$$

Proof. Factorise m as $\prod_{i=1}^s \ell_i^{n_i}$ and set $\ell_{s+1} \coloneqq p$ and $n_{s+1} \coloneqq n$ so that $mp^n = \prod_{i=1}^{s+1} \ell_i^{n_i}$. We shall prove by induction on $0 \leq j \leq s$ that one has

$$x_{mp^n} = \big(\prod_{i=1}^{j} \mathrm{Eul}_{\ell_i}(\tilde{\sigma}_{\ell_i})^{-1} \cdot \nu_{mp^n}^{(\ell_i)}\big) \cdot \Big(\sum_{m_{j,0}|d|m_j} \big(\prod_{i=j+1}^{s+1} \mathrm{Eul}_{\ell_i}(\hat{\sigma}_{\ell_i})^{-1}\big)(X)\Big)(\zeta_{dmp^n/m_j}) \tag{13}$$

with $m_j \coloneqq \prod_{i=1}^{j} \ell_i^{n_i}$. Taking $j = s$, this then implies claim (a). If $j = 0$, the claim follows directly from the definition of x_{mp^n}. For the inductive step we assume that $j > 0$ and that (13) is valid for $j - 1$. We introduce the notation

$$\tilde{c}_q^{(\ell_i)} \coloneqq \begin{cases} c_q^{(\ell_i)} & \text{if } 0 \leq q \leq n_i - 1, \\ \widetilde{F}_\ell^{(n_i)}(\hat{\sigma}_\ell)\mathrm{Eul}_\ell(\hat{\sigma}_\ell)^{-1} & \text{if } q = n_i, \end{cases}$$

so that the relation (10) can be compactly written as

$$\mathrm{Eul}_{\ell_i}(\hat{\sigma}_{\ell_i})^{-1} = \sum_{q=0}^{n_i} \tilde{c}_{q+1}^{(\ell_i)} \hat{\sigma}_{\ell_i}^q.$$

Define $\mathscr{A}(j) \coloneqq \prod_{i=j+1}^{s+1} \{0, \ldots, n_i\}$ and, for every $a = (a_{j+1}, \ldots, a_s) \in \mathscr{A}(j)$, write $|a| \coloneqq \prod_{i=j+1}^{s+1} a_i$. Then we have

$$\begin{aligned} \big(\prod_{i=j}^{s+1} \mathrm{Eul}_{\ell_i}(\hat{\sigma}_{\ell_i})^{-1}\big)(X) &= \Big(\mathrm{Eul}_{\ell_j}(\hat{\sigma}_{\ell_j})^{-1} \cdot \prod_{i=j+1}^{s+1} \big(\sum_{q=0}^{n_i} \tilde{c}_{q+1}^{(\ell_i)} \hat{\sigma}_{\ell_i}^q\big)\Big)(X) \\ &= \sum_{a \in \mathscr{A}(j)} \big(\prod_{i=j+1}^{s+1} \tilde{c}_{a_i}^{(\ell_i)}\big) \cdot \mathrm{Eul}_{\ell_j}(\hat{\sigma}_{\ell_j})^{-1}(X^{|a|}). \end{aligned} \tag{14}$$

Fix a divisor d' of m_{j-1} and define $d'_j \coloneqq d'mp^n/m_{j-1}$. If we set

$$C_q^{(\ell_i)} \coloneqq \begin{cases} c_q^{(\ell_i)} & \text{if } 0 \leq q \leq n_i - 1, \\ \widetilde{F}_\ell^{(n_i)}(\sigma_\ell)\mathrm{Eul}_\ell(\sigma_\ell)^{-1} & \text{if } q = n_i, \end{cases}$$

then (14) combines with (12) to imply that

$$\big(\prod_{i=j}^{s+1} \mathrm{Eul}_{\ell_i}(\hat{\sigma}_{\ell_i})^{-1}\big)(X)(\zeta_{d'_j}) = \sum_{a \in \mathscr{A}(j)} \big(\prod_{i=j+1}^{s+1} C_{a_i}^{(\ell_i)}\big) \cdot \big(\mathrm{Eul}_{\ell_j}(\hat{\sigma}_{\ell_j})^{-1}(X)\big)(\zeta_{d'_j/|a|}).$$

Let d be a divisor of m_j and set $d_j \coloneqq dmp^n/m_j$, then the same computation also shows that one has

$$\big(\prod_{i=j+1}^{s+1} \mathrm{Eul}_{\ell_i}(\hat{\sigma}_{\ell_i})^{-1}\big)(X)(\zeta_{d_j}) = \sum_{a \in \mathscr{A}(j)} \big(\prod_{i=j+1}^{s+1} C_{a_i}^{(\ell_i)}\big) \cdot \zeta_{d_j/|a|}. \tag{15}$$

Next we recall that Lemma (2.15) proves an equality

$$\big(\mathrm{Eul}_{\ell_j}(\hat{\sigma}_{\ell_j})^{-1}(X)\big)(\zeta_{d'_j/|a|}) = \mathrm{Eul}_{\ell_j}(\tilde{\sigma}_{\ell_j})^{-1} \cdot \lambda_{n_j}(\tilde{\sigma}_\ell) \cdot \sum_{q=0}^{n_j-1} \zeta_{d'_j/(\ell^q|a|)}. \tag{16}$$

Now, every $m_{j,0} \mid d \mid m_j$ is of the form $d'\ell^{n_j-q}$ for some $m_{j-1,0} \mid d' \mid m_{j-1}$ and $q \in \{0,\dots,n_j-1\}$ so that d_j is of the form d'_j/ℓ^q. As a consequence, we may calculate that

$$\begin{aligned}
&\sum_{m_{j-1,0}|d'|m_{j-1}} \big(\prod_{i=j}^{s+1} \mathrm{Eul}_{\ell_i}(\hat{\sigma}_{\ell_i})^{-1}\big)(X)(\zeta_{d'_j}) \\
&\overset{(14)}{=} \sum_{m_{j-1,0}|d'|m_{j-1}} \sum_{a\in\mathscr{A}(j)} \big(\prod_{i=j+1}^{s+1} \tilde{c}_{a_i}^{(\ell_i)}\big) \cdot \big(\mathrm{Eul}_{\ell_j}(\hat{\sigma}_{\ell_j})^{-1}(X)\big)(\zeta_{d'_j/|a|}) \\
&\overset{(2.15)}{=} \sum_{m_{j-1,0}|d'|m_{j-1}} \sum_{a\in\mathscr{A}(j)} \big(\prod_{i=j+1}^{s+1} C_{a_i}^{(\ell_i)}\big) \cdot \big(\mathrm{Eul}_{\ell_j}(\tilde{\sigma}_{\ell_j})^{-1} \cdot \lambda_{n_j}^{(\ell_j)}(\tilde{\sigma}_\ell) \cdot \sum_{q=0}^{n_j-1} \zeta_{d'_j/(\ell^q|a|)}\big) \\
&\overset{(16)}{=} \mathrm{Eul}_{\ell_j}(\tilde{\sigma}_{\ell_j})^{-1} \cdot \lambda_{n_j}^{(\ell_j)}(\tilde{\sigma}_\ell) \cdot \sum_{m_{j,0}|d|m_j} \sum_{a\in\mathscr{A}(j)} \big(\prod_{i=j+1}^{s+1} C_{a_i}^{(\ell_i)}\big) \cdot \zeta_{d_j/|a|} \\
&\overset{(15)}{=} \mathrm{Eul}_{\ell_j}(\tilde{\sigma}_{\ell_j})^{-1} \cdot \lambda_{n_j}^{(\ell_j)}(\tilde{\sigma}_\ell) \cdot \Big(\sum_{m_{j,0}|d|m_j} \big(\prod_{i=j+1}^{s+1} \mathrm{Eul}_{\ell_i}(\hat{\sigma}_{\ell_i})^{-1}\big)(X)\Big)(\zeta_{d_j}).
\end{aligned}$$

By the induction hypothesis, this shows the claimed equality (13) and therefore concludes the proof of the proposition. □

2.4.3. Congruences modulo augmentation ideals

In this section we investigate when the elements $\nu_{mp^n}^{(\ell)}$ belong to a relevant augmentation ideal and also compute its class modulo the square of the augmentation ideal. In particular, the second part of Theorem (2.10) (d) will be a consequence of these calculations.
We recall that we have fixed an *odd* prime p, which will be important in the proof of the following result.

(2.17) Proposition. *Let $m > 1$ be a natural number, let $\ell \neq p$ be a prime number, and set $n \coloneqq \mathrm{ord}_\ell(m)$. Then the following claims are valid.*

(a) Write $\mathcal{D}_m^{(\ell)} \subseteq G_m$ for the decomposition group of ℓ. The element $\nu_m^{(\ell)}$ belongs to $I_{\mathcal{D}_m^{(\ell)}} \coloneqq \ker\{\mathbb{Z}_p[G_m] \to \mathbb{Z}_p[G_m/\mathcal{D}_m^{(\ell)}]\}$ if any of the following hold:
- *$a_\ell = 2$, $\ell \nmid N$ and $\ell^2 \nmid m$,*
- *$a_\ell = 1$ and $\ell \mid N$,*
- *$a_\ell = 0$, $\ell \mid N$ and $\ell^2 \mid m$.*

(b) One has $\nu_m^{(\ell)} \equiv c_n^{(\ell)}(1 - a_\ell\tilde{\sigma}_\ell) + \frac{\mathbf{1}_N(\ell)}{\ell}(\ell c_n^{(\ell)}\tilde{\sigma}_\ell^2 + c_{n-1}^{(\ell)}\tilde{\sigma}_\ell(\ell-1)) \pmod{I_{D_m^{(\ell)}}^2}$.

Proof. It is convenient to set $m' \coloneqq m\ell^{-n}$ in this proof. To prove claim (a), we first note that, since ℓ is totally ramified in $F_{m'\ell^n}/F_{m'\ell^j}$, one has that $\mathrm{Gal}(F_{m'\ell^n}/F_{m'\ell^j})$ is contained in $\mathcal{D}_m^{(\ell)}$ for every $j \in \{0,\dots,n\}$. As a consequence, we have

$$e_{n,j}^{(\ell)} \equiv 1 \pmod{I_{\mathcal{D}_m^{(\ell)}}} \quad \text{if } j \in \{1,\dots,n\}. \tag{17}$$

In particular, $e_{n,n-i}^{(\ell)} - e_{n,n-i-1}^{(\ell)}$ belongs to $I_{\mathcal{D}_m^{(\ell)}}$ for $i \in \{0,\dots,n-2\}$, and therefore

$$\begin{aligned}
\nu_m^{(\ell)} = \lambda_n^{(\ell)}(\tilde{\sigma}_\ell) &\equiv \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)c_n^{(\ell)}e_{n,1}^{(\ell)} - \widetilde{F}_\ell^{(n)}(\tilde{\sigma}_\ell)\tilde{\sigma}_\ell e_{n,0}^{(\ell)} \pmod{I_{\mathcal{D}_m^{(\ell)}}} \\
&\overset{(17)}{\equiv} \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)c_n^{(\ell)} - \widetilde{F}_\ell^{(n)}(\tilde{\sigma}_\ell)(\ell-1) \pmod{I_{\mathcal{D}_m^{(\ell)}}}.
\end{aligned} \tag{18}$$

For ease of notation we write $\overline{\lambda}_{m',i}^{(\ell)}$ for the quantity on the right hand side of (18) with n replaced by i. Note that, if $i = n$, then (18) gives that $\lambda_n^{(\ell)}(\tilde{\sigma}_\ell) \equiv \overline{\lambda}_{m',n}^{(\ell)} \pmod{I_{\mathcal{D}_m^{(\ell)}}}$. We work

inductively on i and begin by considering $\overline{\lambda}^{(\ell)}_{m',1}$. Since, $c^{(\ell)}_0 \coloneqq 0$ and $c^{(\ell)}_1 \coloneqq 1$ we can calculate

$$\begin{aligned}\overline{\lambda}^{(\ell)}_{m',1} &= \mathrm{Eul}_\ell(\tilde{\sigma}_\ell) - (\frac{a_\ell}{\ell} - \frac{\mathbf{1}_N(\ell)}{\ell}\tilde{\sigma}_\ell)(\ell-1)\\ &= \frac{1}{\ell}(\ell - a_\ell\tilde{\sigma}_\ell + \mathbf{1}_N(\ell)\tilde{\sigma}_\ell^2) - (\frac{a_\ell}{\ell} - \frac{\mathbf{1}_N(\ell)}{\ell}\tilde{\sigma}_\ell)(\ell-1)\\ &\equiv \frac{1}{\ell}(\ell - a_\ell + \mathbf{1}_N(\ell)) - (\frac{a_\ell}{\ell} - \frac{\mathbf{1}_N(\ell)}{\ell})(\ell-1) \pmod{I_{\mathcal{D}^{(\ell)}_m}}\\ &\equiv 1 - a_\ell + \mathbf{1}_N(\ell) \pmod{I_{\mathcal{D}^{(\ell)}_m}}.\end{aligned}$$

It follows that $\overline{\lambda}^{(\ell)}_{m',1} \in I_{\mathcal{D}^{(\ell)}_m}$ if either of the following hold:

- $a_\ell = 2$, $\ell \nmid N$,
- $a_\ell = 1$ and $\ell \mid N$.

If $n = 1$ then $\lambda^{(\ell)}_1(\tilde{\sigma}_\ell) \equiv \overline{\lambda}^{(\ell)}_{m',1} \pmod{I_{\mathcal{D}^{(\ell)}_m}}$, therefore the first two points in claim (a) hold in this case. We now consider $\overline{\lambda}^{(\ell)}_{m',2}$. Using (9) we calculate

$$\overline{\lambda}^{(\ell)}_{m',2} = \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)\frac{a_\ell}{\ell} - (\frac{a_\ell}{\ell}\frac{a_\ell}{\ell} - \frac{\mathbf{1}_N(\ell)}{\ell} - \frac{\mathbf{1}_N(\ell)}{\ell}\frac{a_\ell}{\ell}\tilde{\sigma}_\ell)(\ell-1) = \frac{a_\ell}{\ell}\overline{\lambda}^{(\ell)}_{m',1} + \frac{\mathbf{1}_N(\ell)}{\ell}(\ell-1). \quad (19)$$

Therefore, if either

- $\overline{\lambda}^{(\ell)}_{m',1} \in I_{\mathcal{D}^{(\ell)}_m}$ and $\ell \mid N$, or
- $a_\ell = 0$ and $\ell \mid N$.

Then $\overline{\lambda}^{(\ell)}_{m',2} \in I_{\mathcal{D}^{(\ell)}_m}$. By the calculations done for $\overline{\lambda}^{(\ell)}_{m',1}$ we have that claim (a) holds if $n \in \{1,2\}$. Suppose $n \geq 3$ and let $i = 3, \ldots, n$. By applying (9) to $\overline{\lambda}^{(\ell)}_{m',i}$ one calculates

$$\overline{\lambda}^{(\ell)}_{m',i} = \frac{a_\ell}{\ell}\overline{\lambda}^{(\ell)}_{m',i-1} - \frac{\mathbf{1}_N(\ell)}{\ell}\overline{\lambda}^{(\ell)}_{m',i-2}.$$

As with $\overline{\lambda}^{(\ell)}_{m',2}$, we observe that if either

- $\overline{\lambda}^{(\ell)}_{m',i-1} \in I_{\mathcal{D}^{(\ell)}_m}$ and $\ell \mid N$, or
- $a_\ell = 0$ and $\ell \mid N$,

then $\overline{\lambda}^{(\ell)}_{m',i} \in I_{\mathcal{D}^{(\ell)}_m}$. Considering this argument inductively completes the proof of (a).
To prove claim (b), let $j \in \{1, \ldots, n\}$ and calculate

$$e^{(\ell)}_{n,j} = \frac{1}{\ell^{n-j}}\mathrm{N}_{F_{\ell^n}/F_{\ell^j}} = \frac{1}{\ell^{n-j}}\big(\ell^{n-j} + \sum\nolimits_{\sigma \in \mathrm{Gal}(F_{\ell^n}/F_{\ell^j})}(\sigma - 1)\big). \quad (20)$$

Under the isomorphism $I_{\mathcal{D}^{(\ell)}_m}/I^2_{\mathcal{D}^{(\ell)}_m} \cong \mathcal{D}^{(\ell)}_m \otimes \mathbb{Z}_p$ induced by $\sigma - 1 \mapsto \sigma$, the sum in (20) is mapped to $\prod_{\sigma \in \mathrm{Gal}(F_{\ell^n}/F_{\ell^j})}\sigma$. If σ has odd order, then $\sigma \neq \sigma^{-1}$ and so both (element and its inverse) appear in the above product. It follows that only the (unique) element of order 2 does not cancel. Since p is odd, this element is trivial in $\mathcal{D}^{(\ell)}_m \otimes \mathbb{Z}_p$. Therefore,

$$e^{(\ell)}_{n,j} \equiv 1 \pmod{I^2_{\mathcal{D}^{(\ell)}_m}}.$$

Similarly, we have $\tilde{\sigma}_\ell e^{(\ell)}_{n,0} \equiv \tilde{\sigma}_\ell(\ell-1) \pmod{I^2_{\mathcal{D}^{(\ell)}_m}}$. It therefore follows from the definition that

$$\begin{aligned}\nu^{(\ell)}_m = \lambda^{(\ell)}_n(\tilde{\sigma}_\ell) &\equiv \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)c^{(\ell)}_n - \tilde{F}^{(n)}_\ell(\tilde{\sigma}_\ell)\tilde{\sigma}_\ell(\ell-1) \pmod{I^2_{\mathcal{D}^{(\ell)}_m}}\\ &\equiv \frac{1}{\ell}(\ell - a_\ell\tilde{\sigma}_\ell + \mathbf{1}_N(\ell)\tilde{\sigma}_\ell^2)c^{(\ell)}_n - (c^{(\ell)}_{n+1} - \frac{\mathbf{1}_N(\ell)}{\ell}c^{(\ell)}_n\tilde{\sigma}_\ell)\tilde{\sigma}_\ell(\ell-1) \pmod{I^2_{\mathcal{D}^{(\ell)}_m}}\end{aligned}$$

The result follows from rearranging and the fact that $c^{(\ell)}_{n+1} = \frac{a_\ell}{\ell}c^{(\ell)}_n - \frac{\mathbf{1}_N(\ell)}{\ell}c^{(\ell)}_{n-1}$. □

2.4.4. Norm relations

We end this section by proving two norm relations for the elements $\nu_{mp^n}^{(\ell)}$ which are required to establish the claimed congruence of Mazur–Tate elements in Theorem (1.7).
For natural numbers $a, b \in \mathbb{N}$ with $a \mid b$ we denote by $\pi_{b/a} \colon \mathbb{Z}_p[G_b] \to \mathbb{Z}_p[G_a]$ the natural map induced by the restriction map $G_b \to G_a$.

(2.18) Lemma. *Let $m > 1$ be a natural number and let $\ell \neq p$ be a prime divisor of m. If $d \in \mathbb{N}$ is a divisor of m with $\mathrm{ord}_\ell(m) = \mathrm{ord}_\ell(d)$, then one has*

$$\pi_{m/d}(\nu_m^{(\ell)}) = \nu_d^{(\ell)}.$$

Proof. We set $n \coloneqq \mathrm{ord}_\ell(m)$ and $m' \coloneqq m\ell^{-n}$ so that $m = m'\ell^n$. For clarity, let us write $\tilde{\sigma}_\ell^{(m)}$ for the element previously denoted $\tilde{\sigma}_\ell$ if it is regarded as an element of G_m. That is, $\tilde{\sigma}_\ell^{(m)}$ is the image of $(\sigma_\ell, \mathrm{id})$ under the isomorphism $G_{m'} \times G_{\ell^n} \cong G_m$. Similarly, the element $\tilde{\sigma}_\ell^{(d)}$ is the image of $(\sigma_\ell, \mathrm{id})$ under $G_{d'} \times G_\ell \cong G_d$ with $d' \coloneqq d\ell^{-n}$. The commutative diagram

$$\begin{array}{ccccc} G_{m'} & \hookrightarrow & G_{m'} \times G_{\ell^n} & \xrightarrow{\cong} & G_m \\ \downarrow{\scriptstyle \pi_{m'/d'}} & & & & \downarrow{\scriptstyle \pi_{m/d}} \\ G_{d'} & \hookrightarrow & G_{d'} \times G_{\ell^n} & \xrightarrow{\cong} & G_d, \end{array}$$

then shows that we have $\pi_{m/d}(\tilde{\sigma}_\ell^{(m)}) = \tilde{\sigma}_\ell^{(d)}$. Using this, we may compute that

$$\pi_{m/d}(\nu_m^{(\ell)}) = \pi_{m/d}(\lambda_n^{(\ell)}(\tilde{\sigma}_\ell^{(m)})) = \lambda_n^{(\ell)}(\pi_{m/d}(\tilde{\sigma}_\ell^{(m)})) = \lambda_n^{(\ell)}(\tilde{\sigma}_\ell^{(d)}) = \nu_d^{(\ell)},$$

as claimed. □

2.5. A construction of local points

In this section we use the theory of formal groups to construct certain local points, and this will allow us to prove Theorem (2.10) in § 2.5.3.

2.5.1. Review of Honda theory

For the convenience of the reader, we review relevant aspects of Honda's article [Hon70] (see also [Kob03, § 8.1]).
Suppose $\mathcal{Q}$ is a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{R}$, maximal ideal $\mathcal{M} = (\pi)$, and an automorphism $\phi \colon \mathcal{Q} \to \mathcal{Q}$ that satisfies $\phi(a) \equiv a^p \mod \mathcal{M}$ for every $a \in \mathcal{R}$. We then define the 'Frobenius operator'

$$\widehat{\phi} \colon \mathcal{Q}[\![X]\!] \to \mathcal{Q}[\![X]\!], \quad \sum_{i=0}^{\infty} \beta_i X^i \mapsto \sum_{i=0}^{\infty} \phi(\beta_i) X^{ip}.$$

Given $f, g \in \mathcal{Q}[\![X]\!]$ and an ideal $\mathfrak{a}$ of $\mathcal{R}[\![X]\!]$, we write $f \equiv g \mod \mathfrak{a}$ if $f - g \in \mathfrak{a}$.

(2.19) Lemma. *Suppose $f = \sum_{i=0}^{\infty} \beta_i X^i$ is a power series in $\mathcal{Q}[\![X]\!]$ with the property that $i\beta_i \in \mathcal{R}$ for every $i \geq 0$, and that the power series $g \coloneqq \sum_{i=0}^{\infty} \phi(\beta_i)((X+1)^{ip} - 1)$ exists in $\mathcal{Q}[\![X]\!]$. Then one has*

$$\widehat{\phi}(f) \equiv g \mod \pi\mathcal{R}[\![X]\!].$$

Proof. This follows from the congruence $i^{-1}(X + \pi Y)^i \equiv i^{-1}X^i \mod \pi$ in [Hon70, Lem. 2.1]. □

(2.20) Definition. *Let $u \in \mathcal{R}[X]$ be a polynomial with $u(0) = \pi$. A power series $f = \sum_{i=0}^{\infty} \beta_i X^i$ in $\mathcal{Q}[\![X]\!]$ is of 'Honda type u' if $\beta_0 = 0$, $\beta_1 = 1$, and*

$$(u(\widehat{\phi}))(f) \equiv 0 \mod \pi\mathcal{R}[\![X]\!].$$

(2.21) Theorem (Honda)**.** *The following claims are valid.*

(a) Suppose $f \in \mathcal{Q}[\![X]\!]$ is a power series of type $u \in \mathcal{R}[X]$. Then there exists a one-dimensional commutative formal group $\mathcal{F}$ over $\mathcal{R}$ such that $\log_{\mathcal{F}} = f$.

(b) Suppose that $\mathcal{F}$ and $\mathcal{G}$ are two one-dimensional commutative formal groups such that $\log_{\mathcal{F}}$ and $\log_{\mathcal{G}}$ have the same type. Then $\exp_{\mathcal{G}} \circ \log_{\mathcal{F}}$ belongs to $\mathcal{R}[\![X]\!]$ and defines an isomorphism $\mathcal{F} \xrightarrow{\simeq} \mathcal{G}$ over $\mathcal{R}$.

Proof. Claim (a) is proved in [Hon70, Thm. 2]. To prove claim (b), we note that $\mathcal{F}(X,Y) = \exp_{\mathcal{F}}(\log_{\mathcal{F}}(X) + \log_{\mathcal{F}}(Y))$ and $\mathcal{G}(X,Y) = \exp_{\mathcal{G}}(\log_{\mathcal{G}}(X) + \log_{\mathcal{G}}(Y))$ by [Hon70, Thm. 1]. If these have the same type, then they are isomorphic over $\mathcal{R}$ by [Hon70, Thm. 2]. By [Hon70, Prop. 1.6] the latter holds if and only if $\exp_{\mathcal{G}} \circ \log_{\mathcal{F}}$ belongs to $\mathcal{R}[\![X]\!]$, as required to prove claim (b). □

We conclude our review of Honda theory with the following result.

(2.22) Proposition. *Let $\widehat{E}$ denote the formal group of the minimal model (over $\mathbb{Z}_p$) of an elliptic curve E defined over $\mathbb{Q}$. Then $\log_{\widehat{E}}$ is of Honda type $p - a_p X + \mathbf{1}_N(p)X^2$.*

Proof. This is proved in [Hon70, Thm. 9, (6.6)] in the case of good reduction and in [Hon68, Thm. 5] for the case of bad reduction. □

2.5.2. An 'Artin–Hasse type' exponential

In this section we will apply the results from Honda theory reviewed in the last section to a certain explicit power series. To define this power series, we fix $m \in \mathbb{N}$ with $p \nmid m$ and also let q denote an auxiliary prime number coprime to $m(p-1)p$. Take $\mathcal{Q}$ to be the unramified extension of $\mathbb{Q}_p$ obtained as the completion of F_{mq} at a p-adic place, $\phi := \sigma_p$ its Frobenius automorphism, and write $(p) \subseteq \mathcal{R}$ for the maximal ideal and ring of integers of $\mathcal{Q}$, respectively. Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ that allows to view ζ_a, for every $a \in \mathbb{N}$, as an element of $\overline{\mathbb{Q}_p}$. In the following, we define, for an element $\delta \in \mathbb{Z}_p$, the power series

$$(1+X)^{\delta} := \exp(\delta \log(1+X)) = \sum_{i=0}^{\infty} \binom{\delta}{i} X^i$$

with $\binom{\delta}{i} := i!^{-1} \prod_{j=0}^{i-1}(\delta - i) \in \mathbb{Z}_p$.
Given $F = \sum_{i=0}^{\infty} \beta_i X^i \in \mathcal{Q}[\![X]\!]$ and $\sigma \in \mathrm{Gal}(\mathcal{Q}/\mathbb{Q}_p)$, we also write $\sigma(F) := \sum_{i=0}^{\infty} \sigma(\beta_i) X^i$.

(2.23) Proposition. *Write $\tau\colon (\mathbb{Z}/p\mathbb{Z})^{\times} \hookrightarrow \mathbb{Z}_p^{\times}$ for the p-adic Teichmüller character. For every $m_0 \mid d \mid m$ (viewed as an element of $\mathbb{Z}_p^{\times}$) and Dirichlet character $\chi\colon (\mathbb{Z}/p\mathbb{Z})^{\times} \to \mathbb{Z}_p^{\times}$ with $\chi \neq \tau$, we define*

$$g_{\chi,d}(X) := \log_{\widehat{E}}(X) + (p-1)^{-1} \sum_{i=0}^{\infty} c_{i+1}^{(p)} \zeta_d^{p^i} \sum_{j=1}^{p-1} \chi^{-1}(j)((X+1)^{d^{-1}\tau(j)p^i} - 1). \tag{21}$$

Then the following claims are valid.

(a) $g_{\chi,d}(X)$ is a well-defined element of $\mathcal{Q}[\![X]\!]$ and of Honda type $p - a_p X + \mathbf{1}_N(p)X^2$.

(b) $(\sigma_p^{-n} g_{\chi,d})(X)$ converges at $X = \zeta_{p^n} - 1$ for every $n \in \mathbb{N}$, and one has

$$(\sigma_p^{-n} g_{\chi,d})(\zeta_{p^n} - 1) = \log_{\widehat{E}}(\zeta_{p^n} - 1) + e_{\chi} \cdot \sum_{i=0}^{n-1} c_{i+1}^{(p)} \sigma_p^{i-n}(\zeta_d)(\zeta_{p^n}^{d^{-1}p^i} - 1)$$

with the usual idempotent $e_{\chi} := (p-1)^{-1} \sum_{a=1}^{p-1} \chi(a)^{-1} \sigma_a$.

(c) Set $h_{\chi,d} := \exp_{\widehat{E}} \circ g_{\chi,d}$. Then $h_{\chi,d}$ is a well-defined element of $\mathcal{R}[\![X]\!]$, the power series $(\sigma_p^{-n} g_{\chi,d})(X)$ converges in $\zeta_{p^n} - 1$, and one has

$$\log_{\widehat{E}}((\sigma_p^{-n} h_{\chi,d})(\zeta_{p^n} - 1)) = (\sigma_p^{-n} g_{\chi,d})(\zeta_{p^n} - 1).$$

Proof. To prove the first part of claim (a), we note that when expanding out the expression $\sum_{i=0}^{\infty} c_{i+1}^{(p)} \zeta_d^{p^i} \sum_{j=1}^{p-1} \chi^{-1}(j)((X+1)^{d^{-1}\tau(j)p^i}-1)$, one obtains a power series of the form $\sum_{l=0}^{\infty} \beta_l X^l$ where $\beta_l = \sum_{i=0}^{\infty} c_{i+1}^{(p)} \zeta_d^{p^i} \sum_{j=1}^{p-1} \chi(j)^{-1} \binom{p^i d^{-1}\tau(j)}{l}$. Now,

$$\sum_{j=1}^{p-1} \chi(j) \binom{p^i d^{-1}\tau(j)}{l} = \frac{1}{l!} \sum_{j=1}^{p-1} \chi^{-1}(j) \prod_{\alpha=0}^{l-1} (p^i d^{-1}\tau(j) - \alpha)$$
$$= \frac{1}{l!} \sum_{j=1}^{p-1} \chi^{-1}(j) \sum_{a=1}^{l} B_a (p^i d^{-1}\tau(j))^a. \tag{22}$$

with suitable integers $B_a \in \mathbb{Z}$. Since $\tau \neq \chi$, we have $\sum_{j=1}^{p-1} \chi(j)^{-1}\tau(j) = 0$ and so the p-adic valuation of (22) is at least $2i - l$. Here we are using Legendre's formula to observe the bound $\mathrm{ord}_p(l!) \leq l$. This then combines with the observations that $\mathrm{ord}_p(c_{i+1}^{(p)}) \geq -i$ and $\mathrm{ord}_p(\zeta_d^{p^i}) = 0$ to imply that β_l is a sum of terms that have p-adic valuation at least $i-l$, and hence converges. To show that $g_{\chi,d}(X)$ is of type $p - a_p X + \mathbf{1}_N(p)X^2$ we begin by noting that it is immediate from the definition of $g_{\chi,d}(X)$ that its constant term is $\log_{\widehat{E}}(0) + \beta_0 = 0$. Similarly, we see that $g'_{\chi,d}(0) = 1$ because $\beta_1 = \sum_{i\geq 0} c_{i+1}^{(p)} \zeta_d^{p^i} p^i d^{-1} \sum_{j=1}^{p-1} \chi^{-1}(j)\tau(j) = 0$.
We next verify that $(p - a_p\widehat{\phi} + \mathbf{1}_N(p)\widehat{\phi}^2) g_{\chi,d}(X)$ belongs to $p\mathcal{R}[\![X]\!]$. In light of Proposition (2.22), we need only verify that $(p - a_p\widehat{\phi} + \mathbf{1}_N(p)\widehat{\phi}^2) \sum_{l=0}^{\infty} \beta_l X^l$ belongs to $p\mathcal{R}[\![X]\!]$.
Let us consider the p-order of the binomial expression in the definition of β_l. We have

$$\binom{p^i d^{-1}\tau(j)}{l} = \frac{1}{l!}(p^i d^{-1}\tau(j)) \prod_{a=1}^{l-1} (p^i d^{-1}\tau(j) - a).$$

Write $l-1$ in its p-adic expansion, $l - 1 = x_n p^n + \cdots + x_1 p + x_0$, i.e. $x_i \in \{0, 1, \ldots, p-1\}$ and $x_n \neq 0$. We then note the following equality of sets, for $\gamma \in \{1, \ldots, x_n\}$,

$$\{p^i d^{-1}\tau(j) - a \pmod{p^n} \mid (\gamma-1)p^n + 1 \leq a \leq \gamma p^n\}$$
$$= \{a \pmod{p^n} \mid (\gamma-1)p^n + 1 \leq a \leq \gamma p^n\}.$$

Therefore,

$$\mathrm{ord}_p \left(\frac{\prod_{a=1}^{x_n p^n} (p^i d^{-1}\tau(j) - a)}{(x_n p^n)!} \right) \geq 0. \tag{23}$$

Similarly, we have for $\gamma = 1, \ldots, x_{n-1}$,

$$\{p^i d^{-1}\tau(j) - a \pmod{p^{n-1}} \mid p^n + (\gamma-1)p^{n-1} + 1 \leq a \leq p^n + \gamma p^{n-1}\}$$
$$= \{a \pmod{p^{n-1}} \mid p^n + (\gamma-1)p^{n-1} + 1 \leq a \leq p^n + \gamma p^{n-1}\}.$$

We note that for any a in the range used in the set above the highest power of p that can divide it is p^{n-1}. Combining this calculation with (23) we have

$$\mathrm{ord}_p \left(\frac{\prod_{a=1}^{x_n p^n + x_{n-1} p^{n-1}} (p^i d^{-1}\tau(j) - a)}{(x_n p^n + x_{n-1} p^{n-1})!} \right) \geq 0.$$

Repeating this process one observes that

$$\mathrm{ord}_p \left(\frac{\prod_{a=1}^{l} (p^i d^{-1}\tau(j) - a)}{(l-1)!} \right) \geq 0.$$

In particular, $\mathrm{ord}_p(\binom{p^i d^{-1}\tau(j)}{l}) \geq i - \mathrm{ord}_p(l)$. Therefore, by the observations made above we have $l c_{i+1}^{(p)} \binom{p^i d^{-1}\tau(j)}{l} \in \mathbb{Z}_p$. Thus, we can deduce from Lemma (2.19) that

$$\widehat{\phi}\big(c_{i+1}^{(p)}((X+1)^{d^{-1}\tau(j)p^i} - 1)\big) = c_{i+1}^{(p)}((X^p+1)^{d^{-1}\tau(j)p^i} - 1)$$
$$\equiv c_{i+1}^{(p)}((X+1)^{d^{-1}\tau(j)p^{i+1}} - 1) \mod p\mathbb{Z}_p[\![X]\!]$$

for every $i \geq 0$ and $j \in (\mathbb{Z}/p\mathbb{Z})^\times$. For the first equality we note that ϕ acts trivially on $c_{i+1}^{(p)}\binom{p^i d^{-1}\tau(j)}{l} \in \mathbb{Q}_p$. We may therefore use the relation $pc_{i+1}^{(p)} - a_p c_i^{(p)} + \mathbf{1}_N(p)c_{i-1}^{(p)} = 0$ to calculate that

$$\begin{aligned}
&(p - a_p\widehat{\phi} + \mathbf{1}_N(p)\widehat{\phi}^2)\sum_{i=0}^{\infty} c_{i+1}^{(p)}\zeta_d^{p^i}((X+1)^{d^{-1}\tau(j)p^i} - 1) \\
&\equiv \sum_{i=0}^{\infty} c_{i+1}^{(p)}\big(p\zeta_d^{p^i}((X+1)^{d^{-1}\tau(j)p^i} - 1) - a_p\zeta_d^{p^{i+1}}((X+1)^{d^{-1}\tau(j)p^{i+1}} - 1) \\
&\qquad + \mathbf{1}_N(p)\zeta_d^{p^{i+2}}((X+1)^{d^{-1}\tau(j)p^{i+2}} - 1)\big) \mod p\mathbb{Z}_p[\![X]\!] \\
&= p\zeta_d^p c_1^{(p)} X + \sum_{i=1}^{\infty}\zeta_d^{p^i}\big(pc_{i+1}^{(p)} - a_p c_i^{(p)} + \mathbf{1}_N(p)c_{i-1}^{(p)}\big)(X+1)^{d^{-1}\tau(j)p^i} - 1) \\
&= p\zeta_d^p X.
\end{aligned}$$

This implies the congruence required to establish that $g_{\chi,d}(X)$ is of the claimed Honda type. As for claim (b), it follows immediately from the calculations made in the proof of (a) that $l\beta_l \in \mathcal{R}$ for all $l \geq 0$. Given this, it follows from [Sil09, Ch. IV, Lem. 6.3 (a)] that $(\sigma_p^{-n}g_{\chi,d})(X)$ converges when evaluated at $\zeta_{p^n} - 1$ and we may compute $(\sigma_p^{-n}g_{\chi,d})(\zeta_{p^n} - 1)$ by evaluating (21) after applying σ_p^{-n} (cf. [Kat21, Lem. 3.17]).
Since $g_{\chi,d}(X)$ and $\log_{\widehat{E}}(X)$ have the same Honda type (by claim (a) and Proposition (2.22)), it follows from Theorem (2.21) that $h_{\chi,d}$ belongs to $\mathcal{R}[\![X]\!]$ and, in particular, converges when evaluated at $\zeta_{p^n} - 1$. To prove the remaining part of claim (c), we note that we have the formal identity $(\log_{\widehat{E}} \circ \exp_{\widehat{E}})(X) = X$, which implies that $(\log_{\widehat{E}} \circ h_{\chi,d})(X) = g_{\chi,d}(X)$ as power series. Since $\log_{\widehat{E}}$ has coefficients in $\mathbb{Q}_p$, this also implies that $(\log_{\widehat{E}} \circ \sigma_p^{-n}(h_{\chi,d}))(X) = \sigma_p^{-n}(g_{\chi,d})(X)$. The latter equality still holds true when evaluated at $\zeta_{p^n} - 1$ because the coefficients of $\sigma_p^{-n}(h_{\chi,d})$ are in $\mathcal{R}$ (see, for example, [Rob00, § 6.1.5]). □

(2.24) Remark. The purpose of the sum $\sum_{j=1}^{p-1}$ in (21) is to avoid delicate convergence issues, and this extends an idea of Kobayashi. That is, our definition of $g_{\chi,d}$ is directly inspired by a definition of Kobayashi in [Kob06, § 2] that can be seen as a special case of (21) for $\chi = \mathbf{1}$.

We can now define useful local points by appropriately evaluating the power series $h_{\chi,d}$ defined in Proposition (2.23).

(2.25) Definition. *Take ϵ_d to be a preimage of $\zeta_d p$ under $\log_{\widehat{E}}\colon \widehat{E}(p\mathcal{R}) \xrightarrow{\simeq} \mathbb{G}_a(p\mathcal{R})$. We define an element of $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \widehat{E}(\mathcal{M}_{\mathcal{Q}(\zeta_{p^n})})$ as*

$$\widetilde{x}_{mp^n} := \sum_{m_0|d|m}\Big(\sum_{\chi\neq\tau}\big(\sigma_p^{-n}(h_{\chi,d})(\zeta_{p^n} - 1) -_{\widehat{E}} (\zeta_{p^n} - 1)\big) +_{\widehat{E}} (p\mathrm{Eul}_p(\sigma_p))^{-1}\sigma_p^{-n}(\epsilon_d)\Big),$$

where the sum ranges over all characters $\chi\colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p^\times$ that are not equal to the Teichmüller character τ and $\mathcal{M}_{\mathcal{Q}(\zeta_{p^n})}$ is the maximal ideal of $\mathcal{Q}(\zeta_{p^n})$.

The following result establishes the connection of these local points with Otsuki's elements from Definition (2.13).

(2.26) Lemma. *In $\mathbb{Q}_p(\zeta_{mp^n})$, one has the equality*

$$\log_{\widehat{E}}(\widetilde{x}_{mp^n}) = (1 - e_\tau)\cdot\sum_{m_0|d|m}\big(\mathrm{Eul}_p(\hat{\sigma}_p)^{-1}(X)\big)(\zeta_{dp^n}).$$

Proof. At the outset we recall that the idempotent $1 - e_\tau$ acts as the identity on $\mathcal{Q}$. Using Proposition (2.23) and Otsuki's relation (10) (for the equalities $(*)$), we may then calculate

that

$$\begin{aligned}
\log_{\widehat{E}}(\widetilde{x}_{mp^n}) &= \sum_{m_0|d|m} \big(\sum_{\chi \neq \tau} \big(\sigma_p^{-n}(g_{\chi,d})(\zeta_{p^n}-1) - \log_{\widehat{E}}(\zeta_{p^n}-1)\big) + (p\mathrm{Eul}_p(\sigma_p))^{-1} p\sigma_p^{-n}(\zeta_d)\big) \\
&\overset{(*)}{=} \sum_{m_0|d|m} \big((1-e_\tau) \sum_{i=0}^{n-1} c_{i+1}\sigma_p^{i-n}(\zeta_d)(\zeta_{p^n}^{d^{-1}p^i}-1) \\
&\qquad + \big(\sum_{i=0}^{n-1} c_{i+1}\sigma_p^i + \widetilde{F}_p^{(n)}(\sigma_p)\cdot \mathrm{Eul}_p(\sigma_p)^{-1}\big)\sigma_p^{-n}(\zeta_d)\big) \\
&= \sum_{m_0|d|m} \big((1-e_\tau)\big(\sum_{i=0}^{n-1} c_{i+1}\sigma_p^{i-n}(\zeta_d)\zeta_{p^n}^{d^{-1}p^i} + \widetilde{F}_p^{(n)}(\sigma_p)\cdot \mathrm{Eul}_p(\sigma_p)^{-1}\cdot \sigma_p^{-1}(\zeta_d)\big)\big) \\
&= (1-e_\tau)\cdot \sum_{m_0|d|m} \big(\big(\sum_{i=0}^{n-1} c_{i+1}\hat{\sigma}_p^i + \widetilde{F}_p^{(n)}(\sigma_p)\cdot \mathrm{Eul}_p(\sigma_p)^{-1}\hat{\sigma}_p^n\big)(X)\big)(\sigma_p^{-n}(\zeta_d)\zeta_{p^n}^{d^{-1}}) \\
&\overset{(*)}{=} (1-e_\tau)\cdot \sum_{m_0|d|m} \big(\mathrm{Eul}_p(\hat{\sigma}_p)^{-1}(X)\big)(\zeta_{dp^n}),
\end{aligned}$$

where the last equality uses that $\sigma_p^{-n}(\zeta_d)\zeta_{p^n}^{d^{-1}} = \zeta_{dp^n}$. □

2.5.3. An explicit reciprocity law and the proof of Theorem (2.10)

We require the following modification of Kato's explicit reciprocity law (as stated in Theorem (2.8) (c)).

(2.27) Proposition (Otsuki)**.** *For every $m \in \mathbb{N}$ coprime to p and $n \in \mathbb{Z}_{\geq 0}$ one has*

$$\sum\nolimits_{\sigma\in G} \mathrm{Tr}_{(\mathbb{Q}_p\otimes_{\mathbb{Q}} F_{mp^n})/\mathbb{Q}_p}(\sigma(x_{mp^n})\cdot(\exp^*_{\omega_E}\circ \mathrm{loc}^{(p)}_{/f})(y^{\mathrm{Kato}}_{mp^n}))\sigma = \theta^{\mathrm{MT}}_{mp^n}.$$

Proof. This is proved in [Ots09, Thm. 3.6]. Note that p is assumed to be a prime of good reduction for E in loc. cit. but this assumption is not needed for the proof of [Ots09, Thm. 3.6]. Furthermore, the difference between x_m and x_m^{Otsuki} noted in Remark (2.14) is taken into account by our definition of y_m^{Kato} (which differs from the element used by Otsuki in [Ots09, Prop. 3.2] by $\mathrm{Eul}_p(\sigma_p^{-1})^{-1}$). □

We now give the proof of Theorem (2.10).

Proof (of Theorem (2.10)): Let $\mathfrak{k}_{mp^n}$ be the preimage of $\sum_{m_0|d|m}(\mathrm{Eul}_p(\hat{\sigma}_p)^{-1}(X))(\zeta_{dp^n}) \in \mathbb{Q}_p\otimes_{\mathbb{Z}} F_{mp^n}$ under the isomorphism

$$H^1_f(\mathbb{Q}_p, \mathrm{V}_p E_{F_{mp^n}/\mathbb{Q}}) = \bigoplus\nolimits_{v|p}(\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\widehat{E}(F_{mp^n,v})) \xrightarrow{\simeq} \bigoplus\nolimits_{v|p}(\mathbb{Q}_p\otimes_{\mathbb{Z}_p}\mathcal{O}_{F_{mp^n,v}}) = \mathbb{Q}_p\otimes_{\mathbb{Z}} F_{mp^n}$$

defined as the sum $\oplus_{v|p}\log_{\widehat{E}}$ of the formal logarithm of $E/F_{mp^n,v}$. Claim (a) of Theorem (2.10) follows by combining Proposition (2.16) with Proposition (2.27) and Lemma (2.7) (a, b). To prove claim (b) of Theorem (2.10), we recall that Otsuki has proved, in [Ots09, Prop. 4.5], that

$$\mathrm{Eul}_p(\hat{\sigma}_p)\cdot(\oplus_{v|p}\log_{\widehat{E}})(E_1(F_{mp^n,p})) = \mathbb{Z}_p\otimes_{\mathbb{Z}}\mathcal{O}_{F_{mp^n}}$$

if p is a good prime with $a_p \not\equiv 1 \mod p$, and the same proof works if p is an additive prime (and $n=0$). In this case, therefore, $\mathfrak{k}_{mp^n}$ belongs to $E_1(F_{mp^n,p})$, as claimed.
We observe that Lemma (2.26) implies that $(1-e_\tau)\mathfrak{k}_{mp^n}$ is equal to the family $(\tilde{x}_{mp^n,v})_{v|p}$ with $\tilde{x}_{mp^n,v}$ the element from Definition (2.25) with $\mathcal{Q}$ taken to be the completion of F_m at the place lying below v (so that $\mathcal{Q}(\zeta_{p^n})$ is the completion of F_{mp^n} at v). By construction, $p\mathrm{Eul}_p(\tilde{\sigma}_p)\tilde{x}_{mp^n,v}$ belongs to $\widehat{E}(\mathcal{M}_{F_{mp^n,v}})$, with $\mathcal{M}_{F_{mp^n,v}}$ the maximal ideal of $F_{mp^n,v}$. Hence $(1-e_\tau)p\mathrm{Eul}_p(\tilde{\sigma}_p)\mathfrak{k}_{mp^n}$ belongs to $E_1(F_{mp^n,p})$, as claimed.
We now turn to the proof of claim (c). At the outset we note that it suffices to prove the

claimed relations for the elements $(\oplus_{v|p}\log_{\widehat{E}})(\mathfrak{k}_{mp^n}) = \mathrm{Eul}_p(\hat{\sigma}_p)^{-1}\cdot\sum_{m_0|d|m}\zeta_{dp^n}$. Equality (i) then follows from the fact that by [Ots09, Prop. 2.5] one has

$$\begin{aligned}\mathrm{Tr}_{mp^{n+1}/mp^n}\big((\mathrm{Eul}_p(\hat{\sigma}_p)^{-1}(X))(\zeta_{dp^n})\big) &= \mathrm{Tr}_{dp^{n+1}/dp^n}\big((\mathrm{Eul}_p(\hat{\sigma}_p)^{-1}(X))(\zeta_{dp^n})\big)\\ &= \begin{cases} a_p\zeta_{dp^n} - \mathbf{1}_N(p)\zeta_{dp^{n-1}} & \text{if } n>2,\\ a_p\zeta_{dp^n} - \mathbf{1}_N(p)\mathrm{Eul}_p(\sigma_p)^{-1}\zeta_d & \text{if } n=1,\\ (a_p - \mathbf{1}_N(p)\sigma_p - \sigma_p^{-1})\mathrm{Eul}_p(\sigma_p)^{-1}\zeta_d & \text{if } n=0.\end{cases}\end{aligned}$$

As for the equality in (ii), we let d be a natural number with $m_0 \mid d \mid m$ and first recall that $\mathrm{Tr}_{\ell dp^n/dp^n}(\zeta_{\ell dp^n})$ vanishes if $\ell \mid d$, so that

$$\mathrm{Tr}_{\ell mp^n/mp^n}\Big(\sum_{(\ell m)_0|d'|\ell m}\zeta_{d'p^n}\Big) = \begin{cases}\mathrm{Tr}_{\ell mp^n/mp^n}(\sum_{m_0|d|m}\zeta_{dp^n}) & \text{if } \ell\mid m,\\ \mathrm{Tr}_{\ell mp^n/mp^n}(\sum_{m_0|d|m}\zeta_{\ell dp^n}) & \text{if } \ell\nmid m.\end{cases}$$

Claim (ii) therefore follows from the observation that, for a natural number $d' \mid \ell m$, one has

$$\mathrm{Tr}_{\ell mp^n/mp^n}(\zeta_{d'p^n}) = \begin{cases}\ell\zeta_{d'p^n} & \text{if } \ell\nmid d',\\ -\sigma_\ell^{-1}\zeta_{d'/\ell} & \text{if } \ell\mid d'.\end{cases}$$

We show claim (d) of Theorem (2.10) working case by case.
If $a_\ell = 2$, $\ell\nmid N$ and $\ell^2\nmid m$, then $\mathrm{ord}_\ell(m)=1$ and thus from Proposition (2.17) (b) we have

$$\nu^{(\ell)}_{mp^n} \equiv c_1^{(\ell)}(1-a_\ell\tilde{\sigma}_\ell) + \frac{\mathbf{1}_N(\ell)}{\ell}(\ell_j c_1^{(\ell)}\tilde{\sigma}_\ell^2 + c_0^{(\ell)}\tilde{\sigma}_\ell(\ell-1)) \pmod{I^2_{\mathcal{D}^{(\ell)}_{mp^n}}}.$$

Since $c_0^{(\ell)}=0$ and $c_1^{(\ell)}=1$ we can calculate

$$\nu^{(\ell)}_{mp^n} \equiv 1 - 2\tilde{\sigma}_\ell + \tilde{\sigma}_\ell^2 = (1-\tilde{\sigma}_\ell) \equiv 0 \pmod{I^2_{\mathcal{D}^{(\ell)}_{mp^n}}}.$$

If $\mathbf{1}_N(\ell)=0$ then one can inductively show that $c_j^{(\ell)} = (\frac{a_\ell}{\ell})^{j-1}$ for $j\geq 1$. Proposition (2.17) (b) now gives that, in this case,

$$\nu^{(\ell)}_{mp^n} \equiv c_1^{(\ell)}(1-a_\ell\tilde{\sigma}_\ell) \pmod{I^2_{\mathcal{D}^{(\ell)}_{mp^n}}}.$$

In both the remaining cases of claim (d) of Theorem (2.10) we have $\mathbf{1}_N(\ell)=0$, hence the result follows immediately from the above equation and definition of $c_j^{(\ell)}$ in these cases.
Finally, claim (e) is immediate from the definition of $\lambda^{(\ell)}_{\mathrm{ord}_\ell(m)}(X)$ upon noting that the element $\omega^{(\ell)}_{\mathrm{ord}_\ell(m),0} = -\tilde{\sigma}_\ell\ell^{-\mathrm{ord}_\ell(m)}\mathrm{N}_{F_{\ell^{\mathrm{ord}_\ell(m)}}/\mathbb{Q}}$ differs from $\mathrm{N}_{\mathcal{I}^{(\ell)}_{mp^n}}$ only by a unit in $\mathbb{Z}_p[G_{mp^n}]$. □

3. Nekovář–Selmer complexes and the equivariant Tamagawa Number Conjecture

In this section we recall some general aspects of the theory of Nekovář–Selmer complexes and discuss examples of such complexes that will be important to us. Even though most material contained in this section extends to general p-adic representations, we prefer to restrict attention to the setting most relevant to us – namely that of the representation given by the p-adic Tate module of E. For a more in-depth treatment of Nekovář–Selmer complexes an interested reader is invited to refer to [Nek06] or [BB25, § 3].
We freely use some of the notation and conventions introduced in Appendix B. In particular, we write $D(\mathcal{R})$ for the derived category of $\mathcal{R}$-modules of a ring $\mathcal{R}$ and $D^{\mathrm{perf}}(\mathcal{R})$ for its full triangulated subcategory of complexes that are perfect.
Given a profinite group $\mathscr{G}$ and a finitely generated $\mathcal{R}$-module M endowed with a continuous action of $\mathscr{G}$, we write $\mathscr{C}^\bullet(\mathscr{G},M)$ for the associated complex of continuous cochains and $\mathrm{R}\Gamma(\mathscr{G},M)$ for the object of $D(\mathcal{R})$ defined by $\mathscr{C}^\bullet(\mathscr{G},M)$. If F is a field with absolute Galois

group $\mathscr{G}_F := \mathrm{Gal}(\overline{F}/F)$, then we abbreviate this to $\mathrm{R}\Gamma(F, M) := \mathrm{R}\Gamma(\mathscr{G}_F, M)$. If F is a number field and the action of $\mathscr{G}_F$ on M is unramified outside a finite set U of places of F, then M is naturally a module for $\mathscr{G}_{F,U} := \mathrm{Gal}(F^U/F)$ with $F^U \subseteq \overline{F}$ the maximal extension unramified outside S and we write $\mathrm{R}\Gamma(\mathcal{O}_{F,U}, M) := \mathrm{R}\Gamma(\mathscr{G}_{F,U}, M)$.

3.1. Nekovář–Selmer structures

We begin by introducing a suitable variant of the notion of 'Selmer structure' used by Mazur and Rubin in [MR04, Def. 2.1.1]. Recall that we have defined $S(K) = S_{pNm\infty}$, where m denotes conductor of K and N is the conductor of E, and that Shapiro's lemma gives natural isomorphisms $\mathrm{R}\Gamma(\mathcal{O}_{\mathbb{Q},U}, T_{K/\mathbb{Q}}) \cong \mathrm{R}\Gamma(\mathcal{O}_{K,U}, \mathrm{T}_p E)$ and $\mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \cong \bigoplus_{w|v} \mathrm{R}\Gamma(K_w, \mathrm{T}_p E)$ for every finite set $U \subseteq S(K)$ and place v of $\mathbb{Q}$.

(3.1) Definition. *A 'Nekovář–Selmer structure' $\mathcal{F}$ for $T_{K/\mathbb{Q}}$ consists of the following data:*

- *A finite set $S(\mathcal{F})$ of places of $\mathbb{Q}$ that contains $S(K)$.*
- *For every place $v \in S(\mathcal{F})$ a complex $\mathrm{R}\Gamma_{\mathcal{F}}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ of $\mathbb{Z}_p[G]$-modules together with a morphism $i_{\mathcal{F},v}\colon \mathrm{R}\Gamma_{\mathcal{F}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ in $D(\mathbb{Z}_p[G])$.*

One then defines the 'Nekovář–Selmer complex' $\mathrm{R}\Gamma_{\mathcal{F}}(K, \mathrm{T}_p E)$ as

$$\mathrm{cone}\Big\{\mathrm{R}\Gamma(\mathcal{O}_{K,S(\mathcal{F})}, \mathrm{T}_p E) \oplus \bigoplus_{v\in S(\mathcal{F})} \mathrm{R}\Gamma_{\mathcal{F}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \xrightarrow{\oplus_{v\in S(\mathcal{F})}(\mathrm{loc}_v - i_{\mathcal{F},v})} \bigoplus_{v\in S(\mathcal{F})} \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}})\Big\}[-1],$$

where loc_v denotes the natural localisation map

$$\mathrm{R}\Gamma(\mathcal{O}_{K,S(\mathcal{F})}, \mathrm{T}_p E) \to \bigoplus_{w|v} \mathrm{R}\Gamma(K_w, \mathrm{T}_p E) = \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}})$$

for every $v \in S(\mathcal{F})$, and sets $H^i_{\mathcal{F}}(K, \mathrm{T}_p E) := H^i(\mathrm{R}\Gamma_{\mathcal{F}}(K, \mathrm{T}_p E))$ for all $i \in \mathbb{Z}$.

(3.2) Remark. For every Selmer structure $\mathcal{F}$, the octrahedral axiom implies the existence of an exact triangle

$$\mathrm{R}\Gamma_{\mathcal{F}}(K, \mathrm{T}_p E) \longrightarrow \mathrm{R}\Gamma(K, \mathrm{T}_p E) \longrightarrow \textstyle\bigoplus_{v\in S(\mathcal{F})} \mathrm{R}\Gamma_{/\mathcal{F}}(K_v, \mathrm{T}_p E) \longrightarrow \mathrm{R}\Gamma_{\mathcal{F}}(K, \mathrm{T}_p E)[1]$$

with $\mathrm{R}\Gamma_{/\mathcal{F}}(K_v, \mathrm{T}_p E) := \mathrm{cone}(i_{\mathcal{F},v})[-1]$.

(3.3) Examples. (a) (Relaxed structures) For every finite set Σ of places of $\mathbb{Q}$ that contains $S(K)$ we define a 'relaxed' Nekovář–Selmer structure $\mathcal{F}_{\Sigma,\mathrm{rel}}$ by taking

- $S(\mathcal{F}_{\Sigma,\mathrm{rel}}) := \Sigma$,
- $\mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\mathrm{rel}}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) := \mathrm{R}\Gamma((\mathbb{Q}_v, T_{K/\mathbb{Q}})$ for all $v \in S(\mathcal{F}_{\Sigma,\mathrm{rel}})$,
- $i_{\mathcal{F}_{\Sigma,\mathrm{rel}}}$ to be the identity map for all $v \in S(\mathcal{F}_{\Sigma,\mathrm{rel}})$.

The associated Nekovář–Selmer complex $\mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\mathrm{rel}}}(K, \mathrm{T}_p E)$ then coincides with $\mathrm{R}\Gamma(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$.

(b) (Strict structures) For every finite set of places of $\mathbb{Q}$ that contains $S(K)$ we define a 'strict' Nekovář–Selmer structure $\mathcal{F}_{\Sigma,\mathrm{str}}$ by means of

- $S(\mathcal{F}_{\Sigma,\mathrm{str}}) := \Sigma$,
- $\mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\mathrm{str}}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) = 0$ for all $v \in S(\mathcal{F}_{\Sigma,\mathrm{str}})$,
- $i_{\mathcal{F}_{\Sigma,\mathrm{str}},v} := 0$ for all $v \in S(\mathcal{F}_{\Sigma,\mathrm{str}})$.

The associated Nekovář–Selmer complex $\mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\mathrm{rel}}}(K, \mathrm{T}_p E)$ then coincides with the 'compact-support' cohomology complex $\mathrm{R}\Gamma_{\mathrm{c}}(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$.

(3.4) Remark (Dual structures)**.** For every finite place v of $\mathbb{Q}$ local Tate duality induces an isomorphism (cf. [Nek06, Th. 5.2.6])

$$\mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}), \mathbb{Z}_p)[-2] \xrightarrow{\simeq} \mathrm{R}\Gamma(\mathbb{Q}_v, T^*_{K/\mathbb{Q}}(1)) \cong \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}). \tag{24}$$

(Here the second isomorphism is induced by the Weil pairing.) Any Nekovář–Selmer structure $\mathcal{F}$ on $T_{K/\mathbb{Q}}$ therefore naturally induces a dual structure $\mathcal{F}^*$ by taking

- $S(\mathcal{F}^*) \coloneqq S(\mathcal{F})$,
- $\mathrm{R}\Gamma_{\mathcal{F}^*}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \coloneqq \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma_{/\mathcal{F}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}), \mathbb{Z}_p)[-2]$ if v is finite and zero otherwise,
- $i_{\mathcal{F}^*,v}$ is the composite of $\mathrm{RHom}_{\mathbb{Z}_p}(i_{\mathcal{F},v}, \mathbb{Z}_p)[-2]$ and (24) if v is finite (and the zero map otherwise).

3.2. Compactly supported étale cohomology

Fix a finite set Σ of places of $\mathbb{Q}$ that contains $S(K)$. In the next section, we often use the complex

$$C^\bullet_{K,\Sigma} \coloneqq \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma_{\mathrm{c}}(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E), \mathbb{Z}_p)[-3].$$

The following result records useful properties of the complex $C^\bullet_{K,\Sigma}$.

(3.5) Lemma. *Let Σ be a finite set of places of $\mathbb{Q}$ that contains $S(K)$, and assume that $E(K)$ has no point of order p. The following then hold.*

(a) $C^\bullet_{K,\Sigma}$ is a perfect object of $D(\mathbb{Z}_p[G])$ that has vanishing Euler characteristic in $K_0(\mathbb{Z}_p[G])$ and is acyclic outside degrees one and two. There is a canonical isomorphism $H^1(C^\bullet_{K,\Sigma}) \cong H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$ and a split-exact sequence

$$0 \longrightarrow H^2(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \longrightarrow H^2(C^\bullet_{K,\Sigma}) \xrightarrow{\pi} (T^+_{K/\mathbb{Q}})^* \longrightarrow 0$$

with $T^+_{K/\mathbb{Q}} \coloneqq H^0(\mathbb{R}, T_{K/\mathbb{Q}})$.

(b) $C^\bullet_{K,\Sigma}$ admits a standard representative in the sense of Definition (B.3) with $F^0 = 0$.

Proof. The assumption that $E(K)[p]$ vanishes implies that $H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$ is $\mathbb{Z}_p$-torsion free (cf. [BD21, Ex. 3.3 (b)]). That is, [BS21, Hyp. 2.16] is satisfied and so [BS21, Prop. 2.22 (ii)] combines with [BS21, Prop. A.11] to imply claims (a) and (b). We only note that the description of the cohomology given in claim (a) is a consequence of the fact that Artin–Verdier duality (as in [BF01, Lem. 12 (b)]) induces an exact triangle

$$\mathrm{R}\Gamma(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \longrightarrow C^\bullet_{K,\Sigma} \longrightarrow (T^+_{K/\mathbb{Q}})^*[-2] \longrightarrow \mathrm{R}\Gamma(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)[1]$$

in $D(\mathbb{Z}_p[G])$. □

We next make a convenient choice of $\mathbb{Z}_p[G]$-basis for $T^+_{K/\mathbb{Q}}$. To do this, write w_ι for the place of K corresponding with ι_K, the restriction to K of the embedding $\iota\colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ fixed in § 1.3, and denote by $\mathcal{D}^{(\iota)}_K \subseteq G$ the associated decomposition group. Viewing w_ι as an equivalence class of embeddings $\sigma\colon K \hookrightarrow \mathbb{C}$, one has that $\mathbb{Z}_p \otimes_{\mathbb{Z}} (\bigoplus_{\sigma \in w_\iota} H^1(E^\sigma_K(\mathbb{C}), \mathbb{Z}))^+ = \big((\bigoplus_{\sigma \in w_\iota} \mathbb{Z}_p\sigma) \otimes_{\mathbb{Z}} H^1(E(\mathbb{C}), \mathbb{Z}))\big)^+$ is a free $\mathbb{Z}_p[\mathcal{D}^{(\iota)}_K]$-module of rank one with basis

$$\gamma_K \coloneqq (\tfrac{1}{2}(1+c)\iota_K \otimes \gamma_+) + (\tfrac{1}{2}(1-c)\iota_K \otimes \gamma_-).$$

We then define $b \coloneqq b_K$ to be the image of γ_K under the comparison isomorphism

$$\mathbb{Z}_p \otimes_{\mathbb{Z}} (\bigoplus\nolimits_{\sigma \in w_\iota} H^1(E^\sigma_K(\mathbb{C}), \mathbb{Z}))^+ \cong H^0(K_{w_\iota}, \mathrm{T}_p E).$$

By construction, the element b is indeed a $\mathbb{Z}_p[G]$-basis of $T^+_{K/\mathbb{Q}} \cong \bigoplus_{w|\infty} H^0(K_w, \mathrm{T}_p E)$.
Let Σ be a finite set of places of $\mathbb{Q}$ that contains $S(K)$, and write

$$\Theta_{K,\Sigma} \coloneqq \vartheta_{C^\bullet_{K,\Sigma}, \{b^*\}}\colon \mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,\Sigma})^{-1} \to H^1(\mathcal{O}_{K,\Sigma}, \mathrm{V}_p E)$$

for the map from Definition (B.2) with b^* the $\mathbb{Z}_p[G]$-linear dual of the basis element $b \in T^+_{K/\mathbb{Q}}$ defined above.

(3.6) Theorem. *Assume $p > 3$ is a prime number such that the image of $\rho_{E,p}$ contains $\mathrm{SL}_2(\mathbb{Z}_p)$. If E does not have potentially good reduction at p, then we also assume that K does not contain a primitive p-th root of unity. Then z^{Kato}_K is contained in the image of $\Theta_{K,S(K)}$.*

Proof. This is proved by Burns and the first author in [BB25, Cor. 9.6 (i)]. □

(3.7) Remark. The result of Theorem (3.6) is directly related to the 'equivariant Tamagawa Number Conjecture' for the pair $(h^1(E/K)(1), \mathbb{Z}_p[G])$, see [BB25, Rk. 9.7] for more details.

3.3. Bloch–Kato Selmer complexes

Following Bloch and Kato [BK90], we define the local 'finite-support' cohomology complex

$$\mathrm{R}\Gamma_f(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \coloneqq \begin{cases} \bigoplus_{w|v} E(K_v)^\wedge[-1] & \text{if } v \nmid \infty, \\ \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) & \text{if } v = \infty, \end{cases}$$

for every place v of $\mathbb{Q}$. For every finite set of places Σ containing $S(K)$, one then defines the Bloch–Kato Selmer structure $\mathcal{F}_{\Sigma,\mathrm{BK}}$ for $T_{K/\mathbb{Q}}$ as follows.

- $S(\mathcal{F}_{\Sigma,\mathrm{BK}}) = \Sigma$,
- $\mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\mathrm{BK}}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \coloneqq \mathrm{R}\Gamma_f(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ for all $v \in \Sigma$,
- $i_{\mathcal{F}_{\Sigma,\mathrm{BK}},v}$ is taken to be the map induced by the Kummer map if $v \in \Sigma$ is a finite place and the identity map if $v = \infty$.

As is customary, we then replace any adornments $\mathcal{F}_{\Sigma,\mathrm{BK}}$ by simply f and, for example, write

$$\mathrm{R}\Gamma_f(K, \mathrm{T}_p E) \coloneqq \mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\mathrm{BK}}}(K, \mathrm{T}_p E)$$

and $H^i_f(K, \mathrm{T}_p E) \coloneqq H^i_{\mathcal{F}_{\Sigma,\mathrm{BK}}}(K, \mathrm{T}_p E)$ for every $i \in \mathbb{Z}$ (this is consistent with the definition for ℓ-adic fields given in § 2.2). Note that this definition of $\mathrm{R}\Gamma_f(K, \mathrm{T}_p E)$ does not depend on the choice of Σ, see [BMC24, Lem. 2.5].

(3.8) Lemma. *One has canonical identifications*

$$H^i_f(K, \mathrm{T}_p E) = \begin{cases} \mathrm{Sel}^\wedge_{p,E/K} & \text{if } i = 1, \\ \mathrm{Sel}^\vee_{p,E/K} & \text{if } i = 2, \\ E(K)[p^\infty]^\vee & \text{if } i = 3, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. See, for example, [BF24, Lem. 1]. □

(3.9) Remark. Local Tate duality induces an isomorphism

$$\mathrm{R}\Gamma_{/f}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \cong \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}), \mathbb{Z}_p)[-2] \tag{25}$$

that is valid for every prime number ℓ. This is a special case of the general result of [BF01, Lem. 19] and, in the case at hand, can also be checked explicitly as in [BF24, Lem. 2].

4. Nekovář–Selmer complexes and weak main conjectures

The fundamental difficulty in deriving explicit statements such as Conjecture (1.1) from the equivariant Tamagawa Number Conjecture is that the finite-support cohomology complex $\mathrm{R}\Gamma_f(K, \mathrm{T}_p E)$ is rarely perfect as an object in $D(\mathbb{Z}_p[G])$ (cf. [BMC24, Lem. 5.1] or [EN18, § 4.1]). In this subsection we therefore construct auxiliary perfect Selmer complexes that approximate $\mathrm{R}\Gamma(K, \mathrm{T}_p E)$.

Throughout this subsection we fix an abelian number field K with Galois group $G = G_K \coloneqq \mathrm{Gal}(K/\mathbb{Q})$. For every place v of K, we denote the residue field at v by $\mathbb{F}_v$.

4.1. Unramified cohomology

Write $\widetilde{E}$ for the reduction of E modulo p, denote the group of non-singular $\mathbb{F}_v$-rational points on $\widetilde{E}$ by $\widetilde{E}^{\mathrm{ns}}(\mathbb{F}_v)$, and set

$$(E_1/E_0)(K_\ell) \coloneqq \bigoplus\nolimits_{v|\ell}(\widetilde{E}^{\mathrm{ns}}(\mathbb{F}_v) \otimes_{\mathbb{Z}} \mathbb{Z}_p).$$

(4.1) Lemma. *For every prime number ℓ there exists a natural number n_ℓ such that, if ℓ is unramified in K, there exists an $(n_\ell \times n_\ell)$-matrix $A_{\ell,K}$ with the following properties.*

(a) $\det_{\mathbb{Z}_p[G]}(A_{\ell,K}) \cdot \mathbb{Z}_p[G] = \ell \cdot \mathrm{Eul}_\ell(\sigma_\ell^{-1}) \cdot \mathbb{Z}_p[G]$.

(b) There is an exact sequence

$$0 \longrightarrow \mathbb{Z}_p[G]^{\oplus n_\ell} \xrightarrow{\cdot A_\ell} \mathbb{Z}_p[G]^{\oplus n_\ell} \longrightarrow (E_1/E_0)(K_\ell) \longrightarrow 0.$$

In particular, we have the equality $\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}\big((E_1/E_0)(K_\ell)\big) = \ell \cdot \mathrm{Eul}_\ell(\sigma_\ell^{-1}) \cdot \mathbb{Z}_p[G]$.

(c) If L is a subfield of K, then $\pi_{K/L}(A_{\ell,K}) = A_{\ell,L}$.

Proof. We abbreviate (a choice of) inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at ℓ to $\mathcal{I}_\ell \coloneqq \mathcal{I}_{\mathbb{Q}}^{(\ell)}$. If $\ell \nmid p$, then we have an exact sequence (see, for example, the argument of [Kin11, Lecture 5, Lem. 5])

$$0 \longrightarrow (T_{K/\mathbb{Q}})^{\mathcal{I}_\ell} \xrightarrow{1-\sigma_\ell^{-1}} (T_{K/\mathbb{Q}})^{\mathcal{I}_\ell} \longrightarrow (E_1/E_0)(K_\ell) \longrightarrow 0. \tag{26}$$

This sequence may be used for the computation of the Fitting ideal because

$$(T_{K/\mathbb{Q}})^{\mathcal{I}_\ell} = (\mathrm{T}_p E \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G])^{\mathcal{I}_\ell} = (\mathrm{T}_p E)^{\mathcal{I}_\ell} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]$$

is a free $\mathbb{Z}_p[G]$-module of rank $n_\ell \coloneqq \mathrm{rk}_{\mathbb{Z}_p}((\mathrm{T}_p E)^{\mathcal{I}_\ell})$. (We have used here that ℓ is unramified in K.) It follows that the Fitting ideal of $(E_1/E_0)(K_\ell)$ is generated by

$$\det_{\mathbb{Z}_p[G]}(1 - \sigma_\ell^{-1} \mid (T_{K/\mathbb{Q}})^{\mathcal{I}_\ell}) = \det_{\mathbb{Z}_p}(1 - \sigma_\ell^{-1} X \mid (\mathrm{T}_p E)^{\mathcal{I}_\ell})_{|_{X=\sigma_\ell^{-1}}} = \mathrm{Eul}_\ell(\sigma_\ell^{-1}),$$

which generates the same ideal of $\mathbb{Z}_p[G]$ as $\ell \cdot \mathrm{Eul}_\ell(\sigma_\ell^{-1})$ because $\ell \neq p$. Upon fixing a $\mathbb{Z}_p$-basis of $(\mathrm{T}_p E)^{\mathcal{I}_\ell}$, we therefore obtain an $(n_\ell \times n_\ell)$-matrix $A_{\ell,K}$ that represents multiplication by $1 - \sigma_\ell^{-1}$ on $(\mathrm{T}_p E)^{\mathcal{I}_\ell} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G]$ and has all properties listed in the lemma.
In the case $\ell = p$ and E has good reduction at p, the claim follows from (the proof of) [BMCW18, Lem. 4.4] (see also [BMC24, Lem. 6.12]). It therefore suffices to consider the case that E has bad reduction at p. To do this, we first note that the reduction type of E (over K) at v agrees with the reduction type of E (over $\mathbb{Q}$) at p because p is assumed to be unramified in K. If p is a prime of multiplicative reduction, then $(E_1/E_0)(K_\ell) \cong \bigoplus_{v|p}(\mathbb{F}_v^\times \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ therefore vanishes and so in this case the claim follows upon taking $n_p = 1$ and $A_p = 1$, and noting that $p\mathrm{Eul}_p(\sigma_p^{-1}) = p \pm \sigma_p^{-1}$ is a unit in $\mathbb{Z}_p[G]$. If p is a prime of additive reduction, on the other hand, then $(E_1/E_0)(K_\ell) \cong \bigoplus_{v|p} \mathbb{F}_v$. Now, the latter is isomorphic to $\mathbb{F}_p[G]$ by the normal basis theorem and so we deduce that its Fitting ideal over $\mathbb{Z}_p[G]$ is generated by $p = p\mathrm{Eul}_p(\sigma_p^{-1})$, and that we may take $n_p = 1$ and $A_p = p$. □

4.2. Local finite-support cohomology

We define, for $i \in \{0, 1\}$,

$$(E/E_i)(K_\ell) \coloneqq \prod\nolimits_{v|\ell}(E(K_v)/E_i(K_v))^\wedge.$$

We will use without comment that if $\ell \neq p$, then $(E/E_1)(K_\ell)$ agrees with $E(K_\ell) \coloneqq \bigoplus_{v|\ell}(K_v)^\wedge$ because $E_1(K_\ell)$ is pro-ℓ. Note that the Tamagawa number $|E(K_v)/E_0(K_v)|$ is independent of the choice of place $v \mid \ell$ because K is an abelian field. For simplicity we therefore denote this number as $\mathrm{Tam}_{K,\ell}$.

(4.2) Lemma. *Assume that p is unramified in K if E has additive reduction at p. Then the following claims are valid.*

(a) For every prime number ℓ, there exists a morphism

$$\rho_\ell\colon D_\ell^\bullet \to (E/E_1)(K_\ell)[-1]$$

in $D(\mathbb{Z}_p[G])$ with $D_\ell^\bullet$ a perfect complex of $\mathbb{Z}_p[G]$-modules that has the following properties:

(i) $D_\ell^\bullet$ is acyclic outside degree one.

(ii) $D_\ell^\bullet$ admits a representative of the form $[F \to F]$ for a free $\mathbb{Z}_p[G]$-module of finite rank (here the first term is placed in degree 0).

(iii) One has $\vartheta_{D_\ell^\bullet,\varnothing}(\mathrm{Det}_{\mathbb{Z}_p[G]}(D_\ell^\bullet)) = \ell \cdot \mathrm{Eul}_\ell(\tilde\sigma_\ell^{-1}) \cdot \mathbb{Z}_p[G]$.

(iv) If ℓ is unramified in K and $p \nmid \mathrm{Tam}_{K,\ell}$, then ρ_ℓ is a quasi-isomorphism.

(b) For every point Q in $E_1(K_p)$, there exists a morphism

$$\rho_{p,Q}\colon D_{p,Q}^\bullet \coloneqq D_p^\bullet \oplus (\mathbb{Z}_p[G][-1]) \to \mathrm{R}\Gamma_f(\mathbb{Q}_p, T_{K/\mathbb{Q}})$$

in $D(\mathbb{Z}_p[G])$ such that the restriction of $H^1(\rho_{p,Q})$ to $\mathbb{Z}_p[G]$ maps 1 to Q.

Proof. Write m for the conductor of K and $m' \coloneqq m\ell^{-\mathrm{ord}_\ell(m)}$ for the prime-to-ℓ part of m. We can then define a $\mathbb{Z}_p[G_m]$-algebra map $j_\ell\colon \mathbb{Z}_p[G_{m'}] \to \mathbb{Z}_p[G_m]$ by sending σ_a to $\tilde\sigma_a$ (with $\tilde\sigma_a$ as defined before Theorem (2.10) in § 2.3). Write $j_\ell(A_{\ell,F_{m'}})$ for the matrix obtained by applying j_ℓ to each of entry of the matrix $A_{\ell,m'}$ from Lemma (4.1) and set $\widetilde{A_\ell} \coloneqq \pi_{F_m/K}(j_\ell(A_{\ell,F_{m'}}))$. Let $\mathcal{I}^{(\ell)} \subseteq G$ be the inertia subgroup at ℓ, and $\pi_\ell\colon \mathbb{Z}_p[G] \to \mathbb{Z}_p[G/\mathcal{I}^{(\ell)}]$ the natural restriction map. It then follows Lemma (4.1) (c) that $\pi_\ell(\widetilde{A_\ell})$ agrees with $A_\ell \coloneqq A_{\ell,K}$. The exact sequence from Lemma (4.1) (b) therefore fits into a commutative diagram of the form

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}_p[G]^{\oplus n_\ell} & \xrightarrow{\cdot\widetilde{A_\ell}} & \mathbb{Z}_p[G]^{\oplus n_\ell} & \longrightarrow & \mathrm{coker}(j_\ell(A_\ell)) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \pi_\ell^{\oplus n_\ell}} & & \downarrow{\scriptstyle \pi_\ell^{\oplus n_\ell}} & & \vdots & & \\
0 & \longrightarrow & \mathbb{Z}_p[G/\mathcal{I}^{(\ell)}]^{\oplus n_\ell} & \xrightarrow{\cdot A_\ell} & \mathbb{Z}_p[G/\mathcal{I}^{(\ell)}]^{\oplus n_\ell} & \longrightarrow & (E_0/E_1)((K^{\mathcal{I}_\ell})_\ell) & \longrightarrow & 0.
\end{array}$$

The surjectivity of the dashed arrow follows from the snake lemma, and multiplication by $j_\ell(A_\ell)$ is injective by [Bou74, Ch. III, § 8.2, Prop. 3] because

$$\det(j_\ell(A_{\ell,F_{m'}})) = j_\ell(\det(A_{\ell,F_{m'}})) = j_\ell(\mathrm{Eul}_\ell(\sigma_\ell^{-1})) = \ell \cdot \mathrm{Eul}_\ell(\tilde\sigma_\ell^{-1})$$

is a nonzero divisor. Indeed, for this it is enough to prove that $\chi(\mathrm{Eul}_\ell(\tilde\sigma_\ell^{-1})) = \mathrm{Eul}_\ell(\chi(\tilde\sigma_\ell^{-1}))$ is nonzero for ever character χ of G, which is true because the polynomial $\mathrm{Eul}_\ell(X)$ has no root of complex absolute value 1.

Note that $(E_0/E_1)((K^{\mathcal{I}_\ell})_\ell)$ and $(E_0/E_1)(K_\ell)_\ell)$ agree if ℓ is not an additive ramified prime because in any such case K and $K^{\mathcal{I}_\ell}$ have the same residue field at ℓ. If ℓ is additive and ramified in K, then $\ell \neq p$ by the assumed validity of Hypothesis (1.2) (iii) and so $(E_0/E_1)((K^{\mathcal{I}_\ell})_\ell) = 0$.

Writing $D_\ell^\bullet$ for the perfect complex $\big[\mathbb{Z}_p[G]^{\oplus n_\ell} \xrightarrow{\cdot\widetilde{A_\ell}} \mathbb{Z}_p[G]^{\oplus n_\ell}\big]$, where the first term is placed in degree zero, in all cases we have therefore constructed a composite morphism

$$\rho_\ell\colon D_\ell^\bullet = \mathrm{coker}(\widetilde{A_\ell}))[-1] \to (E_0/E_1)((K^{\mathcal{I}_\ell})_\ell)[-1] \to (E_0/E_1)(K_\ell)[-1]$$

in $D(\mathbb{Z}_p[G])$. We also note that $D_\ell^\bullet$ is acyclic outside degree one and that one has

$$\mathrm{Det}_{\mathbb{Z}_p[G]}(D_\ell^\bullet) = \det(\widetilde{A_\ell}) \cdot \mathbb{Z}_p[G] = \ell \cdot \mathrm{Eul}_\ell(\tilde\sigma_\ell^{-1}) \cdot \mathbb{Z}_p[G].$$

It is then clear from the construction that $D_\ell^\bullet$ has all the properties claimd in (i) – (iii). Moreover, it follows from Lemma (4.1) (b) that ρ_ℓ is a quasi-isomorphism if ℓ is unramified in K and $p \nmid \mathrm{Tam}_{K,\ell}$. This proves claim (a) (iv), thereby concluding the proof of (a).

To prove claim (b), we take $\rho_{p,Q}$ to be any map that makes the diagram

$$\begin{array}{ccccc} \mathbb{Z}_p[G][-1] & \longrightarrow & \mathbb{Z}_p[G][-1] \oplus D_p^\bullet & \longrightarrow & D_p^\bullet \longrightarrow \\ \downarrow{\scriptstyle 1\mapsto Q} & & \vdots{\scriptstyle \rho_{p,Q}} & & \downarrow{\scriptstyle \rho_p} \\ E_1(K_p)[-1] & \longrightarrow & \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) & \longrightarrow & (E/E_1)(K_p)[-1] \longrightarrow \end{array}$$

commute. □

(4.3) Remark. If one wants to account for Tamagawa numbers, on can modify $D_\ell^\bullet$ as follows. Since p is odd, each quotient $E(K_v)/E_0(K_v)$ is a cyclic group by the Kodaira–Néron Theorem and hence $(E/E_0)(K_p)$ is a cyclic $\mathbb{Z}_p[G]$-module generated by t_ℓ, say. We therefore have a well-defined map $\mathbb{Z}_p[G]/\mathrm{Tam}_{K,\ell}\mathbb{Z}_p[G] \to (E/E_0)(K_\ell)$ induced by sending 1 to t_ℓ. We then obtain a morphism

$$\rho_{\ell,\mathrm{Tam},0}\colon D_{\ell,\mathrm{Tam}}^\bullet \coloneqq \big[\mathbb{Z}_p[G] \xrightarrow{\cdot \mathrm{Tam}_{K,\ell}} \mathbb{Z}_p[G]\big] \to (E/E_0)(K_\ell)[-1]$$

in $D(\mathbb{Z}_p[G])$ by taking $\rho^0_{\ell,\mathrm{Tam}}$ to be the zero map and $\rho^1_{\ell,\mathrm{Tam}}$ the map that sends 1 to t_ℓ. If we define $D_{\ell,\mathrm{Tam}}^\bullet \coloneqq D_\ell^\bullet \oplus D_{\ell,\mathrm{Tam}}^\bullet$ and $\rho_{\ell,\mathrm{Tam}} \coloneqq \rho_\ell \oplus \rho_{\ell,\mathrm{Tam}}$, then the modified complex $D_{\ell,\mathrm{Tam}}^\bullet$ also has all of the properties listed in Lemma (4.2) (a) as long as one replaces (iii) by

$$\begin{aligned} \vartheta_{D_{\ell,\mathrm{Tam}}^\bullet,\varnothing}(\mathrm{Det}_{\mathbb{Z}_p[G]}(D_{\ell,\mathrm{Tam}}^\bullet)) &= \vartheta_{D_\ell^\bullet,\varnothing}(\mathrm{Det}_{\mathbb{Z}_p[G]}(D_\ell^\bullet)) \cdot \vartheta_{D_{\ell,\mathrm{Tam},0}^\bullet,\varnothing}(\mathrm{Det}_{\mathbb{Z}_p[G]}(D_{\ell,\mathrm{Tam},0}^\bullet)) \\ &= \ell \cdot \mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1}) \cdot \mathrm{Tam}_{K,\ell} \cdot \mathbb{Z}_p[G]. \end{aligned}$$

By defining $D_{p,Q,\mathrm{Tam}} \coloneqq D_{p,\mathrm{Tam}}^\bullet \oplus (\mathbb{Z}_p[G][-1])$ one can then also adapt the construction made in Lemma (4.2) (b).

4.3. Global finite-support cohomology

In this section we use the complexes from Lemma (4.2) to define an auxiliary Nekovář–Selmer complex. To do this, let Π be a finite set of finite places of K, fix $Q \in E_1(K_p)$, and define a Selmer structure $\mathcal{F}_{\Sigma,\Pi,Q}$ on $T_{K/\mathbb{Q}}$ as follows. We take $S(\mathcal{F}_{\Sigma,\Pi,Q}) \coloneqq \Sigma \cup \Pi$, set

$$\mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \coloneqq \begin{cases} D_\ell^\bullet & \text{if } \ell \in \Pi \setminus \{p\}, \\ D_{p,Q}^\bullet & \text{if } \ell = p \in \Pi, \\ \mathbb{Z}_p[G][-1] & \text{if } \ell = p \notin \Pi, \\ 0 & \text{otherwise,} \end{cases}$$

and define $i_{\mathcal{F}_{\Sigma,\Pi,Q},v}$ to be the composite map

$$\mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma_f(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}),$$

where the first arrow is ρ_ℓ, $\rho_{p,Q}$ (both constructed in Lemma (4.2)), or the zero map as appropriate. If p is a good prime that ramifies in K, then by $\rho_{p,Q}$ we mean the restriction of $\rho_{p,Q}$ to $\mathbb{Z}_p[G][-1]$, so the map induced by sending 1 to Q.
To lighten notation, we then introduce the abbreviations

$$\widetilde{D}_{K,\Sigma,\Pi,Q}^\bullet \coloneqq \mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E) \quad \text{and} \quad D_{K,\Sigma,\Pi,Q} \coloneqq \mathrm{RHom}_{\mathbb{Z}_p}(\widetilde{D}_{K,\Sigma,\Pi,Q}^\bullet, \mathbb{Z}_p)[-3].$$

The next result records the basic properties of these complexes.

(4.4) Lemma. *Assume that $E(K)[p] = 0$. For every $Q \in E_1(K_p)$, finite set $\Sigma \supseteq S(K)$ of places of $\mathbb{Q}$, and finite set Π of finite places of $\mathbb{Q}$, the following claims are valid.*

(a) One has an inclusion

$$\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\widetilde{D}_{K,\Sigma,\Pi,Q}^\bullet)) \subseteq \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2_f(K, \mathrm{T}_p E)).$$

(b) Let F be a subfield of K and define $Q' \coloneqq \mathrm{Tr}_{K/F}(Q)$. Then one has

$$\pi_{K/F}(\mathrm{Fitt}^0_{\mathbb{Z}_p[G_K]}(H^2(\widetilde{D}_{K,\Sigma,\Pi,Q}^\bullet))) = \mathrm{Fitt}^0_{\mathbb{Z}_p[G_F]}(H^2(\widetilde{D}_{F,\Sigma,\Pi,Q'}^\bullet)).$$

(c) Let Σ' be a finite set of places of K that contains Σ. Then one has an exact triangle

$$\bigoplus_{\ell\in(\Sigma'\setminus\Sigma)} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \longrightarrow \widetilde{D}^\bullet_{K,\Sigma',\Pi,Q} \longrightarrow \widetilde{D}^\bullet_{K,\Sigma,\Pi,Q} \longrightarrow \bigoplus_{\ell\in(\Sigma'\setminus\Sigma)} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})[1].$$

(d) If $\ell \in \Pi \setminus S(K)$, then $\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q} = \widetilde{D}^\bullet_{K,\Sigma\setminus\{\ell\},\Pi\setminus\{\ell\},Q}$.

Proof. At the outset we define

$$\widetilde{D}^\bullet_{\mathrm{loc},\Pi,Q} \coloneqq \bigoplus_{\ell\in\Pi\cup\{p\}} \mathrm{R}\Gamma_{\mathcal{F}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})$$

and $\rho_\Pi \coloneqq \rho_{p,Q} \oplus \bigoplus_{\ell\in\Pi} \rho_\ell$, and note that the definition of $D^\bullet_{K,\Sigma,\Pi,Q}$ implies that there is an exact triangle

$$\mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE) \longrightarrow \widetilde{D}^\bullet_{K,\Sigma,\Pi,Q} \longrightarrow \widetilde{D}^\bullet_{\mathrm{loc},\Pi,Q} \longrightarrow \mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE)[1]. \tag{27}$$

This combines with the definition of the complex $\mathrm{R}\Gamma_f(K, \mathrm{T}_pE)$ and the octahedral axiom to yield an exact triangle of the form

$$\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q} \longrightarrow \mathrm{R}\Gamma_f(K, \mathrm{T}_pE) \longrightarrow \mathrm{cone}(\rho_\Pi) \oplus \bigoplus_{\ell\in\Sigma\setminus(\Pi\cup\{p\}} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \longrightarrow \widetilde{D}^\bullet_{K,\Sigma,\Pi,Q}[1]. \tag{28}$$

Since the cone of the morphism ρ_Π and $\bigoplus_{\ell\in\Sigma\setminus\Pi} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})$ both have no nonzero cohomology in degrees greater than one, this exact triangle induces a surjection

$$H^2(\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q}) \twoheadrightarrow H^2_f(K, \mathrm{T}_pE).$$

A standard property of Fitting ideals then combines with this surjection to imply the inclusion claimed in (a). Similarly, the properties of Fitting ideals reduce claim (b) to the claim that one has an isomorphism

$$H^2(\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q}) \otimes_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[G_F] \cong H^2(\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q'}).$$

Now, the triangle (27) combines with the assumption $E(K)[p] = 0$ to imply $\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q}$ is acyclic in degree greater than two and so the desired isomorphism follows from Lemma (B.13) (a) if we can demonstrate that one has an isomorphism

$$\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q} \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[G_F] \cong \widetilde{D}^\bullet_{F,\Sigma,\Pi,Q'}$$

in $D(\mathbb{Z}_p[G_F])$. To do this, we first note that one has $D^\bullet_{p,Q} \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[G_F] \cong D^\bullet_{p,Q'}$ and $D^\bullet_\ell \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[G_F] \cong D^\bullet_\ell$, as can be checked from Lemma (4.1) (c) and the explicit definitions of these complexes. In addition, one has commutative diagrams

$$\begin{array}{ccc} D^\bullet_{K,p,Q} \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[G_F] & \xrightarrow{\overline{\rho_{K,p,Q}}} & E(K_p)[-1] \\ \downarrow\simeq & & \downarrow \mathrm{Tr}_{K/F} \\ D_{F,p,Q'} & \xrightarrow{\rho_{F,p,Q}} & E(F_p)[-1] \end{array} \qquad \begin{array}{ccc} D^\bullet_{K,\ell} \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[G_F] & \xrightarrow{\overline{\rho_{K,\ell}}} & (E/E_0)(K_\ell)[-1] \\ \downarrow\simeq & & \downarrow \mathrm{Tr}_{K/F} \\ D^\bullet_{F,\ell} & \xrightarrow{\rho_{F,\ell}} & (E/E_0)(F_\ell), \end{array}$$

where we have introduced subscripts K and F to emphasise the field of definition, and $\overline{\rho_{K,p,Q}}$ and $\overline{\rho_{K,\ell}}$ denote the maps induced by $\rho_{K,p,Q}$ and $\rho_{K,\ell}$, respectively. The claimed property of $\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q}$ then follows by combining this with the triangle (27) and the well-known isomorphism

$$\mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE) \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G_K]} \mathbb{Z}_p[G_F] \cong \mathrm{R}\Gamma_c(\mathcal{O}_{F,\Sigma}, \mathrm{T}_pE),$$

(see, for example, [FK06, Prop. 1.6.5 (3)]). Claim (c) follows from (27) and the triangle

$$\bigoplus_{\ell\in(\Sigma'\setminus\Sigma)} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma'}, \mathrm{T}_pE) \to \mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE) \to \bigoplus_{\ell\in(\Sigma'\setminus\Sigma)} \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})[1]$$

via the octrahedral axiom. Finally, claim (d) is a consequence of the fact that, if $\ell \in \Pi \setminus S(K)$ (and so $\ell \neq p$ is a prime of good reduction that is unramified in K), then the map $\rho_\ell\colon D^\bullet_\ell \to \mathrm{R}\Gamma_f(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})$ is a quasi-isomomorphism by Lemma (4.2) (a) (iv) (cf. also the argument of [BMC24, Lem. 2.5]). □

(4.5) Lemma. *Assume $E(K)[p] = 0$ and, for given $Q \in E_1(K_p)$, consider the composite morphism*

$$\begin{aligned}\rho'_{p,Q}\colon C^\bullet_{K,\Sigma} &\longrightarrow \mathrm{R}\Gamma_{/f}(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \cong \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma_f(\mathbb{Q}_p, T_{K/\mathbb{Q}}), \mathbb{Z}_p)[-2]\\ &\xrightarrow{\rho^*_{p,Q}} \mathrm{RHom}_{\mathbb{Z}_p}(D^\bullet_{p,Q}, \mathbb{Z}_p)[-2] = \mathrm{RHom}_{\mathbb{Z}_p}(D^\bullet_p, \mathbb{Z}_p)[-2] \oplus \mathbb{Z}_p[G][-1]\\ &\longrightarrow \mathbb{Z}_p[G][-1].\end{aligned}$$

Here the first arrow is the natural localisation map composed with the morphism $\mathrm{R}\Gamma(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma_{/f}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$, the isomorphism is by local Tate duality (25), $\rho^*_{p,Q} := \mathrm{RHom}_{\mathbb{Z}_p}(\rho_{p,Q}, \mathbb{Z}_p)[-2]$ is the dual of the map $\rho_{p,Q}$ defined in Lemma (4.2) (b), and the last arrow is projection onto the direct summand $\mathbb{Z}_p[G][-1]$. Then the map $H^1(\rho'_{p,Q})$ induced by $\rho'_{p,Q}$ on cohomology in degree one coincides with the composite map

$$H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \to H^1_{/f}(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \xrightarrow{\mathcal{P}_K(\cdot,Q)} \mathbb{Z}_p[G].$$

Proof. Using the (dual of the) representative of $C^\bullet_{K,\Sigma}$ constructed in Lemma (3.5), we have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}_p[G] & = & \mathbb{Z}_p[G] & \longrightarrow & 0\\ \downarrow & & \downarrow{\scriptstyle \rho^2_{p,Q}} & & \downarrow{\scriptstyle H^2(\rho_{p,Q})} & & \\ P & \xrightarrow{\phi^*} & P & \longrightarrow & H^2_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) & \longrightarrow & 0, \end{array}$$

where the first commutative square represents the morphism $\rho_{p,Q}$ composed with the morphism $\mathrm{R}\Gamma_f(\mathbb{Q}_p, T_{K/\mathbb{Q}})[-1] \to \mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \cong \mathrm{RHom}_{\mathbb{Z}_p}(C^\bullet_{K,\Sigma}, \mathbb{Z}_p)[-3]$ (and $\rho^2_{p,Q}$ is the map induced by $\rho_{p,Q}$ in degree two). By dualising, we therefore obtain the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) & \longrightarrow & P & \xrightarrow{\phi} & P\\ & & \downarrow{\scriptstyle H^0(\rho'_{p,Q})} & & \downarrow{\scriptstyle (\rho'_{p,Q})^0} & & \downarrow\\ 0 & \longrightarrow & \mathbb{Z}_p[G] & = & \mathbb{Z}_p[G] & \longrightarrow & 0, \end{array}$$

where now the second commutative square represents the morphism $\rho'_{p,Q}$ (and $(\rho'_{p,Q})^0$ is the map induced by $\rho'_{p,Q}$ in degree zero). In particular, $H^0(\rho'_{p,Q})$ coincides with the dual of $H^2(\rho_{p,Q})$. The claim therefore follows from the observation that $H^2(\varrho_{p,Q})$ is the composite map

$$\mathbb{Z}_p[G] \xrightarrow{1\mapsto Q} H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \to H^2_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$$

so that its dual map is given by the composite

$$H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \to H^1_{/f}(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \cong H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}})^* \to \mathbb{Z}_p[G].$$

Here the first arrow is the localisation map (followed by projection), the isomorphism is induced by the pairing $(\cdot,\cdot)_{E/K}$, and the last arrow is evaluation at Q. □

4.4. Determinantal ideals

In this section we establish a connection between elements in the image of the map $\Theta_{K,\Sigma}$ (defined before the statement of Theorem (3.6)) and the Selmer complexes $\widetilde{D}_{K,\Sigma,\Pi,Q}$ introduced in the last section. Our main result in this direction is as follows.

(4.6) Proposition. *Assume that $E(K)[p] = 0$, fix $Q \in E_1(K_p)$, and let Σ be a finite set of places of K that contains $S(K)$. If $\Pi \subseteq \Sigma$ is a subset of rational primes that are either unramified in K or at which E has multiplicative reduction, then for every*

- $a \in \mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,\Sigma})^{-1}$,
- $t \in \prod_{\ell\in\Pi} \mathrm{Ann}_{\mathbb{Z}_p[G]}((E/E_0)(K_\ell))^{-1,\#}$.

- $\nu \in \big(\prod_{\ell\in\Pi}(\ell^{-1}\mathrm{Eul}_\ell(\widetilde{\sigma}_\ell^{-1})^{-1}\mathrm{N}_{\mathcal{I}_K^{(\ell)}}\mathbb{Z}_p[G] + \mathbb{Z}_p[G]\big)$,

one has the containments

$$\nu \cdot \mathcal{P}_K(\Theta_{K,\Sigma}(a), Q) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q}))^\#, \tag{29}$$

$$t \cdot \nu \cdot \mathcal{P}_K(\Theta_{K,\Sigma}(a), Q) \in \mathbb{Z}_p[G]. \tag{30}$$

Before proving Proposition (4.6), we first establish an auxiliary result that concerns the maps

$$\vartheta_{K,\Sigma,\Pi,Q} \coloneqq \vartheta_{D^\bullet_{K,\Sigma,\Pi,Q},\{b^*\}} \quad \text{and} \quad \widetilde{\vartheta}_{K,\Sigma,\Pi,Q} \coloneqq \vartheta_{\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q},\varnothing}$$

(with b^* the dual of the $\mathbb{Z}_p[G]$-basis b of $T^+_{K/\mathbb{Q}}$ from § 3.2) defined as the relevant instances of Definition (B.2).
Setting $D^\bullet_{\mathrm{loc},\Pi,Q} \coloneqq \mathrm{RHom}_{\mathbb{Z}_p}(\widetilde{D}^\bullet_{\mathrm{loc},\Pi,Q}, \mathbb{Z}_p)[-2]$ and dualising the triangle (27) gives an exact triangle

$$D^\bullet_{K,\Sigma,\Pi,Q} \longrightarrow C^\bullet_{K,\Sigma} \xrightarrow{\rho_{\mathrm{loc},\Pi,Q}} D^\bullet_{\mathrm{loc},\Pi,Q} \longrightarrow D^\bullet_{K,\Sigma,\Pi,Q}[1]. \tag{31}$$

To state the next lemma below, we will make use of the isomorphism

$$\begin{aligned}\mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,\Sigma})^{-1} &\cong \mathrm{Det}_{\mathbb{Z}_p[G]}(D^\bullet_{K,\Sigma,\Pi,Q})^{-1} \otimes \mathrm{Det}_{\mathbb{Z}_p[G]}(D^\bullet_{\mathrm{loc},\Pi,Q})^{-1}\\ &\cong \mathrm{Det}_{\mathbb{Z}_p[G]}(D^\bullet_{K,\Sigma,\Pi,Q})^{-1}.\end{aligned} \tag{32}$$

Here the first isomorphism is induced by the the triangle (31) and the second isomorphism is induced by the isomorphism

$$(\otimes_{\ell\in\Pi}\mathrm{Ev}(a_\ell))\colon \mathrm{Det}_{\mathbb{Z}_p[G]}(D^\bullet_{\mathrm{loc},\Pi,Q})^{-1} \xrightarrow{\simeq} \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G][-1])^{-1} = \mathbb{Z}_p[G]$$

with a_ℓ the canonical element of $\mathrm{Det}_{\mathbb{Z}_p[G]}(D^\bullet_\ell)$ that satisfies $\vartheta_{D^\bullet_\ell,\varnothing}(a_\ell) = \ell \cdot \mathrm{Eul}_\ell(\sigma_\ell)$ (which exists by Lemma (4.2) (a) (iii)).

(4.7) Lemma. *Let $Q \in E_1(K_p)$. If $E(K)[p] = 0$, then the following claims are valid.*

(a) Put $\eta_\Pi \coloneqq \prod_{\ell\in\Pi}(\ell \cdot \mathrm{Eul}_\ell(\sigma_\ell^{-1}))$ for brevity. Then the following diagram commutes.

$$\begin{array}{ccc}\mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,\Sigma})^{-1} & \xrightarrow{\Theta_{K,\Sigma}} & H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE)\\ {\scriptstyle(32)}\big\downarrow\simeq & & \big\downarrow{\scriptstyle \pm\eta_\Pi^{-1}\cdot\mathcal{P}_K(\cdot,Q)}\\ \mathrm{Det}_{\mathbb{Z}_p[G]}(D^\bullet_{K,\Sigma,\Pi,Q})^{-1} & \xrightarrow{\vartheta_{K,\Sigma,\Pi,Q}} & \mathbb{Q}_p[G].\end{array}$$

(b) One has the equality $\vartheta_{K,\Sigma,\Pi,Q}(\mathrm{Det}_{\mathbb{Z}_p[G]}(D^\bullet_{K,\Sigma,\Pi,Q})^{-1}) = \widetilde{\vartheta}_{K,\Sigma,\Pi,Q}(\mathrm{Det}_{\mathbb{Z}_p[G]}(\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q})^{-1})^\#$ and an inclusion

$$\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^1(\widetilde{D}_{K,\Sigma,\Pi,Q})^\vee_{\mathrm{tor}}) \cdot \widetilde{\vartheta}_{K,\Sigma,\Pi,Q}(\mathrm{Det}_{\mathbb{Z}_p[G]}(\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q})^{-1}) \subseteq \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\widetilde{D}^\bullet_{K,\Sigma,\Pi,Q})).$$

Proof. Claim (a) follows from Proposition (B.7) (a) (i), applied for every Ev_{a_ℓ}, and Proposition (B.7) (b) (combined with Lemma (4.5)).
To justify claim (b), we first note that, by Lemma (4.2) (a) (ii), the complex $D^\bullet_{\mathrm{loc},\Pi,Q}$ admits a representative of the form $[F \oplus \mathbb{Z}_p[G] \xrightarrow{\partial\oplus 0} F]$ for some free $\mathbb{Z}_p[G]$-module F of finite rank and endomorphism ∂ of F. In the following we set $F' \coloneqq F \oplus \mathbb{Z}_p[G]$ and fix a $\mathbb{Z}_p[G]$-basis $y_1, \dots, y_s$ of F' such that F is identified with $\bigoplus_{i=2}^s \mathbb{Z}_p[G]y_i$.
Write $[P \xrightarrow{\phi} P]$ for the representative of $C^\bullet_{K,\Sigma}$ provided by Lemma (3.5). That is, P is a free $\mathbb{Z}_p[G]$-module of rank d, say, with basis $x_1, \dots, x_d$, and $P = P' \oplus (T_{K/\mathbb{Q}})^+$ with $P' \coloneqq \bigoplus_{i=2}^d \mathbb{Z}_p[G]x_i$. From this choice of bases we see that, by (31) and the definition of the mapping cone, that $D^\bullet_{K,\Sigma,\Pi,Q}$ is represented by $[P \xrightarrow{\phi'} P \oplus F' \xrightarrow{\partial'} F]$ with the first term placed in degree one. Here $\phi' = -(\phi \oplus \rho^1)$ and $\partial' = -\rho^2 + \partial$ with ρ^i the component in degree i of the morphism $\rho\colon C^\bullet_{K,S} \to D^\bullet_{\mathrm{loc},\Pi,Q}$.
We next recall from (3) that for every $\mathbb{Z}_p[G]$-module M we have a canonical isomorphism

$\mathrm{Hom}_{\mathbb{Z}_p}(M,\mathbb{Z}_p) \xrightarrow{\simeq} \mathrm{Hom}_{\mathbb{Z}_p[G]}(M,\mathbb{Z}_p[G])^{\#}$. It follows that the complex $\widetilde{D}^{\bullet}_{K,\Sigma,\Pi,Q}$, which is isomorphic to the (shifted) $\mathbb{Z}_p$-linear dual of $D^{\bullet}_{K,\Sigma,\Pi,Q}$, can be represented by $[F \xrightarrow{\partial^{\#,\mathrm{tr}}} P \oplus F' \xrightarrow{\phi'^{\#,\mathrm{tr}}} P]$ with the first term placed in degree zero. Here the maps $\partial'^{\#,\mathrm{tr}}$ and $\phi'^{\#,\mathrm{tr}}$ are defined by means of the matrices that are obtained by applying the involution $\#$ to the transpose of the matrices representing ∂' and ϕ', respectively. This shows that $\widetilde{D}^{\bullet}_{K,\Sigma,\Pi,Q}$ admits a standard representative in the sense of Definition (B.3) and so the inclusion claimed in (b) is a special case of Proposition (B.10) (b).

To prove the remainder of claim (b), we note that the complex $[F \xrightarrow{\partial'^{\#,\mathrm{tr}}} P' \oplus F' \xrightarrow{\phi'^{\#,\mathrm{tr}}} P]$ is a perfect complex of $\mathbb{Z}_p[G]$-modules that is both acyclic outside degrees one and two (this uses that $\partial^{\#,\mathrm{tr}}$, and hence also $\partial'^{\#,\mathrm{tr}}$, is injective) and has vanishing Euler characteristic in $K_0(\mathbb{Z}_p[G])$. We may then apply Proposition (B.7) (c) to deduce that

$$\begin{aligned}\widetilde{\vartheta}_{K,\Sigma,\Pi,Q}(\mathrm{Det}_{\mathbb{Z}_p[G]}(\widetilde{D}^{\bullet}_{K,\Sigma,\Pi,Q})^{-1})^{\#} &\overset{(3)}{=} \widetilde{\vartheta}_{K,\Sigma,\Pi,Q}(\mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{RHom}_{\mathbb{Z}_p[G]}(D^{\bullet}_{K,\Sigma,\Pi,Q},\mathbb{Z}_p[G]))^{-1})\\ &= \vartheta_{K,\Sigma,\Pi,Q}(\mathrm{Det}_{\mathbb{Z}_p[G]}(D^{\bullet}_{K,\Sigma,\Pi,Q})^{-1}),\end{aligned}$$

as claimed. □

We can now give the proof of Proposition (4.6).

Proof (of Proposition (4.6)): We first explain how to deduce the inclusion (29) from Lemma (4.7). To do this, we note that, as $H^1_f(K,\mathrm{T}_pE) = E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_p$ is assumed to be $\mathbb{Z}_p$-torsion free, it follows from the triangle (28) that we have an identification

$$\begin{aligned}H^1(\widetilde{D}_{K,\Sigma,\Pi,Q})_{\mathrm{tor}} &= H^0\big(\mathrm{cone}(\widetilde{\rho}_{\mathrm{loc},\Pi,Q})\big)_{\mathrm{tor}}\\ &= \ker\big\{\textstyle\bigoplus_{\ell\in\Pi}\big(\mathbb{Z}_p[G]^{n_\ell}/(j_\ell(A_\ell))\big) \longrightarrow \bigoplus_{\ell\in\Pi}(E/E_0)(K_\ell)\big\}\\ &= \ker\big\{\textstyle\bigoplus_{\ell\in\Pi_{\mathrm{bad}}}\big(\mathbb{Z}_p[G]/(\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell))\big) \longrightarrow \bigoplus_{\ell\in\Pi_{\mathrm{bad}}}(E/E_0)(K_\ell)\big\}\\ &= \textstyle\bigoplus_{\ell\in\Pi_{\mathrm{bad}}}\big(\mathrm{Ann}_{\mathbb{Z}_p[G]}((E_0/E_1)(K_\ell))/(\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell))\big).\end{aligned}$$

Here $\Pi_{\mathrm{bad}}\subseteq\Pi$ denotes the subset of places at which E has bad reduction (in which case $n_\ell=1$ and $j_\ell(A_\ell)=\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)$), and we have used that any prime $\ell\in\Pi\setminus\Pi_{\mathrm{bad}}$ is by assumption unramified in K and so does not contribute to the above kernel because ρ_ℓ is an quasi-isomorphism for any such ℓ by Lemma (4.2).

Before proceeding, it is convenient to first make a general observation concerning an ideal $\mathfrak{a}$ of $\mathbb{Z}_p[G]$ that contains a nonzero divisor x. In any such situation one has

$$\big(\mathfrak{a}/\mathbb{Z}_p[G]x\big)^{\vee} \cong \big((\mathbb{Z}_p[G]x)^*/\mathfrak{a}^*\big)^{\#} \cong \big((x^{-1}\mathbb{Z}_p[G])/\mathfrak{a}^{-1}\big)^{\#} \cong \mathbb{Z}_p[G]/(x\mathfrak{a}^{-1})^{\#}, \tag{33}$$

where we have used the isomorphism $\mathfrak{a}^*\cong\mathfrak{a}^{-1}:=\{y\in\mathbb{Q}_p[G]\mid y\mathfrak{a}\subseteq\mathbb{Z}_p[G]\}$ that is valid because $\mathfrak{a}$ contains a nonzero divisor (cf. [Bas63, Prop. 6.1 (4)]). From (33) we then conclude that $\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}((\mathfrak{a}/\mathbb{Z}_p[G]x)^\vee)=(x\mathfrak{a}^{-1})^{\#}$. This general observation applied with $\mathfrak{a}$ and x taken to be $\mathrm{Ann}_{\mathbb{Z}_p[G]}((E_0/E_1)(K_\ell))$ and $\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})$, respectively, shows that $\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^1(\widetilde{D}_{K,\Sigma,\Pi,Q})^\vee_{\mathrm{tor}})$ is equal to the product ideal

$$\textstyle\prod_{\ell\in\Pi_{\mathrm{bad}}}\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})\cdot\mathrm{Ann}_{\mathbb{Z}_p[G]}((E_0/E_1)(K_\ell))^{-1,\#}.$$

Now, the factors $\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})$ cancel with the corresponding factors in the definition of the element η_Π^{-1} from Lemma (4.7), and so Lemma (4.7) (a) implies that

$$\big(\textstyle\prod_{\ell\in\Pi_{\mathrm{bad}}}\mathrm{Ann}_{\mathbb{Z}_p[G]}((E_0/E_1)(K_\ell))^{-1,\#}\big)\cdot\mathcal{P}_K(\Theta_{K,\Sigma}(a),Q)$$

is contained in

$$\big(\textstyle\prod_{\ell\in\Pi\setminus\Pi_{\mathrm{bad}}}\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})\big)\cdot\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\widetilde{D}^{\bullet}_{K,\Sigma,\Pi,Q}))^{\#}.$$

It now only remains to observe that, for every $\ell \in \Pi_{\mathrm{bad}}$, one has that $\mathrm{Ann}_{\mathbb{Z}_p[G]}((E_0/E_1)(K_\ell))^{-1,\#}$ contains $\ell^{-1}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})^{-1}\mathrm{N}_{\mathcal{I}_K^{(\ell)}}\mathbb{Z}_p[G] + \mathbb{Z}_p[G]$ because $\mathrm{Ann}_{\mathbb{Z}_p[G]}((E_0/E_1)(K_\ell))$ is generated by $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)$ and the augmentation ideal $I(\mathcal{I}_K^{(\ell)})$ as a consequence of Lemma (4.1) and the assumption that Π_{bad} contains no additive primes. Since $\mathcal{I}_K^{(\ell)}$ is trivial for any $\ell \in \Pi \setminus \Pi_{\mathrm{bad}}$ by assumption (and so $\ell^{-1}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\mathrm{N}_{\mathcal{I}_K^{(\ell)}}\mathbb{Z}_p[G]+\mathbb{Z}_p[G]$ simplifies to $\ell^{-1}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\mathbb{Z}_p[G]$ for such ℓ), this concludes the proof of (29).

As for the proof of (30), this follows from a very similar argument and so we only provide a sketch. Using the complexes defined in Remark (4.3), we may define a modified Nekovář–Selmer structure $\mathcal{F}^{\mathrm{Tam}}_{\Sigma,\Pi,Q}$ by taking $S(\mathcal{F}^{\mathrm{Tam}}_{\Sigma,\Pi,Q}) \coloneqq \Sigma \cup \Pi$ and

$$\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{Tam}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \coloneqq \begin{cases} D^\bullet_{\ell,\mathrm{Tam}} & \text{if } \ell \in \Pi \setminus \{p\}, \\ D^\bullet_{p,Q,\mathrm{Tam}} & \text{if } \ell = p \in \Pi, \\ \mathbb{Z}_p[G][-1] & \text{if } \ell = p \notin \Pi, \\ 0 & \text{otherwise.} \end{cases}$$

Now, if we set $\eta^{\mathrm{Tam}}_\Pi \coloneqq \prod_{\ell\in\Pi}(\mathrm{Tam}_{K,\ell}\cdot\ell\cdot\mathrm{Eul}_\ell(\sigma_\ell^{-1}))$ and $\widetilde{D}_{\mathrm{Tam}} \coloneqq \mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{Tam}}_{\Sigma,\Pi,Q}}(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE)$, then the argument of Lemma (4.7) (a) shows that we have a commutative diagram of the form

$$\begin{array}{ccc} \mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,\Sigma})^{-1} & \xrightarrow{\Theta_{K,\Sigma}} & H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE) \\ \downarrow\simeq & & \downarrow{\scriptstyle \pm(\eta^{\mathrm{Tam}}_\Pi)^{-1}\cdot\mathcal{P}_K(\cdot,Q)} \\ \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{RHom}_{\mathbb{Z}_p}(\widetilde{D}_{\mathrm{Tam}}, \mathbb{Z}_p)[-3])^{-1} & \xrightarrow{\vartheta^{\mathrm{Tam}}} & \mathbb{Q}_p[G], \end{array}$$

where the map ϑ^{Tam} is defined as the relevant special case of Definition (B.2). In addition, the argument of Lemma (4.7) (b) shows that

$$\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^1(\widetilde{D}_{\mathrm{Tam}})^\vee_{\mathrm{tor}})\cdot(\mathrm{im}\,\vartheta^{\mathrm{Tam}})^\# \subseteq \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\widetilde{D}^\bullet_{\mathrm{Tam}})) \subseteq \mathbb{Z}_p[G].$$

The inclusion (30) can therefore be proved in exactly the same way as the inclusion (29) once we have observed that $H^1(\widetilde{D}_{\mathrm{Tam}})_{\mathrm{tor}}$ identifies with

$$\bigoplus\nolimits_{\ell\in\Pi_{\mathrm{bad}}}\big(\mathrm{Ann}_{\mathbb{Z}_p[G]}((E/E_0)(K_\ell))/(\mathrm{Tam}_{K,\ell})\big) \oplus \big(\mathrm{Ann}_{\mathbb{Z}_p[G]}((E_0/E_1)(K_\ell))/(\ell\mathrm{Eul}_\ell(\tilde{\sigma}_\ell))\big). \quad \square$$

4.5. The proof of Theorem (1.4) (b)

In this section we prove Theorem (1.4) (b), our main result towards the 'weak main conjecture' of Mazur and Tate. If the Euler factors $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}$ are invertible in $\mathbb{Z}_p[G_{mp^n}]$ for all prime divisors ℓ of m and the element $\mathfrak{k}_{mp^n}$ from Theorem (2.10) is in $E_1(K_p)$, then this is a straightforward consequence of Theorem (3.6) and Proposition (4.6). However, this will not be the case in general and so a more detailed analysis is required in order to prove Theorem (1.4) (b). This will be done in the rather technical Lemma (4.9) below, where we will use the Euler system norm relations in order to prove that the denominators arising from factors of the form $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}$ can be 'absorbed' by $z^{\mathrm{Kato}}_{mp^n}$.

Before stating this result, we first give a different characterisation of the set of prime numbers $C^{(p)}_\times(K)$ that was defined in Remark (1.5) (c).

(4.8) Lemma. *A prime number $\ell \neq p$ belongs to $C^{(p)}_\times(K)$ if and only if $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell) \in \mathbb{Z}_p[G]^\times$.*

Proof. Let $G^{(p)} \subseteq G$ denote the p-Sylow subgroup of G and set $\Delta \coloneqq G/G^{(p)}$. We then write $\widehat{\Delta}$ for the group of all characters $\chi\colon \Delta \to \overline{\mathbb{Q}_p}^\times$ and let $\mathcal{O}$ be the unramified extension of $\mathbb{Z}_p$ that is generated by the values of all $\chi \in \widehat{\Delta}$. An element of $\mathbb{Z}_p[G]$ is then a unit if and only if it is a unit in the integral extension $\mathcal{O}[G]$ of $\mathbb{Z}_p[G]$. Now, one has a decomposition $\mathcal{O}[G] \cong \bigoplus_{\chi\in\widehat{\Delta}}\mathcal{O}[G^{(p)}]$ induced by the isomorphism $\mathcal{O}[\Delta] \xrightarrow{\simeq} \bigoplus_{\chi\in\widehat{\Delta}}\mathcal{O}, x \mapsto (\chi(x))_\chi$. Each $\mathcal{O}[G^{(p)}]$ is a local ring with

maximal ideal $(p, I_{\mathcal{O},G^{(p)}})$, so this argument proves that an element x of $\mathbb{Z}_p[G]$ is a unit if and only if $\chi(x) \not\equiv 0 \mod p$ for all $\chi \in \widehat{\Delta}$. To prove that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell) \in \mathbb{Z}_p[G]^\times$ if and only if ℓ satisfies the explicit condition given in the definition of $C_\times^{(p)}$ in Remark (1.4) (c) it now suffices to prove that the set $\{\chi(\tilde{\sigma}_\ell) : \chi \in \widehat{\Delta}\}$ coincides with the group of $f_{K/\mathbb{Q}}^{(p)}$-th roots of unity of $\overline{\mathbb{Q}_p}^\times$. For this it is in turn enough to prove that the order of $(\tilde{\sigma}_\ell)_{|K}$ in G is equal to the residue degree of ℓ in $K/\mathbb{Q}$ or, equivalently, the order of $(\sigma_\ell)_{|K'}$ with K' the maximal subextension of K unramified at ℓ. To do this, we write m for the conductor of K and set $M \coloneqq m\ell^{-\operatorname{ord}_\ell(m)}$. Then $K' = K \cap F_M$ so that the restriction map induces an isomorphism $\mathrm{Gal}(F_m/K) \cong \mathrm{Gal}(F_M/K')$. Given this, it follows directly from the definition of $\tilde{\sigma}_\ell$ that a power $\tilde{\sigma}_\ell^n$ belongs to $\mathrm{Gal}(F_m/K)$ if and only if σ_ℓ^n belongs to $\mathrm{Gal}(F_M/K')$, as required to prove the claim. □

To prepare for the statement of the next result, we write the conductor of K as mp^n with $m \in \mathbb{N}$ coprime to p and $n \in \mathbb{Z}_{\geq 0}$. Given a subset $\mathscr{L} \subseteq S_{mp^n}$, we set $(mp^n)_{\mathscr{L}} \coloneqq mp^n \cdot (\prod_{\ell \in \mathscr{L}} \ell^{\operatorname{ord}_\ell(m)})^{-1}$ and $z_{\mathscr{L}}^{\mathrm{Kato}} \coloneqq z_{(mp^n)_{\mathscr{L}}}^{\mathrm{Kato}}$. Write $F_{\mathscr{L}} \coloneqq F_{(mp^n)_{\mathscr{L}}}$ and $G_{\mathscr{L}} \coloneqq G_{(mp^n)_{\mathscr{L}}}$. We also define the following sets of primes,

$$\mathscr{Z}(K) \coloneqq \{\ell \mid mp^n : \ell \nmid N, \ell \notin C_\times^{(p)}\}$$
$$\mathscr{Y}(K) \coloneqq \{\ell \mid m : \ell \in C_\times^{(p)}\}.$$

For further ease of notation we write $N_p = N \cdot p^{-\operatorname{ord}_p(N)}$ and define

$$\eta_{K,N_p} \coloneqq \prod_{\ell \mid N_p,\ \ell \notin \mathscr{Y}(K)} (\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \nu_{mp^n}^{(\ell)})^{\#} \in \mathbb{Q}_p[G_{mp^n}].$$

(4.9) Lemma. *Assume p is unramified in K if E has additive reduction at p, and suppose $(\mathfrak{a}_{\mathscr{L}})_{\mathscr{L} \subseteq \mathscr{Z}(mp^n)}$ is a collection of ideals $\mathfrak{a}_{\mathscr{L}} \subseteq \mathbb{Z}_p[G_{\mathscr{L}}]$ with the property that*

$$(p\mathrm{Eul}_p(\sigma_p^{-1}))^{-\mathbf{1}_{\mathscr{L}}(p)} \cdot \eta_{K,N_p} \cdot \mathcal{P}_{F_{\mathscr{L}}}(z_{\mathscr{L}}^{\mathrm{Kato}}, \mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}(Q)) \in \mathfrak{a}_{\mathscr{L}} \tag{34}$$

for all $Q \in E_1(F_{m,p})$. Then

$$(1 - e_\tau)\theta_K^{\mathrm{MT}} \in (\textstyle\prod_{\ell \in \mathscr{Y}(K)} \nu_{mp^n}^{(\ell)})^{\#} \cdot \pi_{F_{mp^n}/K}\big(\sum_{\mathscr{L} \subseteq \mathscr{Z}(mp^n)} \mathfrak{a}_{\mathscr{L}} \mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}}\big) \quad \subseteq \mathbb{Z}_p[G]. \tag{35}$$

If $a_p \not\equiv 1 \mod p$ and p is either of good reduction for E a prime of potentially good reduction for E, then the same conclusion holds with $(1 - e_\tau)\theta_K^{\mathrm{MT}}$ replaced by θ_K^{MT}.

Proof. This is an extension of the argument used by Otsuki in [Ots09, Lem. 4.2].
At the outset we note that, by Lemma (4.8) the Euler factor $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)$ is a unit in $\mathbb{Z}_p[G]$ for a prime number $\ell \mid m$ if and only if $\ell \in \mathscr{Y}(K)$. In order to simplify some statements later on it is convenient to set $\nu_{mp^n}^{(\ell)} \coloneqq 1$ if $\ell \mid N$ and $\ell \nmid m$. From the equation

$$\begin{aligned}(1 - e_\tau)\theta_{mp^n}^{\mathrm{MT}} &= (1 - e_\tau)\big(\prod_{\ell \in S_m} \mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \nu_{mp^n}^{(\ell)}\big)^{\#} \cdot \mathcal{P}_{F_{mp^n}}(y_{mp^n}^{\mathrm{Kato}}, \mathfrak{k}_{mp^n}) \\ &= \big(\prod_{\ell \in S_{mN_p}} \mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})^{-1} \cdot \nu_{mp^n}^{(\ell),\#}\big) \cdot \mathcal{P}_{F_{mp^n}}(z_{mp^n}^{\mathrm{Kato}}, (1 - e_\tau)\mathfrak{k}_{mp^n}),\end{aligned}$$

proved in Theorem (2.10) (a), one sees that it is enough to prove that

$$\big(\prod_{\ell \in S_{mN_p} \setminus \mathscr{Y}(K)} \mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})^{-1} \cdot \nu_{mp^n}^{(\ell),\#}\big) \cdot \mathcal{P}_{F_{mp^n}}(z_{mp^n}^{\mathrm{Kato}}, (1 - e_\tau)\mathfrak{k}_{mp^n}) \in \sum_{\mathscr{L} \subseteq \mathscr{Z}(K)} \mathfrak{a}_{\mathscr{L}} \mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}}.$$

By Theorem (2.10) (e) we can write, for each prime $\ell \mid m$,

$$\mathrm{Eul}_\ell(\widetilde{\sigma}_\ell)^{-1} \nu_{mp^n}^{(\ell)} = \alpha_\ell + \beta_\ell \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell)^{-1} \mathrm{N}_{\mathcal{I}_{mp^n}^{(\ell)}}$$

with suitable $\alpha_\ell, \beta_\ell \in \mathbb{Z}_p[G_{mp^n}]$. For any subset $\mathscr{L}$ of $\mathscr{Z}(K)$, we then define $\mathcal{I}_{\mathscr{L}}$ to be the subgroup of G_{mp^n} generated by $\mathcal{I}_{mp^n}^{(\ell)}$ for $\ell \in \mathscr{L}$ and note that $\mathcal{I}_{\mathscr{L}} = \prod_{\ell \in \mathscr{L}} \mathcal{I}_{mp^n}^{(\ell)}$ because the

$\mathcal{I}^{(\ell)}_{mp^n}$ are disjoint. As a consequence, we also have $\mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}} = \prod_{\ell\in\mathscr{L}} \mathrm{N}_{\mathcal{I}^{(\ell)}_{mp^n}}$.
We can then write

$$\begin{aligned}\big(\prod\nolimits_{\ell\in S_{mN_p}\setminus\mathscr{Y}(K)} \mathrm{Eul}_\ell(\tilde\sigma_\ell^{-1})^{-1}\cdot \nu^{(\ell),\#}_{mp^n}\big) &= \big(\prod\nolimits_{\ell\in\mathscr{Z}(K)} \mathrm{Eul}_\ell(\tilde\sigma_\ell^{-1})^{-1}\cdot \nu^{(\ell),\#}_{mp^n}\big)\cdot\eta_{K,N_p}\\ &= \big(\prod\nolimits_{\ell\in\mathscr{Z}(K)} (\alpha^{\#}_\ell + \beta^{\#}_\ell \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell^{-1})^{-1}\mathrm{N}_{\mathcal{I}^{(\ell)}_{mp^n}})\big)\cdot\eta_{m,N_p}\\ &= \sum_{\mathscr{L}\subseteq\mathscr{Z}(K)} A_{\mathscr{L}}\big(\prod_{\ell\in\mathscr{L}} \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell^{-1})^{-1}\big)\mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}}\cdot\eta_{K,N_p} \quad (36)\end{aligned}$$

with suitable $A_{\mathscr{L}}\in\mathbb{Z}_p[G_{mp^n}]$ and the sum ranging over all subsets of $\mathscr{Z}(K)$ (including the empty set). We then calculate, by Lemma (2.7) (b, c), that for every subset $\mathscr{L}$ of $\mathscr{Z}(K)$

$$\begin{aligned}&\mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}}\cdot\mathcal{P}_{F_{mp^n}}(z^{\mathrm{Kato}}_{mp^n},(1-e_\tau)\mathfrak{k}_{mp^n})\\ &= \mathcal{P}_{F_{mp^n}}(\mathrm{cores}_{F_{mp^n}/F_{\mathscr{L}}}(z^{\mathrm{Kato}}_{mp^n}),(1-e_\tau)\mathfrak{k}_{mp^n})\\ &= \mathcal{P}_{F_{\mathscr{L}}}(\mathrm{cores}_{F_{mp^n}/F_{\mathscr{L}}}(z^{\mathrm{Kato}}_{mp^n}),\mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}((1-e_\tau)\mathfrak{k}_{mp^n}))\cdot\mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}}. \quad (37)\end{aligned}$$

In addition, by Theorem (2.10) (b), one has

$$(1-e_\tau)\mathfrak{k}_{mp^n} = Q + (p\mathrm{Eul}_p(\sigma_p))^{-1}P \quad (38)$$

with suitable $Q\in E_1(F_{mp^n})$ and $P\in E_1(F_m)$. For every subset $\mathscr{L}$ of $\mathscr{Z}(K)$, we then have

$$\begin{aligned}&\mathcal{P}_{F_{\mathscr{L}}}(\,\cdot\,,\mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}((1-e_\tau)\mathfrak{k}_{mp^n}))\\ &= \mathcal{P}_{F_{\mathscr{L}}}(\,\cdot\,,\mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}(Q + (p\mathrm{Eul}_p(\sigma_p))^{-1}P))\\ &= \mathcal{P}_{F_{\mathscr{L}}}(\,\cdot\,,\mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}(Q))\\ &\quad + (p\mathrm{Eul}_p(\sigma_p^{-1}))^{-1}\cdot\mathcal{P}_{F_{\mathscr{L}\cup\{p\}}}(\mathrm{N}_{F_{\mathscr{L}}/F_{\mathscr{L}\cup\{p\}}}\cdot,\mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}(P))\mathrm{N}_{\mathcal{I}^{(p)}_{mp^n}} \quad (39)\end{aligned}$$

because $\mathcal{P}_{F_{mp^n}}(\cdot,\cdot)$ is #-semilinear in the second component by Lemma (2.7) (b). Combining (36), (37) and (39) we have thereby proved that

$$\begin{aligned}&\big(\prod\nolimits_{\ell\in S_{mN_p}\setminus\mathscr{Y}(K)} \mathrm{Eul}_\ell(\tilde\sigma_\ell^{-1})^{-1}\cdot \nu^{(\ell),\#}_{mp^n}\big)\cdot\mathcal{P}_{F_{mp^n}}(z^{\mathrm{Kato}}_{mp^n},(1-e_\tau)\mathfrak{k}_{mp^n})\\ &= \sum_{\mathscr{L}\subseteq\mathscr{Z}(K)} A'_{\mathscr{L}}\big(\prod_{\ell\in\mathscr{L}\setminus\{p\}} \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell^{-1})^{-1}\big)\cdot\eta_{K,N_p}\cdot\mathcal{P}_{F_{\mathscr{L}}}(\mathrm{cores}_{F_{mp^n}/F_{\mathscr{L}}}(z^{\mathrm{Kato}}_{mp^n}),Q_{\mathscr{L}})\mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}}\end{aligned}$$

with

$$A'_{\mathscr{L}} := (p\mathrm{Eul}_p(\sigma_p^{-1}))^{-\mathbf{1}_{\mathscr{L}}(p)}\cdot A_{\mathscr{L}\setminus\{p\}} \quad\text{and}\quad Q_{\mathscr{L}} := \begin{cases} Q & \text{if } \mathscr{L}=\varnothing,\\ \mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}(Q) & \text{if } p\notin\mathscr{L},\\ \mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}(P) & \text{if } p\in\mathscr{L}.\end{cases}$$

In light of the Euler system relation $\mathrm{cores}_{F_{mp^n}/F_{\mathscr{L}}}(z^{\mathrm{Kato}}_{mp^n}) = \big(\prod_{\ell\in\mathscr{L}\setminus\{p\}}\mathrm{Eul}_\ell(\sigma_\ell^{-1})\big)\cdot z^{\mathrm{Kato}}_{\mathscr{L}}$ we have therefore proved that

$$(1-e_\tau)\theta^{\mathrm{MT}}_{mp^n} = \sum\nolimits_{\mathscr{L}\subseteq\mathscr{Z}(K)} A'_{\mathscr{L}}\cdot\eta_{K,N_p}\cdot\mathcal{P}_{F_{\mathscr{L}}}(z^{\mathrm{Kato}}_{\mathscr{L}},Q_{\mathscr{L}})\mathrm{N}_{F_{mp^n}/F_{\mathscr{L}}}, \quad (40)$$

and this combines with the assumption (34) to imply the claimed inclusion (35).
If $a_p\not\equiv 1 \mod p$, then $\mathfrak{k}_{mp^n}$ belongs to $E_1(F_{mp^n})$ by Theorem (2.10) (b) so that (38) holds without the factor $(1-e_\tau)$ and with $P=0$. With this changed definition of P, (40) then holds without the factor $(1-e_\tau)$. Again considering the assumption (34) one sees that the second claim of the theorem holds as well. □

(4.10) Remark. The proof of Lemma (4.9) shows that if p is a prime number with the property that $p\mathrm{Eul}_p(\sigma_p)$ belongs to $\mathbb{Z}_p[G_{mp^n}]^\times$, then (34) can be replaced by the simpler condition

$$\eta_{m,N_p}\cdot\mathcal{P}_{F_{\mathscr{L}}}(z^{\mathrm{Kato}}_{\mathscr{L}},(1-e_\tau)\cdot\mathrm{Tr}_{F_{mp^n}/F_{\mathscr{L}}}(\mathfrak{k}_{mp^n}))\in\mathfrak{a}_{\mathscr{L}}$$

in order for (35) to hold.

We now give the proof of Theorem (1.4) (b).

Proof of Theorem (1.4) (b): Write the conductor of K as mp^n with $p \nmid m$ and $n \in \mathbb{Z}_{\geq 0}$. By Theorem (2.10) (d) we can write, for each $\ell \mid m$,

$$\mathrm{Eul}_\ell(\widetilde{\sigma}_\ell)^{-1}\nu^{(\ell)}_{mp^n} = \alpha_\ell + \beta_\ell \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell)^{-1}\mathrm{N}_{\mathcal{I}^{(\ell)}_{mp^n}}$$

with suitable $\alpha_\ell, \beta_\ell \in \mathbb{Z}_p[G_{mp^n}]$. Let $\mathscr{L}$ be a subset of $\mathscr{Z}(K)$. Using the element η_{K,N_p} defined before Lemma (4.9), we now set

$$\eta'_{\mathscr{L}} := (p\mathrm{Eul}_p(\sigma_p^{-1}))^{-\mathbf{1}_{\mathscr{L}}(p)}\eta_{K,N_p} \quad \text{and} \quad \Pi_{\mathscr{L}} := \begin{cases} \{p\} \cup (S_N \setminus \mathscr{Y}(K)) & \text{if } p \in \mathscr{L}, \\ S_N \setminus \mathscr{Y}(K) & \text{if } p \notin \mathscr{L}. \end{cases}$$

By construction, we then have

$$\eta'_{\mathscr{L}} \in \prod\nolimits_{\ell \in \Pi_{\mathscr{L}}} \big(\ell^{-1}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell^{-1})^{-1}\mathrm{N}_{\mathcal{I}^{(\ell)}_{mp^n}}\mathbb{Z}_p[G] + \mathbb{Z}_p[G_{mp^n}]\big).$$

Now, assuming condition (ii) of Theorem (1.4), it follows from Theorem (3.6) that there is $a_{\mathscr{L}} \in \mathrm{Det}_{\mathbb{Z}_p[G_{\mathscr{L}}]}(C^\bullet_{F_{\mathscr{L}},S(F_{\mathscr{L}})})^{-1}$ with $\Theta_{F_{\mathscr{L}},S(F_{\mathscr{L}})}(a_{\mathscr{L}}) = z^{\mathrm{Kato}}_{\mathscr{L}}$. From the first inclusion in Proposition (4.6) we therefore deduce that

$$\eta'_{\mathscr{L}} \cdot \mathscr{P}_{F_{\mathscr{L}}}(z^{\mathrm{Kato}}_{\mathscr{L}}, Q_{\mathscr{L}}) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G_{F_{\mathscr{L}}}]}(H^2(\widetilde{D}^\bullet_{F_{\mathscr{L}},S(F_{\mathscr{L}}),\Pi_{\mathscr{L}},Q_{\mathscr{L}}}))^\#$$

for every $Q_{\mathscr{L}} := \mathrm{Tr}_{F_m/F_{\mathscr{L}}}(Q)$ with $Q \in E_1(F_{m,p})$. Setting $\Pi'_{\mathscr{L}} := \Pi_{\mathscr{L}} \cup (S(F_{mp^n}) \setminus S(F_{\mathscr{L}}))$, Lemma (4.4) (d) moreover gives

$$H^2(\widetilde{D}^\bullet_{F_{\mathscr{L}},S(F_{\mathscr{L}}),\Pi_{\mathscr{L}},Q_{\mathscr{L}}})) = H^2(\widetilde{D}^\bullet_{F_{\mathscr{L}},S(F_{mp^n}),\Pi'_{\mathscr{L}},Q_{\mathscr{L}}}).$$

This combines with Lemma (4.9) to imply that

$$\begin{aligned}(1-e_\tau)\theta_K^{\mathrm{MT}} &\in \pi_{F_{mp^n}/K}\big(\textstyle\sum_{\mathscr{L}\subseteq\mathscr{Z}(K)} \mathrm{Fitt}^0_{\mathbb{Z}_p[G_{F_{\mathscr{L}}}]}(H^2(\widetilde{D}^\bullet_{F_{\mathscr{L}},S(F_{mp^n}),\Pi'_{\mathscr{L}},Q_{\mathscr{L}}}))^\#\mathrm{N}_{\mathcal{I}_{\mathscr{L}}}\big) \\ &\subseteq \pi_{F_{mp^n}/K}\big(\textstyle\sum_{\mathscr{L}\subseteq\mathscr{Z}(K)} \mathrm{Fitt}^0_{\mathbb{Z}_p[G_{mp^n}]}(H^2(\widetilde{D}^\bullet_{F_{mp^n},S(F_{mp^n}),\Pi'_{\mathscr{L}},Q}))^\#\big) \\ &\subseteq \pi_{F_{mp^n}/K}\big(\mathrm{Fitt}^0_{\mathbb{Z}_p[G_{mp^n}]}(\mathrm{Sel}^\vee_{p,E/F_{mp^n}})^\#\big). \end{aligned} \tag{41}$$

Here the first inclusion follows from Lemma (4.4) (b), in particular from the fact that

$$H^2(\widetilde{D}^\bullet_{F_{mp^n},S(F_{mp^n}),\Pi_{\mathscr{L}},Q}) \otimes_{\mathbb{Z}_p[G_{mp^n}]} \mathbb{Z}_p[G_{\mathscr{L}}] \cong H^2(\widetilde{D}^\bullet_{F_{\mathscr{L}},S(F_{mp^n}),\Pi_{\mathscr{L}},Q_{\mathscr{L}}}),$$

by Lemma (B.13) (a), and the properties of Fitting ideals. The second inclusion follows from Lemma (4.4) (a) and Lemma (3.8).

We next note that, since $E(F_{mp^n})$ has trivial p-torsion, the natural map $H^1(\mathcal{O}_{K,S(K)}, E[p^\infty]) \to H^1(\mathcal{O}_{F_{mp^n},S(K)}, E[p^\infty])$ is injective and so restricts to an injection $\mathrm{Sel}_{p,E/K} \hookrightarrow \mathrm{Sel}_{p,E/F_{mp^n}}$. Upon taking Pontryagin duals, we therefore deduce a surjection $\mathrm{Sel}^\vee_{p,E/F_{mp^n}} \twoheadrightarrow \mathrm{Sel}^\vee_{p,E/K}$. By a standard property of Fitting ideals, the existence of this surjection implies an inclusion

$$\begin{aligned}\pi_{F_{mp^n}/K}(\mathrm{Fitt}^0_{\mathbb{Z}_p[G_{mp^n}]}(\mathrm{Sel}^\vee_{p,E/F_{mp^n}})) &= \mathrm{Fitt}^0_{\mathbb{Z}_p[G_K]}(\mathrm{Sel}^\vee_{p,E/F_{mp^n}} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[G_K]) \\ &\subseteq \mathrm{Fitt}^0_{\mathbb{Z}_p[G_K]}(\mathrm{Sel}^\vee_{p,E/K}),\end{aligned}$$

which combines with (41) to prove that $\theta_K^{\mathrm{MT},\#}$ is contained in $\mathrm{Fitt}^0_{\mathbb{Z}_p[G_K]}(\mathrm{Sel}^\vee_{p,E/K})$ if K contains no primitive p-th root of unity.

If $a_p \not\equiv 1 \mod p$ and E has potentially good reduction at p, then one can again use Theorem (3.6) and Lemma (4.9) to deduce (41), (without the factor of $(1-e_\tau)$), and so we conclude that $\theta_K^{\mathrm{MT},\#}$ is contained in $\mathrm{Fitt}^0_{\mathbb{Z}_p[G_K]}(\mathrm{Sel}^\vee_{p,E/K})$.

This concludes the proof of Theorem (1.4) (b). □

5. The multiplicative group

In this section we prove a number of auxiliary results that are concerned with the multiplicative group $\mathbb{G}_m$ and that will be key in the proofs of Theorem (1.4) (a) and Theorem (1.7).

5.1. A cohomological interpretation of Otsuki's points

Fix a finite abelian extension K of $\mathbb{Q}$ with Galois group $G \coloneqq \mathrm{Gal}(K/\mathbb{Q})$ and consider the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $\mathbb{Z}_p(1)_{K/\mathbb{Q}} \coloneqq \mathrm{Ind}_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}^{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}(\mathbb{Z}_p(1))$. Upon fixing a prime number ℓ and an embedding $\iota_\ell\colon \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_\ell}$, we may regard $\mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$ as a subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and hence $\mathbb{Z}_p(1)_{K/\mathbb{Q}}$ as a $\mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$-module. Consequently, we have the complex

$$A_{K,\ell}^\bullet \coloneqq \mathrm{R}\Gamma(\mathbb{Q}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}),$$

which is perfect as an object of $D(\mathbb{Z}_p[G])$ and acyclic outside degrees 1 and 2. Moreover, one has canonical isomorphisms

$$H^1(A_{K,\ell}^\bullet) \cong \widehat{K_\ell^\times} \coloneqq \bigotimes\nolimits_{v|\ell} \widehat{K_v^\times} \quad \text{and} \quad H^2(A_{K,\ell}^\bullet) \cong \bigotimes\nolimits_{v|\ell} \mathbb{Z}_p v$$

induced by the Kummer map and the invariant map of local class field theory, respectively. The Euler characteristic of $A_{K,\ell}^\bullet$ in $K_0(\mathbb{Z}_p[G])$ is equal to $-[\mathbb{Z}_p[G]^{\oplus(1-\mathbf{1}_p(\ell))}]$ (cf. [Fla00, § 5]), and so Definition (B.2) provides us with a map

$$\vartheta_{K,\ell}^0 \coloneqq \vartheta_{A_{K,\ell}^\bullet,\varnothing}\colon \mathrm{Det}_{\mathbb{Z}_p[G]}(A_{K,\ell}^\bullet)^{-1} \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigwedge\nolimits_{\mathbb{Z}_p[G]}^{1-\mathbf{1}_p(\ell)} \widehat{K_\ell^\times}.$$

Write v_0 for the place of K that corresponds to the restriction of ι_ℓ to K. If ℓ splits completely in K, then v_0 defines a $\mathbb{Z}_p[G]$-basis of $\bigoplus_{v|\ell} \mathbb{Z}_p v$ and hence Definition (B.2) also gives a map

$$\vartheta_{K,\ell,v_0} \coloneqq \vartheta_{A_{K,\ell}^\bullet,\{v_0\}}\colon \mathrm{Det}_{\mathbb{Z}_p[G]}(A_{K,\ell}^\bullet)^{-1} \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \bigwedge\nolimits_{\mathbb{Z}_p[G]}^{2-\mathbf{1}_p(\ell)} \widehat{K_\ell^\times}.$$

We moreover recall that, after letting $L/\mathbb{Q}$ denote another finite abelian extension that contains K and setting $\mathcal{G} \coloneqq \mathrm{Gal}(L/\mathbb{Q})$, by [FK06, Prop. 1.6.5] one has an isomorphism

$$A_{L,\ell}^\bullet \otimes_{\mathbb{Z}_p[\mathcal{G}]}^{\mathbb{L}} \mathbb{Z}_p[G] \cong A_{K,\ell}^\bullet \tag{42}$$

in $D(\mathbb{Z}_p[G])$ that induces a map

$$\mathrm{pr}_{L/K}\colon \mathrm{Det}_{\mathbb{Z}_p[\mathcal{G}]}(A_{L,\ell}^\bullet)^{-1} \to \mathrm{Det}_{\mathbb{Z}_p[\mathcal{G}]}(A_{L,\ell}^\bullet)^{-1} \otimes_{\mathbb{Z}_p[\mathcal{G}]} \mathbb{Z}_p[G] \cong \mathrm{Det}_{\mathbb{Z}_p[G]}(A_{K,\ell}^\bullet)^{-1}.$$

If E has split-multiplicative reduction at p, Tate uniformisation induces an isomorphism $F\colon \widehat{E} \xrightarrow{\simeq} \mathbb{G}_m$ given by $\exp_{\mathbb{G}_m} \circ \log_{\widehat{E}}(1+X) - 1 \in \mathbb{Z}_p[\![X]\!]$ (for details see, for example, [Kob06, § 3]).

(5.1) Definition. *Suppose that E has split-multiplicative reduction at p. For every natural number m coprime with p and integer $n \geq 0$, we define*

$$\mathfrak{l}_{mp^n} \coloneqq F(\widetilde{x}_{mp^n}) \in \widehat{F_{mp^n,v_0}^\times} \subseteq H^1(A_{F_{mp^n},p}^\bullet)$$

with the element $\widetilde{x}_{mp^n}$ from Definition (2.25). (Here we have used that $p\mathrm{Eul}_p(\tilde{\sigma}_p) = p - \tilde{\sigma}_p$ is invertible in $\mathbb{Z}_p[G]$ and hence that $\widetilde{x}_{mp^n}$ belongs to $E_1(F_{mp^n,v_0})$.)

The following is the main result of this section.

(5.2) Theorem. *Fix a natural number m coprime with p and an integer $n \geq 0$. For every prime divisor ℓ of mp^n at which E has split-multiplicative reduction the following claims are valid.*

(a) If $\ell \neq p$, then there exists a unique family $(t_{mp^n}^{(\ell)})_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathrm{Det}_{\mathbb{Z}_p[G_{mp^n}]}(A_{F_{mp^n},\ell}^\bullet)^{-1}$, where the limit is taken with respect to the the maps $\mathrm{pr}_{F_{mp^{n+1}}/F_{mp^n}}$, such that

$$\vartheta_{F_{mp^n},\ell}^0(t_{mp^n}^{(\ell)}) = \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell)^{-1} \cdot \nu_{mp^n}^{(\ell)}$$

for all $n \in \mathbb{N}$. If K is a subfield of F_{mp^n} in which ℓ splits completely, then moreover

$$(\vartheta_{K,\ell,v_0} \circ \mathrm{pr}_{F_{mp^n}/K})(t_{mp^n}^{(\ell)}) = -\ell^{-(\mathrm{ord}_\ell(m)-1)}\mathrm{Eul}_\ell(1)^{-1} \otimes \ell$$

as an equality in $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} \widehat{K_{v_0}^\times} = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \widehat{\mathbb{Q}_\ell^\times} \subseteq \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \widehat{K_\ell^\times}$.

(b) If $\ell = p$, then there exists a unique family $(t^{(p)}_{mp^n})_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}} \mathrm{Det}_{\mathbb{Z}_p[G_{mp^n}]}(A_{F_{mp^n},p})^{-1}$ such that

$$\vartheta^0_{F_{mp^n},p}(t^{(p)}_{mp^n}) = \mathfrak{l}_{mp^n}$$

for all $n \in \mathbb{N}$. If K is a subfield of F_{mp^n} in which p splits completely, then moreover

$$(\vartheta_{K,p,v_0} \circ \mathrm{pr}_{F_{mp^n}/K})(t^{(p)}_{mp^n}) = \mathrm{N}_{F_m/K}(\mathfrak{l}_m) \wedge p \quad \in \bigwedge^2_{\mathbb{Z}_p} \widehat{K^\times_{v_0}}.$$

(Here the right hand side is viewed as an element of $\bigwedge^2_{\mathbb{Z}_p[G]} \widehat{K^\times_\ell}$ via the isomorphism $\bigwedge^2_{\mathbb{Z}_p[G]} \widehat{K^\times_\ell} \cong \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} \bigwedge^2_{\mathbb{Z}_p} \widehat{K^\times_{v_0}}$.)

The proof of this result will occupy the remainder of this section.

(5.3) Remark. The element $\mathfrak{l}_1 \wedge p = (p\mathrm{Eul}_p(1))^{-1} \exp_{\mathbb{G}}(p) \wedge p$ is a $\mathbb{Z}_p$-basis of $\bigwedge^2_{\mathbb{Z}_p} \widehat{\mathbb{Q}^\times_p}$ and so Theorem (5.2) (b) combines with Nakayama's lemma to imply that $t^{(p)}_{p^n}$ is a $\mathbb{Z}_p[G_{p^n}]$-basis of $\mathrm{Det}_{\mathbb{Z}_p[G_{p^n}]}(A^\bullet_{F_{p^n},p})^{-1}$ for all $n \geq 0$. This is perhaps reason to more generally expect a direct relation between $t^{(p)}_{mp^n}$ and the canonical basis of $\mathrm{Det}_{\mathbb{Z}_p[G_{p^n}]}(A^\bullet_{F_{p^n},p})^{-1}$ given by Kato's local ϵ-constant [Kat].

5.2. Iwasawa theory

Fix a natural number m coprime with p and define the complex

$$A^\bullet_{F_{mp^\infty},\ell} := \varprojlim_{n\in\mathbb{N}} A^\bullet_{F_{mp^n},\ell},$$

where the limit is taken with respect to the maps induced by the relevant instances of the isomorphisms (42). Setting $\Lambda_m := \varprojlim_{n\in\mathbb{N}} \mathbb{Z}_p[G_{mp^n}]$, the complex $A_{F_{mp^\infty}}$ is then perfect as a complex of Λ_m-modules that is acyclic outside degrees 1 and 2, and one has canonical isomorphisms

$$H^1(A^\bullet_{mp^\infty,\ell}) \cong \varprojlim_{n\in\mathbb{N}} \widehat{F^\times_{mp^n,\ell}} \quad \text{and} \quad H^2(A^\bullet_{mp^\infty,\ell}) \cong \bigoplus_{v|\ell} \mathbb{Z}_p.$$

In particular, since no finite prime splits completely in F_{mp^∞}, it follows that $H^2(A^\bullet_{mp^\infty,\ell})$ is a Λ_m-torsion module and Definition (B.2) provides us with an injective map

$$\vartheta_{mp^\infty,\ell} := \vartheta_{A^\bullet_{mp^\infty,\ell},\varnothing} \colon \mathrm{Det}_{\Lambda_m}(A^\bullet_{mp^\infty,\ell})^{-1} \hookrightarrow Q(\Lambda_m) \otimes_{\Lambda_m} \bigwedge^{1-\mathbf{1}_p(\ell)}_{\Lambda_m} H^1(A^\bullet_{mp^\infty,\ell})$$

where $Q(\Lambda_m)$ is the total ring of fractions of Λ_m.
In the following result we write $I(U) := \ker\{\mathbb{Z}_p[\![U]\!] \to \mathbb{Z}_p\}$ for the (p-adic) augmentation ideal of an abelian group U, and we use the notation $\bigcap^r_R M$ for the r-th 'exterior bidual' of an R-module M (see § B.2 for details). In addition, we recall that for any ideal $\mathfrak{a} \subseteq \Lambda_m$ we can naturally regard $\mathfrak{a}^{**}$ as an ideal of Λ_m via the injective map $\mathfrak{a}^{**} \to (\Lambda_m)^{**} \cong \Lambda_m$.

(5.4) Lemma. *Fix a natural number m coprime with p and write $\mathcal{D}^{(\ell)}_{mp^\infty} \subseteq G_{mp^\infty}$ for the decomposition group at ℓ. Then one has*

$$\mathrm{im}(\vartheta_{mp^\infty,\ell}) = \big(\mathrm{Ann}_{\Lambda_m}(\textstyle\bigoplus_{v|\ell} \mathbb{Z}_p(1))^{-1} \cdot I(\mathcal{D}^{(\ell)}_{mp^\infty})\big)^{**} \cdot \bigcap^{1-\mathbf{1}_p(\ell)}_{\Lambda_m} H^1(A^\bullet_{mp^\infty,\ell}).$$

Proof. Since $\mathrm{Det}_{\Lambda_m}(A^\bullet_{mp^\infty,\ell})^{-1}$ is a free rank-one module and $\vartheta_{mp^\infty,\ell}$ is injective, the image of $\vartheta_{mp^\infty,\ell}$ is reflexive and so, by the argument of [Sak23, Lem. C.11], it suffices to verify the claimed equality after localising at an arbitrary prime ideal $\mathfrak{p} \subseteq \Lambda_m$ of height at most one.
To do this, we first note that $A^\bullet_{mp^\infty,\ell}$ is acyclic outside degrees 1 and 2 so that the argument of [BS21, Prop. A.11 (i)] shows that $A^\bullet_{mp^\infty,\ell}$ admits a representative of the form $Q \to P$, where P is a finitely generated free Λ_m-module and Q is a finitely generated Λ_m-module of finite projective dimension (that is placed in degree 1). The Auslander–Buchsbaum formula implies

that the localisation $Q_{\mathfrak{p}}$ of Q at $\mathfrak{p}$ is of projective dimension at most one, and so there is an exact sequence $0 \to F_1 \to F_0 \to Q \to 0$ with finitely generated free $\Lambda_{m,\mathfrak{p}}$-modules F_1 and F_0. It follows that $F_1 \to F_0 \to P_{\mathfrak{p}}$ is a standard representative in the sense of Definition (B.3) (with respect to $(0, \varnothing)$) for the complex $A^{\bullet}_{mp^\infty,\ell} \otimes^{\mathbb{L}}_{\Lambda_m} \Lambda_{m,\mathfrak{p}}$.

To proceed, we first verify that the Matlis dual of the $\Lambda_{m,\mathfrak{p}}$-torsion submodule of $H^1(A^{\bullet}_{mp^\infty,\ell})_{\mathfrak{p}}$ coincides with $(\bigoplus_{v|\ell} \mathbb{Z}_p(1))_{\mathfrak{p}}$. By Lemma (B.12) it suffices to compute $\mathrm{Ext}^1_{\Lambda_m}(H^1(A^{\bullet}_{mp^\infty,\ell}), \Lambda_m)_{\mathfrak{p}}$ for this. To do this, we will use the convergent spectral sequence

$$E_2^{i,j} = \mathrm{Ext}^i_{\Lambda_m}(H^{-j}(A^{\bullet}_{mp^\infty,\ell}), \Lambda_m) \Rightarrow E^{i+j} = H^{i+j}(\mathrm{RHom}_{\Lambda_m}(A^{\bullet}_{F_{mp^\infty},\ell}, \Lambda_m)).$$

Since $\Lambda_{m,\mathfrak{p}}$ is a Gorenstein ring of dimension one, one has that $\mathrm{Ext}^i_{\Lambda_m}(-, \Lambda_m)_{\mathfrak{p}} = 0$ if $i > 1$, and so this spectral sequence gives an isomorphism

$$\begin{aligned}
\mathrm{Ext}^1_{\Lambda_m}(H^1(A^{\bullet}_{mp^\infty,\ell}), \Lambda_m)_{\mathfrak{p}} &\cong H^0(\mathrm{RHom}_{\Lambda_m}(A^{\bullet}_{F_{mp^\infty},\ell}, \Lambda_m))_{\mathfrak{p}} \\
&\cong \big(\varprojlim_{n\in\mathbb{N}} H^2(\mathbb{Q}_\ell, (\mathbb{Z}_p)_{F_{mp^n}/\mathbb{Q}})\big)_{\mathfrak{p}} \\
&\cong \big(\bigoplus\nolimits_{v|\ell} \mathbb{Z}_p(1)\big)_{\mathfrak{p}}.
\end{aligned}$$

Here the second isomorphism is by (derived) local Tate duality [Nek06, Thm. 5.2.6] and the final isomorphism follows easily from (classical) local Tate duality.

If $\mathfrak{p}$ does not contain p, then the localisation of Λ_m at $\mathfrak{p}$ is a regular local ring (see, for example, the discussion in [BKS17, § 3C1]) and hence, in this case, the claim follows from Proposition (B.10) (c) applied to the complex $A^{\bullet}_{mp^\infty,\ell} \otimes^{\mathbb{L}}_{\Lambda_m} \Lambda_{m,\mathfrak{p}}$ and the computation of $H^1(A^{\bullet}_{mp^\infty,\ell})^\vee_{\mathrm{tor},\mathfrak{p}}$ above.

Furthermore, if $\mathfrak{p}$ contains p, then the localisation of $H^2(A^{\bullet}_{mp^\infty,\ell})$ at $\mathfrak{p}$ vanishes by the general result of [Fla04, Lem. 5.6] because $H^2(A^{\bullet}_{mp^\infty,\ell})$ is a finitely generated $\mathbb{Z}_p$-module. Similarly, $\mathrm{Ext}^1_{\Lambda_m}(H^1(A^{\bullet}_{mp^\infty,\ell}), \Lambda_m) = \mathbb{Z}_p(1)$ is a finitely generated $\mathbb{Z}_p$-module and so also vanishes when localised at $\mathfrak{p}$. It follows from Lemma (B.12) that

$$\mathrm{Ext}^1_{\Lambda_m}(H^1(A^{\bullet}_{mp^\infty,\ell}), \Lambda_m)_{\mathfrak{p}} = \mathrm{Hom}_{\Lambda_m}(H^1(A^{\bullet}_{mp^\infty,\ell})_{\mathrm{tor}}, Q(\Lambda_m)/\Lambda_m)_{\mathfrak{p}} = 0$$

so that $H^1(A^{\bullet}_{mp^\infty,\ell})_{\mathfrak{p}}$ has depth 1 as a $\Lambda_{m,\mathfrak{p}}$-module. By the Auslander–Buchsbaum formula, this implies that it is in fact a free, possibly zero, $\Lambda_{m,\mathfrak{p}}$-module. Given this, the same proof as Proposition (B.10) (c) works and shows the claim. □

Suppose that $\ell \neq p$. In this case, Lemma (2.18) shows that the family $\nu^{(\ell)}_{mp^\infty} := (\nu^{(\ell)}_{mp^n})_{n\in\mathbb{N}}$ defines an element of Λ_m. If we can prove that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \nu^{(\ell)}_{mp^\infty}$ belongs to the image of $\vartheta_{mp^\infty,\ell}$, then it follows from the diagram

$$\begin{array}{ccc}
\mathrm{Det}_{\Lambda_m}(A^{\bullet}_{mp^\infty,\ell})^{-1} & \xrightarrow{\vartheta_{mp^\infty,\ell}} & \big(\mathrm{Ann}_{\Lambda_m}(\bigoplus_{v|\ell}\mathbb{Z}_p(1))^{-1} \cdot I(\mathcal{D}^{(\ell)}_{mp^\infty})\big)^{**} \\
{\scriptstyle \mathrm{pr}_{F_{mp^\infty}/F_{mp^n}}}\downarrow & & \downarrow{\scriptstyle \pi_{F_{mp^\infty}/F_{mp^n}}} \\
\mathrm{Det}_{\mathbb{Z}_p[G_{mp^n}]}(A_{F_{mp^n},\ell}) & \xrightarrow{\vartheta^0_{F_{mp^n},\ell}} & \mathbb{Q}_p[G_{mp^n}],
\end{array} \tag{43}$$

which commutes for every $n \in \mathbb{N}$ as can be checked using the explicit description of the maps $\vartheta_{mp^\infty,\ell}$ and $\vartheta^0_{F_{mp^n},\ell}$ given in Lemma (B.5), that the first claim in Theorem (5.2) (a) is valid.

To prove that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \nu^{(\ell)}_{mp^\infty}$ is indeed in the image of $\vartheta_{mp^\infty,\ell}$, [Sak23, Lem. C.11] allows us to check the claimed containment locally at a height-one prime $\mathfrak{p}$ of Λ_m. To do this, let us first assume that $\mathfrak{p}$ contains p. In this case, then, Lemma (5.4) combines with [Fla04, Lem. 5.6] to imply that $(\mathrm{im}\,\vartheta_{mp^\infty,\ell})_{\mathfrak{p}} = \Lambda_{m,\mathfrak{p}}$. It therefore suffices to prove that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1} \cdot \nu^{(\ell)}_{mp^\infty}$ belongs to $\Lambda_{m,\mathfrak{p}}$ and this will follow if we can show that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell) = \ell^{-1}(\ell - \tilde{\sigma}_\ell)$ is a unit in $\Lambda_{m,\mathfrak{p}}$. Fix a decomposition $G_{mp^\infty} \cong \Delta \times \Gamma$ with a finite group Δ and $\Gamma := \mathrm{Gal}(\mathbb{Q}(\zeta_{mp^\infty})/\mathbb{Q}(\zeta_{mp}))$, and write $\Delta^{(p)}$ for the p-Sylow subgroup of Δ. The discussion in [BKS17, § 3C1] then implies that there exists a prime-to-p-order character $\chi_{\mathfrak{p}} \colon \Delta \to \overline{\mathbb{Q}_p}^\times$ such that $\Lambda_{m,\mathfrak{p}}$ naturally identifies with the localisation of $\mathbb{Z}_p[\mathrm{im}\,\chi_{\mathfrak{p}}][\Delta^{(p)}][\![\Gamma]\!]$ at the prime ideal $(p, I_{\mathbb{Z}_p[\mathrm{im}\,\chi_{\mathfrak{p}}],\Delta^{(p)}})$. Since $\ell - \chi_{\mathfrak{p}}(\tilde{\sigma}_\ell)\sigma_\ell$ is

not divisible by p in $\Lambda[\operatorname{im}\chi_{\mathfrak{p}}][\![\Gamma]\!]$, we conclude that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)$ is a unit in $\Lambda_{m,\mathfrak{p}}$, as claimed.
We next assume $\mathfrak{p} \subseteq \Lambda_m$ is a height-one prime that does not contain p. By [BKS17, § 3C1] one then has that there exists a character $\chi_{\mathfrak{p}}\colon \Delta \to \overline{\mathbb{Q}_p}^\times$ such that $\Lambda_{m,\mathfrak{p}}$ identifies with the localisation of $\mathbb{Z}_p[\operatorname{im}\chi_{\mathfrak{p}}]$ at one of its height-one primes, and [BB25, Lem. 8.23 (i)] moreover shows that

$$\mathrm{Ann}_{\Lambda_m}\big(\bigoplus\nolimits_{v|\ell}\mathbb{Z}_p(1)\big)_{\mathfrak{p}} = \begin{cases}\mathrm{Eul}_\ell(\sigma_\ell)\Lambda_{m,\mathfrak{p}} & \text{if } \chi_{\mathfrak{p}}(\mathcal{I}^{(\ell)}_{mp^\infty}) = 1,\\ \Lambda_{m,\mathfrak{p}} & \text{if } \chi_{\mathfrak{p}}(\mathcal{I}^{(\ell)}_{mp^\infty}) \neq 1.\end{cases}$$

Recall from Theorem (2.10) (e) that the element $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\nu^{(\ell)}_{mp^\infty}$ belongs to the submodule $\Lambda_m + \mathrm{Eul}_\ell(\sigma_\ell)^{-1}\mathrm{N}_{\mathcal{I}^{(\ell)}_{mp^\infty}}\Lambda_m$ of $Q(\Lambda_m)$, and hence also to $\mathrm{Ann}_{\Lambda_m}(\mathbb{Z}_p(1))_{\mathfrak{p}}^{-1}$. In addition, we know from Theorem (2.10) (d) that $\nu^{(\ell)}_{mp^\infty}$ is contained in $I_{\mathcal{D}^{(\ell)}_{mp^\infty}} = \Lambda_m \cdot I(\mathcal{D}^{(\ell)}_{mp^\infty})$. However, one can explicitly check that the supports of $\Lambda_m/I_{\mathcal{D}^{(\ell)}_{mp^\infty}}$ and $\Lambda_m/\mathrm{Ann}_{\Lambda_m}(\bigoplus_{v|\ell}\mathbb{Z}_p(1))$ are disjoint. Indeed, if $\mathfrak{p}$ is in the support of $\Lambda_m/I_{\mathcal{D}^{(\ell)}_{mp^\infty}}$, then $\mathfrak{p} = \ker\{\Lambda_m \to \mathbb{Z}_p[G_{mp^\infty}/\mathcal{D}^{(\ell)}_{mp^\infty}] \xrightarrow{\chi} \mathbb{Q}_p(\chi)\}$ for some character χ. Since $\chi(\sigma_\ell) - \ell \neq 1$, we see that $\mathrm{Ann}_{\Lambda_m}(\bigoplus_{v|\ell}\mathbb{Z}_p(1))$ contains an element that is a unit in $\Lambda_{m,\mathfrak{p}}$, as required to prove the claim. We have thereby proved that

$$\begin{aligned}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\nu^{(\ell)}_{mp^\infty} &\in \big(\mathrm{Ann}_{\Lambda_m}(\bigoplus\nolimits_{v|\ell}\mathbb{Z}_p(1))^{-1} \cap I_{\mathcal{D}^{(\ell)}_{mp^\infty}}\big)_{\mathfrak{p}}\\ &= \big(\mathrm{Ann}_{\Lambda_m}(\bigoplus\nolimits_{v|\ell}\mathbb{Z}_p(1))^{-1} \cdot I_{\mathcal{D}^{(\ell)}_{mp^\infty}}\big)_{\mathfrak{p}}\end{aligned}$$

for every height-one prime ideal $\mathfrak{p}$ of Λ_m that does not contain p. Together with the earlier argument for primes $\mathfrak{p}$ that contain p, this shows that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\nu^{(\ell)}_{mp^\infty}$ is in $(\mathrm{Ann}_{\Lambda_m}(\bigoplus_{v|\ell}\mathbb{Z}_p(1))^{-1} \cdot I(\mathcal{D}^{(\ell)}_{mp^\infty}))^{**}$, and hence in $\mathrm{im}(\vartheta_{mp^\infty,\ell})$ by Lemma (5.4). This proves the first claim in Theorem (5.2) (a).
Let us now turn to the the case $\ell = p$ and the proof of the first claim in Theorem (5.2) (b). By construction, the elements $\mathfrak{l}_{mp^n}$ belong to the $(1-e_\tau)$-isotypic component of $H^1(A^\bullet_{F_{mp^n},p})$ which, in particular, is torsion free. Since p is assumed to be a split-multiplicative prime, Theorem (2.10) (c) (i) moreover shows that $\mathfrak{l}_{mp^\infty} := (\mathfrak{l}_{mp^n})_{n\in\mathbb{N}}$ is a norm-coherent family with trivial bottom value. By the argument of [BD21, Thm. 3.8 (b)], applied to the complex $C^\bullet_{F_{mp^\infty},p} \otimes^{\mathbb{L}}_{\Lambda_m} (1-e_\tau)\Lambda_m$, this implies that $\mathfrak{l}_{mp^\infty}$ is in $I^{**}_{\mathcal{D}^{(\ell)}_{mp^\infty}} \cdot (1-e_\tau)H^1(A^\bullet_{mp^\infty,p})$. We therefore deduce from Lemma (5.4) that $\mathfrak{l}_{mp^\infty}$ belongs to $(1-e_\tau)\,\mathrm{im}(\vartheta_{mp^\infty,p})$. Now, one has a commutative diagram comparing $\vartheta_{mp^\infty,p}$ and $\vartheta_{mp^n,p}$ as in (43), and so it follows that $\mathfrak{l}_{mp^n}$ is in the image of $\vartheta_{mp^n,p}$ for all $n \in \mathbb{N}$, as claimed in Theorem (5.2) (b).
This proves the first two claims in parts (a) and (b) of Theorem (5.2).

5.3. Descent calculations

To prove the remaining claims of Theorem (5.2), we will perform descent calculations similar to those in [BKS17, § 5]. In doing so we will, in particular, prove local analogues of the 'Mazur–Rubin–Sano' conjecture from [BKS17]. We remark that, as our setting is entirely local, we do not need to assume the validity of 'global-to-local' hypotheses used in [BKS17] such as the conjectures of Leopoldt or Gross–Kuz'min.
Let L be a finite abelian extension of $\mathbb{Q}$ and K a subfield of L in which a prime ℓ splits completely. We also fix a place w_0 of L above v_0. Setting $\mathcal{G} := \mathrm{Gal}(L/\mathbb{Q})$, $H := \mathrm{Gal}(L/K)$, and $I_H := I(H)\cdot\mathbb{Z}_p[\mathcal{G}]$, we then write

$$\beta^{(\ell)}_{L/K}\colon H^1(A^\bullet_{K,\ell}) \cong H^1(A^\bullet_{L,\ell} \otimes^{\mathbb{L}}_{\mathbb{Z}_p[\mathcal{G}]} \mathbb{Z}_p[G]) \xrightarrow{\beta_{A^\bullet_{K,\ell},I_H}} H^2(A^\bullet_{L,\ell}) \otimes_{\mathbb{Z}_p[\mathcal{G}]} I_H \xrightarrow{w_0^*} I_H/I(D^{(\ell)}_L)I_H$$

for the relevant instance of the Bockstein map from Definition (B.16). This map has the following explicit description.

(5.5) Lemma. *Suppose ℓ splits completely in K. For every $a = (a_v)_{v|\ell} \in \bigoplus_{v|\ell} \widehat{K_v^\times} = H^1(A^\bullet_{K,\ell})$ one then has*

$$\beta^{(\ell)}_{L/K}(a) = \sum_{\sigma \in G_K} (\mathrm{rec}_\ell(a_{\sigma v_0}) - 1)\widetilde{\sigma}^{-1} \in I_H/I(D^{(\ell)}_L)I_H$$

with the local reciprocity map $\mathrm{rec}_\ell \colon \mathbb{Q}_\ell \to \mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{ab}}/\mathbb{Q}_\ell) \twoheadrightarrow \mathcal{D}^{(\ell)}_L \subseteq H$ and a choice of lift $\widetilde{\sigma} \in \mathcal{G}$ of $\sigma \in G$.

Proof. See [Bur07, Lem. 10.3] or [BKS16, Lem. 5.21]. □

Throughout the remainder of this section let K_∞ denote the cyclotomic $\mathbb{Z}_p$-extension of K and, for every $n \in \mathbb{N}$, write K_n for its n-th layer. We will write $\Gamma \coloneqq \mathrm{Gal}(K_\infty/K)$ and $\Gamma_n \coloneqq \mathrm{Gal}(K_n/K)$ for the relevant Galois groups. If K_n has conductor mp^{n+t} for some $t \geq 0$, we define

$$t^{(p)}_{K_n} \coloneqq \mathrm{pr}_{F_{mp^{n+t}/K}}(t^{(p)}_{mp^{n+t}}).$$

As the remaining calculations are subtantially different according to whether the prime ℓ is equal to p or not, we now consider these two cases separately.

5.3.1. The case $\ell \neq p$

Let us first assume that $\ell \neq p$. By enlarging K is necessary, we may assume that the decomposition group $D^{(\ell)}_{K_n}$ of ℓ in $K_n/\mathbb{Q}$ is equal to Γ_n for all $n \in \mathbb{N}$. In particular, $\beta^{(\ell)}_{K_n/K}$ defines a map $H^1(A^\bullet_{K_n,\ell}) \to I_{\Gamma_n}/I^2_{\Gamma_n}$. In order to apply Proposition (B.17) (c) in this situation, we need to verify that $\mathrm{pd}_{\mathbb{Z}_p[G_{K_n}]}((\widehat{K^\times_{n,\ell}})_{\mathrm{tor}}) \leq 1$ and $\mathrm{pd}_{\mathbb{Z}_p}((\widehat{K^\times_\ell})_{\mathrm{tor}}) \leq 1$. (This will also verify condition (85) by Remark (B.15).) The second inequality is clear because $\mathbb{Z}_p$ is a discrete valuation ring, and for the first inequality it is sufficient to prove that $(K^\times_{n,v_0})_{\mathrm{tor}}$ is Γ_n-cohomologically trivial. The required cohomological triviality is however true because the extension $K_{n,v_0}/\mathbb{Q}_\ell$ is unramified (cf. [NSW08, Prop 9.1.4]).
Proposition (B.17) (c) now shows that

$$(\beta^{(\ell)}_{K_n/K} \circ \vartheta_{K,\ell,v_0} \circ \mathrm{pr}_{K_n/K})(t^{(\ell)}_{mp^n}) \equiv \vartheta^0_{K_n,\ell}(t^{(\ell)}_{K_n}) \mod I^2_{\Gamma_n} \tag{44}$$

as an equality in $\mathrm{Ann}_{\mathbb{Z}_p}((\mathbb{Q}^\times_\ell)_{\mathrm{tor}})^{-1} \otimes_{\mathbb{Z}_p} (I_{\Gamma_n}/I^2_{\Gamma_n})$. The right hand side of this congruence we can compute, using Theorem (2.10) (d), to be

$$\begin{aligned} \vartheta^0_{K_n,\ell}(t^{(\ell)}_{K_n}) &= \pi_{F_{mp^{n+t}/K_n}}(\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\nu^{(\ell)}_{mp^{n+t}}) \\ &\equiv \ell(\ell-1)^{-1} \otimes \ell^{-(\mathrm{ord}_\ell(m)-1)}(1-\tilde{\sigma}_\ell) \mod I^2_{\Gamma_n}. \end{aligned} \tag{45}$$

(Note that $\mathrm{Ann}_{\mathbb{Z}_p}((\mathbb{Q}^\times_\ell)_{\mathrm{tor}})^{-1}$ is generated by $(\ell-1)^{-1}$.) Combining (44) and (45) we obtain

$$(\beta^{(\ell)}_{K_n/K} \circ \vartheta_{K,\ell,v_0} \circ \mathrm{pr}_{K_n/K})(t^{(\ell)}_{mp^n}) \equiv \ell(\ell-1)^{-1} \otimes \ell^{-(\mathrm{ord}_\ell(m)-1)}(1-\tilde{\sigma}_\ell) \mod I^2_{\Gamma_n}, \tag{46}$$

which, by using the isomorphism

$$I_{\Gamma_n}/I^2_{\Gamma_n} \cong \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} (I(\Gamma_n)/I(\Gamma_n)^2),$$

we can regard as an equality in $(\ell-1)^{-1}\mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} (I(\Gamma_n)/I(\Gamma_n)^2)$. By taking the limit of the maps $\beta^{(\ell)}_{K_n/K}$ we may define a limit map

$$H^1(A^\bullet_{K,\ell}) \to \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} \big(\varprojlim_{n\in\mathbb{N}} (I(\Gamma_n)/I(\Gamma_n)^2)\big) \cong \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} \Gamma,$$

where the isomorphism is induced by sending $(g-1) \mapsto g$ for every $g \in \Gamma$. Passing to the limit (over n) in (46), we then obtain

$$\begin{aligned} (\beta^{(\ell)}_{K_\infty/K} \circ \vartheta_{K,\ell,v_0} \circ \mathrm{pr}_{K_\infty/K})(t^{(\ell)}_{K_\infty}) &= \ell(\ell-1)^{-1} \otimes \ell^{-(\mathrm{ord}_\ell(m)-1)}(1-\tilde{\sigma}_\ell) \\ &= -\ell(\ell-1)^{-1} \otimes \ell^{-(\mathrm{ord}_\ell(m)-1)}(\tilde{\sigma}_\ell - 1) \end{aligned} \tag{47}$$

in $(\ell-1)^{-1}\mathbb{Z}_p[G]\otimes_{\mathbb{Z}_p}\Gamma$. Since ℓ is unramified in K_∞/K, the composite map

$$\widehat{K_{v_0}^\times}\xrightarrow{\mathrm{rec}_\ell}\mathbb{Z}_p\otimes_{\mathbb{Z}_p}\Gamma\overset{\sigma_\ell\mapsto 1}{\cong}\mathbb{Z}_p$$

agrees with ord_ℓ. This map restricts to an isomorphism on the torsion-free quotient of $\widehat{K_{v_0}^\times}$, and so Lemma (5.5) combines with (47) to imply that

$$(\vartheta_{K,\ell,v_0}\circ\mathrm{pr}_{K_\infty/K})(t^{(\ell)}_{K_\infty})=-\ell^{-\mathrm{ord}_\ell(m)+1}(1-\ell^{-1})^{-1}\otimes\ell,$$

as required to conclude the proof of Theorem (5.2) (a).

5.3.2. The case $\ell=p$

In the remainder of this section we consider the case $\ell=p$. It then suffices to prove that

$$(\vartheta_{K,p,v_0}\circ\mathrm{pr}_{K_n/K})(t^{(p)}_{K_n})=\mathrm{N}_{F_m/K}(\mathfrak{l}_m)\wedge p.$$

As a first step in this direction, we combine Proposition (B.17) (c) with the argument of [BKS16, Thm. 5.10] to deduce that

$$\sum\nolimits_{\sigma\in\Gamma_n}\sigma\vartheta^0_{K_n,p}(t^{(p)}_{K_n})\otimes\sigma^{-1}=-(\beta^{(p)}_{K_n/K}\circ\vartheta_{K,p,v_0}\circ\mathrm{pr}_{K_n/K})(t^{(p)}_{K_n})\tag{48}$$

in $\widehat{K_{n,p}^\times}\otimes_{\mathbb{Z}_p[G_{K_n}]}(I_{\Gamma_n}/I_{\Gamma_n}^2)$ with $\Gamma_n:=\mathrm{Gal}(K_n/K)$.
Recall that for any norm-coherent sequence $u=(u_n)_{n\geq 0}\in\varprojlim_{n\geq 0}(\mathbb{Z}_p\otimes_{\mathbb{Z}}\mathcal{O}_{F_{mp^n}})^\times$ there exists a unique power series $\mathrm{Col}(X)\in(\mathbb{Z}_p\otimes_{\mathbb{Z}}\mathcal{O}_{F_m})[\![X]\!]^\times$, called its 'Coleman power series', with the property that

$$(\sigma_p^{-n}\mathrm{Col})(\zeta_{p^n}-1)=u_n\quad\text{ for all } n\geq 1.$$

(See [Sha95, Ch. I] for details.)
In the following, we will use the maps

$$\mathrm{Ord}_p\colon\bigoplus\nolimits_{v|p}\widehat{K_v^\times}\to\mathbb{Z}_p[G],\quad a\mapsto\sum\nolimits_{\sigma\in G}\mathrm{ord}_p(a_{\sigma v_0})\sigma^{-1},$$
$$\mathrm{Rec}_{p,K_n/K}\colon\bigoplus\nolimits_{v|p}\widehat{K_v^\times}\to I_{\Gamma_n}/I_{\Gamma_n}^2,\quad a\mapsto\sum\nolimits_{\sigma\in G}(\mathrm{rec}_\ell(a_{\sigma v_0})-1)\tilde{\sigma}^{-1},$$

and the induced isomorphisms

$$\mathrm{Ord}_p\colon\bigwedge^2_{\mathbb{Z}_p[G]}\widehat{K_p^\times}\xrightarrow{\simeq}\widehat{\mathcal{O}_{K,p}^\times}\quad\text{ and }\quad\mathrm{Rec}_{p,K_n/K}\colon\bigwedge^2_{\mathbb{Z}_p[G]}\widehat{K_p^\times}\xrightarrow{\simeq}p^{\mathbb{Z}_p[G]}.$$

(5.6) Lemma. *Suppose $u=(u_n)_{n\geq 0}\in\varprojlim_{n\geq 0}(\mathbb{Z}_p\otimes_{\mathbb{Z}}\mathcal{O}_{F_{mp^n}})^\times$ is a norm-coherent sequence with $\mathrm{N}_{F_m/K}(u_0)=1$ and $\mathrm{Col}(0)\in(\mathbb{Z}_p\otimes_{\mathbb{Z}}\mathcal{O}_{F_m})^\times$. For big enough n, one then has*

$$\sum\nolimits_{\sigma\in\Gamma_n}\sigma\mathrm{N}_{F_{mp^n}/K_n}(u_n)\otimes\sigma^{-1}=(\mathrm{Rec}_{p,K_n/K}\circ\mathrm{Ord}_p^{-1})(\mathrm{N}_{F_m/K}(\mathrm{Col}(0)))$$

in $\widehat{K_{n,p}^\times}\otimes_{\mathbb{Z}_p[G_{K_n}]}(I_{\Gamma_n}/I_{\Gamma_n}^2)$.

Proof. This follows from the main result of Bley and Hofer in [BH20] via the argument of [BH23, Thm. 5.1]. For the convenience of the reader, we sketch this argument.
Observe that $K^\times$ contains no primitive p-th root of unity because p is assumed to split completely in K, and hence that also each $\widehat{K_n^\times}$ is $\mathbb{Z}_p$-torsion free by the general result of [NSW08, Prop. 1.6.12]. If we fix a topological generator γ of Γ, then we may therefore use the argument of [BD21, Thm. 3.8 (b)], applied to the complex $A^\bullet_{K_\infty,p}$, to deduce from the assumption $\mathrm{N}_{F_m/K}(u_0)=1$ that the sequence $u':=(\mathrm{N}_{F_{mp^n}/K_n}(u_n))_{n\in\mathbb{N}}$ is divisible by $\gamma-1$ in $\varprojlim_{n\in\mathbb{N}}\widehat{K_{n,p}^\times}$.
Writing $\kappa=(\kappa_n)_{n\geq 0}$ for the unique element of $\varprojlim_{n\geq 0}\widehat{K_{n,p}^\times}$ such that $u'=(\gamma-1)\kappa$, one then has

$$\sum\nolimits_{\sigma\in\Gamma_n}\sigma\mathrm{N}_{F_{mp^n}/K_n}(u_n)\otimes\sigma^{-1}=\kappa_0\otimes(\gamma-1)$$

by [BH23, Lem. 3.14]. To proceed, define the characters $s_\gamma\colon \Gamma \to \mathbb{Z}_p, \gamma^a \mapsto a$ and $s_{\gamma,n}\colon \Gamma_n \to \mathbb{Z}/p^n\mathbb{Z}, \gamma^a \mapsto a \mod p^n$. Applying [BH20, Cor. 3.17] (see also [BH23, Prop. 5.2]) to the character $\rho_{\gamma,n}\colon G_{mp^\infty} \to \Gamma \xrightarrow{s_{\gamma,n}} \mathbb{Z}/p^n\mathbb{Z}$, we obtain the equality

$$\frac{\mathrm{ord}_{K_n}(\kappa_n)}{p^n} = -\frac{(s_{\gamma,n}\circ \mathrm{rec}_p \circ \mathrm{N}_{F_m/K})(\mathrm{Col}(0)))}{p^n} \quad \text{in } \bigoplus\nolimits_{v|p}(\mathbb{Q}/\mathbb{Z}).$$

Now, $\mathrm{ord}_{K_n}(\kappa_n) = \mathrm{ord}_K(\kappa_0)$ because K_n/K is totally ramified at p, and so taking the limit (over n) shows that

$$\mathrm{ord}_p(\kappa_0) = -(s_\gamma \circ \mathrm{rec}_p \circ \mathrm{N}_{F_m/K})(\mathrm{Col}(0))) \quad \text{in } \bigoplus\nolimits_{v|p}\mathbb{Z}_p.$$

In addition, local class field theory implies that the group of universal norms $\bigcap_{n\in\mathbb{N}} \mathrm{N}_{K_n/K}(\widehat{K_n^\times})$ is equal to $\bigoplus_{v|p} p^{\mathbb{Z}_p}$, on which Ord_p is injective. Since κ_0 clearly belongs to this group and the same is true for the image of the isomorphism $\bigwedge^2_{\mathbb{Z}_p[G]} \widehat{K_p^\times} \xrightarrow{\simeq} p^{\mathbb{Z}_p[G_K]}$ induced by $\mathrm{Rec}_{p,K_n/K}$ (cf. the general result of [BB25, Lem. 2.17 (ii)]), the last displayed equality in fact implies that $\kappa_0 \otimes (\gamma - 1) = -(\mathrm{Ord}_p^{-1} \circ \mathrm{Rec}_{p,K_n/K})(\mathrm{N}_{F_m/K}(\mathrm{Col}(0))) = (\mathrm{Rec}_{p,K_n/K} \circ \mathrm{Ord}_p^{-1})(\mathrm{N}_{F_m/K}(\mathrm{Col}(0)))$, as claimed. □

Write $\mathrm{Col}(X) \in \mathbb{Z}_p[\![X]\!]$ for the Coleman power series associated to the norm-coherent sequence $(\mathfrak{l}_{mp^n})_n$. Then Lemma (5.6) combines with (48) and Lemma (5.5) to imply that

$$\begin{aligned}(\mathrm{Rec}_{p,K_n/K} \circ \mathrm{Ord}_p^{-1})(\mathrm{N}_{F_m/K}(\mathrm{Col}(0))) &= \sum\nolimits_{\sigma\in\Gamma_n} \sigma\vartheta^0_{K_n,p}(t^{(p)}_{K_n}) \otimes \sigma^{-1} \\ &= -(\mathrm{Rec}_{p,K_n/K} \circ \vartheta_{K,p,v_0} \circ \mathrm{pr}_{K_n/K})(t^{(p)}_{K_n})\end{aligned}$$

in $\widehat{K^\times_{n,p}} \otimes_{\mathbb{Z}_p[G_{K_n}]} (I_{\Gamma_n}/I^2_{\Gamma_n})$. Note that the outer terms in this equality belong to the image of $\widehat{K^\times} \otimes_{\mathbb{Z}_p[G_{K_n}]} (I_{\Gamma_n}/I^2_{\Gamma_n}) \cong \widehat{K^\times} \otimes_{\mathbb{Z}_p} (I(\Gamma_n)/I(\Gamma_n)^2)$ so that we can regard this as where the equality takes places. Taking the limit over n, the map $\mathrm{Rec}_{p,K_n/K}$ defines an isomorphism $\bigwedge^2_{\mathbb{Z}_p[G]} \widehat{K_p^\times} \xrightarrow{\simeq} p^{\mathbb{Z}_p[G]} \otimes_{\mathbb{Z}_p} (I(\Gamma)/I(\Gamma)^2)$ so that from the last displayed equality we can deduce that

$$\mathrm{Ord}_p^{-1}(\mathrm{N}_{F_m/K}(\mathrm{Col}(0))) = -(\vartheta_{K,p,v_0} \circ \mathrm{pr}_{K_n/K})(t^{(p)}_{K_n}).$$

Now, by definition of $\tilde{x}_{mp^n}$ (Definition (2.25)) one has

$$\begin{aligned}\mathrm{Col}(X) &= \exp_{\mathbb{G}_m} \circ \log_{\widehat{E}} \circ \Big(\sum_{m_0|d|m} \big((\sum_{\chi\neq\tau} h_{\chi,d}(X) -_{\widehat{E}} X) +_{\widehat{E}} (p\mathrm{Eul}_p(\sigma_p))^{-1}\epsilon_d \big) \Big) \\ &= \sum_{m_0|d|m} \big((\sum_{\chi\neq\tau} (\exp_{\mathbb{G}_m} \circ g_{\chi,d}(X)) -_{\mathbb{G}_m} (\exp_{\mathbb{G}_m} \circ \log_{\widehat{E}})(X)) \\ &\qquad +_{\mathbb{G}_m} (p\mathrm{Eul}_p(\sigma_p))^{-1} \exp_{\mathbb{G}_m}(\zeta_d p) \big)\end{aligned}$$

and so we deduce that

$$\mathrm{Col}(0) = (p\mathrm{Eul}_p(\sigma_p))^{-1} \exp_{\mathbb{G}_m} \big(\sum\nolimits_{m_0|d|m} \zeta_d p \big) = \mathfrak{l}_m.$$

The claim now follows from the equality $\mathrm{Ord}_p(\mathrm{N}_{F_m/K}(\mathfrak{l}_m) \wedge p) = -\mathrm{N}_{F_m/K}(\mathfrak{l}_m)$ because the map $\mathrm{Ord}_p\colon \bigwedge^2_{\mathbb{Z}_p[G]} \widehat{K_p^\times} \to (\mathbb{Z}_p \otimes_{\mathbb{Z}} \mathcal{O}_K)^\times$ is an isomorphism.
This concludes the proof of Theorem (5.2). □

6. Nekovář–Selmer complexes and exceptional zeros

In this section we establish Theorems (1.4) (a) and (1.7). The proofs involve an auxiliary Nekovář–Selmer structure, introduced in § 6.1.1 and studied further in § 6.1.2, where we describe the associated Nekovář–Selmer complexes and their cohomology. After some preliminary constructions of § 6.1.3 concerning the determinants of these complexes, we first prove Theorem (1.4) (a) in § 6.2 before turning to the proof of Theorem (1.7) in § 6.3.

6.1. Consequences of Tate uniformisation

If E has split-multiplicative reduction at the prime ℓ, then Tate uniformisation gives rise to an exact sequence (cf. [Sil94, Prop. 6.1])

$$0 \longrightarrow \mathbb{Z}_p(1) \longrightarrow \mathrm{T}_p E \longrightarrow \mathbb{Z}_p \longrightarrow 0 \tag{49}$$

of $\mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$-modules, which induces an exact triangle

$$\mathrm{R}\Gamma(\mathbb{Q}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}) \xrightarrow{g_\ell} \mathrm{R}\Gamma(\mathbb{Q}_\ell, (\mathrm{T}_p E)_{K/\mathbb{Q}}) \xrightarrow{h_\ell} \mathrm{R}\Gamma(\mathbb{Q}_\ell, \mathbb{Z}_{p,K/\mathbb{Q}}) \to \mathrm{R}\Gamma(\mathbb{Q}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}})[1]. \tag{50}$$

(6.1) Remark. For later use we note that the connecting homomorphism $\mathbb{Z}_p \to H^1(\mathbb{Q}_\ell, \mathbb{Z}_p(1))$ arising from the exact sequence (49) sends 1 to the image of the ℓ-adic Tate period $q_{E,\ell}$ of E under the Kummer map $\widehat{\mathbb{Q}_\ell^\times} \xrightarrow{\simeq} H^1(\mathbb{Q}_\ell, \mathbb{Z}_p(1))$.

6.1.1. Definition of a useful Nekovář–Selmer structure

We now use the triangle (50) to define a useful Nekovář–Selmer structure. To do this, we fix $Q \in E_1(K_p)$ and a finite set Π of primes at which E has split-multiplicative reduction. Write Π_{ram} and Π_{unr} for the subsets of Π (resp. of $\Pi \setminus \{p\}$) comprising primes which are ramified and unramified in K, respectively. We further let Σ be a finite set of places of $\mathbb{Q}$ that contains $S(K)$.

We define a Selmer structure $\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$ with $S(\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}) = \Sigma$ as follows.

- If $v \in \Pi_{\mathrm{ram}}$, then we let $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \coloneqq \mathrm{R}\Gamma(\mathbb{Q}_v, \mathbb{Z}_p(1)_{K/\mathbb{Q}})$ and take $i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}$ to be the map g_v from (50).
- If $v \in \Pi_{\mathrm{unr}}$, then we we define $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ and $i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}$ by means of the triangle

  $$\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \xrightarrow{i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}} \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma(\mathbb{F}_v, \mathbb{Z}_p(1)), \mathbb{Z}_p)[-2] \to \quad .$$

  Here the last arrow is the map

  $$\begin{aligned} \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) &\xrightarrow{h_v} \mathrm{R}\Gamma(\mathbb{Q}_v, \mathbb{Z}_{p,K/\mathbb{Q}}) \\ &\xrightarrow{\simeq} \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma(\mathbb{Q}_v, \mathbb{Z}_p(1)_{K/\mathbb{Q}}), \mathbb{Z}_p)[-2] \\ &\longrightarrow \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma(\mathbb{F}_v, \mathbb{Z}_p(1)_{K/\mathbb{Q}}), \mathbb{Z}_p)[-2], \end{aligned}$$

  defined as the composite of the map h_v from (50), the canonical isomorphism induced by local Tate duality, and the inflation map $\mathrm{R}\Gamma(\mathbb{F}_v, \mathbb{Z}_p(1)_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma(\mathbb{Q}_v, \mathbb{Z}_p(1)_{K/\mathbb{Q}})$.
- If $v = p$ is unramified in K, then we define $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ and $i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}$ by the triangle

  $$\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \xrightarrow{i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}} \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{RHom}_{\mathbb{Z}_p}(D^\bullet_{p,Q}, \mathbb{Z}_p)[-2] \to \quad ,$$

  where $D^\bullet_{p,Q}$ is the complex defined in Lemma (4.2) (b) and the second arrow is the composite of the natural map $\mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma_{/f}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ and the map $\rho^*_{p,Q} \coloneqq \mathrm{RHom}_{\mathbb{Z}_p}(\rho_{p,Q}, \mathbb{Z}_p)[-2]$ dual to the morphism $\rho_{p,Q}$ from Lemma (4.2) (b).
- If $v = p$ is ramified in K and does not belong to Π, then we define $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ and $i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}$ by means of the triangle

  $$\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \xrightarrow{i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}} \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \longrightarrow \mathbb{Z}_p[G][-1] \longrightarrow \mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}})[1].$$

  Here the second arrow is induced by $\mathcal{P}_K(\cdot, Q)$ (equivalently, the composite of the natural morphism $\mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma_{/f}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ with the dual of the map $\mathbb{Z}_p[G][-1] \to \mathrm{R}\Gamma_f(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ that sends 1 to Q).

- In all other cases we take $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) := \mathrm{R}\Gamma(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ and $i_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi},v}$ to be the identity map.

(6.2) Lemma. *Let (Σ, Π, Q) be as above. For every place v of $\mathbb{Q}$, the complex $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ is perfect in $D(\mathbb{Z}_p[G])$ and acyclic outside degrees one and two.*

Proof. In all cases perfectness is a consequence of the definitions and the general result of Flach [Fla00, § 5]. The claim regarding acyclicity is clear in all cases apart from when $v = p$ is unramified in K. To justify the claim in this remaining case, we write ρ for the composite of the map $\rho_{p,Q}$ and the map $\mathrm{R}\Gamma_f(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \to \mathrm{R}\Gamma(\mathbb{Q}_p, T_{K/\mathbb{Q}})$. By definition of $\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$, one then has $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \cong \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{cone}(\rho), \mathbb{Z}_p)[-2]$ and this isomorphism gives rise to a convergent spectral sequence

$$E_2^{i,j} = \mathrm{Ext}^i_{\mathbb{Z}_p}(H^{-j}(\mathrm{cone}(\rho)), \mathbb{Z}_p) \quad \Rightarrow \quad E^{i+j} = H^{i+j+2}_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_p, T_{K/\mathbb{Q}}).$$

Since $\mathrm{Ext}^i_{\mathbb{Z}_p}(-, \mathbb{Z}_p) = 0$ if $i \notin \{0, 1\}$, this spectral sequence reduces us to proving that

(i) $H^i(\mathrm{cone}(\rho)) = 0$ if $i \notin \{0, 1, 2\}$,

(ii) $H^2(\mathrm{cone}(\rho))$ is $\mathbb{Z}_p$-torsion,

(iii) $H^0(\mathrm{cone}(\rho))$ is $\mathbb{Z}_p$-torsion free.

By its definition, the complex $D^\bullet_{p,Q} = \mathbb{Z}_p[G][-1] \oplus D^\bullet_p$ is acyclic outside degree one and so claim (i) follows from the long exact sequence in cohomology induced by the defining triangle for $\mathrm{cone}(\rho)$. Moreover, this long exact sequence gives an isomorphism $H^2(\mathrm{cone}(\rho)) \cong H^2(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ and hence proves (ii) because $H^2(\mathbb{Q}_p, T_{K/\mathbb{Q}}) \cong \bigoplus_{v|p}(E(K_v)_{\mathrm{tor}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\vee$ is finite. To prove claim (iii), we recall that the map $H^1(\rho)$ is defined to be the composite of $H^1(\rho_{p,Q})$ and the Kummer map $E(K_p) \hookrightarrow H^1(\mathbb{Q}_p, T_{K/\mathbb{Q}})$. Now, by definition of $\rho_{p,Q}$ one has a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}_p[G] & \longrightarrow & H^1(D^\bullet_{p,Q}) & \longrightarrow & H^1(D^\bullet_p) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 1\mapsto Q} & & \downarrow{\scriptstyle H^1(\rho_{p,Q})} & & \downarrow & & \\
0 & \longrightarrow & E_1(K_p) & \longrightarrow & E(K_p) & \longrightarrow & (E/E_1)(K_p) & \longrightarrow & 0
\end{array}$$

in which the the rightmost vertical arrow is an isomorphism by Lemma (4.1) because p is assumed to be unramified in K. The snake lemma therefore implies that $H^0(\mathrm{cone}(\rho)) = \ker H^1(\rho_{p,Q})$ identifies with an ideal of $\mathbb{Z}_p[G]$, and hence that it is $\mathbb{Z}_p$-torsion free, as required to verify (iii). □

6.1.2. A computation of Nekovář–Selmer groups

The cohomology of the Nekovář–Selmer complex associated to $\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$ has the following important properties.

(6.3) Lemma. *For every triple (Σ, Π, Q) as in § 6.1.1 the following claims are valid.*

(a) One has $\mathrm{rk}_{\mathbb{Z}_p}(H^1_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_pE)^G) \geq |\Pi_{\mathrm{ram}}| + \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Sel}^\vee_{p,E/\mathbb{Q}})$.

(b) If $E(K)[p] = 0$, then there is a surjection

$$H^2_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_pE) \twoheadrightarrow \bigoplus\nolimits_{\ell\in\Pi_{\mathrm{ram}}} H^2(\mathbb{Q}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}) \cong Y_{K,\Pi_{\mathrm{ram}}} := \bigoplus\nolimits_{v|\ell}\bigoplus\nolimits_{\ell\in\Pi_{\mathrm{ram}}} \mathbb{Z}_p v.$$

(c) If $E(K)[p] = 0$, then $H^1_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_pE)$ is $\mathbb{Z}_p$-torsion free.

Proof. To prove claim (a), we will show that $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_pE)^G)$ is at least $|\Pi_{\mathrm{ram}}| + \dim_{\mathbb{Q}_p} H^2_f(\mathbb{Q}, \mathrm{V}_pE)$. To do this, we set $\mathcal{F} := \mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$, write $H^1_{h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ for the image of $H^1(\mathrm{R}\Gamma_{\mathcal{F}}(\mathbb{Q}_p, T_{K/\mathbb{Q}}))$ in $H^1(\mathbb{Q}_p, T_{K/\mathbb{Q}})$, and define $H^1_{/h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ to be the quotient

of $H^1(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ by $H^1_{h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$.
Note that $H^1(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})$ is finite for every $\ell \neq p$, and hence that the relevant instance of the triangle in Remark (3.2) gives the exact sequence

$$\mathbb{Q}_p \otimes_{\mathbb{Z}_p} Y_{K,\Pi_{\mathrm{ram}}} \hookrightarrow \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E) \to H^1(\mathcal{O}_{K,\Sigma}, \mathrm{V}_p E) \to \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_{/h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}}). \tag{51}$$

If we can prove that $H^1_{h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ contains $H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}})$, then exactness of (51) will show that the image of the second arrow in (51) contains $H^1_f(K, \mathrm{V}_p E)$. Since $H^1_f(K, \mathrm{V}_p E)^G \cong H^1_f(\mathbb{Q}, \mathrm{V}_p E)$ has the same $\mathbb{Q}_p$-dimension as $H^2_f(\mathbb{Q}, \mathrm{V}_p E)$ by duality (cf. [BF01, Lem. 19]), taking G-invariants will then imply claim (a).
If $p \in \Pi_{\mathrm{ram}}$, then we have defined $H^1_{h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ to be the kernel of the map $H^1(h_p)$ induced by h_p. From the long exact sequence associated with the triangle (50) we deduce that the kernel of $H^1(h_p)$ is the image of $H^1(g_p)$. Now, one has a commutative diagram

$$\begin{array}{ccc} \bigoplus_{v|p} \widehat{K_v^\times} & \twoheadrightarrow & \bigoplus_{v|p} E(K_v)^\wedge \\ \downarrow\simeq & & \downarrow\kappa \\ H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)_{K/\mathbb{Q}}) & \xrightarrow{H^1(g_p)} & H^1(\mathbb{Q}_p, T_{K/\mathbb{Q}}), \end{array}$$

where the vertical arrows are the respective Kummer maps and the top arrow is induced by Tate uniformisation. This shows that $H^1_{h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}}) = H^1_f(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ in this case, as desired.
If $p \notin \Pi_{\mathrm{ram}}$, then $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_{h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ is by definition the orthogonal complement of $\mathbb{Q}_p[G] \cdot Q$ with respect to local Tate duality. Since Q was chosen to be an element of $H^1_f(\mathbb{Q}_p, V_{K/\mathbb{Q}})$, which is its own orthogonal complement, it follows that $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1_{h(\mathcal{F})}(\mathbb{Q}_p, T_{K/\mathbb{Q}})$ contains $H^1_f(\mathbb{Q}_p, V_{K/\mathbb{Q}})$. This concludes the proof of claim (a).
As for claim (b), by definition of the Nekovář–Selmer structure $\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$ and the octahedral axiom we have an exact triangle

$$\mathrm{R}\Gamma_{\mathrm{c}}(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \to \mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E) \to \bigoplus\nolimits_{\ell \in \Sigma} \mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \to,$$

which, since $H^3_{\mathrm{c}}(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \cong (\mathbb{Z}_p \otimes_{\mathbb{Z}} E(K)_{\mathrm{tor}})^\vee$ is assumed to vanish, induces a surjection

$$H^2_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E) \twoheadrightarrow \bigoplus\nolimits_{\ell \in \Sigma} H^2_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}) \twoheadrightarrow \bigoplus\nolimits_{\ell \in \Pi_{\mathrm{ram}}} H^2(\mathbb{Q}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}),$$

as claimed. Finally, claim (c) follows from the exact sequence (obtained from the relevant instance of the triangle in Remark (3.2))

$$0 \to \bigoplus\nolimits_{v \in \Pi_{\mathrm{ram}}} \mathbb{Z}_p v \to H^1_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E) \to H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$$

and the fact that $H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$ is $\mathbb{Z}_p$-torsion free if $E(K)$ has no point of order p. □

We now write $(\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q})^*$ for the dual Nekovář–Selmer structure of $\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$ (as defined in Remark (3.4)) and define a complex as

$$\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q} := \mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma_{(\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q})^*}(K, \mathrm{T}_p E), \mathbb{Z}_p)[-3].$$

This complex is described in a little more detail in the following result which is an analogue of Lemma (3.5).

(6.4) Lemma. *For every triple (Σ, Π, Q) as in § 6.1.1 the following claims are valid.*

(a) $\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q}$ *is a perfect object of $D(\mathbb{Z}_p[G])$ with Euler characteristic*

$$\chi_{\mathbb{Z}_p[G]}(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q}) = [\mathbb{Z}_p[G]].$$

(b) There is a canonical isomorphism $H^1(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q}) \cong H^1_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E)$. If $E(K)[p] = 0$, then there is also a split-exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \longrightarrow H^2_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E) \longrightarrow H^2(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q}) \longrightarrow T^+_{K/\mathbb{Q}} \longrightarrow 0, \tag{52}$$

and $\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q}$ *is acyclic outside of degrees zero and one.*

(c) In $D(\mathbb{Z}_p[G])$ *there is an exact triangle*

$$\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q} \to C^{\bullet}_{K,\Sigma} \to \bigoplus\nolimits_{v\in\Sigma} \mathrm{R}\Gamma_{/\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q}[1]. \tag{53}$$

Proof. The triangle (53) in claim (c) is obtained by dualising the triangle

$$\mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \to \mathrm{R}\Gamma_{(\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q})^*}(K, \mathrm{T}_p E) \to \bigoplus\nolimits_{v\in\Sigma} \mathrm{R}\Gamma_{(\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q})^*}(\mathbb{Q}_v, T_{K/\mathbb{Q}}) \to \tag{54}$$

that exists by the definition of $\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$ and the octahedral axiom. As a consequence of (53), we deduce that $\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q}$ is perfect and has Euler characteristic $-[\mathbb{Z}_p[G]]$. This is because the complex $C^{\bullet}_{K,\Sigma}$ is perfect with vanishing Euler characteristic (cf. Lemma (3.5) (a)) and each complex $\bigoplus_{v\in\Sigma} \mathrm{R}\Gamma_{/\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_v, T_{K/\mathbb{Q}})$ is by construction perfect and has vanishing Euler characteristic if $v \neq p$ resp. Euler characteristic $[\mathbb{Z}_p[G]]$ if $v = p$ (as follows from the computations of Euler characteristics in [Fla00]). Having thereby proved claim (a), we now turn to claim (b). Firstly, Artin–Verdier induces a canonical exact triangle

$$\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E) \to \mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q} \to (T_{K/\mathbb{Q}})^+[-2] \to, \tag{55}$$

and this directly implies the first part of claim (b). Assuming now that $E(K)[p] = 0$, the isomorphism $H^3_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E) \cong (E(K)_{\mathrm{tor}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\vee$ shows that $\mathrm{R}\Gamma_c(\mathcal{O}_{K,\Sigma}, \mathrm{T}_p E)$ is acyclic outside degree one and two. From the triangle for $\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}$ analogous to (54) and Remark (6.2) we therefore see that $\mathrm{R}\Gamma_{\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(K, \mathrm{T}_p E)$ is acyclic outside degrees one and two. Given this, the triangle (55) implies both that $\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q}$ is acyclic outside degree one and two and that one has the exact sequence (52), which is split-exact because $(T_{K/\mathbb{Q}})^+$ is a free $\mathbb{Z}_p[G]$-module. This concludes the proof of claim (b). □

6.1.3. Determinants and passage to cohomology

Let (Σ, Π, Q) as in § 6.1.1 and recall the basis b_K of $T^+_{K/\mathbb{Q}}$ defined in § 3.2. In light of Lemma (6.4), Definition (B.2) provides us with a map

$$F_{K,\Sigma,\Pi,Q} \coloneqq \vartheta_{\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q},\{b^*_K\}} \colon \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q})^{-1} \to \mathbb{Q}_p[G].$$

We next define a composite isomorphism $f_{K,\Sigma,\Pi,Q}$ as

$$\begin{aligned}\mathrm{Det}_{\mathbb{Z}_p[G]}(C^{\bullet}_{K,\Sigma})^{-1} &\xrightarrow{\simeq} \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q})^{-1} \otimes_{\mathbb{Z}_p[G]} \bigotimes_{\ell\in\Pi\cup\{p\}} \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma_{/\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}}))^{-1} \\ &\xrightarrow{\simeq} \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{SC}^{\bullet}_{K,\Sigma,\Pi,Q})^{-1},\end{aligned}$$

where the first arrow is the isomorphism induced by the triangle (53) and the second arrow is $\mathrm{id} \otimes (\otimes_{\ell\in\Pi\cup\{p\}} \mathrm{Ev}_{x_\ell})$ with x_ℓ defined as follows.

- For any prime number $\ell \in \Pi \setminus (\Pi_{\mathrm{ram}} \cup \{p\}$, the complex $\mathrm{R}\Gamma(\mathbb{F}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}})$ can be represented by
$$\mathbb{Z}_p[G] \xrightarrow{\cdot(1-\ell^{-1}\sigma_\ell)} \mathbb{Z}_p[G].$$
We may therefore define a canonical element $s_\ell \coloneqq \mathrm{id}_{\mathbb{Z}_p[G]} \otimes 1$ of $\mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma(\mathbb{F}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}))^{-1}$ that satisfies $\vartheta_{\mathrm{R}\Gamma(\mathbb{F}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}),\varnothing}(s_\ell) = 1 - \ell^{-1}\sigma_\ell = \mathrm{Eul}_\ell(\sigma_\ell)$. Given this, we define x_ℓ as the image of s_ℓ under the isomorphism
$$\begin{aligned}\mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma_{/\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})) &= \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{RHom}_{\mathbb{Z}_p}(\mathrm{R}\Gamma(\mathbb{F}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}), \mathbb{Z}_p)[-2]) \\ &\cong \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma(\mathbb{F}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}}))^{-1,\#}\end{aligned}$$
that is induced by the isomorphism (3).

- If $\ell \in \Pi_{\mathrm{ram}}$, then we we use the element $t_K^{(\ell)}$ from Theorem (5.2) to define x_ℓ as the image of $(-1)^{\mathbf{1}_\ell(p)} \cdot t_K^{(\ell)}$ under the isomorphism
$$\begin{aligned}\mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma_{/\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})) &\cong \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma(\mathbb{Q}_\ell, \mathbb{Z}_{p,K/\mathbb{Q}})) \\ &\cong \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma(\mathbb{Q}_\ell, \mathbb{Z}_p(1)_{K/\mathbb{Q}})^{-1,\#}.\end{aligned}$$
Here the first isomorphism is induced by the triangle (50) and the second isomorphism by local Tate duality (24) and the isomorphism (3).
- If p is ramified in K but not in Π, then we take x_p to be the element corresponding to $\mathrm{id}_{\mathbb{Z}_p[G]}$ in $\mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma_{/\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})) \cong \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathbb{Z}_p[G][-1]) \cong \mathbb{Z}_p[G]^*$.
- If p is unramified in K, then we let x_p be the unique element of
$$\mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma_{/\mathcal{F}^{\mathrm{sp}}_{\Sigma,\Pi,Q}}(\mathbb{Q}_\ell, T_{K/\mathbb{Q}})) \cong \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{RHom}_{\mathbb{Z}_p}(D^\bullet_{p,Q}, \mathbb{Z}_p)[-2]) \cong \mathrm{Det}_{\mathbb{Z}_p[G]}(F^\bullet_{p,Q})^{-1,\#}$$
with $\vartheta_{D^\bullet_{p,Q},\{\mathrm{id}_{\mathbb{Z}_p[G]}\}}(x_p^\#) = p\mathrm{Eul}_p(\sigma_p)$ (which exists by Lemma (4.2) (a) (iii)).

The following result gives an explicit description of the map $F_{K,\Sigma,\Pi,Q} \circ f_{K,\Sigma,\Pi,Q}$.

(6.5) Lemma. *Let K be a finite abelian extension of $\mathbb{Q}$ of conductor mp^n with $m \in \mathbb{N}$ coprime to p and $n \geq 0$. For every $a \in \mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,\Sigma})^{-1}$ one has the following equality in $\mathbb{Q}_p[G]$.*
$$\begin{aligned}(F_{K,\Sigma,\Pi,Q} \circ f_{K,\Sigma,\Pi,Q})(a) = &\big(\prod\nolimits_{\ell \in \Pi_{\mathrm{ram}}} \nu^{(\ell)}_{mp^n}\big)^\# \cdot \big(\prod\nolimits_{\ell \in \Pi \setminus \{p\}} \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell^{-1})\big)^{-1} \\ &\cdot (p\mathrm{Eul}_p(\sigma_p^{-1}))^{-\mathbf{1}_{p^n}(p)} \cdot \mathcal{P}_K(\Theta_{K,\Sigma}(a), Q). \qquad (56)\end{aligned}$$

Proof. In the case that $p \notin \Pi_{\mathrm{ram}}$, this is a consequence of Proposition (B.7) (a). In the case that $p \in \Pi_{\mathrm{ram}}$ we note that $1 - e_{\mathbf{1}}$ acts as the identity on both sides of the claimed equality, and hence that we may verify this equality over $(1 - e_{\mathbf{1}})\mathbb{Q}_p[G]$. Since in $D(\mathbb{Q}_p[G])$ we have the isomorphism
$$\begin{aligned}(1 - e_{\mathbf{1}})\mathbb{Q}_p[G] \otimes^{\mathbb{L}}_{\mathbb{Z}_p[G]} \mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{Z}_p(1)_{K/\mathbb{Q}}) &= ((1 - e_{\mathbf{1}})\mathbb{Q}_p[G] \otimes_{\mathbb{Z}_p[G]} H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)_{K/\mathbb{Q}}))[-1] \\ &\cong (1 - e_{\mathbf{1}})\mathbb{Q}_p[G][-1],\end{aligned}$$
the claim again follows from Proposition (B.7) (a). □

6.2. Bounds on the order of vanishing of Mazur–Tate elements

In this section we prove the following result, thereby also establishing Theorem (1.4) (a).

(6.6) Theorem. *Fix an abelian number field K and write the conductor of K as mp^n with $m, n \geq 0$ integers such that $p \nmid m$. Suppose that the pair (K, p) satisfies Hypothesis (1.2). Then one has the inclusions*
$$\theta_K^{\mathrm{MT}} \in I(G)^{r_p + \mathrm{sp}(mp^n) + 2c^{(p)}(K)}$$
and
$$\theta_K^{\mathrm{MT}} \in \big(\prod\nolimits_{\ell \in \mathrm{Sp}(mp^n)} I(\mathcal{D}_K^{(\ell)})\big) \cdot \big(\prod\nolimits_{\ell \in C_0^{(p)}(m) \cup C_2^{(p)}(K)} I(\mathcal{D}_K^{(\ell)})\big)^2.$$

Proof. Our approach in this proof is to apply Lemma (4.9), so we begin by verifying the conditions required for this.
If $p \in \Pi_{\mathrm{ram}}$, then we take $Q := (1 - e_\tau)\mathrm{Tr}_{F_{mp^n}/K}(\mathfrak{k}_{mp^n})$. If $p \notin \Pi_{\mathrm{ram}}$, then we let Q be an arbitrary element of $E_1(K_p)$.
By Theorem (3.6), there exists an element $\mathfrak{z}_{K,\Sigma}$ of $\mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,\Sigma})^{-1}$ with the property that $\Theta_{K,\Sigma}(\mathfrak{z}_{K,\Sigma}) = z_K^{\mathrm{Kato}}$. By Lemma (6.5) one then has
$$\begin{aligned}(F_{K,\Sigma,\Pi,Q} \circ f_{K,\Sigma,\Pi,Q})(\mathfrak{z}_{K,\Sigma}) = &\big(\prod\nolimits_{\ell \in \Pi_{\mathrm{ram}}} \nu^{(\ell)}_{mp^n}\big)^\# \cdot \big(\prod\nolimits_{\ell \in \Pi \setminus \{p\}} \mathrm{Eul}_\ell(\widetilde{\sigma}_\ell^{-1})\big)^{-1} \\ &\cdot (p\mathrm{Eul}_p(\sigma_p^{-1}))^{-\mathbf{1}_{p^n}(p)} \cdot \mathcal{P}_K(z^{\mathrm{Kato}}, Q). \qquad (57)\end{aligned}$$

Now, from Lemma (6.3) (c) we know that $H^1(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q})$ is $\mathbb{Z}_p$-torsion free if $H^1(\mathcal{O}_{K,\Sigma}, \mathrm{T}_pE)$ is. The computation of the Euler characteristic of $\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q}$ in Lemma (6.4) (a) combines with the exact sequence (52) to show that $H^2(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q}) \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p$ has the same rank as $H^1(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q})^G$. From Lemma (6.3) (a) we therefore deduce that

$$\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q})) \subseteq \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,\mathrm{Tr}_{K/\mathbb{Q}}(Q)}) \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p) \subseteq I(G)^{|\Pi_{\mathrm{ram}}|+r_p} \quad (58)$$

with $r_p \coloneqq \mathrm{rk}_{\mathbb{Z}_p}(\mathrm{Sel}^\vee_{p,E/\mathbb{Q}})$. In addition, the surjection in Lemma (6.3) (b) implies that

$$\mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q})) \subseteq \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(Y_{K,\Pi_{\mathrm{ram}}}) = \prod\nolimits_{\ell\in\Pi_{\mathrm{ram}}} I(\mathcal{D}_K^{(\ell)}). \quad (59)$$

We next combine these observations with Proposition (B.10). By Lemma (6.4) we may apply [BS21, Prop. A.11 (i)] to the complex $\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q}$ in order to deduce that it admits a standard representative in the sense of Definition (B.3). Given this, it follows from Proposition (B.10) and the inclusions (58) and (59) that

$$(F_{K,\Sigma,\Pi,Q} \circ f_{K,\Sigma,\Pi,Q})(\mathfrak{z}_{K,\Sigma}) \in \mathrm{Fitt}^0_{\mathbb{Z}_p[G]}(H^2(\mathrm{SC}^\bullet_{K,\Sigma,\Pi,Q})) \subseteq I(G)^{r_p+|\Pi_{\mathrm{ram}}|} \cap \prod\nolimits_{\ell\in\Pi_{\mathrm{ram}}} I(\mathcal{D}_K^{(\ell)}).$$

Since this containment is true for every field K satisfying Hypothesis (1.2), it combines with (57) to imply that we have verified the conditions of Lemma (4.9) (in the version of Remark (4.10) if $p \in \Pi_{\mathrm{ram}}$). The inclusions claimed in Theorem (6.6) therefore now follow from Lemma (4.9) upon noting that Theorem (2.10) (d) shows $\nu^{(\ell)}_{mp^n} \in I(\mathcal{D}^{(\ell)}_{mp^n})^2$ for every prime number ℓ that belongs to the subset $C_0^{(p)}(m) \cup C_2^{(p)}(K)$ of the set $\mathscr{Y}(K)$ appearing in Lemma (4.9). □

6.3. Congruences for Mazur–Tate elements

In this section we will prove Theorem (1.7) as an application of the formalism of Bockstein morphisms from § B.3. We begin by introducing some general notation that will be in place throughout the section. We will assume the conditions of Theorem (1.7) to be valid in this section.

To do this, we fix a finite abelian extension L of $\mathbb{Q}$ and let K be a subfield of L. The relevant Galois groups will be denoted as $\mathcal{G} \coloneqq \mathrm{Gal}(L/\mathbb{Q})$, $G \coloneqq \mathrm{Gal}(K/\mathbb{Q})$, and $H \coloneqq \mathrm{Gal}(L/K)$. We denote the conductors of K and L as mp^n and $m'p^{n'}$, respectively, where $m, m' \in \mathbb{N}$ are coprime with p and $n, n' \geq 0$ are integers. As before, we write Π for the set of split-multiplicative primes of E, and $\Pi_{\mathrm{ram}} \subseteq \Pi$ for the subset of primes that ramify in L. Write $\Pi'_{\mathrm{ram}} \subseteq \Pi_{\mathrm{ram}}$ for the subset of primes that split completely in K and fix an ordering $\Pi'_{\mathrm{ram}} = \{\ell_1, \dots, \ell_s\}$, where we adopt the convention that $\ell_1 = p$ if $p \in \Pi'_{\mathrm{ram}}$. We define $M' \coloneqq m'p^{n'} \prod_{\ell\in\Pi'_{\mathrm{ram}}} \ell^{-\mathrm{ord}_\ell(m'p^{n'})}$ and take

$$Q \coloneqq (p\mathrm{Eul}_p(\sigma_p))^{\mathbf{1}_{M'}(p)} \cdot \mathrm{Tr}_{F_{m'p^{n'}}/L}(\mathfrak{k}_{m'p^{n'}})$$

with $\mathfrak{k}_{m'p^{n'}}$ the element constructed in Theorem (2.10). Note that Q belongs to $E_1(L_p)$ under the assumptions of Theorem (1.7). This uses Theorem (2.10) (b) and that $p\mathrm{Eul}_p(\sigma_p)$ belongs to $\mathbb{Z}_p[\mathcal{G}]^\times$ if p ramifies in L by Lemma (4.8) and the condition on M' assumed in Theorem (1.7). For any subset U of Π, we will use the abbreviations

$$\overline{\mathrm{SC}}^\bullet_U \coloneqq \mathrm{SC}^\bullet_{L,S(L),U,Q} \quad \text{and} \quad \overline{\mathrm{SC}}^\bullet_U \coloneqq \mathrm{SC}^\bullet_U \otimes^{\mathbb{L}}_{\mathbb{Z}_p[\mathcal{G}]} \mathbb{Z}_p[G].$$

The complexes $\overline{\mathrm{SC}}^\bullet_U$ inherits from $\mathrm{SC}^\bullet_U$ the properties of being perfect, acyclic outside degrees one and two, and that $H^1(\overline{\mathrm{SC}}^\bullet_U)$ is $\mathbb{Z}_p$-torsion free if $E(K)[p] = 0$.

6.3.1. Definition of Bockstein morphisms

By Lemmas (6.3) (b) and (6.4) (b) the module $Y_{L,\Pi'_{\mathrm{ram}}}$ is a quotient of $H^2(\mathrm{SC}^\bullet_\Pi)$. Write $\mathfrak{X}(\Pi'_{\mathrm{ram}})$ for the ordered set of $\mathbb{Z}_p[\mathcal{G}]$-generators of the module $Y_{L,\Pi'_{\mathrm{ram}}}$ that is induced by our choices

of places $\{w_1, \dots, w_s\}$ of L above $\{\ell_1, \dots, \ell_s\}$. As a special case of Definition (B.16), we then have Bockstein maps

$$\beta_i \colon H^1(\overline{\mathrm{SC}}^\bullet_\Pi) \xrightarrow{\beta_{\mathrm{SC}^\bullet_\Pi, I_H}} H^2(\mathrm{SC}^\bullet_\Pi) \otimes_{\mathbb{Z}_p[\mathcal{G}]} I_H/I_H^2 \longrightarrow Y_{L,\Pi'_{\mathrm{ram}}} \otimes_{\mathbb{Z}_p[\mathcal{G}]} I_H \xrightarrow{w_i^*} I_H/I_iI_H$$

with $I_i \coloneqq I(\mathcal{D}_L^{(\ell_i)})$ the augmentation ideal associated with the decomposition group $\mathcal{D}_L^{(\ell_i)}$ of ℓ_i. On the other hand, applying Definition (B.16) to the complexes $A^\bullet_{K,\ell_i}$ also provides us with 'local' Bockstein maps

$$\beta_i^{\mathrm{loc}} \colon H^1(A^\bullet_{K,\ell_i}) \xrightarrow{\beta_{A^\bullet_{K,\ell_i}, I_H}} H^2(A^\bullet_{L,\ell_i}) \otimes_{\mathbb{Z}_p[\mathcal{G}]} I_H/I_H^2 \xrightarrow{w_i^*} I_H/I_iI_H$$

that have already appeared in § 5.3. To state the relation between β_i and β_i^{loc}, we write $\mathrm{loc}_i \colon \overline{\mathrm{SC}}^\bullet_\Pi \to A^\bullet_{K,\ell_i}$ for the natural 'localisation morphism'. Since $H^2(\mathrm{loc}_i)$ agrees with the composite map $H^2(\overline{\mathrm{SC}}^\bullet_\Pi) \to Y_{K,\Pi'_{\mathrm{ram}}} \to Y_{K,\{\ell_i\}} = H^2(A^\bullet_{L,\ell_i})$, the naturality of the definition of Bockstein maps implies that we have a commutative diagram

$$\begin{array}{ccc} H^1(\overline{\mathrm{SC}}^\bullet_\Pi) & \xrightarrow{\beta_i} & I_H/I_iI_H \\ {\scriptstyle H^1(\mathrm{loc}_i)}\downarrow & & \| \\ H^1(A^\bullet_{K,\ell_i}) & \xrightarrow{\beta_i^{\mathrm{loc}}} & I_H/I_iI_H. \end{array} \tag{60}$$

To proceed, it is convenient to set $v_i \coloneqq (w_i)_{|K}$ and to recall that we have isomorphisms

$$I_H/I_iI_H \cong \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} (I(H)/I_iI(H)) \quad \text{and} \quad H^1(A^\bullet_{K,\ell_i}) \cong \mathbb{Z}_p[G] \otimes_{\mathbb{Z}_p} H^1(K_{v_i}, \mathbb{Z}_p(1)),$$

for the first of which we refer to [San14, (3)] for details. Since $H^1(\overline{\mathrm{SC}}^\bullet_\Pi)$ is $\mathbb{Z}_p$-free, we therefore obtain isomorphisms (cf. [MR16, Prop. A.6] or [San14, Lem. 2.5] for more details)

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(H^1(\overline{\mathrm{SC}}^\bullet_\Pi), I_H/I_iI_H) \xrightarrow{\simeq} H^1(\overline{\mathrm{SC}}^\bullet_\Pi)^* \otimes_{\mathbb{Z}_p} (I(H)/I_iI(H))$$

$$\mathrm{Hom}_{\mathbb{Z}_p[G]}(H^1(\overline{\mathrm{SC}}^\bullet_\Pi), H^1(A^\bullet_{K,\ell_i})) \xrightarrow{\simeq} H^1(\overline{\mathrm{SC}}^\bullet_\Pi)^* \otimes_{\mathbb{Z}_p} H^1(A^\bullet_{K,\ell_i}).$$

As in Proposition (B.17) (b), it follows that the maps β_i and $H^1(\mathrm{loc}_i)$ induce maps

$$(\textstyle\bigwedge_{1\le i\le s} \beta_i) \colon \bigcap^s_{\mathbb{Z}_p[G]} H^1(\overline{\mathrm{SC}}^\bullet_\Pi) \longrightarrow I(H)^s/\mathfrak{A}I(H)$$

$$(\textstyle\bigwedge_{1\le i\le s} H^1(\mathrm{loc}_i)) \colon \bigcap^s_{\mathbb{Z}_p[G]} H^1(\overline{\mathrm{SC}}^\bullet_\Pi) \longrightarrow \bigotimes_{i=1}^s H^1(A^\bullet_{K,\ell_i})$$

with $\mathfrak{A} \coloneqq \prod_{i=1}^s I_i$, and the diagram (60) implies that we have

$$(\textstyle\bigwedge_{1\le i\le s} \beta_i) = (\otimes_{i=1}^s \beta_i^{\mathrm{loc}}) \circ (\bigwedge_{1\le i\le s} H^1(\mathrm{loc}_i)). \tag{61}$$

6.3.2. Congruences for Bockstein morphisms

Recall that in § 3.2 we have defined a $\mathbb{Z}_p[\mathcal{G}]$-basis b_L of $T^+_{L/\mathbb{Q}}$. Let $\mathfrak{X}'(\Pi'_{\mathrm{ram}})$ denote the ordered set of generators of $T^+_{K/\mathbb{Q}} \oplus Y_{K,\Pi'_{\mathrm{ram}}}$ induced by $\{b_L\} \cup \mathfrak{X}(\Pi'_{\mathrm{ram}})$ and define

$$\overline{F}_U \coloneqq \vartheta_{\overline{\mathrm{SC}}^\bullet_U, \mathfrak{X}'(\Pi'_{\mathrm{ram}})} \colon \mathrm{Det}_{\mathbb{Z}_p[G]}(\overline{\mathrm{SC}}^\bullet_U)^{-1} \to \bigcap^s_{\mathbb{Z}_p[G]} H^1(\overline{\mathrm{SC}}^\bullet_{\Sigma,\Pi,Q})$$

as the relevant instance of Definition (B.2). We also write pr for the 'projection map'

$$\mathrm{Det}_{\mathbb{Z}_p[\mathcal{G}]}(\mathrm{SC}^\bullet_\Pi)^{-1} \to \mathrm{Det}_{\mathbb{Z}_p[\mathcal{G}]}(\mathrm{SC}^\bullet_\Pi)^{-1} \otimes_{\mathbb{Z}_p[\mathcal{G}]} \mathbb{Z}_p[G] \cong \mathrm{Det}_{\mathbb{Z}_p[G]}(\overline{\mathrm{SC}}^\bullet_{\Sigma,\Pi,Q})^{-1}$$

and $\mathfrak{z}_L$ for the element of $\mathrm{Det}_{\mathbb{Z}_p[\mathcal{G}]}(C^\bullet_{L,S(L)})^{-1}$ with $\Theta_{L,\Sigma}(\mathfrak{z}_L) = z_L^{\mathrm{Kato}}$ that exists by Theorem (3.6). With this notation in place, Proposition (B.17) (c) shows that

$$(F_\Pi \circ f_\Pi)(\mathfrak{z}_L) \equiv \big((\textstyle\bigwedge_{1\le i\le s} \beta_i) \circ \overline{F}_\Pi \circ \mathrm{pr} \circ f_\Pi\big)(\mathfrak{z}_L) \mod I_H\mathfrak{A} \tag{62}$$

with $F_\Pi \coloneqq F_{L,S(L),\Pi,Q}$ and $f_\Pi \coloneqq f_{L,S(L),\Pi,Q}$ as in Lemma (6.5).
Having computed the left-hand side of (62) in Lemma (6.5), we will explicitly calculate its right-hand side in the next section § 6.3.3. Theorem (1.7) is then obtained as a consequence of (62) and these calculations in § 6.3.4.

6.3.3. A computation of Bockstein morphisms

To state the next result, it is convenient to introduce the notation

$$\eta_{L/K} \coloneqq \big(\prod\nolimits_{\ell\in\Pi'_{\mathrm{ram}}} \mathrm{Tam}_\ell^{-1}\mathrm{Eul}_\ell(1)^{-1}\big)\cdot\big(\prod\nolimits_{\ell\in\Pi\setminus\Pi'_{\mathrm{ram}}} \mathrm{Eul}_\ell(\sigma_\ell)^{-1}\nu^{(\ell)}_{mp^n}\big)^{\#} \quad \in \mathbb{Q}_p[G_{mp^n}].$$

The following lemma then computes the right-hand side of (62).

(6.7) Lemma. *With notation as above, one has*

$$\big(\big(\bigwedge_{1\le i\le s}\beta_i\big)\circ\overline{F}_\Pi\circ\mathrm{pr}\circ f_\Pi\big)(\mathfrak{z}_L) = \eta_{L/K}\cdot\pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(z^{\mathrm{Kato}}_{M'},\mathfrak{k}_{M'}))\cdot\prod_{i=1}^{s}(\mathrm{rec}_{\ell_i}(q_{E,\ell_i})-1)$$

as an equality in $\mathbb{Z}_p[\mathcal{G}]/I_H\mathfrak{A}$.

In light of the relation (61), the first step towards proving this result will be the calculation of the image under the map $\bigwedge_{1\le i\le s}H^1(\mathrm{loc}_i)$ of the element

$$a_\Pi \coloneqq \big(\overline{F}_\Pi\circ\mathrm{pr}\circ f_\Pi\big)(\mathfrak{z}_L).$$

(6.8) Lemma. *In* $\bigotimes_{i=1}^s(\mathbb{Q}_p\otimes_{\mathbb{Z}_p}H^1(A^\bullet_{K,\ell_i}))$*, one has the equality*

$$\big(\bigwedge\nolimits_{1\le i\le s}H^1(\mathrm{loc}_i)\big)(a_\Pi) = \eta_{L/K}\cdot\pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(z^{\mathrm{Kato}}_{M'},\mathfrak{k}_{M'}))\cdot\otimes_{i=1}^s q_{E,\ell_i}. \tag{63}$$

Proof. Write $\overline{f}_{\Sigma,\Pi,Q}$ for the map obtained from $f_{L,\Sigma,\Pi,Q}$ via base-changing to $\mathbb{Z}_p[G]$ and set $\Pi^\star \coloneqq \Pi\setminus(\Pi_{\mathrm{ram}}\cup\Pi_{\mathrm{unr}})$. Since, by its definition, Π_{unr} does not contain p, it follows that $\Pi^\star$ is equal to $\{p\}$ if $p\in\Pi_{\mathrm{ram}}$ and empty otherwise. We also let $A\subseteq\{1,\dots,s\}$ be the subset with $\{\ell_i\mid i\in A\}=\Pi'_{\mathrm{ram}}$ (so $A=\{1,\dots,s\}$ if $p\notin\Pi'_{\mathrm{ram}}$ and $A=\{2,\dots,s\}$ otherwise).
We may then compute, using Proposition (B.7) and Theorem (5.2), that

$$\begin{aligned}
\big(\bigwedge\nolimits_{i\in A}H^1(\mathrm{loc}_i)\big)(a_\Pi) &= \big(\bigwedge\nolimits_{i\in A}H^1(\mathrm{loc}_i)\big)\big((\overline{F}_\Pi\circ\overline{f}_\Pi\circ\mathrm{pr})(\mathfrak{z}_L)\big)\\
&= \Big(\bigotimes_{i\in A}\vartheta_{K,\ell,v_i}(t_K^{(\ell_i)})\Big)\cdot\Big(\prod_{\ell\in\Pi\setminus\Pi'_{\mathrm{ram}}}\vartheta^0_{K,\ell}(x_\ell)\Big)^{\#}\cdot(\overline{F}_{\Pi^\star}\circ\overline{f}_{\Pi^\star})(\mathrm{pr}(\mathfrak{z}_L))\\
&= \Big(\bigotimes_{\ell\in\Pi'_{\mathrm{ram}}}(-\ell^{-(\mathrm{ord}_\ell(m')-1)}\mathrm{Eul}_\ell(1)^{-1}\otimes\ell)\Big)\\
&\qquad\cdot\Big(\prod_{\ell\in\Pi\setminus\Pi'_{\mathrm{ram}}}\mathrm{Eul}_\ell(\sigma_\ell)^{-1}\nu^{(\ell)}_m\Big)^{\#}\cdot(\overline{F}_{\Pi^\star}\circ\overline{f}_{\Pi^\star})(\mathrm{pr}(\mathfrak{z}_L)).
\end{aligned}$$

If $p\notin\Pi'_{\mathrm{ram}}$, then we can use Lemma (6.5) to compute that

$$\begin{aligned}
(\overline{F}_\varnothing\circ\overline{f}_\varnothing)(\mathrm{pr}(\mathfrak{z}_L)) &= (\pi_{L/K}\circ F_\varnothing\circ f_\varnothing)(\mathfrak{z}_L)\\
&= (p\mathrm{Eul}_p(\sigma_p^{-1}))^{-\mathbf{1}_{M'}(p)}\cdot\pi_{L/K}(\mathcal{P}_L(z^{\mathrm{Kato}}_L,Q))\\
&= \pi_{F_{m'p^{n'}}/K}(\mathcal{P}_L(z^{\mathrm{Kato}}_L,\mathfrak{k}_{m'p^{n'}})\\
&= \Big(\prod\nolimits_{\ell\in\Pi'_{\mathrm{ram}}\setminus\{p\}}(-1)\cdot\ell^{\mathrm{ord}_\ell(m')-1}\Big)\cdot\pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(z^{\mathrm{Kato}}_{M'},\mathfrak{k}_{M'})),
\end{aligned}$$

where the last equality is a consequence of Theorem (2.10) (c),(ii). Since $\mathrm{ord}_\ell(q_{E,\ell})=\mathrm{Tam}_\ell$ for all $\ell\in\Pi'_{\mathrm{ram}}$, this proves the claimed equality in the case $p\notin\Pi'_{\mathrm{ram}}$.
It remains to consider the case that p belongs to Π'_{ram}. In this case, one has

$$\Big(\prod\nolimits_{\ell\in\Pi'_{\mathrm{ram}}\setminus\{p\}}(-1)\cdot\ell^{\mathrm{ord}_\ell(m')-1}\Big)\cdot\pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(z^{\mathrm{Kato}}_{M'},\mathfrak{k}_{M'})) = \pi_{F_{m'}/K}(\mathcal{P}_{F_{m'}}(h^1_p(z^{\mathrm{Kato}}_{m'}),\mathfrak{k}_{F_{m'}}))$$

and so, writing $h^1_p\coloneqq H^1(h_p)$ for the map induced on cohomology by the map h_p in (50), it suffices to prove that

$$(\mathrm{loc}_p\circ\overline{F}_{\{p\}}\circ\overline{f}_{\{p\}})(\mathrm{pr}(\mathfrak{z}_L)) = \pi_{F_{m'}/K}(\mathcal{P}_{F_{m'}}(h^1_p(z^{\mathrm{Kato}}_{m'}),\mathfrak{k}_{F_{m'}}))\cdot q_{E,p}. \tag{64}$$

The equation (64) can be proved via an argument very similar to Proposition (B.7) (b) which we now briefly sketch.

Since p is assumed to split completely, $\mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{Z}_p(1)_{K/\mathbb{Q}})$ and $\mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{Z}_{p,K/\mathbb{Q}})$ are represented by $[\widehat{K_p^\times} \xrightarrow{0} \mathbb{Z}_p[G]]$ (first term in degree 1) and $[\mathbb{Z}_p[G] \xrightarrow{0} (\widehat{K_p^\times})^*]$ (first term in degree 0), respectively. In particular, it follows from $(\vartheta_{K,p,v_0} \circ \mathrm{pr}_{L/K})(t_L^{(p)}) = \mathrm{N}_{F_{m'p^n}/K}(\mathfrak{l}_{F_{m'}}) \wedge p$, as is proved in Theorem (5.2) (b), that $t_K^{(p)}$ can be described as the element $(\mathrm{N}_{F_{m'}/K}(\mathfrak{l}_{F_{m'}}) \wedge p) \otimes \mathrm{id}_{\mathbb{Z}_p[G]}$ of $(\bigwedge^2_{\mathbb{Z}_p[G]} \widehat{K_p^\times}) \otimes_{\mathbb{Z}_p[G]} \mathbb{Z}_p[G]^* = \mathrm{Det}_{\mathbb{Z}_p[G]}(\mathrm{R}\Gamma(\mathbb{Q}_p, \mathbb{Z}_p(1)_{K/\mathbb{Q}}))^{-1}$.

We now write $[P \xrightarrow{\partial} P]$ for the representative of $C^\bullet_{K,S(L)}$ constructed in Lemma (3.5) (b). Here P is a finitely generated free $\mathbb{Z}_p[G]$-module of rank n, say, and we choose a $\mathbb{Z}_p[G]$-basis $x_1, \dots, x_n$ such that the composite map $P \to H^2(C^\bullet_{K,S(L)}) \xrightarrow{\pi} (T^+_{K/\mathbb{Q}})$ sends x_1 to the element b^* defined in § 3.2. It follows from the triangle (53) and a standard mapping cone construction that the complex $\overline{\mathrm{SC}}^\bullet_{\Sigma,\{p\},Q}$ admits a representative of the form $[P \oplus \mathbb{Z}_p[G] \xrightarrow{(\partial \oplus \varphi, 0)} P \oplus (\widehat{K_p^\times})^*]$ with the map

$$\varphi\colon P \to (\widehat{K_p^\times})^*, \quad y \mapsto \{z \mapsto (h_p(z), z)_{\mathbb{G}_m/K}\},$$

where $(\cdot,\cdot)_{\mathbb{G}_m/K}$ denotes the cup product pairing $H^1(\mathbb{Q}_p, \mathbb{Z}_{p,K/\mathbb{Q}}) \times H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)_{K/\mathbb{Q}}) \to \mathbb{Z}_p$ (analogous to (4)). Given $a = a_1 \otimes (\bigwedge_{1 \le i \le n} x_i^*)$ in $\mathrm{Det}_{\mathbb{Z}_p[G]}(C^\bullet_{K,S(L)})^{-1} = (\bigwedge^n_{\mathbb{Z}_p[G]} P) \otimes_{\mathbb{Z}_p[G]} (\bigwedge^n_{\mathbb{Z}_p[G]} P^*)$, one then has

$$\mathrm{Ev}_{t_K^{(p)}}(a) = (a_1 \wedge 1) \otimes \big((\bigwedge\nolimits_{1 \le i \le n} x_i^*) \wedge (\mathrm{N}_{F_{m'}/K}(\mathfrak{l}_{F_{m'}}) \wedge p) \big)$$

when regarded as an element of

$$\mathrm{Det}_{\mathbb{Z}_p[G]}(\overline{\mathrm{SC}^\bullet_{\{p\}}})^{-1} = \big(\bigwedge\nolimits^{n+1}_{\mathbb{Z}_p[G]} (P \oplus \mathbb{Z}_p[G]) \big) \otimes_{\mathbb{Z}_p[G]} \big(\bigwedge\nolimits^{n+2}_{\mathbb{Z}_p[G]} (P^* \oplus \widehat{K_p^\times}) \big).$$

Now, the module $Y_{K,\{p\}}$ is identified with the $\mathbb{Z}_p[G]$-submodule of $(\widehat{K_p^\times})^*$ generated by the map Ord_p (which is the $\mathbb{Z}_p[G]$-dual basis element of p) so that we have $\mathfrak{X}'(\{p\}) = (x_1, p)$. The explicit description of $\vartheta_{\overline{\mathrm{SC}}^\bullet_{\Sigma,\{p\},Q}, \mathfrak{X}'(\Pi'_{\mathrm{ram}})}$ given in Lemma (B.5) therefore allows us to calculate that

$$\begin{aligned}
(\overline{F}_{\{p\}} \circ \overline{f}_{\{p\}})(\mathrm{pr}(\mathfrak{z}_L)) &= \sum\nolimits_{\sigma \in G} \big((h_p^1 \circ \bigwedge\nolimits_{2 \le i \le n} (x_i^* \circ \partial))(\sigma a_1), \mathrm{N}_{F_{m'}/K}(\mathfrak{l}_{F_{m'}}) \big)_{\mathbb{G}_m/K} \sigma^{-1} \\
&= \sum\nolimits_{\sigma \in G} ((h_p^1 \circ \Theta_{K,S(L)})(\sigma a), \mathrm{N}_{F_{m'}/K}(\mathfrak{l}_{F_{m'}}))_{\mathbb{G}_m/K} \sigma^{-1}
\end{aligned}$$

in $\mathbb{Z}_p[G] = H^0(\mathbb{Q}_p, \mathbb{Z}_{p,K/\mathbb{Q}})$. The connecting homomorphism $H^0(\mathbb{Q}_p, \mathbb{Z}_{p,K/\mathbb{Q}}) \to H^1(\mathbb{Q}_p, \mathbb{Z}_p(1)_{K/\mathbb{Q}})$ sends 1 to $q_{E,p}$ by Remark (6.1), hence we conclude that

$$\begin{aligned}
(H^1(\mathrm{loc}_1) \circ \overline{F}_{\{p\}} \circ \overline{f}_{\{p\}})(\mathrm{pr}(\mathfrak{z}_L)) &= \pi_{F_{m'}/K} \big(\sum\nolimits_{\sigma \in G_{m'}} (h_p^1(\sigma z_{m'}^{\mathrm{Kato}}), \mathfrak{l}_{F_{m'}})_{\mathbb{G}_m/F_{m'}} \sigma^{-1} \big) \cdot q_{E,p} \\
&= \pi_{F_{m'}/K} \big(\mathcal{P}_{F_{m'}}(z_{m'}^{\mathrm{Kato}}, \mathfrak{k}_{F_{m'}}) \big) \cdot q_{E,p},
\end{aligned}$$

as claimed in (64). This concludes the proof of the lemma. □

We can now give the proof of Lemma (6.7).

Proof (of Lemma (6.7)). As a first step, we use Lemma (6.8) to calculate $(\bigwedge_{1 \le i \le s} H^1(\mathrm{loc}_i))(a_\Pi)$. An extra argument is necessary because Lemma (6.8) only gives an equality in a $\mathbb{Q}_p$-vector space and so does not contain information about the torsion component.
To do this, we note that we have the commutative diagram

$$\begin{array}{ccccccc}
 & & \bigoplus_{i=1}^s H^0(\mathbb{Q}_{\ell_i}, \mathbb{Z}_{p,K/\mathbb{Q}}) & \longrightarrow & H^1(\overline{\mathrm{SC}}^\bullet_\Pi) & \longrightarrow & H^1(\mathcal{O}_{K,S(L)}, \mathrm{T}_p E) \\
 & & \downarrow \simeq & & \downarrow \oplus_{i=1}^s H^1(\mathrm{loc}_i) & & \downarrow \\
0 & \longrightarrow & \bigoplus_{i=1}^s \mathbb{Z}_p[G] & \xrightarrow{\oplus_{i=1}^s \delta_i} & \bigoplus_{i=1}^s H^1(A^\bullet_{K,\ell_i}) & \longrightarrow & \bigoplus_{i=1}^s H^1(\mathbb{Q}_{\ell_i}, T_{K/\mathbb{Q}}),
\end{array}$$

where the bottom line is induced by the exact sequence (49). By Remark (6.1), the connecting homomorphism arising from (49), labelled δ_i in the diagram above, sends 1 to $q_{E,\ell_i} \in \widehat{K_{v_i}^\times}$

with $v_i \coloneqq (w_i)_{|_K}$ our fixed choice of place of K above ℓ_i (that also induces the isomorphism $H^0(\mathbb{Q}_{\ell_i}, \mathbb{Z}_{p,K/\mathbb{Q}}) \cong \mathbb{Z}_p[G]$). This shows that $\otimes_{i=1}^s q_{E,\ell_i}$ is contained in the image of the composite map

$$\bigotimes_{i=1}^{s} H^0(\mathbb{Q}_{\ell_i}, \mathbb{Z}_{p,K/\mathbb{Q}}) \to \bigcap\nolimits_{\mathbb{Z}_p[G]}^{s} H^1(\overline{\mathrm{SC}}_{\Pi}^{\bullet}) \xrightarrow{\bigwedge_{1\le i\le s} H^1(\mathrm{loc}_i)} \bigotimes_{i=1}^{s} H^1(A_{K,\ell_i}^{\bullet}).$$

In particular, $\otimes_{i=1}^s q_{E,\ell_i}$ is contained in the image of $\bigwedge_{1\le i\le s} H^1(\mathrm{loc}_i)$. Moreover, we know that

$$\eta_{L/K} \cdot \pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(z_{M'}^{\mathrm{Kato}}, \mathfrak{k}_{M'})) = \eta_{L/K} \cdot \pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(\Theta_{F_{M'},S(F_{M'})}(\mathfrak{z}_{F_{M'}}), \mathfrak{k}_{M'}))$$

belongs to $\mathbb{Z}_p[G]$ by (30) in Proposition (4.6) (here we have used that each $\mathrm{Eul}_\ell(\sigma_\ell)^{-1}\nu_m^{(\ell)}$ belongs to the ideal $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1}\mathrm{N}_{\mathcal{I}^{(\ell)}}\mathbb{Z}_p[G] + \mathbb{Z}_p[G]$ of $\mathbb{Q}_p[G]$ for every $\ell \in \Pi$ by Theorem (2.10) (d), and Tam_ℓ^{-1} generates $\mathrm{Ann}_{\mathbb{Z}_p[G]}((E/E_0)(K_\ell))$ if $\ell \in \Pi'$). We have therefore proved that

$$\eta_{L/K} \cdot \pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(z_{M'}^{\mathrm{Kato}}, \mathfrak{k}_{M'})) \cdot (\otimes_{i=1}^s q_{E,\ell_i}) \in (\bigwedge\nolimits_{1\le i\le s} H^1(\mathrm{loc}_i))\big(\bigcap\nolimits_{\mathbb{Z}_p[G]}^{s} H^1(\overline{\mathrm{SC}}_{\Pi}^{\bullet})\big). \quad (65)$$

Now, the composite map

$$(\bigwedge\nolimits_{1\le i\le s} H^1(\mathrm{loc}_i))\big(\bigcap\nolimits_{\mathbb{Z}_p[G]}^{s} H^1(\overline{\mathrm{SC}}_{\Pi}^{\bullet})\big) \xrightarrow{\subseteq} \bigotimes_{i=1}^{s} H^1(A_{K,\ell_i}^{\bullet}) \to \bigotimes_{i=1}^{s} (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(A_{K,\ell_i}^{\bullet}))$$

is injective (because $\bigcap_{\mathbb{Z}_p[G]}^s H^1(\overline{\mathrm{SC}}_{\Pi}^{\bullet})$ is $\mathbb{Z}_p$-torsion free) and so we conclude from (65) that the equality (63) of Lemma (6.8)) in fact already holds in $\bigotimes_{i=1}^s H^1(A_{K,\ell_i}^{\bullet})$. By (61) and Lemma (5.5), this argument shows that

$$(\bigwedge\nolimits_{1\le i\le s} \beta_i)(a_\Pi) = \eta_{L/K} \cdot \pi_{F_{M'}/K}(\mathcal{P}_{F_{M'}}(z_{M'}^{\mathrm{Kato}}, \mathfrak{k}_{M'})) \cdot \prod\nolimits_{i=1}^{s} (\mathrm{rec}_{\ell_i}(q_{E,\ell_i}) - 1),$$

as required to prove Lemma (6.7). □

6.3.4. The proof of Theorem (1.7)

We now explain how the congruence (62) implies Theorem (1.7). By assumption, $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)$ belongs to $\mathbb{Z}_p[\mathcal{G}]^\times$ for every $\ell \notin \Pi$ that divides m'. In addition, Lemma (2.18) shows that

$$\pi_{F_{m'p^{n'}}/L}\Big(\prod_{\ell|m',\ell\notin\Pi} (\nu_{m'p^{n'}}^{(\ell)}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1})^{\#}\Big) \equiv \pi_{F_{M'}/L}\Big(\prod_{\ell|m',\ell\notin\Pi} (\nu_{M'}^{(\ell)}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1})^{\#}\Big) \mod I_H. \quad (66)$$

If we multiply (62) by (66) we then obtain a new congruence valid in $\mathfrak{A}/I_H\mathfrak{A}$. Using Lemma (6.5) and Theorem (2.10) (a) for the left-hand side of this new congruence, and Lemma (6.7) for its right-hand side, we obtain (notice the change from $z_{M'}^{\mathrm{Kato}}$ to $y_{M'}^{\mathrm{Kato}}$)

$$\begin{aligned}\theta_L^{\mathrm{MT}} &\equiv \pi_{F_{M'}/K}\big((\prod_{\ell|M',\ell\neq p} \nu_{M'}^{(\ell)}\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)^{-1})^{\#} \cdot \mathcal{P}_{F_{M'}}(y_{M'}^{\mathrm{Kato}}, \mathfrak{k}_{M'})\big) \cdot \big(\prod_{i=1}^{s} \mathrm{Tam}_\ell^{-1}(\mathrm{rec}_\ell(q_{E,\ell_i}) - 1)\big) \\ &\equiv \pi_{F_{M'}/K}(\theta_{M'}^{\mathrm{MT}}) \cdot \big(\prod_{i=1}^{s} \mathrm{Tam}_\ell^{-1}(\mathrm{rec}_\ell(q_{E,\ell_i}) - 1)\big) \mod \mathfrak{A}I_H.\end{aligned}$$

For this congruence we are also (again) using that we have assumed $\ell \in C_\times^{(p)}(L)$, and therefore that $\mathrm{Eul}_\ell(\tilde{\sigma}_\ell)$ is invertible in $\mathbb{Z}_p[\mathcal{G}]$ by Lemma (4.8), for all $\ell \mid m'$. The final congruence is then by Theorem (2.10) (a).
This concludes the proof of Theorem (1.7). □

(6.9) Remark. It seems possible that the technical condition on M' in Theorem (1.7) can be removed if one combines the calculations of this section with the argument of Lemma (4.9).

A. Integrality of Mazur–Tate elements

In this appendix we derive integrality results for Mazur–Tate elements by following ideas of Stevens [Ste89, § 3] with refinements due to Wiersema and Wuthrich [WW22].

Statement of the main result We write

$$\varphi_0 \colon X_0(N) \to E \quad \text{and} \quad \varphi_1 \colon X_1(N) \to E$$

for the modular parametrisations of E. We then define the Manin and Manin–Stevens constants c_0 and c_1 by the relations

$$\varphi_0^* \omega_E = c_0 \cdot \omega_f \quad \text{and} \quad \varphi_1^* \omega_E = c_1 \cdot \omega_f,$$

where $\omega_f \coloneqq f(q)\frac{\mathrm{d}q}{q}$ is the differential 1-form associated to f. It was first observed by Gabber that c_0 and c_1 are (nonzero) integers (see [Edi91, Prop. 2] and [Ste89, Thm. 1.6]). Manin has conjectured that $c_0 \in \{\pm 1\}$ for some curve in the isogeny class in E (namely the strong Weil curve) and Stevens has conjectured that always $c_1 \in \{\pm 1\}$ (see [Ste89, Conj. 1]).

(A.1) Remark. It is known that if p is a prime number that divides c_1, then p^2 must divide the conductor N of E (for odd p this was proved by Mazur [Maz78], and for $p = 2$ by Česnavičius [Čes18]). This shows that $c_1 \in \{\pm 1\}$ if E is 'semistable' (that is, N is square-free).
In addition, Česnavičius–Neururer–Saha [ČNS24] have proved that c_1 divides the degree of φ_1, and this can often be used to rule out that a given additive prime divides c_1.

Although, to the best of the authors' knowledge, the following result on the integrality of Mazur–Tate elements has not previously appeared in the literature in this exact form, it is probably well-known to experts.
To state this result, we write $D(m) \coloneqq \gcd(m, N)$ and $\delta(m) \coloneqq \gcd(D(m), \frac{N}{D(m)})$.

(A.2) Theorem. *For every $m \in \mathbb{N}$, one has*

$$c_\infty c_0 \mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{\delta(m)})_{\mathrm{tor}}) \cdot \theta_m^{\mathrm{MT}} \subseteq \mathbb{Z}[G_m]$$

and

$$c_\infty c_1 \mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{D(m)})_{\mathrm{tor}}) \cdot \theta_m^{\mathrm{MT}} \subseteq \mathbb{Z}[G_m].$$

The proof of Theorem (A.2) We define the *Néron lattice* $\mathscr{L}_E$ of E to be

$$\mathscr{L}_E \coloneqq \Big\{ \int_\gamma \omega \mid \gamma \in H_1(E(\mathbb{C}), \mathbb{Z}) \Big\} = \begin{cases} \frac{1}{2}\mathbb{Z}\Omega^+ \oplus \mathbb{Z}\Omega^- & \text{if } c_\infty = 2, \\ \mathbb{Z}\Omega^+ \oplus \frac{1}{2}\mathbb{Z}(\Omega^+ + \Omega^-) & \text{if } c_\infty = 1. \end{cases} \tag{67}$$

We define the 'Stevens element' as

$$\theta_m^{\mathrm{St}} \coloneqq \sum\nolimits_{a \in (\mathbb{Z}/m\mathbb{Z})^\times} \lambda_f(\tfrac{a}{m})\sigma_a \quad \in \mathbb{C}[G_m].$$

Recall that we have defined the modular symbol $\lambda_f(\frac{a}{m})$ at the start of § 2.1.

(A.3) Lemma. *The lattice $\mathscr{L}_E \otimes_{\mathbb{Z}} \mathbb{Z}[G_m]$ contains both $c_0 \mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{\delta(m)})_{\mathrm{tor}}) \cdot \theta_m^{\mathrm{St}}$ and $c_1 \mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{D(m)})_{\mathrm{tor}}) \cdot \theta_m^{\mathrm{St}}$ for every $m \in \mathbb{N}$.*

We now first explain how to deduce Theorem (A.2) from Lemma (A.3). Consider the maps

$$\mathrm{Re} \colon \mathbb{C}[G_m] \to \mathbb{R}[G_m], \quad \sum\nolimits_{\sigma \in G_m} x_\sigma \sigma \mapsto \sum\nolimits_{\sigma \in G_m} \mathrm{Re}(x_\sigma)\sigma$$
$$\mathrm{Im} \colon \mathbb{C}[G_m] \to \mathbb{R}[G_m], \quad \sum\nolimits_{\sigma \in G_m} x_\sigma \sigma \mapsto \sum\nolimits_{\sigma \in G_m} \mathrm{Im}(x_\sigma)\sigma.$$

Observe that these maps are $\mathbb{R}[G_m]$-linear. Using the explicit description of $\mathscr{L}_E$ given in (67), we obtain that for every element $\alpha \in \mathscr{L}_E \otimes_{\mathbb{Z}} \mathbb{Z}[G_m]$ one has

$$\frac{\mathrm{Re}(\alpha)}{\Omega^+} + i\frac{\mathrm{Im}(\alpha)}{\Omega^-} \in \frac{1}{c_\infty}\mathbb{Z}[G_m]. \tag{68}$$

We consider the c_0 case, the c_1 case is similar. Fix an element x of $\mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{\delta(m)})_{\mathrm{tor}})$. Lemma (A.3) then combines with (68) to imply that

$$c_\infty c_0 x \cdot \Big(\frac{\mathrm{Re}(\theta_m^{\mathrm{St}})}{\Omega^+} + i\frac{\mathrm{Im}(\theta_m^{\mathrm{St}})}{\Omega^-} \Big) = \frac{c_\infty \mathrm{Re}(c_0 x \cdot \theta_m^{\mathrm{St}})}{\Omega^+} + i\frac{c_\infty \mathrm{Im}(c_0 x \cdot \theta_m^{\mathrm{St}})}{\Omega^-} \subseteq \mathbb{Z}[G_m].$$

To prove Theorem (A.2), it therefore suffices to note that

$$\theta_m^{\mathrm{MT}} = \sum\nolimits_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}([\tfrac{a}{m}]^+ + [\tfrac{a}{m}]^-)\sigma_a = \sum\nolimits_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}\Big(\frac{\mathrm{Re}(\lambda_f(\frac{a}{m}))}{\Omega^+} + i\frac{\mathrm{Im}(\lambda_f(\frac{a}{m}))}{\Omega^-}\Big)\sigma_a$$
$$= \frac{\mathrm{Re}(\theta_m^{\mathrm{St}})}{\Omega^+} + i\frac{\mathrm{Im}(\theta_m^{\mathrm{St}})}{\Omega^-}.$$

We now turn to the proof of Lemma (A.3), again in the c_0 case. At the outset we note that

$$\lambda_f(a) = 2\pi i\int_{i\infty}^{a} f(\tau)\mathrm{d}\tau = c_0^{-1}\int_{\gamma(a)}\omega,$$

where $\gamma(a)$ is the image in $E(\mathbb{C})$ of the path from $i\infty$ to a given by the vertical line in the upper half-plane from $i\infty$ to a. Writing $\mathcal{H}\subseteq\mathbb{C}$ for the complex upper half-plane, one therefore has the commutative diagram (see, for example, [Dar04, Prop. 2.11])

$$\begin{array}{ccc}(\mathbb{P}^1(\mathbb{Q})\cup\mathcal{H})/\sim & = & X_0(N)(\mathbb{C})\\ \downarrow{\scriptstyle c_0\lambda_f} & & \downarrow{\scriptstyle\varphi_0}\\ \mathbb{C}/\mathscr{L}_E & \xrightarrow{\ \simeq\ } & E(\mathbb{C}).\end{array}$$

For any cusp $a\in\mathbb{P}^1(\mathbb{Q})$ we then write $P_a := \varphi_0(a)$ for the point in $E(\overline{\mathbb{Q}})$ corresponding to $c_0^{-1}\lambda_f(a)+\mathscr{L}_E$, and we note that P_a is a torsion point by the Manin–Drinfeld theorem.
From this it is clear that $c_0\lambda_f(a)$ belongs to $\mathscr{L}_E$ if and only if P_a is trivial.
It is proved in [Ste82, Thm. 1.3.1] that any cusp $\frac{r}{s}$ of $X_0(N)$ (with $\gcd(r,s)=1$) is defined over $\mathbb{Q}(\zeta_N)$ and that the action of G_N on $\frac{r}{s}$ is given by

$$\sigma_a\cdot\frac{r}{s} = \frac{a^{-1}r}{s},$$

where a^{-1} denotes the inverse of a mod N. We note that in [Ste82, Thm. 1.3.1] the description of Galois action has the inverted element in the denominator rather than the numerator. However, these two cusps are equivalent in $X_0(n)$, see [DS06, Prop. 3.8.3]. Take $s=m$ and suppose that $a\equiv 1 \mod \delta(m)$. Then also $a^{-1}\equiv 1 \mod \delta(m)$, hence $\frac{a^{-1}r}{m}$ is $\Gamma_0(N)$-equivalent to $\frac{r}{m}$ (this can be deduced from [DS06, Prop. 3.8.3], see the argument on page 103 of loc. cit.). As a consequence, the subgroup $\{\sigma_a \mid (a,N)=1, a\equiv 1 \mod\delta(m)\} = \mathrm{Gal}(F_N/F_{\delta(m)})$ fixes the cusp $\frac{r}{m}$, and so any such cusp is defined over $F_{\delta(m)}$.
We next observe that the map

$$\mathbb{P}^1(\mathbb{Q})\to E(\overline{\mathbb{Q}})_{\mathrm{tor}},\quad a\mapsto P_a=\varphi_0(a)$$

is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant because the modular parametrisation φ_0 is defined over $\mathbb{Q}$ (hence $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant). It follows that the point P_a belongs to $E(F_{\delta(m)})_{\mathrm{tor}}$ for every cusp $a\in\mathbb{P}^1(\mathbb{Q})$ of the form $a=\frac{r}{m}$. Now, we extend the earlier diagram $\mathbb{Z}[G_m]$-linearly to obtain the commutative diagram of $\mathbb{Z}[G_m]$-modules

$$\begin{array}{ccc}\mathbb{P}^1(\mathbb{Q}) & \longrightarrow & \mathbb{C}[G]\\ \downarrow & & \downarrow\\ E(F_m)_{\mathrm{tor}}\otimes_{\mathbb{Z}}\mathbb{Z}[G_m] & \hookrightarrow & (\mathbb{C}/\mathscr{L}_E)[G_m].\end{array}$$

Here the top map sends the class of $\frac{1}{m}$ to $\sum_{\sigma\in G_m}\lambda_f(\sigma\cdot\frac{1}{m})\sigma^{-1} = \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}\lambda_f(\frac{a}{m})\sigma_a = \theta_m^{\mathrm{St}}$, and the vertical map on the left sends $\frac{1}{m}$ to $\sum_{\sigma\in G_m}(\sigma\cdot P_{1/m})\sigma^{-1} = \sum_{a\in(\mathbb{Z}/m\mathbb{Z})^\times}P_{a/m}\sigma_a$.
We have seen above that each of the points $P_{a/m}$ belongs to $E(F_{\delta(m)})_{\mathrm{tor}}$, hence the latter element is annihilated by $\mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{\delta(m)})_{\mathrm{tor}})$. Commutativity of the above diagram therefore shows that the class of θ_m^{St} in the quotient $(\mathbb{C}/\mathscr{L}_E)[G_m]$ is annihilated by $\mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{\delta(m)})_{\mathrm{tor}})$, as required to prove that $\mathrm{Ann}_{\mathbb{Z}[G_m]}(E(F_{\delta(m)})_{\mathrm{tor}})\cdot\theta_m^{\mathrm{St}}$ belongs to $\mathscr{L}[G_m]$.
When considering the c_1 case we note that [Ste89, Thm. 3.11] shows that the cusps of $X_1(N)$ is defined over $\mathbb{Q}(\zeta_N)$ and that the action of G_N is as defined before. Let $a'\equiv 1 \mod m$. It

follows from [DS06, Prop. 3.8.3] that $\frac{r}{m} \sim \frac{a'r}{m}$. Hence, the subgroup $\{\sigma_a \mid (a,m) = 1, a \equiv 1 \bmod D(m)\} = \mathrm{Gal}(F_N/F_{D(m)})$ fixes the cusp $\frac{a}{m}$. The result in this case then follows as before. □

B. Some general algebra

In this section we establish useful results of a general algebraic nature.

B.1. Perfect complexes and their determinants

Let $\mathcal{R}$ be a Noetherian commutative ring. For any $\mathcal{R}$-module M, we endow its $\mathcal{R}$-linear dual $M^* \coloneqq \mathrm{Hom}_{\mathcal{R}}(M, \mathcal{R})$ with the structure of an $\mathcal{R}$-module by means of

$$\mathcal{R} \times M^* \to M^*, \quad (x, f) \mapsto \{y \mapsto x \cdot f(y)\}.$$

We also set $M^\vee \coloneqq \mathrm{Hom}_{\mathcal{R}}(M, \mathcal{Q}/\mathcal{R})$ with $\mathcal{Q}$ the total ring of fractions of $\mathcal{R}$.

(B.1) Remark. Note that in the main text the notation $M^\vee$ was used for the Pontryagin dual $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ of M, which might differ from $\mathrm{Hom}_{\mathcal{R}}(M, \mathcal{Q}/\mathcal{R})$. For example, if $\mathcal{R} = \mathbb{Z}[G]$ for a finite abelian group G, then (3) induces an isomorphism $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})^\# \cong \mathrm{Hom}_{\mathcal{R}}(M, \mathcal{Q}/\mathcal{R})$.

We write $D(\mathcal{R})$ for the derived category of $\mathcal{R}$-modules, and $D^{\mathrm{perf}}(\mathcal{R})$ for its full subcategory of complexes that are 'perfect' (that is, isomorphic in $D(\mathcal{R})$ to a bounded complex of projective $\mathcal{R}$-modules).
Given $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ represented by a bounded complex $\ldots \to C^{i-1} \to C^i \to C^{i+1} \to \ldots$ of projective $\mathcal{R}$-modules C^i that are each placed in degree i, we denote its Euler characteristic as $\chi_{\mathcal{R}}(C^\bullet) \coloneqq \sum_{i \in \mathbb{Z}} (-1)^i \cdot [C^i] \in K_0(\mathcal{R})$. Here $K_0(\mathcal{R})$ denotes the Grothendieck group of the category of finitely generated projective R-modules. If $\mathcal{R}$ is semisimple, then the rank function induces an isomorphism $K_0(R) \cong H^0(\mathrm{Spec}\,\mathcal{R}, \mathbb{Z})$ and so we may regard $\chi_{\mathcal{R}}(C^\bullet)$ as an element of $H^0(\mathrm{Spec}\,\mathcal{R}, \mathbb{Z})$. In this case we write $\chi_{\mathcal{R}}(C^\bullet) \leq d$ if $\chi_{\mathcal{R}}(C^\bullet)$ belongs to $H^0(\mathrm{Spec}\,\mathcal{R}, \mathbb{Z}_{\leq d})$.
The determinant of $C^\bullet$ is denoted by $\mathrm{Det}_{\mathcal{R}}(C^\bullet) \coloneqq \bigotimes_{i \in \mathbb{Z}} \mathrm{Det}_{\mathcal{R}}(C^i)^{(-1)^i}$. In this context we remark that, following Knudsen and Mumford [KM76], $\mathrm{Det}_{\mathcal{R}}(C^\bullet)$ must be considered a graded line bundle in order to avoid technical sign issues. However, since the grading is uniquely determined upon fixing a representative for $C^\bullet$, we have chosen to suppress any explicit reference to the grading in order to simplify the exposition.
For every element $a \in \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} \coloneqq \mathrm{Det}_{\mathcal{R}}(C^\bullet)^*$ we also obtain a canonical 'evaluation map'

$$\mathrm{Ev}_a \colon \mathrm{Det}_{\mathcal{R}}(C^\bullet) \to \mathcal{R}.$$

The following definition underlies many of the constructions in the main text.

(B.2) Definition. *Let $\mathcal{R}$ be a Noetherian reduced ring with total ring of fractions $\mathcal{Q}$. Let $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ be a complex, and fix a surjection $\kappa \colon H^2(C^\bullet) \to \mathcal{Y}$ with $\mathcal{Y}$ a finitely generated free $\mathcal{R}$-module of rank $d \geq \chi \coloneqq \chi_{\mathcal{Q}}(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\bullet)$ together with an ordered $\mathcal{R}$-basis $\mathfrak{B}$ of $\mathcal{Y}$. We define a canonical map as the composite*

$$\begin{aligned}
\vartheta_{C^\bullet, \mathfrak{B}} \colon \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} &\hookrightarrow \mathcal{Q} \otimes_{\mathcal{R}} \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} \\
&\xrightarrow{\simeq} \mathrm{Det}_{\mathcal{Q}}(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\bullet)^{-1} \\
&\xrightarrow{\simeq} \bigotimes\nolimits_{i \in \mathbb{Z}} \mathrm{Det}_{\mathcal{Q}}(H^i(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\bullet))^{(-1)^{i+1}} \\
&\xrightarrow{\cdot e_{C^\bullet, \mathcal{Y}}} \mathrm{Det}_{\mathcal{Q}}(H^1(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\bullet)) \otimes_{\mathcal{Q}} \mathrm{Det}_{\mathcal{Q}}(\mathcal{Q} \otimes_{\mathcal{R}} \mathcal{Y})^{-1} \\
&\xrightarrow{\simeq} \textstyle\bigwedge_{\mathcal{Q}}^{d-\chi}(\mathcal{Q} \otimes_{\mathcal{R}} H^1(C^\bullet)).
\end{aligned}$$

Here the second arrow follows from the base-change property of the determinant functor, the third arrow is the natural 'passage-to-cohomology map' (which exists because $\mathcal{Q}$ is semisimple),

the fourth arrow is multiplication by the idempotent $e_{C^\bullet,\mathcal{Y}}$ of $\mathcal{Q}$ that is defined as the sum of all primitive idempotents of $\mathcal{Q}$ that annihilate $\mathcal{Q}\otimes_{\mathcal{R}}\big((\ker\kappa)\oplus\bigoplus_{i\in\mathbb{Z}\setminus\{1,2\}}H^i(C^\bullet)\big)$, and the final isomorphism is induced by Ev_x with the element $x\coloneqq\bigwedge_{b\in\mathfrak{B}}b$ of $\mathrm{Det}_{\mathcal{R}}(\mathcal{Y})$.

We often work with complexes that satisfy the following slight variant of [BS21, Def. A.6].

(B.3) Definition. *Let $C^\bullet\in D^{\mathrm{perf}}(\mathcal{R})$ be a perfect complex, and suppose we are given a surjection $\kappa\colon H^2(C^\bullet)\to\mathcal{X}$ with $\mathcal{X}$ an $\mathcal{R}$-module generated by an ordered set $\mathfrak{X}=\{x_1,\dots,x_d\}$ of cardinality d. A representative for $C^\bullet$ of the form*

$$F^0\xrightarrow{\partial_0}F^1\xrightarrow{\partial_1}F^2 \tag{69}$$

is called a 'standard representative' for $C^\bullet$ with respect to κ and $\mathfrak{X}$ if the following conditions are satisfied:

- *(i) For every $i\in\{0,1,2\}$, the module F^i is $\mathcal{R}$-free of finite rank n_i and placed in degree i.*
- *(ii) ∂_0 is injective (so $C^\bullet$ is acyclic outside degrees 1 and 2).*
- *(iii) $d+n_1\geq n_0+n_2$.*
- *(iv) There exists a basis $\{b_1,\dots,b_{n_2}\}$ of F^2 such that the composite map $F^2\to H^2(C^\bullet)\to\mathcal{X}$ maps b_i to x_i if $i\in\{1,\dots,d\}$ and to 0 otherwise.*

(B.4) Remark. Standard representatives exist in many contexts; they can often be constructed via the method of [BS21, Prop. A.11 (i)] (see also [BKS16, § 5.4] and [BB25, Lem. 2.35]).

To give an explicit description of the map $\vartheta_{C^\bullet,\mathfrak{B}}$ for complexes that admit standard representatives in the sense of Definition (B.3), we shall use that for any $\mathcal{R}$-module M and integers $0\leq r\leq s$ one has a map

$$\Phi^{r,s}_M\colon\textstyle\bigwedge^s_{\mathcal{R}}M^*\to\mathrm{Hom}_{\mathcal{R}}\big(\bigwedge^r_{\mathcal{R}}M,\bigwedge^{r-s}_{\mathcal{R}}M\big)$$

defined by means of the rule

$$f_1\wedge\cdots\wedge f_s\mapsto\big\{m_1\wedge\cdots\wedge m_r\mapsto\textstyle\sum_{\sigma\in\mathfrak{S}_{r,s}}\mathrm{sgn}(\sigma)\det(f_i(m_{\sigma_j}))_{1\leq i\leq s}\cdot m_{\sigma(s+1)}\wedge\cdots\wedge m_{\sigma(r)}\big\}.$$

Here $\mathfrak{S}_{r,s}\coloneqq\{\sigma\in\mathfrak{S}_r\mid\sigma(1)<\cdots<\sigma(s)\text{ and }\sigma(s+1)<\cdots<\sigma(r)\}$. To simplify notation, we denote $\Phi^{r,s}_M(f)$ also by f.

(B.5) Lemma. *Let $\mathcal{R}$ be a reduced Noetherian ring with total ring of fractions $\mathcal{Q}$. Assume $C^\bullet\in D^{\mathrm{perf}}(\mathcal{R})$ is a complex that admits a standard representative (69) with respect to $(\kappa,\mathfrak{X})$ for some surjection $\kappa\colon H^2(C^\bullet)\to\mathcal{X}$ and set of generators $\mathfrak{X}=\{x_1,\dots,x_{d'}\}$ of $\mathcal{X}$. Suppose $d\leq d'$ is an integer such that $\mathcal{Y}\coloneqq\bigoplus_{i=1}^d\mathcal{R}x_i$ is a free $\mathcal{R}$-module of rank d, $\mathfrak{B}\coloneqq\{x_1,\dots,x_d\}$, and $n\coloneqq(d+n_1)-(n_0+n_2)$. Then the map*

$$\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1}=\big(\textstyle\bigwedge^{n_0}_{\mathcal{R}}(F^0)^*\big)\otimes_{\mathcal{R}}\big(\bigwedge^{n_1}_{\mathcal{R}}F^1\big)\otimes_{\mathcal{R}}\big(\bigwedge^{n_2}_{\mathcal{R}}(F^2)^*\big)\to\mathcal{Q}\otimes_{\mathcal{R}}\bigwedge^n_{\mathcal{R}}F^1$$

defined by means of the rule

$$f\otimes g\otimes\textstyle\bigwedge_{1\leq i\leq n_2}b_i^*\mapsto(-1)^{n(n_2-d)}\cdot\big(\widetilde{f}\wedge\bigwedge_{d+1\leq i\leq n_2}(b_i^*\circ\partial_1)\big)(g),$$

where $\widetilde{f}$ denotes a preimage of f under the surjection $\mathcal{Q}\otimes_{\mathcal{R}}\bigwedge^{n_0}_{\mathcal{R}}(F^1)^*\xrightarrow{\partial_0^*}\mathcal{Q}\otimes_{\mathcal{R}}\bigwedge^{n_0}_{\mathcal{R}}(F^0)^*$, is well-defined, has image in $\mathcal{Q}\otimes\bigwedge^n_{\mathcal{R}}\ker(\partial_1)$ and coincides with $\vartheta_{C^\bullet,\mathfrak{B}}$ when composed with the projection $\mathcal{Q}\otimes_{\mathcal{R}}\bigwedge^n_{\mathcal{R}}\ker(\partial_1)\to\mathcal{Q}\otimes_{\mathcal{R}}\bigwedge^n_{\mathcal{R}}H^1(C^\bullet)$.

Proof. First we observe that condition (iv) in Definition (B.3) means that the map $F^2\to H^2(C^\bullet)\xrightarrow{\kappa'}\mathcal{Y}$ induces a direct sum composition $F^2\cong G^2\oplus\mathcal{Y}$ with $G^2\coloneqq\bigoplus_{i=d+1}^{n_2}\mathcal{R}b_i$. From the free presentation $F^1\xrightarrow{\partial_1}G^2\to\ker(\kappa')\to0$ we then deduce that any element of the form $\big(\bigwedge_{d+1\leq i\leq n_2}(b_i^*\circ\partial_1)\big)(g)$ belongs to $\mathrm{Fitt}^0(\ker(\kappa'))\subseteq\mathrm{Ann}_{\mathcal{R}}(\ker(\kappa'))$. In particular, the idempotent $e\coloneqq e_{C^\bullet,\mathcal{Y}}$ acts as the identity on any such element. Since the definition of $\vartheta_{C^\bullet,\mathfrak{B}}$

involves extending scalars to $\mathcal{Q}$ and multiplication by e, we may prove the lemma after extending scalars to $e\mathcal{Q}$, thereby reducing it to the case that $\mathcal{R} = e\mathcal{Q}$. In particular, $\mathcal{R}$ is a semisimple ring and so we may fix splittings l_0 and l_1 of the exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F_0 & \xrightarrow{\partial_1} & \ker(\partial_1) & \underset{q}{\overset{l_0}{\rightleftarrows}} & H^1(C^\bullet) & \longrightarrow & 0 \\ 0 & \longrightarrow & \ker\partial_1 & \longrightarrow & F_1 & \underset{l_1}{\overset{\partial_1}{\rightleftarrows}} & G^2 & \longrightarrow & 0 \end{array}$$

which induce isomorphisms

$$\begin{aligned} \big(\textstyle\bigwedge_{\mathcal{R}}^{n} F^0\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0} H^1(C^\bullet)\big) &\xrightarrow{\simeq} \textstyle\bigwedge_{\mathcal{R}}^{n+n_0} \ker(\partial_1), \qquad (70)\\ (c_1 \wedge \cdots \wedge c_{n_0}) \otimes (h_1 \wedge \cdots \wedge h_n) &\mapsto \partial_0(c_1) \wedge \cdots \wedge \partial_0(c_{n_0}) \wedge l_0(h_1) \wedge \cdots \wedge l_0(h_n) \end{aligned}$$

and

$$\begin{aligned} \big(\textstyle\bigwedge_{\mathcal{R}}^{n+n_0} \ker(\partial_1)\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} G^2\big) &\xrightarrow{\simeq} \textstyle\bigwedge_{\mathcal{R}}^{n_1} F_1 \qquad (71)\\ j \otimes (i_1 \wedge \ldots i_{n_2-d}) &\mapsto j \wedge (l_1 \circ \partial_1^{-1})(i_1) \wedge \cdots \wedge (l_1 \circ \partial_1^{-1})(i_{n_2-d}) \end{aligned}$$

that are independent of the choices of splittings l_0 and l_1. Fix an $\mathcal{R}$-basis basis $c_1, \ldots, c_{n_0}$ of F^0 for convenience and write $c_1^*, \ldots, c_{n_0}^*$ for the corresponding dual basis. By (71), we may write $g \in \bigwedge_{\mathcal{R}}^{n_1} F^1$ in the form $j \wedge \bigwedge_{d+1\le i\le n_2}(l_1 \circ \partial_1^{-1})(b_i)$ for some $j \in \bigwedge_{\mathcal{R}}^{n+n_0} \ker(\partial_1)$ that, by (70), can in turn be written as $j = \partial_0(c) \wedge l_0(h_1) \wedge \cdots \wedge l_0(h_n)$ with $c = c_1 \wedge \cdots \wedge c_{n_0}$ and a suitable element $h_1 \wedge \cdots \wedge h_n \in \bigwedge_{\mathcal{R}}^{n} H^1(C^\bullet)$. Now, the 'passage-to-cohomology map' in the definition of $\vartheta_{C^\bullet,\mathfrak{B}}$ is given by the composite of isomorphisms

$$\begin{aligned} \mathrm{Det}_{\mathcal{R}}(C^\bullet) &= \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0}(F^0)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_1} F^1\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2}(F^2)^*\big)\\ &\longrightarrow \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0}(F^0)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_1} F^1\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} \mathcal{Y}^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d}(G^2)^*\big)\\ &\xrightarrow{\simeq} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0}(F^0)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_1} F^1\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d}(G^2)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} \mathcal{Y}^*\big)\\ &\xrightarrow{(71)} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0}(F^0)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n+n_0} \ker(\partial_1)\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} G^2\big)\\ &\qquad \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d}(G^2)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} \mathcal{Y}^*\big)\\ &\xrightarrow{(*)} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0}(F^0)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n+n_0} \ker(\partial_1)\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} \mathcal{Y}^*\big)\\ &\xrightarrow{(70)} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0}(F^0)^*\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_0} F^0\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n} H^1(C^\bullet)\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} \mathcal{Y}^*\big)\\ &\xrightarrow{(*)} \big(\textstyle\bigwedge_{\mathcal{R}}^{n} H^1(C^\bullet)\big) \otimes_{\mathcal{R}} \big(\textstyle\bigwedge_{\mathcal{R}}^{n_2-d} \mathcal{Y}^*\big), \end{aligned}$$

where the first arrow is induced by the exact sequence $0 \to \mathcal{Y}^* \to (F^2)^* \to (G^2)^* \to 0$ and the arrows labelled $(*)$ are induced by the relevant evaluation isomorphisms. Set $c^* := c_1^* \wedge \cdots \wedge c_{n_0}^*$. Since the composite of the first and second arrows sends $\bigwedge_{1\le i\le n_2} b_i^*$ to $\bigwedge_{d+1\le i\le n_2} b_i^* \otimes \bigwedge_{1\le i\le d} b_i^*$, one therefore has

$$\vartheta_{C^\bullet,\mathfrak{B}}\big(c^* \otimes g \otimes \textstyle\bigwedge_{1\le i\le n_2} b_i^*\big) = h_1 \wedge \cdots \wedge h_n \quad \in \bigwedge_{\mathcal{R}}^{n} H^1(C^\bullet).$$

Note that this does not depend on the choice of $b_1, \ldots, b_{n_0}$ or $c_1, \ldots, c_{n_0}$. On the other hand, we may compute that

$$\begin{aligned} \big(\widetilde{c^*} \wedge \textstyle\bigwedge_{d+1\le i\le n_2}(b_i^* \circ \partial_1)\big)(g) &= (-1)^{n_0\cdot(n_2-d)} \cdot \widetilde{c^*}\big(\big(\textstyle\bigwedge_{d+1\le i\le n_2}(b_i^* \circ \partial_1)\big)(g)\big)\\ &= (-1)^{n_0\cdot(n_2-d)} \cdot \widetilde{c^*}((-1)^{(n+n_0)(n_2-d)} \cdot j)\\ &= (-1)^{n(n_2-d)} \cdot c^*(c \wedge l_0(h_1) \wedge \cdots \wedge l_0(h_n))\\ &= (-1)^{n(n_2-d)} \cdot l_0(h_1) \wedge \cdots \wedge l_0(h_n), \end{aligned}$$

hence comparing with the last displayed formula gives the desired comparison with $\vartheta_{C^\bullet,\mathfrak{B}}$ after applying $\wedge^n q$, and also shows that the considered map is independent of the choice of $\widetilde{c}^*$. □

(B.6) Remark. If $F^0 = 0$ and $n_1 = n_2$, then Lemma (B.5) recovers [BS21, Prop. A.11].

To prepare for the statement of the next result, we remark that the isomorphism $\bigwedge_{\mathcal{R}}^{\mathrm{rk}_{\mathcal{R}}F} F^* \cong (\bigwedge_{\mathcal{R}}^{\mathrm{rk}_{\mathcal{R}}F} F)^*$ is valid for any finitely generated free $\mathcal{R}$-module F and induces an identification

$$\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} = \mathrm{Det}_{\mathcal{R}}(\mathrm{RHom}_{\mathcal{R}}(C^\bullet, \mathcal{R})).$$

The following result records useful functoriality properties of the map $\vartheta_{C^\bullet,\mathcal{Y}}$.

(B.7) Proposition. *Let $\mathcal{R}$ be a Noetherian reduced ring with total ring of fractions $\mathcal{Q}$.*

(a) Assume we are given an exact triangle

$$A^\bullet \longrightarrow B^\bullet \xrightarrow{g} C^\bullet \longrightarrow A^\bullet[1] \tag{72}$$

in $D^{\mathrm{perf}}(\mathcal{R})$ together with an $\mathcal{R}$-free quotient $\mathcal{Y}$ of $H^2(B^\bullet)$ of rank $d \geq \chi_{\mathcal{Q}}(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} B^\bullet)$ and with ordered $\mathcal{R}$-basis $\mathfrak{B}$. Set $n := d - \chi_{\mathcal{Q}}(\mathcal{Q} \otimes_{\mathcal{R}} B^\bullet)$.

(i) Suppose $\chi_{\mathcal{R}}(C^\bullet) = 0$ and that the map $H^2(A^\bullet) \xrightarrow{H^2(f)} H^2(B^\bullet) \to \mathcal{Y}$ induced by (72) is surjective. For every element $a \in \mathrm{Det}_{\mathcal{R}}(C^\dagger)^{-1} \cong \mathrm{Det}_{\mathcal{R}}(C^\bullet)$ and with the notation $C^\dagger := \mathrm{RHom}_{\mathcal{R}}(C^\bullet, \mathcal{R})[-2]$, one has the commutative diagram

$$\begin{array}{ccccc}
\mathrm{Det}_{\mathcal{R}}(B^\bullet)^{-1} & \xrightarrow[(72)]{\simeq} & \mathrm{Det}_{\mathcal{R}}(A^\bullet)^{-1} \otimes_{\mathcal{R}} \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} & \xrightarrow{\mathrm{id}\otimes \mathrm{Ev}_a} & \mathrm{Det}_{\mathcal{R}}(A^\bullet)^{-1} \\
\downarrow{\scriptstyle \vartheta_{B^\bullet,\mathfrak{B}}} & & & & \downarrow{\scriptstyle \vartheta_{A^\bullet,\mathfrak{B}}} \\
\mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(B^\bullet) & \xrightarrow{\cdot \vartheta_{C^\dagger,\varnothing}(a)} & \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(B^\bullet) & \xleftarrow{\wedge^n H^1(f)} & \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(A^\bullet).
\end{array}$$

(ii) Suppose $\chi_{\mathcal{R}}(A^\bullet) = 0$ and that the map $H^2(B^\bullet) \to \mathcal{Y}$ factors through the map $H^2(g)\colon H^2(B^\bullet) \to H^2(C^\bullet)$ induced by (72). For every $a \in \mathrm{Det}_{\mathcal{R}}(A^\bullet)^{-1}$ one then has the commutative diagram

$$\begin{array}{ccccc}
\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} & \xrightarrow{x \mapsto a \otimes x} & \mathrm{Det}_{\mathcal{R}}(A^\bullet)^{-1} \otimes_{\mathcal{R}} \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} & \xrightarrow[(72)]{\simeq} & \mathrm{Det}_{\mathcal{R}}(B^\bullet) \\
\downarrow{\scriptstyle \vartheta_{C^\bullet,\mathfrak{B}}} & & & & \downarrow{\scriptstyle \vartheta_{B^\bullet,\mathfrak{B}}} \\
\mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(C^\bullet) & \xrightarrow{\cdot \vartheta_{A^\bullet,\varnothing}(a)} & \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(C^\bullet) & \xleftarrow{\wedge^n H^2(g)} & \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(B^\bullet).
\end{array}$$

(b) Let $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ be a complex and $\mathcal{Y}$ a quotient of $H^2(B^\bullet)$ that is $\mathcal{R}$-free of rank $d \geq 1 + \chi_{\mathcal{Q}}(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\bullet)$ and has ordered $\mathcal{R}$-basis $\mathfrak{B}$. Let $f\colon \mathcal{R}[1] \to C^\dagger := \mathrm{RHom}_{\mathcal{R}}(C^\bullet, \mathcal{R})$ be a morphism in $D(\mathcal{R})$ with dual map $f^*\colon C^\bullet \to R[-1]$.

(i) The map $H^1(C^\bullet) \otimes_{\mathcal{R}} \mathcal{Q} \to \mathcal{Q}$ induced by $H^1(f^*)$ via extension of scalars coincides with the composite map

$$H^1(C^\bullet) \otimes_{\mathcal{R}} \mathcal{Q} = H^1(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\bullet) \cong H^{-1}(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\dagger)^* = \mathcal{Q} \otimes_{\mathcal{R}} H^{-1}(C^\dagger)^* \xrightarrow{H^{-1}(f)^*} \mathcal{Q}.$$

(ii) Setting $D^\bullet := \mathrm{cone}(f^*)[-1]$, the following diagram is commutative.

$$\begin{array}{ccccc}
\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} & \xrightarrow{\simeq} & \mathrm{Det}_{\mathcal{R}}(D^\bullet)^{-1} \otimes_{\mathcal{R}} \mathrm{Det}_{\mathcal{R}}(\mathcal{R})^{-1} & \xrightarrow{\mathrm{id}\otimes \mathrm{Ev}_1} & \mathrm{Det}_{\mathcal{R}}(D^\bullet)^{-1} \\
\downarrow{\scriptstyle \vartheta_{C^\bullet,\mathfrak{B}}} & & & & \downarrow{\scriptstyle \vartheta_{D^\bullet,\mathfrak{B}}} \\
\mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(C^\bullet) & \xrightarrow{H^1(f^*)} & \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^{n-1}_{\mathcal{R}} H^1(C^\bullet) & \longleftarrow & \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^{n-1}_{\mathcal{R}} H^1(D^\bullet).
\end{array}$$

(c) Suppose $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ is a complex with $\chi(C^\bullet) = 0$ that is acyclic outside degrees 1 and 2. Setting, $C^\dagger := \mathrm{RHom}_{\mathcal{R}}(C^\bullet, \mathcal{R})[i]$ for a fixed odd integer i, one then has an equality of $\mathcal{R}$-submodules of $\mathcal{Q}$

$$\vartheta_{C^\bullet,\varnothing}(\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1}) = \vartheta_{C^\dagger,\varnothing}(\mathrm{Det}_{\mathcal{R}}(C^\dagger)^{-1}).$$

(d) Let $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ be a complex and $\mathcal{R} \to \mathcal{R}'$ a surjective morphism of reduced Noetherian rings. Write $\rho\colon C^\bullet \to C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathcal{R}'$ and $\rho^{\mathrm{det}}\colon \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} \to \mathrm{Det}_{\mathcal{R}'}(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathcal{R}')$ for the induced morphisms. Suppose $\mathcal{Y}$ is a quotient of $H^2(C^\bullet)$ that is $\mathcal{R}$-free of rank $d \geq \chi_{\mathcal{Q}}(\mathcal{Q} \otimes^{\mathbb{L}}_{\mathcal{R}} C^\bullet)$ and has the property that the map $H^2(C^\bullet) \otimes_{\mathcal{R}} \mathcal{R}' \to \mathcal{Y} \otimes_{\mathcal{R}} \mathcal{R}'$ factors through the map $H^2(C^\bullet) \otimes_{\mathcal{R}} \mathcal{R}' \to H^2(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathcal{R}')$ induced by $H^2(\rho)$. We also fix an ordered $\mathcal{R}$-basis $\mathfrak{B}$ of $\mathcal{Y}$ and write $\mathfrak{B}'$ for the induced $\mathcal{R}'$-basis of $\mathcal{Y} \otimes_{\mathcal{R}} \mathcal{R}'$. Then one has the commutative diagram

$$\begin{array}{ccc} \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} & \xrightarrow{\rho^{\mathrm{det}}} & \mathrm{Det}_{\mathcal{R}'}(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathcal{R}') \\ \downarrow{\scriptstyle \vartheta_{C^\bullet,\mathfrak{B}}} & & \downarrow{\scriptstyle \vartheta_{C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathcal{R}',\mathfrak{B}'}} \\ \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}} H^1(C^\bullet) & \xrightarrow{\wedge^n H^1(\rho)} & \mathcal{Q} \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}'} H^1(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathcal{R}') \end{array}$$

Proof. To prove claim (a) (i), we note that the determinant functor behaves well under base change so that, replacing all appearing complexes by those obtained from applying the functor $(e_{C^\bullet,\varnothing} \cdot e_{B^\bullet,\mathcal{Y}} \cdot \mathcal{Q}) \otimes^{\mathbb{L}}_{\mathcal{R}} (-)$ to them and replacing $\mathcal{Y}$ by $(e_{C^\bullet,\varnothing} \cdot e_{B^\bullet,\mathcal{Y}} \cdot \mathcal{Q}) \otimes_{\mathcal{R}} \mathcal{Y}$ if necessary, we may assume $\mathcal{R} = \mathcal{Q}$ and $e_{B^\bullet,\mathcal{Y}} = 1 = e_{C^\bullet,\varnothing} = e_{C^\dagger,\varnothing}$. In particular, $B^\bullet$ is acyclic outside degrees 1 and 2 with $H^2(C^\bullet) = \mathcal{Y}$ and $C^\bullet$ is acyclic. Since $\mathcal{R}$ is semisimple (even a product of fields), it follows that $B^\bullet$ admits a representative of the form $[H^1(B^\bullet) \xrightarrow{0} \mathcal{Y}]$ and $C^\bullet$ can be represented by the zero complex. Our convention then identifies $\mathrm{Det}_{\mathcal{R}}(C^{\bullet,*})$ with $\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} = \mathcal{R}^*$ and under this identification Ev_a corresponds with the map $\mathcal{Q} \to \mathcal{Q}$ that sends x to $a(x)$. On the other hand, the isomorphism $\mathcal{R}^* \cong \mathcal{R}, f \mapsto f(1)$ combines with Lemma (B.5) to imply that $\vartheta_{C^{\bullet,*},\varnothing}(a) = a(1)$. In addition, for our fixed choices of representatives, the triangle (72) identifies $A^\bullet$ with $B^\bullet$ and so, using the description of $\vartheta_{A^\bullet,\mathfrak{B}}$ given in Lemma (B.5), it is straightforward to check that the diagram in claim (a) (i) is indeed commutative. The commutativity of the diagram in (a) (ii) can be proved in the same fashion.

To prove part (i) of claim (b), it suffices to note that $\mathcal{Q}$ is a finite product of fields and therefore $\mathrm{Hom}_{\mathcal{Q}}(-, \mathcal{Q})$ an exact functor. As for part (ii) of claim (b), we may again reduce to the case that $\mathcal{R} = \mathcal{Q}$. To justify a further reduction, we let e be a primitive orthogonal idempotent of $\mathcal{Q}$ such that $e \cdot ((\wedge^n H^1(f^*)) \circ \vartheta_{C^\bullet,\mathfrak{B}})$ is nonzero. In particular, the map $eH^1(f^*)\colon eH^1(C) \to e\mathcal{Q}$ is nonzero and hence surjective because $e\mathcal{Q}$ is a field. From the exact sequence

$$0 \longrightarrow H^1(D^\bullet) \longrightarrow H^1(C^\bullet) \xrightarrow{H^1(f^*)} R \longrightarrow H^2(D^\bullet) \longrightarrow H^2(C^\bullet) \longrightarrow 0$$

we then conclude that $eH^2(D^\bullet) \cong eH^2(C^\bullet)$. On the other hand, if $e\vartheta_{C^\bullet,\mathfrak{B}}$ is nonzero, then $ee_{C^\bullet,\mathfrak{B}} = e$ and this combines with the isomorphism $eH^i(D^\bullet) \cong eH^i(C^\bullet)$ that is valid for every integer $i \neq 1$ to imply that also $ee_{D^\bullet,\mathfrak{B}} = e$. This proves that $e_{D^\bullet,\mathfrak{B}}$ acts as the identity on the image of $(\wedge^n H^1(f^*)) \circ \vartheta_{C^\bullet,\mathfrak{B}}$. Since the same is true for the image of $\vartheta_{D^\bullet,\mathfrak{B}}$ by its very definition, we may replace the complexes $C^\bullet$ and $D^\bullet$ by $e_{D^\bullet,\mathfrak{B}} \otimes^{\mathbb{L}}_{\mathcal{Q}} C^\bullet$ and $e_{D^\bullet,\mathfrak{B}} \otimes^{\mathbb{L}}_{\mathcal{Q}} D^\bullet$, respectively, to reduce to the case that $e_{C^\bullet,\mathfrak{B}} = 1 = e_{D^\bullet,\mathfrak{B}}$.

In this case, then, $C^\bullet$ admits a representative of the form $[H^1(C^\bullet) \xrightarrow{0} \mathcal{Y}]$ and a standard mapping cone construction yields the representative $[H^1(C^\bullet) \xrightarrow{H^1(f^*) \oplus 0} \mathcal{R} \oplus \mathcal{Y}]$ for $D^\bullet$. Given these explicit representatives, the commutativity of the diagram in claim (b) (ii) is a direct consequence of the descriptions of the maps $\vartheta_{C^\bullet,\mathfrak{B}}$ and $\vartheta_{D^\bullet,\mathfrak{B}}$ obtained in Lemma (B.5).

To prove claim (c), we fix a representative

$$\cdots \to 0 \to C^{-n} \xrightarrow{\partial_{-n}} C^{-n+1} \to \cdots \to C^{m-1} \xrightarrow{\partial_{m-1}} C^m \to 0 \to \ldots \tag{73}$$

of $C^\bullet$ with suitable natural numbers $n, m \in \mathbb{N}$ and finitely generated free $\mathcal{R}$-modules C^j for $j \in \{-n, \ldots, m\}$ that are each placed in degree j.

The assumption that $C^\bullet$ has vanishing cohomology outside degrees 1 and 2 combines with the vanishing of $\chi(C^\bullet)$ to imply that $C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} e\mathcal{Q}$, with $e \coloneqq e_{C^\bullet,\varnothing}$, is acyclic. In particular, for every

j we may fix a splitting

$$f_j\colon e\mathcal{Q}\otimes_{\mathcal{R}} C^j \cong e\mathcal{Q}\otimes_{\mathcal{R}} \left(\operatorname{im}\partial_{j-1}\oplus (C^j/\ker\partial_j)\right)$$

as well as an isomorphism of $\mathcal{R}$-modules

$$\phi\colon \mathcal{Q}\otimes_{\mathcal{R}} C^{\mathrm{odd}} \coloneqq \bigoplus\nolimits_{j\ \mathrm{odd}} (\mathcal{Q}\otimes_{\mathcal{R}} C^j) \to C^{\mathrm{even}} \coloneqq \bigoplus\nolimits_{j\ \mathrm{even}} (\mathcal{Q}\otimes_{\mathcal{R}} C^j)$$

that restricts to give the isomorphism

$$e\mathcal{Q}\otimes_{\mathcal{R}} C^{\mathrm{odd}} \xrightarrow{\simeq} e\mathcal{Q}\otimes_{\mathcal{R}} C^{\mathrm{even}},\quad (a_j)_j \mapsto ((\partial_{j-1}\circ f_{j-1})^{-1}\oplus \partial_j)(f_j(a_j)).$$

Writing $M(\phi)$ for the matrix (with entries in $\mathcal{Q}$) representing ϕ in a choice of $\mathcal{R}$-bases for C^{even} and C^{odd}, one has the equality of $\mathcal{R}$-submodules of $\mathcal{Q}$

$$\vartheta_{C^\bullet,\varnothing}(\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1}) = e\cdot \det_{\mathcal{R}}(M(\phi))\cdot\mathcal{R}.$$

On the other hand, applying $\mathrm{RHom}_{\mathcal{R}}(-,\mathcal{R})$ to the representative (73), we see that $C^\dagger$ is represented by

$$\cdots\to 0\to C^m \xrightarrow{\partial^{\mathrm{tr}}_{m-1}} C^{m-1}\to\cdots\to C^{-n+1}\xrightarrow{\partial^{\mathrm{tr}}_{-n}} C^{-n}\to 0\to\dots,$$

where now C^j is placed in degree $-j+3$, and the maps ∂_j^{tr} are obtained from ∂_j in the following way: Fix $\mathcal{R}$-bases of C^j and C^{j+1}, and write A_j for the matrix representing ∂_j with respect to these bases. Then ∂_j^{tr} is the unique $\mathcal{R}$-linear morphism $C^{j+1}\to C^j$ that, for our fixed choices of bases, is represented by the transpose A_j^{tr} of the matrix A_j.
An analysis similar to the one above shows that

$$\vartheta_{C^\dagger,\varnothing}(\mathrm{Det}_{\mathcal{R}}(C^\dagger)) = \det_{\mathcal{R}}(M(\phi'))\cdot\mathcal{R},$$

where now $\phi'\colon \mathcal{Q}\otimes_{\mathcal{R}} C^{\dagger,\mathrm{odd}} = \mathcal{Q}\otimes_{\mathcal{R}} C^{\mathrm{even}}\to \mathcal{Q}\otimes_{\mathcal{R}} C^{\mathrm{odd}} = \mathcal{Q}\otimes_{\mathcal{R}} C^{\dagger,\mathrm{even}}$ (for the identification we have used that i is odd) is any isomorphism of $\mathcal{R}$-modules that restricts to

$$e\mathcal{Q}\otimes_{\mathcal{R}} C^{\mathrm{even}}\to e\mathcal{Q}\otimes_{\mathcal{R}} C^{\mathrm{odd}},\quad (a_j)_j\mapsto (\partial^{\mathrm{tr}}_{j-1}\oplus(\partial_j^{\mathrm{tr}}\circ f_j)^{-1})(f_j(a_j)).$$

The equality claimed in (c) therefore follows upon noting that $\det_{\mathcal{R}}(M(\phi)) = \det_{\mathcal{R}}(M(\phi'))$.
Finally, claim (d) is valid because the definitions of $\vartheta_{C^\bullet,\mathfrak{B}}$ and $\vartheta_{C^\bullet\otimes^{\mathbb{L}}_{\mathcal{R}}\mathcal{R}',\mathfrak{B}'}$ both involve the passage-to-cohomology map. □

(B.8) Remark. Part (a) of Proposition (B.7) generalises the observation of Burns and Flach in [BF98, Lem. 1].

B.2. Fitting ideals and exterior biduals

In this subsection we study integrality properties of the maps from Definition (B.2). In doing so, we will be naturally lead to consider $\mathcal{R}$-modules of the form

$$\left(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge\nolimits^r_{\mathcal{R}} M^*\right)^* \tag{74}$$

for an ideal $\mathfrak{a}\subseteq\mathcal{R}$, an $\mathcal{R}$-module M, and an integer $r\geq 0$. Taking $\mathfrak{a}=\mathcal{R}$, this construction specialises to give the 'r-th exterior bidual' $\bigcap^r_{\mathcal{R}} M \coloneqq (\bigwedge^r_{\mathcal{R}} M^*)^*$ of M that has been studied in detail by Burns and Sano [BS21, App.] and Sakamoto [Sak23, App. B] as a generalisation of the lattice utilised by Rubin in [Rub96]. The following observation shows that modules of the form (74) should be considered a generalisation of Rubin's lattice with 'denominators bounded by $\mathfrak{a}$' and, in particular, specialise to the lattices studied by Popescu in [Pop02].

(B.9) Lemma. *Let $\mathcal{R}$ be a reduced Noetherian ring with total ring of fractions $\mathcal{Q}$. For every ideal $\mathfrak{a}\subseteq\mathcal{R}$, finitely generated $\mathcal{R}$-module M, and integer $r\geq 0$, there is a canonical isomorphism*

$$\xi^r_{M,\mathfrak{a}}\colon \left\{a\in\mathcal{Q}\otimes_{\mathcal{R}}\bigwedge\nolimits^r_{\mathcal{R}} M \mid \mathrm{Ann}_{\mathcal{R}}(\mathfrak{a})\cdot a = 0, f(a)\in\mathfrak{a}^{-1} \text{ for all } f\in\bigwedge\nolimits^r_{\mathcal{R}} M^*\right\}\xrightarrow{\simeq}\left(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge\nolimits^r_{\mathcal{R}} M^*\right)^*.$$

Here $\mathfrak{a}^{-1}\coloneqq\{q\in\mathcal{Q}\mid qa\in\mathcal{R} \text{ for all } a\in\mathfrak{a}\}$.

Proof. This is a natural generalisation of the result of [BS21, Prop. A.8]. For the convenience of the reader, we provide the argument.
Applying the functor $\mathrm{Hom}_{\mathcal{R}}(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M^*,-)$ to the exact sequence $0\to\mathcal{R}\to\mathcal{Q}\to\mathcal{R}/\mathcal{Q}\to 0$ gives that

$$\big(\mathfrak{a}\otimes_{\mathcal{R}}\textstyle\bigwedge^r_{\mathcal{R}}M^*\big)^* = \ker\Big\{\mathrm{Hom}_{\mathcal{R}}\big(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M^*,\mathcal{Q}\big)\to\mathrm{Hom}_{\mathcal{R}}\big(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M^*,\mathcal{Q}/\mathcal{R}\big)\Big\}.$$

As $\mathcal{Q}$ is a finite product of fields, the ideal $\mathcal{Q}\cdot\mathrm{Ann}_{\mathcal{R}}(\mathfrak{a})$ is generated by an idempotent $e\in\mathcal{Q}$ (so that $\mathcal{Q}\cdot\mathfrak{a}=(1-e)\mathcal{Q}$) and $\mathcal{Q}\otimes_{\mathcal{R}}M$ is a finitely generated projective $\mathcal{Q}$-module. By [BS21, Lem. A.1] we therefore have an isomorphism

$$(1-e)\mathcal{Q}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M\cong(1-e)\bigwedge^r_{\mathcal{Q}}(\mathcal{Q}\otimes_R M)\xrightarrow{\simeq}(1-e)\bigcap^r_{\mathcal{Q}}(\mathcal{Q}\otimes_R M),\quad a\mapsto\{\varphi\mapsto\varphi(a)\}.$$

Furthermore, there is an isomorphism $\mathrm{Hom}_{\mathcal{Q}}(\mathcal{Q}\otimes_{\mathcal{R}}N,\mathcal{Q})\cong\mathrm{Hom}_{\mathcal{R}}(N,\mathcal{Q})$ for any $\mathcal{R}$-module N by the tensor-hom adjunction. It follows that $(1-e)\bigcap^r_{\mathcal{Q}}(\mathcal{Q}\otimes_R M)\cong\mathrm{Hom}_{\mathcal{R}}(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M^*,\mathcal{Q})$. The lemma now follows upon noting that an element a of $(1-e)\mathcal{Q}\otimes_R\bigwedge^r_R M$ belongs to the kernel of $\mathrm{Hom}_{\mathcal{R}}(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M^*,\mathcal{Q})\to\mathrm{Hom}_{\mathcal{R}}(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M^*,\mathcal{Q}/\mathcal{R})$ under these identifications if and only if one has $xf(a)\in\mathcal{R}$ for all $x\in\mathfrak{a}$ and $f\in\bigwedge^r_{\mathcal{R}}M^*$. □

Note that, for every integer $s\le r$ and $f\in\bigwedge^s_{\mathcal{R}}M^*$, we obtain a map

$$\big(\mathfrak{a}\otimes_{\mathcal{R}}\textstyle\bigwedge^r_{\mathcal{R}}M^*\big)^*\to\big(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^{r-s}_{\mathcal{R}}M^*\big)^*,\quad\varphi\mapsto\{a\otimes g\mapsto\varphi(a\otimes(f\wedge g))\}$$

that, by abuse of notation, will also be denoted as f. This construction gives a commutative diagram

$$\begin{array}{ccc}\bigwedge^r_{\mathcal{R}}M & \xrightarrow{\quad f\quad} & \bigwedge^{r-s}_{\mathcal{R}}M\\ \downarrow & & \downarrow\\ \big(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^r_{\mathcal{R}}M^*\big)^* & \xrightarrow{f} & \big(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^{r-s}_{\mathcal{R}}M^*\big)^*,\end{array}$$

where the top arrow is the map $\Phi^{r,s}_M(f)$ defined earlier and the vertical arrows are the maps (with $t\in\{r,r-s\}$)

$$\bigwedge^t_{\mathcal{R}}M\to\big(\mathfrak{a}\otimes_{\mathcal{R}}\bigwedge^t_{\mathcal{R}}M^*\big)^*,\quad m_1\wedge\cdots\wedge m_t\mapsto\big\{a\otimes f_1\wedge\cdots\wedge f_t\mapsto a\cdot\det(f_i(m_j))_{1\le i,j\le t}\big\}.$$

Following Sakamoto [Sak23], the results in the remainder of this section are most naturally stated for rings that are 'quasi-normal'. That is, Noetherian rings $\mathcal{R}$ that satisfy the following two conditions.

(G_1) The localisation $\mathcal{R}_{\mathfrak{p}}$ of $\mathcal{R}$, at any prime ideal $\mathfrak{p}\subseteq\mathcal{R}$ of height at most one, is Gorenstein.

(S_2) The localisation $\mathcal{R}_{\mathfrak{p}}$ of $\mathcal{R}$, at any prime ideal $\mathfrak{p}\subseteq\mathcal{R}$ of height n, has depth at least $\min\{2,n\}$.

(B.10) Proposition. *Let $\mathcal{R}$ be a quasi-normal ring and $C^\bullet\in D^{\mathrm{perf}}(\mathcal{R})$ a complex that admits a standard representative (69) with respect to a surjection $\kappa\colon H^2(C^\bullet)\to\mathcal{Y}$ for a free $\mathcal{R}$-module $\mathcal{Y}$ of rank d and an ordered $\mathcal{R}$-basis $\mathfrak{B}$ of $\mathcal{Y}$. We also set $n:=d+n_1-(n_0+n_2)$.*

(a) There exists a well-defined canonical map

$$\varpi_{C^\bullet,\mathfrak{B}}\colon\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1}\to\big(\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})\otimes_{\mathcal{R}}\bigwedge^n_{\mathcal{R}}H^1(C^\bullet)^*\big)^*$$

with the property that, if $\mathcal{R}$ is reduced, then one has

$$\xi^{-1}\circ\varpi_{C^\bullet,\mathfrak{B}}=\vartheta_{C^\bullet,\mathfrak{B}}$$

with $\xi:=\xi^n_{H^1(C^\bullet),\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})}$ the isomorphism from Lemma (B.9).

(b) One has an inclusion of $\mathcal{R}$-modules

$$\big\{f(a)\mid a\in\mathrm{im}(\varpi_{C^\bullet,\mathfrak{B}}),f\in\bigwedge^n_{\mathcal{R}}H^1(C^\bullet)^*\big\}\subseteq\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^*\otimes_{\mathcal{R}}\mathrm{Fitt}^d_{\mathcal{R}}(H^2(C^\bullet))^{**}.$$

Moreover, if $\mathfrak{p}\subseteq\mathcal{R}$ is a height-one prime ideal in the support of the cokernel of this inclusion, then $(H^1(C^\bullet)^\vee_{\mathrm{tor}})_{\mathfrak{p}}$ does not have finite projective dimension as an $\mathcal{R}_{\mathfrak{p}}$-module.

(c) If $\mathfrak{p} \subseteq \mathcal{R}$ is a prime ideal of height at most one with the property that $\mathcal{R}_\mathfrak{p}$ is a regular local ring, then one has the equality

$$\mathrm{im}(\vartheta_{C^\bullet,\mathfrak{B}})_\mathfrak{p} = \mathrm{Fitt}^d_\mathcal{R}(H^2(C^\bullet))_\mathfrak{p} \cdot \mathrm{Fitt}^0_\mathcal{R}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^{-1}_\mathfrak{p} \cdot \big(\textstyle\bigcap^n_\mathcal{R} H^1(C^\bullet)\big)_\mathfrak{p}.$$

Proof. Dualising the tautological exact sequence $0 \to F^0 \to F^1 \to F^1/F^0 \to 0$ gives the exact sequence

$$0 \longrightarrow (F^1/F^0)^* \longrightarrow (F^1)^* \xrightarrow{\partial_0^*} (F^0)^* \longrightarrow \mathrm{Ext}^1_\mathcal{R}(F^1/F^0, \mathcal{R}) \longrightarrow 0, \tag{75}$$

from which we deduce, by the definition of Fitting ideals, that one has

$$\mathrm{im}\big\{\textstyle\bigwedge^{n_0}_\mathcal{R}(F^1)^* \xrightarrow{\partial_0^*} \bigwedge^{n_0}_\mathcal{R}(F^0)^*\big\} = \mathrm{Fitt}^0_\mathcal{R}(\mathrm{Ext}^1_\mathcal{R}(F^1/F^0,\mathcal{R})) \cdot \textstyle\bigwedge^{n_0}_\mathcal{R}(F^0)^*. \tag{76}$$

In particular, for every $f \in \bigwedge^{n_0}_\mathcal{R}(F^0)^*$ and $\lambda \in \mathrm{Fitt}^0_\mathcal{R}(\mathrm{Ext}^1_\mathcal{R}(F^1/F^0,\mathcal{R}))$ we can find $\widetilde{\lambda f} \in \bigwedge^{n_0}_\mathcal{R}(F^1)^*$ with $\partial_0^*(\widetilde{\lambda f}) = \lambda \cdot f$.
Write $b_1, \dots, b_{n_2}$ for the basis from condition (iv) in Definition (B.3). Given an element $f \otimes a \otimes \bigwedge_{1\le i\le n_2} b_i^*$ of $\mathrm{Det}_\mathcal{R}(C^\bullet)^{-1} = \bigwedge^{n_0}_\mathcal{R}(F^0)^* \otimes_\mathcal{R} \bigwedge^{n_1}_\mathcal{R} F^1 \otimes_\mathcal{R} \bigwedge^{n_2}_\mathcal{R}(F^2)^*$ we now consider

$$a'_{\widetilde{\lambda f}} := (\widetilde{\lambda f} \wedge \textstyle\bigwedge_{d+1\le i\le n_2}(b_i^* \circ \partial_1))(a) \in \bigwedge^n_\mathcal{R} F^1.$$

Set $F' := \bigoplus_{i=d+1}^{n_2}(\mathcal{R}\cdot b_i)$ so that we have a direct sum decomposition $F^2 = F' \oplus \mathcal{Y}$. By property (iv) in Definition (B.3), ∂_1 maps to F' and therefore it follows from [BB25, Lem. 2.17 (ii)] that the map $\bigwedge_{d+1\le i\le n_2}(b_i^* \circ \partial_1)\colon \bigwedge^{n_1-n_0}_\mathcal{R} F_1 \to \bigwedge^n_\mathcal{R} F_1$ has image in $\bigcap^n_\mathcal{R} \ker(\partial_1)$. In particular, $a'_{\widetilde{\lambda f}}$ belongs to $\bigcap^n_\mathcal{R} \ker(\partial_1)$. Writing ϕ for the map $\bigcap^n_\mathcal{R} \ker(\partial_1) \to \bigcap^n_\mathcal{R} H^1(C^\bullet)$ induced by the projection $\ker(\partial_1) \to \ker(\partial_1)/F_0 = H^1(C^\bullet)$, we may then define the map

$$\begin{aligned} \mathrm{Det}_\mathcal{R}(C^\bullet)^{-1} &\to \big(\mathrm{Fitt}^0_\mathcal{R}(\mathrm{Ext}^1_\mathcal{R}(F^1/F^0,\mathcal{R})) \otimes_\mathcal{R} \textstyle\bigwedge^n_\mathcal{R} H^1(C^\bullet)^*\big)^*, \\ a &\mapsto \{\lambda \otimes \varphi \mapsto (-1)^{n(n_2-d)} \cdot \varphi(\phi(a'_{\widetilde{\lambda f}}))\}. \end{aligned} \tag{77}$$

We now claim that $\varphi(\phi(a'_{\widetilde{\lambda f}}))$ is independent of the choice of lift $\widetilde{\lambda f}$ of λf even though $a'_{\widetilde{\lambda f}}$ might depend on it. Let g_1 and g_2 be two such lifts of λf, then we shall show $\varphi(\phi(a'_{g_1})) = \varphi(\phi(a'_{g_2}))$ by verifying that $\varphi(\phi(a'_{g_1} - a'_{g_2}))$ vanishes in the total ring of fractions $\mathcal{Q}$ of $\mathcal{R}$. For this it is enough to prove the required vanishing in the localisation $\mathcal{R}_\mathfrak{p}$ at every minimal prime ideal $\mathfrak{p}$ of $\mathcal{R}$. By the validity of condition (G_1) the ring $\mathcal{R}_\mathfrak{p}$ is self-injective and so $\mathcal{R}_\mathfrak{p} \otimes_\mathcal{R} \mathrm{Ext}^1_\mathcal{R}(F^1/F^0,\mathcal{R})$ vanishes. It therefore follows from (75) that $(F^1/F^0)_\mathfrak{p}$ is a free $\mathcal{R}_\mathfrak{p}$-module of rank $n_1 - n_0$ and that we have a canonical isomorphism

$$\textstyle\bigwedge^{n_1}_{\mathcal{R}_\mathfrak{p}}(F^1)^*_\mathfrak{p} \cong (\bigwedge^{n_0}_{\mathcal{R}_\mathfrak{p}}(F^0)^*_\mathfrak{p}) \otimes_\mathcal{R} \bigwedge^{n_1-n_0}_{\mathcal{R}_\mathfrak{p}}(F^1/F^0)^*_\mathfrak{p}. \tag{78}$$

In addition, as $\mathcal{R}_\mathfrak{p}$ is self-injective, dualising the injection $H^1(C^\bullet) = \ker(\partial_1)/F_0 \hookrightarrow F_1/F_0$ shows that the restriction map $(F_1/F_0)^*_\mathfrak{p} \to H^1(C^\bullet)^*_\mathfrak{p}$ is surjective so that we may assume φ is the restriction of an element $\widetilde{\varphi} \in \bigwedge^r_{\mathcal{R}_\mathfrak{p}}(F_1/F_0)^*_\mathfrak{p}$. Now, the element

$$(\lambda f) \otimes \big(\widetilde{\varphi} \wedge \textstyle\bigwedge_{d+1\le i\le n_2}(b_i^* \circ \partial_1)\big) \in (\bigwedge^{n_0}_{\mathcal{R}_\mathfrak{p}}(F^0)^*_\mathfrak{p}) \otimes_\mathcal{R} \bigwedge^{n_1-n_0}_{\mathcal{R}_\mathfrak{p}}(F^1/F^0)^*_\mathfrak{p}$$

is a preimage of both $g_1 \wedge \widetilde{\varphi} \wedge \bigwedge_{d+1\le i\le n_2}(b_i^* \circ \partial_1)$ and $g_2 \wedge \widetilde{\varphi} \wedge \bigwedge_{d+1\le i\le n_2}(b_i^* \circ \partial_1)$ under the isomorphism (78), and this implies the claimed independence from the lift $\widetilde{\lambda f}$ of λf.
Next we note that there is an exact sequence

$$\mathrm{Ext}^1_\mathcal{R}(J,\mathcal{R}) \longrightarrow \mathrm{Ext}^1_\mathcal{R}(F^1/F^0,\mathcal{R}) \longrightarrow \mathrm{Ext}^1_\mathcal{R}(H^1(C^\bullet),\mathcal{R}) \longrightarrow \mathrm{Ext}^2_\mathcal{R}(J,\mathcal{R}),$$

where J denotes the cokernel of $H^1(C^\bullet) \to F^1/F^0$. We claim that the middle arrow in this exact sequence is a pseudo-isomorphism. Indeed, from the exact sequence $0 \to J \to F^2 \to H^2(C^\bullet) \to 0$ we obtain isomorphisms $\mathrm{Ext}^i_\mathcal{R}(J,\mathcal{R}) \cong \mathrm{Ext}^{i+1}_\mathcal{R}(H^2(C^\bullet),\mathcal{R})$ for every $i \ge 1$, which shows these modules to be pseudo-null because $\mathcal{R}$ is assumed to satisfy condition (G_1). Since

one also has a pseudo-isomorphism $\mathrm{Ext}^1_{\mathcal{R}}(H^1(C^\bullet),\mathcal{R}) \to H^1(C^\bullet)^\vee_{\mathrm{tor}}$ by Lemma (B.12) below and reflexive ideals of $\mathcal{R}$ are uniquely determined by their localisation at primes of height at most one (cf. [Sak23, Lem. C.11]), one has an equality of reflexive hulls

$$\mathfrak{A} \coloneqq \mathrm{Fitt}^0_{\mathcal{R}}(\mathrm{Ext}^1_{\mathcal{R}}(F^1/F^0,\mathcal{R}))^{**} = \mathrm{Fitt}^0_{\mathcal{R}}(\mathrm{Ext}^1_{\mathcal{R}}(H^1(C^\bullet),\mathcal{R}))^{**} = \mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^{**}.$$

For any finitely generated $\mathcal{R}$-module M, we therefore obtain pseudo-isomorphisms

$$\mathrm{Fitt}^0_{\mathcal{R}}(\mathrm{Ext}^1_{\mathcal{R}}(F^1/F^0,\mathcal{R})) \otimes_{\mathcal{R}} M \longrightarrow \mathfrak{A} \otimes_{\mathcal{R}} M \longleftarrow \mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}}) \otimes_{\mathcal{R}} M$$

and this combines with condition (S_2) to imply that, by [Sak23, Lem. B.5], taking duals gives isomorphisms

$$\big(\mathrm{Fitt}^0_{\mathcal{R}}(\mathrm{Ext}^1_{\mathcal{R}}(F^1/F^0,\mathcal{R})) \otimes_{\mathcal{R}} M\big)^* \xleftarrow{\simeq} \big(\mathfrak{A} \otimes_{\mathcal{R}} M\big)^* \xrightarrow{\simeq} \big(\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}}) \otimes_{\mathcal{R}} M\big)^*.$$

We then define the map $\varpi_{C^\bullet,\mathfrak{B}}$ in claim (a) to be the map defined in (77) composed with these isomorphisms for $M = \bigwedge^n_{\mathcal{R}} H^1(C^\bullet)^*$. With this definition, it follows from Lemma (B.5) and the definition of the map ξ that one has $\xi^{-1} \circ \varpi_{C^\bullet,\mathfrak{B}} = \vartheta_{C^\bullet,\mathfrak{B}}$, as required to prove claim (a).
As for claim (b), Lemma [Sak23, Lem. C.11] reduces to prove the claim locally at primes $\mathfrak{p} \subseteq \mathcal{R}$ of height at most one. To do this, we first observe that by [BS21, Prop. A.2 (ii)] one has

$$\begin{aligned}\Big\{h(\textstyle\bigwedge_{d+1\le i\le n_2}(b_i^*\circ\partial_1)(x)) \,\Big|\, x \in \bigwedge^{n_1}_{\mathcal{R}_\mathfrak{p}} F^1_\mathfrak{p}, h \in \bigwedge^{n+n_0}_{\mathcal{R}_\mathfrak{p}}(F^1_\mathfrak{p})^*\Big\} &= \mathrm{Fitt}^0_{\mathcal{R}}(\ker\{H^2(C^\bullet) \xrightarrow{\kappa} \mathcal{Y}\})_\mathfrak{p}\\ &= \mathrm{Fitt}^d_{\mathcal{R}}(H^2(C^\bullet))_\mathfrak{p}.\end{aligned}$$

Now, the cokernel of the restriction map $(F^1/F^0)^* \to H^1(C^\bullet)^*$ identifies with a submodule of $\mathrm{Ext}^1_{\mathcal{R}}(J,\mathcal{R})$ and so, as observed above, is pseudo-null. Given this, the inclusion claimed in the first part of (a) follows by taking $h = \widetilde{\lambda f} \wedge \widetilde{\varphi}$ with $\widetilde{\varphi}$ a lift of $\varphi \in \bigwedge^n_{\mathcal{R}_\mathfrak{p}} H^1(C^\bullet)^*_\mathfrak{p}$ so that $h(\bigwedge_{d+1\le i\le n_2}(b_i^*\circ\partial_1)(a)) = \varphi(a_{\widetilde{f\lambda}})$.
In addition, said inclusion is an equality (at $\mathfrak{p}$) whenever the subset of $\bigwedge^{n+n_0}_{\mathcal{R}_\mathfrak{p}}(F^1_\mathfrak{p})^*$ comprising all such $\widetilde{\lambda f} \wedge \widetilde{\varphi}$ is equal to $\bigwedge^{n+n_0}_{\mathcal{R}_\mathfrak{p}}(F^1_\mathfrak{p})^*$. To investigate when this happens, assume that $\mathrm{Ext}^1_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}},\mathcal{R})_\mathfrak{p} = \mathrm{Ext}^1_{\mathcal{R}}(F^1/F^0,\mathcal{R})_\mathfrak{p}$ has finite projective dimension. From the Auslander–Buchsbaum formula we then see that $\mathrm{Ext}^1_{\mathcal{R}}(F^1/F^0,\mathcal{R})_\mathfrak{p}$ has projective dimension at most one. From (75) it therefore follows that $\mathrm{im}(\partial_0^*)_\mathfrak{p}$ is a projective (hence free) $\mathcal{R}_\mathfrak{p}$-module of rank n_0 so that we have an isomorphism

$$\begin{aligned}\textstyle\bigwedge^{n_1}_{\mathcal{R}_\mathfrak{p}}(F^1)^*_\mathfrak{p} &\cong \big(\bigwedge^{n_1-n_0}_{\mathcal{R}_\mathfrak{p}}(F^1/F^0)^*_\mathfrak{p}\big) \otimes_{\mathcal{R}} \big(\bigwedge^{n_1-n_0}_{\mathcal{R}_\mathfrak{p}} \mathrm{im}(\partial_0^*)_\mathfrak{p}\big)\\ &\overset{(76)}{=} \big(\bigwedge^{n_1-n_0}_{\mathcal{R}_\mathfrak{p}}(F^1/F^0)^*_\mathfrak{p}\big) \otimes_{\mathcal{R}} \mathrm{Fitt}^0_{\mathcal{R}}(\mathrm{Ext}^1_{\mathcal{R}}(F^1/F^0,\mathcal{R})) \cdot \bigwedge^{n_0}_{\mathcal{R}_p}(F^0)^*_\mathfrak{p}.\end{aligned}$$

To finish the proof of claim (b), it therefore suffices to recall that, as already observed earlier, the restriction map $(F^1/F^0)^*_\mathfrak{p} \to H^1(C^\bullet)^*_\mathfrak{p}$ is surjective.
To prove claim (c), assume that $\mathfrak{p} \subseteq \mathcal{R}$ is a prime ideal of height at most one such that $\mathcal{R}_\mathfrak{p}$ is a regular local ring, so either a field or a discrete valuation domain. In this case, one has identifications $\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^*_\mathfrak{p} \cong \mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^{-1}_\mathfrak{p}$ and $\big(\bigcap^n_{\mathcal{R}} H^1(C^\bullet)\big)_\mathfrak{p} \cong \big(\bigwedge^n_{\mathcal{R}} H^1(C^\bullet)_{\mathrm{tf}}\big)_\mathfrak{p}$ with $H^1(C^\bullet)_{\mathrm{tf}} \coloneqq H^1(C^\bullet)/H^1(C^\bullet)_{\mathrm{tor}}$ the torsion-free quotient of $H^1(C^\bullet)$. Since the latter is a free $\mathcal{R}_\mathfrak{p}$-module, claim (c) follows from claim (b) and the equality

$$A \cdot M = \{a \in M \mid f(a) \in A \text{ for all } f \in M^*\}$$

that holds for every free $\mathcal{R}_\mathfrak{p}$-module M and $\mathcal{R}_\mathfrak{p}$-submodule A of the total ring of fractions of $\mathcal{R}_\mathfrak{p}$. □

(B.11) Remark. Results similar to Proposition (B.10) have previously appeared in various places, see for example [BS21, Prop. A.11]. The main novelty of Proposition (B.10) is that we do not need to assume $H^1(C^\bullet)^\vee_{\mathrm{tor}}$ to vanish, and in this regard our approach is related to [BST21a, Prop. 3.18].

(B.12) Lemma. *Let $\mathcal{R}$ be a ring that satisfies* (G_1). *For every finitely generated $\mathcal{R}$-module M with $\mathcal{R}$-torsion submodule M_{tor} there is a pseudo-isomorphism*

$$\mathrm{Ext}^1_{\mathcal{R}}(M,\mathcal{R}) \to M^\vee_{\mathrm{tor}}.$$

Proof. Since $\mathcal{R}$ is assumed to be quasi-normal, its total ring of fractions $\mathcal{Q}$ is a self-injective ring and so $\mathrm{Hom}_{\mathcal{R}}(-,\mathcal{Q}) \cong \mathrm{Hom}_{\mathcal{Q}}(-\otimes_{\mathcal{R}}\mathcal{Q},\mathcal{Q})$ is an exact functor. As a consequence, $\mathrm{Ext}^1_{\mathcal{R}}(-,\mathcal{Q})$ vanishes and we obtain a commutative diagram with exact rows of the form

$$\begin{array}{ccccccc}
\mathrm{Hom}_{\mathcal{R}}(M/M_{\mathrm{tor}},\mathcal{Q}) & \longrightarrow & \mathrm{Hom}_{\mathcal{R}}(M/M_{\mathrm{tor}},\mathcal{Q}/\mathcal{R}) & \longrightarrow & \mathrm{Ext}^1_{\mathcal{R}}(M/M_{\mathrm{tor}},\mathcal{R}) & \longrightarrow & 0 \\
\downarrow\simeq & & \downarrow & & \downarrow & & \\
\mathrm{Hom}_{\mathcal{R}}(M,\mathcal{Q}) & \longrightarrow & \mathrm{Hom}_{\mathcal{R}}(M,\mathcal{Q}/\mathcal{R}) & \longrightarrow & \mathrm{Ext}^1_{\mathcal{R}}(M,\mathcal{R}) & \longrightarrow & 0.
\end{array}$$

A diagram chase then shows that one has a composite map

$$\begin{aligned}
\mathrm{Ext}^1_{\mathcal{R}}(M,\mathcal{R}) &\twoheadrightarrow \mathrm{coker}\{\mathrm{Hom}_{\mathcal{R}}(M/M_{\mathrm{tor}},\mathcal{R}) \to \mathrm{Ext}^1_{\mathcal{R}}(M,\mathcal{R})\} &(79)\\
&\cong \mathrm{coker}\{\mathrm{Hom}_{\mathcal{R}}(M/M_{\mathrm{tor}},\mathcal{Q}/\mathcal{R}) \to \mathrm{Hom}_{\mathcal{R}}(M,\mathcal{Q}/\mathcal{R})\}\\
&\hookrightarrow \mathrm{Hom}_{\mathcal{R}}(M_{\mathrm{tor}},\mathcal{Q}/\mathcal{R}). &(80)
\end{aligned}$$

To show that this map is a pseudo-isomorphism, we may reduce to the case that $\mathcal{R}$ is a Gorenstein ring of dimension at most one. In this case, then, $\mathcal{Q}/\mathcal{R}$ is an injective $\mathcal{R}$-module (see [Bas63, Thm. 6.2 (2)]) and so the map (80) is an isomorphism. To show that (79) is an isomorphism it suffices to prove that $\mathrm{Ext}^1_{\mathcal{R}}(M/M_{\mathrm{tor}},\mathcal{R})$ vanishes. This follows from the fact that M/M_{tor} is a reflexive module (as can be seen from combining [Bas63, Thm. 6.2 (4)] and [Vas68, Thm. A.1]) so that dualising a projective presentation $P_1 \to P_0 \to (M/M_{\mathrm{tor}})^* \to 0$ gives an exact sequence $0 \to (M/M_{\mathrm{tor}}) \to P_0^* \to P_1^*$ from which we conclude that

$$\mathrm{Ext}^1_{\mathcal{R}}(M/M_{\mathrm{tor}},\mathcal{R}) \cong \mathrm{Ext}^3_{\mathcal{R}}(\mathrm{coker}\{P_0^* \to P_1^*\},\mathcal{R}) = 0$$

vanishes because $\mathcal{R}$ is Gorenstein of dimension at most one. □

B.3. Bockstein morphisms

In this section we recall the formalism of Bockstein morphisms that is a variant of the theory of algebraic height pairings developed by Nekovář in [Nek06, § 11]. We follow the treatment in [Bur07, § 10] but generalise it to the setting of Proposition (B.10).
We begin with an elementary, but important, observation.

(B.13) Lemma. *Let $\mathcal{R}$ be a commutative Noetherian ring, $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ a complex, and M a finitely generated $\mathcal{R}$-module.*

(a) If $i \in \mathbb{Z}$ is an integer such that $H^j(C^\bullet) = 0$ for all $j > i$, then the morphism $C^\bullet \to C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} M$ induces a natural isomorphism

$$H^i(C^\bullet) \otimes_{\mathcal{R}} M \xrightarrow{\simeq} H^i(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} M). \tag{81}$$

(b) Let $\mathfrak{a} \subseteq \mathcal{R}$ be an ideal and suppose there is an isomorphism $\nu\colon \mathcal{R}/\mathfrak{a} \xrightarrow{\simeq} \mathcal{R}[\mathfrak{a}]$ of $\mathcal{R}$-modules. Then ν induces a morphism $\nu_M\colon M \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}) \to M$ of $\mathcal{R}$-modules and an isomorphism

$$\nu_{C^\bullet}\colon C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}) \xrightarrow{\simeq} \mathrm{RHom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}, C^\bullet) \tag{82}$$

in $D(\mathcal{R})$. If $i \in \mathbb{Z}$ is an integer with $H^j(C^\bullet) = 0$ for all $j < i$, then $\nu_{C^\bullet}$ induces an injection

$$H^i(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})) \hookrightarrow H^i(C^\bullet)[\mathfrak{a}]. \tag{83}$$

Proof. Assuming $C^\bullet$ is acyclic in degrees greater than i, it admits a representative of the form

$$\cdots \to C^{i-2} \to C^{i-1} \to C^i \to 0, \tag{84}$$

where each C^j is a finitely generated projective $\mathcal{R}$-module that is placed in degree j. For every finitely generated $\mathcal{R}$-module M, the complex $C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} M$ can then be represented by

$$\cdots \to C^{i-2} \otimes_{\mathcal{R}} M \to C^{i-1} \otimes_{\mathcal{R}} M \to C^i \otimes_{\mathcal{R}} M \to 0$$

and, as the functor $(-)\otimes_{\mathcal{R}} M$ is right exact, this implies claim (a).
As for claim (b), we may define $\nu_M\colon M\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})\to M$ by means of the rule $m\otimes x\mapsto \nu(x)\cdot m$. To justify the isomorphism (82), we will identify $\mathrm{Hom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a},\mathcal{R})$ with the $\mathfrak{a}$-torsion submodule $R[\mathfrak{a}]$ of $\mathcal{R}$ via the isomorphism $\varphi\mapsto\varphi(1)$. For any morphism $f\colon A\to B$ of finitely generated free $\mathcal{R}$-modules one has a commutative diagram

$$\begin{array}{ccc} A\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}) & \xrightarrow{f} & B\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}) \\ \downarrow\simeq & & \downarrow\simeq \\ \mathrm{Hom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a},A) & \xrightarrow{f_*} & \mathrm{Hom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a},B), \end{array}$$

where the vertical isomorphisms are given by ν_A. Applying the functors $-\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})$ and $\mathrm{Hom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a},-)$ to the representative (84) we therefore see that the collection of maps $(\nu_{C^j})_{j\in\mathbb{Z}}$ defines an isomorphism of the form (82).
Assuming $C^\bullet$ is acyclic in degrees less than i, we may set $Q:=\mathrm{coker}\{C^{i-1}\to C^i\}$ to obtain the representative $0\to Q\xrightarrow{\partial} C^{i+1}\to\dots$ of $C^\bullet$. Consequently, $C^\bullet\otimes^{\mathbb{L}}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})$ is represented by $0\to Q\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})\to C^{i+1}\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})\to\dots$. In particular, we get the vertical dashed arrow on the left hand side in the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^i(C^\bullet) & \longrightarrow & Q & \xrightarrow{\partial} & C^{i+1} \\ & & \uparrow & & \nu_Q\uparrow & & \nu_{C^{i+1}}\uparrow \\ 0 & \longrightarrow & H^i(C^\bullet\otimes^{\mathbb{L}}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})) & \longrightarrow & Q\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}) & \xrightarrow{\partial\otimes\mathrm{id}} & C^{i+1}\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}). \end{array}$$

If we can prove that ν_Q is injective, then it will follow that the dashed arrow is injective as well, and this will prove the last part of claim (b). To do this, let l be the least integer with $C^l\neq 0$ and set $Q^j:=\mathrm{coker}(C^j\to C^{j-1}\}$ for all $j\in\{l,\dots,i-1\}$. We will then prove by induction on j that $\nu_{Q^j}\colon Q^j/\mathfrak{a}Q^j\to Q^j[\mathfrak{a}]$ is an isomorphism and $\mathrm{Ext}^1_{\mathcal{R}}(\mathcal{R}/\mathfrak{a},Q^j)=0$ for all $j\in\{l,\dots,i-1\}$. Taking $j=i-1$, this then proves the claimed injectivity of ν_Q.
For the base case of the induction we note that, because $C^j=0$ for all $j>l$ and $C^\bullet$ is acylic in degrees less than i, we have an exact sequence $0\to C^l\to C^{l-1}\to Q^l\to 0$. The long exact sequence obtained from applying the functor $(-)[\mathfrak{a}]\cong\mathrm{Hom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a},-)$ then shows that $\mathrm{Ext}^j_{\mathcal{R}}(\mathcal{R}/\mathfrak{a},Q^l)=0$ for all $j\geq 1$, and that we have a commutative diagram of the form

$$\begin{array}{ccccccc} C^l\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}) & \longrightarrow & C^{l-1}\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}) & \longrightarrow & Q^l\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}) & \longrightarrow & 0 \\ \nu_{C^l}\downarrow\simeq & & \nu_{C^{l-1}}\downarrow\simeq & & \downarrow\nu_{Q^l} & & \\ C^l[\mathfrak{a}] & \longrightarrow & C^{l-1}[\mathfrak{a}] & \longrightarrow & Q^l[\mathfrak{a}] & \longrightarrow & 0. \end{array}$$

It then follows from the Five Lemma that also ν_{Q^l} is an isomorphism. This proves the base case of the induction, and the inductive step follows by the same argument when instead applied to the exact sequence $0\to Q^j\to C^{j-2}\to Q^{j-1}\to 0$ for some $j\in\{l+1,\dots,i\}$ such that the claim has already been proven for all $j'<j$. □

The following technical consequence of Lemma (B.13) will be useful later on.

(B.14) Lemma. *Let $\mathcal{R}$ be a one-dimensional Gorenstein ring and $\mathfrak{a}\subseteq\mathcal{R}$ an ideal such that also $\mathcal{R}/\mathfrak{a}$ is a one-dimensional Gorenstein ring. We also suppose to be given a complex $C^\bullet\in D^{\mathrm{perf}}(\mathcal{R})$ that admits a representative of the form (69) and assume that*

$$\mathrm{pd}_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})\leq 1 \quad \textit{and} \quad \mathrm{pd}_{(\mathcal{R}/\mathfrak{a})}(H^1(C^\bullet)^\vee_{\mathrm{tor}}\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}))\leq 1. \tag{85}$$

Then there is an isomorphism

$$\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^*\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})\xrightarrow{\simeq}\mathrm{Fitt}^0_{(\mathcal{R}/\mathfrak{a})}(H^1(C^\bullet\otimes^{\mathbb{L}}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}))^\vee_{\mathrm{tor}})^*.$$

Proof. Consider the complex $D^\bullet:=\mathrm{RHom}_{\mathcal{R}}(C^\bullet,\mathcal{R})$. By dualising (69) we see that $H^i(D^\bullet)=0$ for all $i>0$ and so an application of Lemma (B.13) (a) shows that

$$H^0(D^\bullet)\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})\cong H^0(D^\bullet\otimes^{\mathbb{L}}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a})). \tag{86}$$

In addition, we may use the spectral sequence

$$E_2^{i,j} = \mathrm{Ext}^i_{\mathcal{R}}(H^{-j}(C^\bullet), \mathcal{R}) \quad \Rightarrow \quad E^{i+j} = H^{i+j}(D^\bullet)$$

to deduce that there is an isomorphism $H^0(D^\bullet) \cong \mathrm{Ext}^1_{\mathcal{R}}(H^1(C^\bullet), \mathcal{R})$. It therefore follows from Lemma (B.12) that

$$H^0(D^\bullet) \cong H^1(C^\bullet_{\mathrm{tor}})^\vee. \tag{87}$$

Now, the assumption (85) implies that $\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})$ is a principal ideal (x) generated by an element $x \in \mathcal{R}$ that is a nonzero divisor both in $\mathcal{R}$ and $\mathcal{R}/\mathfrak{a}$. By a standard property of Fitting ideals one has the exact sequence

$$\mathrm{Tor}_1^{\mathcal{R}}(\mathcal{R}/(x), \mathcal{R}/\mathfrak{a}) \to \mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}}) \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}) \to \mathrm{Fitt}^0_{(\mathcal{R}/\mathfrak{a})}(H^1(C^\bullet)^\vee_{\mathrm{tor}} \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})) \to 0$$

in which the first term is isomorphic to $(\mathcal{R}/\mathfrak{a})[x]$ and so vanishes because x is a nonzero divisor in $\mathcal{R}/\mathfrak{a}$ by (85). Thus, the second arrow is an isomorphism and so we have a composite isomorphism

$$\begin{aligned}
\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^* \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}) &\cong \mathrm{Hom}_{\mathcal{R}}(\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}}), \mathcal{R}/\mathfrak{a}) \\
&\cong \mathrm{Hom}_{\mathcal{R}}(\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}}) \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}), \mathcal{R}/\mathfrak{a}) \\
&\overset{(87)}{\cong} \mathrm{Hom}_{(\mathcal{R}/\mathfrak{a})}(\mathrm{Fitt}^0_{\mathcal{R}}(H^0(D^\bullet)) \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}), \mathcal{R}/\mathfrak{a}) \\
&\overset{(86)}{\cong} \mathrm{Fitt}^0_{(\mathcal{R}/\mathfrak{a})}(H^0(D^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})))^* \\
&\cong \mathrm{Fitt}^0_{(\mathcal{R}/\mathfrak{a})}(H^1(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}))^\vee_{\mathrm{tor}})^*
\end{aligned}$$

where the first isomorphism holds because $\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})$ is a free $\mathcal{R}$-module of rank one and the last isomorphism is (87) with $\mathcal{R}$ and $C^\bullet$ replaced by $\mathcal{R}/\mathfrak{a}$ and $C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})$. (Note that also the complex $D^\bullet \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}) \cong \mathrm{RHom}_{(\mathcal{R}/\mathfrak{a})}(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}), \mathcal{R}/\mathfrak{a})$ admits a representative of the form (69).) This concludes the proof of the lemma. □

(B.15) Remark. The proof of Lemma (B.14) shows that if, in the setting of said result, $\dim(\mathcal{R}) = 1$, then there is a canonical isomorphism $H^1(C^\bullet)^\vee_{\mathrm{tor}} \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}) \cong H^1(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}))^\vee_{\mathrm{tor}}$.

Let $\mathfrak{a} \subseteq \mathcal{R}$ be an ideal and $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ a complex. By tensoring the exact sequence $0 \to \mathfrak{a} \to \mathcal{R} \to \mathcal{R}/\mathfrak{a} \to 0$, with $C^\bullet$, we then obtain an exact triangle in $D(\mathcal{R})$ of the form

$$C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathfrak{a} \longrightarrow C^\bullet \longrightarrow C^\bullet \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}) \longrightarrow (C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathfrak{a})[1]. \tag{88}$$

The long exact sequence in cohomology associated with this triangle allows for the following definition.

(B.16) Definition. *Let $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ be a complex that is acyclic in degrees greater than 2. The 'Bockstein morphism' associated to $C^\bullet$ and an ideal $\mathfrak{a} \subseteq \mathcal{R}$ is defined to be the composite map*

$$\beta_{C^\bullet,\mathfrak{a}} \colon H^1(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})) \to H^2(C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \mathfrak{a}) \xrightarrow{\simeq} H^2(C^\bullet) \otimes_{\mathcal{R}} \mathfrak{a}$$

Here the first arrow is the connecting homomorphism of the triangle (88) and the second arrow is the isomorphism (81) with $M = \mathfrak{a}$.

We shall apply this construction in the setting of Definition (B.2). More precisely, we now assume we are given a quotient $\mathcal{Y}'$ of $H^2(C^\bullet)$ that is of the form

$$\mathcal{Y}' = \bigoplus_{i=1}^{d'} (\mathcal{R}/\mathfrak{a}_i) \tag{89}$$

for an integer $d' \geq 0$ and ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_{d'}$ of $\mathcal{R}$.
For every $i \in \{1, \ldots, d'\}$, we write $x_i^* \colon \mathcal{Y}' \to \mathcal{R}/\mathfrak{a}_i$ for the projection onto the i-th component and use this to define the map

$$\beta_i \colon H^1(C^\bullet \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})) \xrightarrow{\beta_{C^\bullet,\mathfrak{a}}} H^2(C^\bullet) \otimes_{\mathcal{R}} \mathfrak{a} \to \mathcal{Y}' \otimes_{\mathcal{R}} \mathfrak{a} \xrightarrow{x_i^*} \mathfrak{a}/\mathfrak{a}_i\mathfrak{a}.$$

To state the main result of this subsection, we now assume that $C^\bullet$ is acyclic outside degrees 1 and 2, and that there is an $\mathcal{R}$-linear isomorphism $\nu\colon \mathcal{R}/\mathfrak{a} \xrightarrow{\sim} \mathcal{R}[\mathfrak{a}]$. For every $f \in H^1(C^\bullet)^*$ we may then define an associated map $f^\nu \in H^1(C^\bullet \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}))^*$ as the composite map

$$H^1(C^\bullet \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})) \xrightarrow{(83)} \mathrm{Hom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}, H^1(C^\bullet)) \xrightarrow{f_*} \mathrm{Hom}_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}, \mathcal{R}) \xrightarrow{\nu^{-1}} \mathcal{R}/\mathfrak{a}.$$

Given $f \in \bigwedge^s_{\mathcal{R}} H^1(C^\bullet)^*$ for some integer $s \geq 0$, we write f^ν for the image of f under the map $\bigwedge^s_{\mathcal{R}} H^1(C^\bullet)^* \to \bigwedge^s_{\mathcal{R}/\mathfrak{a}} H^1(C^\bullet \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a}))^*$ induced by sending $f_1 \wedge \cdots \wedge f_s \mapsto f_1^\nu \wedge \cdots \wedge f_s^\nu$.

(B.17) Proposition. *Let $\mathcal{R}$ be a quasi-normal ring and $C^\bullet \in D^{\mathrm{perf}}(\mathcal{R})$ a complex that admits a standard representative with respect to a surjection $\kappa\colon H^2(C^\bullet) \to \mathcal{Y}'$ onto a module $\mathcal{Y}'$ of the form (89), and write $\mathfrak{X}$ for its standard ordered set of generators. We also assume $\mathfrak{a}_i = 0$ if $i \in \{1, \dots, d\}$ for some $d \leq d'$. Let $\mathfrak{a}$ be an ideal containing $\mathfrak{a}_{d+i}$ for all $i \in \{1, \dots, d'-d\}$, and write $\mathfrak{B}$ (resp. $\mathfrak{B}'$) for the canonical ordered $\mathcal{R}$-basis (resp. $\mathcal{R}/\mathfrak{a}$-basis) of $\mathcal{Y} := \bigoplus_{i=1}^d \mathcal{R}$ (resp. of $\mathcal{Y}' \otimes_{\mathcal{R}} (\mathcal{R}/\mathfrak{a})$). Setting $n := d + n_1 - (n_0 + n_2)$, $s := d' - d$, and $\mathfrak{A} := \prod_{i=d+1}^{d'} \mathfrak{a}_i$, the following claims are then valid.*

(a) For every $a \in \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1}$ and $f \in \bigwedge^n_{\mathcal{R}} H^1(C^\bullet)^*$, one has a containment

$$f(\varpi_{C^\bullet,\mathfrak{B}}(a)) \in \mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^* \otimes_{\mathcal{R}} \mathfrak{A}^{**}.$$

(b) Assume that $\overline{\mathcal{R}} := \mathcal{R}/\mathfrak{a}$ is a one-dimensional Gorenstein ring, set $\overline{C}^\bullet := C^\bullet \otimes^{\mathbb{L}}_{\mathcal{R}} \overline{\mathcal{R}}$, and suppose that $\mathrm{pd}_{\mathcal{R}}(H^1(\overline{C}^\bullet)^\vee_{\mathrm{tor}}) \leq 1$. For every $i \in \{1, \dots, s\}$ there is a morphism $\widetilde{\beta}_{d+i} \in \mathrm{Hom}_{\overline{\mathcal{R}}}(H^1(\overline{C}^\bullet), \overline{\mathcal{R}}) \otimes_{\overline{\mathcal{R}}} (\mathfrak{a}/\mathfrak{a}_{d+i}\mathfrak{a})$ such that the natural map

$$\mathrm{Hom}_{\overline{\mathcal{R}}}(H^1(\overline{C}^\bullet), \overline{\mathcal{R}}) \otimes_{\overline{\mathcal{R}}} (\mathfrak{a}/\mathfrak{a}_{d+i}\mathfrak{a}) \to \mathrm{Hom}_{\overline{\mathcal{R}}}(H^1(\overline{C}^\bullet), \mathfrak{a}/\mathfrak{a}_{d+i}\mathfrak{a})$$

sends $\widetilde{\beta}_{d+i}$ to β_{d+i}, and the maps $(\widetilde{\beta}_{d+i})_{1 \leq i \leq s}$ induce a map

$$(\textstyle\bigwedge_{1 \leq i \leq s} \widetilde{\beta}_{d+i})\colon \big(I \otimes_{\overline{\mathcal{R}}} \bigwedge^{n+s}_{\overline{\mathcal{R}}} H^1(\overline{C}^\bullet)^*\big)^* \to \big(I \otimes_{\overline{\mathcal{R}}} \bigwedge^{n}_{\overline{\mathcal{R}}} H^1(\overline{C}^\bullet)^*\big)^* \otimes_{\overline{\mathcal{R}}} (\mathfrak{a}^s/\mathfrak{a}\mathfrak{A}),$$

where $I := \mathrm{Fitt}^0_{\overline{\mathcal{R}}}(H^1(\overline{C}^\bullet)^\vee_{\mathrm{tor}})$.

(c) Assume $\mathcal{R}$ and $\overline{\mathcal{R}}$ are one-dimensional Gorenstein rings and that (85) is valid so that, by Lemma (B.14)), one has an isomorphism

$$\mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})^* \otimes_{\mathcal{R}} (\mathfrak{a}^s/\mathfrak{a}\mathfrak{A}) \cong I^* \otimes_{\overline{\mathcal{R}}} (\mathfrak{a}^s/\mathfrak{a}\mathfrak{A}). \tag{90}$$

Then, for every $a \in \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1}$ and $f \in \bigwedge^{n+d}_{\mathcal{R}} H^1(C^\bullet)^*$ one has an equality

$$f(\varpi_{C^\bullet,\mathfrak{B}}(a)) = (-1)^{ns} \cdot (f^\nu \circ \textstyle\bigwedge_{1 \leq i \leq s} \widetilde{\beta}_{d+i})(\varpi_{\overline{C}^\bullet,\mathfrak{B}'}(\overline{a}))$$

in (90), where $\overline{a}$ denotes the image of a under the canonical map

$$\mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} \to \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1} \otimes_{\mathcal{R}} \overline{\mathcal{R}} \cong \mathrm{Det}_{\overline{\mathcal{R}}}(\overline{C}^\bullet)^{-1}.$$

Proof. This is a generalisation of the argument of [Bur07, Lem. 10.2] (see also [BKS16, Lem. 5.22]). By assumption, one has a surjective map $H^2(C^\bullet) \twoheadrightarrow \mathcal{Y}'$, from which it follows that $\mathrm{Fitt}^d_{\mathcal{R}}(H^2(C^\bullet))$ is contained in $\mathrm{Fitt}^d_{\mathcal{R}}(\mathcal{Y}') = \mathfrak{A}$. The first claim therefore follows from Proposition (B.10) (b).

To prove claim (b), we fix a standard representative $F^0 \xrightarrow{\partial_0} F^1 \xrightarrow{\partial_1} F_2$ of $C^\bullet$ with respect to κ and $\mathfrak{X}$. We also set $\overline{F}^i := F^i \otimes_{\mathcal{R}} \overline{\mathcal{R}}$ for every $i \in \{0, 1, 2\}$, write $\overline{\partial}_i\colon \overline{F}^i \to \overline{F}^{i+1}$ for the map induced by ∂_i, and note that $\overline{F}^0 \xrightarrow{\overline{\partial}_0} \overline{F}^1 \xrightarrow{\overline{\partial}_1} \overline{F}_2$ is a standard representative for $\overline{C}^\bullet$. Define $\overline{Q} := \overline{F}^1/\overline{F}^0$ and note that taking $\overline{\mathcal{R}}$-linear duals leads to an exact sequence

$$0 \to \overline{Q}^* \to (\overline{F}^0)^* \xrightarrow{\overline{\partial}_0^*} (\overline{F}^1)^* \to \mathrm{Ext}^1_{\overline{\mathcal{R}}}(\overline{Q}, \overline{\mathcal{R}}) \to 0.$$

We have seen in the proof of Proposition (B.10) that the natural map $\mathrm{Ext}^1_{\overline{\mathcal{R}}}(\overline{Q}, \overline{\mathcal{R}}) \to \mathrm{Ext}^1_{\overline{\mathcal{R}}}(H^1(\overline{C}^\bullet), \overline{\mathcal{R}})$ is a pseudo-isomorphism, and hence an isomorphism because we are assuming $\overline{\mathcal{R}}$ to be one-dimensional. Our assumption that $\mathrm{Ext}^1_{\overline{\mathcal{R}}}(H^1(\overline{C}^\bullet), \overline{\mathcal{R}})$ is of projective dimension at most one therefore implies that the kernel of $\overline{\partial}_0^*$ is projective (by Schanuel's lemma). From the above

exact sequence we conclude that $\overline{Q}^*$, and hence also $\overline{Q}^{**}$, is $\overline{\mathcal{R}}$-projective. In particular, for every finitely generated $\overline{\mathcal{R}}$-module M, the central vertical map in the following commutative diagram is an isomorphism.

$$\begin{array}{ccccccc} & & \overline{\partial_1}(\overline{F}^1)^* \otimes_{\overline{\mathcal{R}}} M & \longrightarrow & \overline{Q}^* \otimes_{\overline{\mathcal{R}}} M & \longrightarrow & H^1(\overline{C}^\bullet) \otimes_{\overline{\mathcal{R}}} M \longrightarrow 0 \\ & & \downarrow & & \downarrow\simeq & & \downarrow \\ 0 & \longrightarrow & \mathrm{Hom}_{\overline{\mathcal{R}}}(\overline{\partial_1}(\overline{F}^1), M) & \longrightarrow & \mathrm{Hom}_{\overline{\mathcal{R}}}(\overline{Q}, M) & \longrightarrow & \mathrm{Hom}_{\overline{\mathcal{R}}}(H^1(\overline{C}^\bullet), M) \end{array} \tag{91}$$

To justify exactness of the top line of this diagram we recall that if N is a finitely generated torsion-free $\overline{\mathcal{R}}$-module, then $\mathrm{Ext}^1_{\overline{\mathcal{R}}}(N, \overline{\mathcal{R}})$ vanishes because $\overline{\mathcal{R}}$ is a one-dimensional Gorenstein ring. Dualising the exact sequence

$$0 \to H^1(\overline{C}^\bullet) \to \overline{Q} \to \overline{\partial_1}(\overline{F}^1) \to 0 \tag{92}$$

and tensoring the resulting exact sequence with M then gives the top line of the above diagram. The bottom line, on the other hand, is obtained by applying the functor $\mathrm{Hom}_{\overline{\mathcal{R}}}(-, M)$ to (92). From the diagram (91), applied with $M = \mathfrak{a}/\mathfrak{a}_{d+i}\mathfrak{a}$, we see that it suffices to prove that β_{d+i} can be lifted to $\mathrm{Hom}_{\overline{\mathcal{R}}}(\overline{Q}, \mathfrak{a}/\mathfrak{a}_{d+1}\mathfrak{a})$ in order to define $\widetilde{\beta}_{d+i}$. To do this, we note that by definition β_{d+i} coincides with the composition of the snake lemma map arising from the diagram

$$\begin{array}{ccccccc} \mathfrak{a} \otimes_{\mathcal{R}} Q & \longrightarrow & Q & \longrightarrow & Q \otimes_{\mathcal{R}} \overline{\mathcal{R}} & \longrightarrow & 0 \\ \downarrow\partial_1 & & \downarrow\partial_1 & & \downarrow\partial_1 & & \\ 0 \longrightarrow \mathfrak{a} \otimes_{\mathcal{R}} F^2 & \longrightarrow & F^2 & \longrightarrow & F^2 \otimes_{\mathcal{R}} \overline{\mathcal{R}} & \longrightarrow & 0 \end{array}$$

composed with x^*_{d+i}. By condition (iv) in Definition (B.3) one therefore has

$$\beta_{d+i}(\overline{m}) = (b^*_{d+i} \circ \partial_1)(m) \mod \mathfrak{a}_{d+i}\mathfrak{a} \tag{93}$$

if $\overline{m} \in H^1(\overline{C}^\bullet)$ is the image of $m \in F^1$ under the surjective map $F^1 \to \overline{F}^1 \to \overline{Q}$. This definition clearly extends to $\overline{Q}$ and so by the above discussion we obtain the desired lift $\widetilde{\beta}_i$ of β_{d+i} to $H^1(\overline{C}^\bullet)^* \otimes_{\overline{\mathcal{R}}} (\mathfrak{a}/\mathfrak{a}_{d+i}\mathfrak{a})$.

For every $i \in \{1, \dots, s\}$ we may then write $\widetilde{\beta}_{d+i} = \sum_{j=1}^{n_i} \psi_j \otimes c_j$ for suitable $n_i \in \mathbb{N}$, $\psi_j \in H^1(\overline{C}^\bullet)^*$, and $c_j \in \mathfrak{a}/\mathfrak{a}_{d+i}\mathfrak{a}$. Given this, we may define the map $\bigwedge_{1 \le i \le s} \widetilde{\beta}_{d+i}$ in the statement of claim (b) by means of

$$(\textstyle\bigwedge_{1 \le i \le s} \widetilde{\beta}_{d+i})(\lambda \otimes \varphi) \coloneqq \displaystyle\sum_{j_1=1}^{n_1} \cdots \sum_{j_s=1}^{n_s} \Phi(\lambda \otimes \psi_{j_1} \wedge \cdots \wedge \psi_{j_s} \wedge \varphi) \otimes \prod_{i=1}^{s} c_{j_i}$$

for all $\Phi \in (I \otimes_{\overline{\mathcal{R}}} \bigwedge^{n+s}_{\overline{\mathcal{R}}} H^1(\overline{C}^\bullet)^*)^*$.

To prove claim (c), we fix $a \in \mathrm{Det}_{\mathcal{R}}(C^\bullet)^{-1}$, set $J \coloneqq \mathrm{Fitt}^0_{\mathcal{R}}(H^1(C^\bullet)^\vee_{\mathrm{tor}})$, and and regard $\varpi_{C^\bullet,\mathfrak{B}}(a)$ as an element of $(J \otimes_{\mathcal{R}} \bigwedge^{n+d}_{\mathcal{R}}(F^1)^*)^*$. If we fix an $\mathcal{R}$-basis $c_1, \dots, c_{n_0}$ of F^0, then we can write a as $(\bigwedge_{1 \le i \le n_0} c_i^*) \otimes a' \otimes (\bigwedge_{1 \le i \le n_2} b_i^*)$ for some $a' \in \bigwedge^{n_1}_{\mathcal{R}} F^1$. By definition of $\varpi_{C^\bullet,\mathfrak{B}}$, one then has for all $\lambda \otimes \varphi \in J \otimes_{\mathcal{R}} \bigwedge^{n+s}_{\mathcal{R}} F_1^*$ that

$$\begin{aligned} \varpi_{C^\bullet,\mathfrak{B}}(a)(\lambda \otimes \varphi) &= (-1)^{n(n_2-d)} \cdot \varphi\big(\lambda \cdot \textstyle\bigwedge_{1 \le i \le n_0} c_i^* \wedge \bigwedge_{d+1 \le i \le n_2} (b_i^* \circ \partial_1)\big)(a') \\ &= (-1)^{s(n_2-d')} \cdot (-1)^{n(n_2-d)} \cdot (\textstyle\bigwedge_{d+1 \le i \le d'} (b_i^* \circ \partial_1) \wedge \varphi)(z) \end{aligned}$$

with the abbreviation

$$z \coloneqq \big(\lambda \cdot \textstyle\bigwedge_{1 \le i \le n_0} c_i^* \wedge \bigwedge_{d'+1 \le i \le n_2} (b_i^* \circ \partial_1)\big)(a').$$

On the other hand, for all $\lambda \otimes \varphi \in I \otimes_{\overline{\mathcal{R}}} \bigwedge^{n+s}_{\overline{\mathcal{R}}}(\overline{F}^1)^*$ one has

$$\varpi_{\overline{C}^\bullet,\mathfrak{B}'}(\overline{a})(\lambda \otimes \varphi) = (-1)^{n'(n_2-d')} \cdot \varphi\big(\lambda \cdot \textstyle\bigwedge_{1 \le i \le n_0} c_i^* \wedge \bigwedge_{d'+1 \le i \le n_2} (b_i^* \circ \partial_1)\big)(a') \mod \mathfrak{a}$$

with $n' \coloneqq n+s$. Here we have used that $\overline{F}^0 \to \overline{F}^1 \to \overline{F}^2$ is a standard representative for $\overline{C}^\bullet$ with respect to $(\overline{\kappa}, \mathfrak{B}')$, where $\overline{\kappa}\colon H^2(\overline{C}^\bullet) \to \mathcal{Y}'$ is the map induced by κ. Writing π for the canonical projection $\mathfrak{A}\cdot(J \otimes_{\mathcal{R}} \bigwedge^n_{\mathcal{R}}(F^1)^*)^* \to \mathfrak{A} \otimes_{\overline{\mathcal{R}}} (I \otimes_{\overline{\mathcal{R}}} \bigwedge^n_{\overline{\mathcal{R}}}(\overline{F}^1)^*)^*$, we arrive at

$$\pi(\varpi_{C^\bullet,\mathfrak{B}}(a)) = (-1)^{ns} \cdot (\textstyle\bigwedge_{1\le i\le s}(b^*_{d+i}\circ\partial_1))(\varpi_{\overline{C}^\bullet,\mathfrak{B}'}(\overline{a})) \mod \mathfrak{a}\mathfrak{A}$$

by comparing with the definition of z. Given this, the equality claimed in (b) follows from (93) and Lemma (B.19) below. □

(B.18) Remark. The maps $\widetilde{\beta}_i$ could in principle be not uniquely specified by their properties described in Proposition (B.17) (b). This ambiguity will however not cause any problems in any of the applications of Proposition (B.17) (c) in the main body of the article.

(B.19) Lemma. *Let M be an $\mathcal{R}$-module and denote the canonical projection $M \to M\otimes(\mathcal{R}/\mathfrak{a})$ by π_M. Assume there is an $\mathcal{R}$-linear isomorphism $\nu\colon \mathcal{R}/\mathfrak{a} \xrightarrow{\simeq} \mathcal{R}[\mathfrak{a}]$ and, for every $f \in M^*$, define $f^\nu\colon M\otimes_{\mathcal{R}}(\mathcal{R}/\mathfrak{a}) \to \mathcal{R}/\mathfrak{a}$ by $f^\nu(m\otimes\pi_{\mathcal{R}}(r)) \coloneqq \nu^{-1}(f(\nu(\pi_{\mathcal{R}}(r))\cdot m))$. Then one has*

$$\pi_{\mathcal{R}}(f(m)) = f^\nu(\pi_M(m)) \quad \text{in } \mathcal{R}/\mathfrak{a}$$

for every $f \in M^*$.

Proof. We may calculate that

$$\begin{aligned} f^\nu(\pi_M(m)) = f^\nu(m\otimes\pi_{\mathcal{R}}(1)) = \nu^{-1}(f(\nu(\pi_{\mathcal{R}}(1))\cdot m)) = \nu^{-1}(\nu(\pi_{\mathcal{R}}(1))\cdot f(m)) \\ = \nu^{-1}(\nu(\pi_{\mathcal{R}}(1)\cdot f(m))) = \pi_{\mathcal{R}}(1\cdot f(m)) = \pi_{\mathcal{R}}(f(m)), \end{aligned}$$

as claimed. □

Acknowledgments The authors would like to extend their gratitude to Daniel Barrera Salazar, David Burns, Masato Kurihara, Juan-Pablo Llerena-Córdova, Daniel Macías Castillo, Rei Otsuki, Rob Rockwood, Takamichi Sano, and Christian Wuthrich for helpful comments and discussions.

The research for this article was carried out while the first and second authors held, respectively, a Doctoral Prize Fellowship funded by the Engineering and Physical Sciences Research Council [EP/W524335/1] at University College London and a Heilbronn Research Fellowship at Imperial College London. The authors gratefully acknowledge the support of these institutions.

References

[Bas63] Hyman Bass. *On the ubiquity of Gorenstein rings*. Math. Z. 82 (1963), pp. 8–28.

[BG17] Felix Bergunde and Lennart Gehrmann. *On the order of vanishing of Stickelberger elements of Hilbert modular forms*. Proc. Lond. Math. Soc. (3) 114.1 (2017), pp. 103–132.

[BD94] Massimo Bertolini and Henri Darmon. *Derived heights and generalized Mazur-Tate regulators*. Duke Math. J. 76.1 (1994), pp. 75–111.

[BSD65] Bryan Birch and Peter Swinnerton-Dyer. *Notes on elliptic curves. II*. J. Reine Angew. Math. 218 (1965), pp. 79–108.

[BH20] Werner Bley and Martin Hofer. *Construction of elliptic $\mathfrak{p}$-units*. In: ***Development of Iwasawa Theory - the Centennial of K. Iwasawa's Birth***. Advanced Studies in Pure Mathematics 86. 2020, pp. 79–111.

[BK90] Spencer Bloch and Kazuya Kato. "L-functions and Tamagawa numbers of motives". In: ***The Grothendieck Festschrift, Vol. I***. Vol. 86. Progr. Math. Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[Bou74] Nicolas Bourbaki. *Elements of mathematics. Algebra, Part I: Chapters 1-3*. Translated from the French, Hermann, Paris (1974).

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond and Richard Taylor. *On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises*. J. Amer. Math. Soc. 14.4 (2001), pp. 843–939.

[BB25] Dominik Bullach and David Burns. *On Euler systems and Nekovář–Selmer complexes*. Preprint (2025).

[BD21] Dominik Bullach and Alexandre Daoud. *On universal norms for p-adic representations in higher-rank Iwasawa theory*. Acta Arith. 201.1 (2021), pp. 63–108.

[BH23] Dominik Bullach and Martin Hofer. *The equivariant Tamagawa Number Conjecture for abelian extensions of imaginary quadratic fields*. Doc. Math. 28.2 (2023), pp. 369–418.

[Bur07] David Burns. *Congruences between derivatives of abelian L-functions at $s = 0$*. Invent. Math. 169.3 (2007), pp. 451–499.

[BF98] David Burns and Matthias Flach. *On Galois structure invariants associated to Tate motives*. Amer. J. Math. 120.6 (1998), pp. 1343–1397.

[BF01] David Burns and Matthias Flach. *Tamagawa numbers for motives with (non-commutative) coefficients*. Doc. Math. 6 (2001), pp. 501–570.

[BKS16] David Burns, Masato Kurihara and Takamichi Sano. *On zeta elements for $\mathbb{G}_m$*. Doc. Math. 21 (2016), pp. 555–626.

[BKS17] David Burns, Masato Kurihara and Takamichi Sano. *On Iwasawa theory, zeta elements for $\mathbb{G}_m$, and the equivariant Tamagawa number conjecture*. Algebra Number Theory 11.7 (2017), pp. 1527–1571.

[BKS25] David Burns, Masato Kurihara and Takamichi Sano. *On derivatives of Kato's Euler system and the Mazur-Tate Conjecture*. Int. Math. Res. Not. 4 (2025), pp. 1–26.

[BMC24] David Burns and Daniel Macias Castillo. *On refined conjectures of Birch and Swinnerton-Dyer type for Hasse-Weil-Artin L-series*. Mem. Amer. Math. Soc. 297.1482 (2024).

[BMCW18] David Burns, Daniel Macias Castillo and Christian Wuthrich. *On Mordell-Weil groups and congruences between derivatives of twisted Hasse-Weil L-functions*. J. Reine Angew. Math. 734 (2018), pp. 187–228.

[BSS25] David Burns, Ryotaro Sakamoto and Takamichi Sano. *On the theory of higher rank Euler, Kolyvagin and Stark systems, II*. To appear in Algebra Number Theory (2025). arXiv: `1805.08448`.

[BS21] David Burns and Takamichi Sano. *On the theory of higher rank Euler, Kolyvagin and Stark systems*. Int. Math. Res. Not. 13 (2021), pp. 10118–10206.

[BST21a] David Burns, Takamichi Sano and Kwok-Wing Tsoi. *On higher special elements of p-adic representations*. Int. Math. Res. Not 20 (2021), pp. 15337–15411.

[BF24] Ashay Burungale and Matthias Flach. *The conjecture of Birch and Swinnerton-Dyer for certain elliptic curves with complex multiplication*. Cambridge J. Math. 12.2 (2024), pp. 357–415.

[BST21b] Ashay A. Burungale, Christopher Skinner and Ye Tian. "The Birch and Swinnerton-Dyer conjecture: a brief survey". In: ***Nine mathematical challenges—an elucidation***. Vol. 104. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI, 2021, pp. 11–29.

[CL22] Antonio Cauchi and Antonio Lei. *On analogues of Mazur-Tate type conjectures in the Rankin-Selberg setting*. Publ. Mat. 66.2 (2022), pp. 571–630.

[Čes18] Kestutis Česnavičius. *The Manin constant in the semistable case*. Compos. Math. 154.9 (2018), pp. 1889–1920.

[ČNS24] Kestutis Česnavičius, Michael Neururer and Abhishek Saha. *The Manin constant and the modular degree*. J. Eur. Math. Soc. (JEMS) 26.2 (2024), pp. 573–637.

[Dar92] Henri Darmon. *A refined conjecture of Mazur-Tate type for Heegner points*. Invent. Math. 110.1 (1992), pp. 123–146.

[Dar95] Henri Darmon. *Thaine's method for circular units and a conjecture of Gross*. Canad. J. Math. 47.2 (1995), pp. 302–317.

[Dar04] Henri Darmon. ***Rational points on modular elliptic curves***. Vol. 101. CBMS Regional Conference Series in Mathematics. Conference Board of the Mathematical Sciences Washington DC; by the American Mathematical Society Providence RI, 2004.

[Del08] Daniel Delbourgo. ***Elliptic curves and big Galois representations***. Vol. 356. London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2008.

[DS06] Fred Diamond and Jerry Shurman. ***A First Course in Modular Forms***. Graduate Texts in Mathematics. Springer New York, 2006. ISBN: 9780387272269.

[DD10] Tim Dokchitser and Vladimir Dokchitser. *On the Birch-Swinnerton-Dyer quotients modulo squares*. Ann. of Math. (2) 172.1 (2010), pp. 567–596.

[Dri73] Vladimir G. Drinfeld. *Two theorems on modular curves*. Funkcional. Anal. i Priložen. 7.2 (1973), pp. 83–84.

[Edi91] Bas Edixhoven. "On the Manin constants of modular elliptic curves". In: ***Arithmetic algebraic geometry (Texel, 1989)***. Vol. 89. Progr. Math. Birkhäuser Boston, Boston, MA, 1991, pp. 25–39.

[EN18] Nils Ellerbrock and Andreas Nickel. *On formal groups and Tate cohomology in local fields*. Acta Arith. 182.3 (2018), pp. 285–299.

[EPW25] Matthew Emerton, Robert Pollack and Tom Weston. *Explicit reciprocity laws and Iwasawa theory for modular forms*. Duke Math. J. 174 (2025).

[Fla00] Matthias Flach. *Euler characteristics in relative K-groups*. Bull. London Math. Soc. 32.3 (2000), pp. 272–284.

[Fla04] Matthias Flach. "The equivariant Tamagawa number conjecture: a survey". In: ***Stark's conjectures: recent work and new directions***. Vol. 358. Contemp. Math. With an appendix by C. Greither. Amer. Math. Soc., Providence, RI, 2004, pp. 79–125.

[FPR94] Jean-Marc Fontaine and Bernadette Perrin-Riou. "Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L". In: ***Motives (Seattle, WA, 1991)***. Vol. 55. Proc. Sympos. Pure Math. Amer. Math. Soc., Providence, RI, 1994, pp. 599–706.

[FK06] Takako Fukaya and Kazuya Kato. *A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory*. In: ***Proceedings of the St. Petersburg Mathematical Society. Vol. XII***. Vol. 219. Amer. Math. Soc. Transl. Ser. 2. Amer. Math. Soc., Providence, RI, 2006, pp. 1–85.

[GS93] Ralph Greenberg and Glenn Stevens. *p-adic L-functions and p-adic periods of modular forms*. Invent. Math. 111.2 (1993), pp. 407–447.

[Gro88] Benedict H. Gross. *On the values of abelian L-functions at s= 0*. J. Fac. Sci. Univ. Tokyo Sect. IA Math 35.1 (1988), pp. 177–197.

[Gro11] Benedict H. Gross. "Lectures on the conjecture of Birch and Swinnerton-Dyer". In: ***Arithmetic of L-functions***. Vol. 18. IAS/Park City Math. Ser. Amer. Math. Soc., Providence, RI, 2011, pp. 169–209.

[Hon68] Taira Honda. *Formal groups and zeta-functions*. Osaka Math. J. 5 (1968), pp. 199–213.

[Hon70] Taira Honda. *On the theory of commutative formal groups*. J. Math. Soc. Japan 22 (1970), pp. 213–246.

[Kat21] Takenori Kataoka. *Equivariant Iwasawa theory for elliptic curves*. Math. Z. 298.3-4 (2021), pp. 1653–1725.

[Kat22] Takenori Kataoka. *Stark systems and equivariant main conjectures*. Osaka J. Math. 59.2 (2022), pp. 417–452.

[Kat] Kazuya Kato. *Lectures on the approach to Iwasawa theory of Hasse-Weil L-functions via B_{dR}. Part II. Local main conjecture.* Unpublished ().

[Kat93] Kazuya Kato. "Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via B_{dR}. I". In: ***Arithmetic algebraic geometry (Trento, 1991)***. Vol. 1553. Lecture Notes in Math. Springer, Berlin, 1993, pp. 50–163.

[Kat04] Kazuya Kato. "p-adic Hodge theory and values of zeta functions of modular forms". In: 295. Cohomologies p-adiques et applications arithmétiques. III. 2004.

[Kim23] Chan-Ho Kim. ***Refined applications of Kato's Euler systems for modular forms***. 2023. arXiv: 2203.12157.

[KK21] Chan-Ho Kim and Masato Kurihara. *On the refined conjectures on Fitting ideals of Selmer groups of elliptic curves with supersingular reduction*. Int. Math. Res. Not. 14 (2021), pp. 10559–10599.

[Kin11] Guido Kings. "The equivariant Tamagawa number conjecture and the Birch-Swinnerton-Dyer conjecture". In: ***Arithmetic of L-functions***. Vol. 18. IAS/Park City Math. Ser. Amer. Math. Soc., Providence, RI, 2011, pp. 315–349.

[KM76] Finn Faye Knudsen and David Mumford. *The projectivity of the moduli space of stable curves. I. Preliminaries on "det" and "Div"*. Math. Scand. 39.1 (1976), pp. 19–55.

[Kob03] Shinichi Kobayashi. *Iwasawa theory for elliptic curves at supersingular primes*. Invent. Math. 152.1 (2003), pp. 1–36.

[Kob06] Shinichi Kobayashi. *An elementary proof of the Mazur-Tate-Teitelbaum conjecture for elliptic curves*. Doc. Math. (2006), pp. 567–575.

[Kur02] Masato Kurihara. *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction. I*. Invent. Math. 149.1 (2002), pp. 195–224.

[Kur03] Masato Kurihara. *Iwasawa theory and Fitting ideals*. J. Reine Angew. Math. 561 (2003), pp. 39–86.

[Kur14] Masato Kurihara. "The structure of Selmer groups of elliptic curves and modular symbols". In: ***Iwasawa theory 2012***. Vol. 7. Contrib. Math. Comput. Sci. Springer, Heidelberg, 2014, pp. 317–356.

[LT76] Serge Lang and Hale Trotter. ***Frobenius distributions in GL_2-extensions***. Vol. Vol. 504. Lecture Notes in Mathematics. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. Springer-Verlag, Berlin-New York, 1976.

[Lec23] Emmanuel Lecouturier. *On the Mazur-Tate conjecture for prime conductor and Mazur's Eisenstein ideal*. Amer. J. Math. 145.5 (2023), pp. 1365–1387.

[LC24] Juan-Pablo Llerena-Córdova. *Numerical study of refined conjectures of the BSD type* (2024). arXiv: 2412.17703.

[Man72] Yuri I. Manin. *Parabolic points and zeta functions of modular curves*. Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), pp. 19–66.

[Maz72] Barry Mazur. *Rational points of abelian varieties with values in towers of number fields*. Invent. Math. 18 (1972), pp. 183–266.

[Maz78] Barry Mazur. *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*. Invent. Math. 44.2 (1978), pp. 129–162.

[MR04] Barry Mazur and Karl Rubin. *Kolyvagin systems*. Mem. Amer. Math. Soc. 168.799 (2004), pp. viii+96.

[MR16] Barry Mazur and Karl Rubin. *Refined class number formulas for $\mathbb{G}_m$*. J. Théor. Nombres Bordeaux 28.1 (2016), pp. 185–211.

[MT87] Barry Mazur and John Tate. *Refined conjectures of the "Birch and Swinnerton-Dyer type"*. Duke Math. J. 54.2 (1987), pp. 711–750.

[MTT86] Barry Mazur, John Tate and Jeremy Teitelbaum. *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*. Invent. Math. 84.1 (1986), pp. 1–48.

[Nek06] Jan Nekovář. *Selmer complexes*. Astérisque 310 (2006), pp. viii+559.

[NSW08] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg. ***Cohomology of number fields***. Second. Vol. 323. Fundamental Principles of Mathematical Sciences. Springer-Verlag, Berlin, 2008.

[Ota18] Kazuto Ota. *Kato's Euler system and the Mazur-Tate refined conjecture of BSD type*. Amer. J. Math. 140.2 (2018), pp. 495–542.

[Ota23] Kazuto Ota. *On the rank-part of the Mazur-Tate refined conjecture for higher weight modular forms*. Ann. Inst. Fourier (Grenoble) 73.3 (2023), pp. 1319–1364.

[Ots09] Rei Otsuki. *Construction of a homomorphism concerning Euler systems for an elliptic curve*. Tokyo J. Math. 32.1 (2009), pp. 253–278.

[Pol05] Robert Pollack. *An algebraic version of a theorem of Kurihara*. J. Number Theory 110.1 (2005), pp. 164–177.

[Pop02] Cristian D. Popescu. *Base change for Stark-type conjectures "over $\mathbb{Z}$"*. J. Reine Angew. Math. 542 (2002), pp. 85–111.

[PB19] Francisco X. Portillo-Bobadilla. *Experimental evidence on a refined conjecture of the BSD type*. Bol. Soc. Mat. Mex. (3) 25.3 (2019), pp. 529–541.

[Qin16] Hourong Qin. *Anomalous primes of the elliptic curve $E_D\colon y^2 = x^3 + D$*. Proc. Lond. Math. Soc. (3) 112.2 (2016), pp. 415–453.

[Rob00] Alain M. Robert. ***A course in p-adic analysis***. Vol. 198. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000.

[Rub96] Karl Rubin. *A Stark conjecture "over $\mathbb{Z}$" for abelian L-functions with multiple zeros*. Ann. Inst. Fourier (Grenoble) 46.1 (1996), pp. 33–62.

[Sak23] Ryotaro Sakamoto. *A higher rank Euler system for $\mathbb{G}_m$ over a totally real field*. Amer. J. Math. 145.1 (2023), pp. 65–108.

[San14] Takamichi Sano. *Refined abelian Stark conjectures and the equivariant leading term conjecture of Burns*. Compos. Math. 150.11 (2014), pp. 1809–1835.

[Ser72] Jean-Pierre Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. 15.4 (1972), pp. 259–331.

[Ser81] Jean-Pierre Serre. *Quelques applications du théorème de densité de Chebotarev*. Inst. Hautes Études Sci. Publ. Math. 54 (1981), pp. 323–401.

[Sha95] Ehud de Shalit. *p-adic periods and modular symbols of elliptic curves of prime conductor*. Invent. Math. 121.2 (1995), pp. 225–255.

[Sil94] Joseph H. Silverman. ***Advanced topics in the arithmetic of elliptic curves***. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994, pp. xiv+525.

[Sil09] Joseph H. Silverman. ***The arithmetic of elliptic curves***. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009.

[Ste82] Glenn Stevens. ***Arithmetic on modular curves***. Vol. 20. Progress in Mathematics. Birkhäuser Boston, 1982.

[Ste89] Glenn Stevens. *Stickelberger elements and modular parametrizations of elliptic curves*. Invent. Math. 98.1 (1989), pp. 75–106.

[SD67] Peter Swinnerton-Dyer. *The conjectures of Birch and Swinnerton-Dyer, and of Tate*. In: ***Proc. Conf. Local Fields (Driebergen, 1966)***. Springer, Berlin-New York, 1967, pp. 132–157.

[Tat95] John Tate. "On the conjectures of Birch and Swinnerton-Dyer and a geometric analog". In: ***Séminaire Bourbaki, Vol. 9***. Soc. Math. France, Paris, 1995, Exp. No. 306, 415–440.

[Tat04] John Tate. "Refining Gross's conjecture on the values of abelian L-functions". In: ***Stark's conjectures: recent work and new directions***. Vol. 358. Contemp. Math. Amer. Math. Soc., Providence, RI, 2004, pp. 189–192.

[Vas68] Wolmer V. Vasconcelos. *Reflexive modules over Gorenstein rings*. Proc. Amer. Math. Soc. 19 (1968), pp. 1349–1355.

[Ven07] Otmar Venjakob. "From the Birch and Swinnerton-Dyer conjecture to non-commutative Iwasawa theory via the equivariant Tamagawa number conjecture—a survey". In: ***L-functions and Galois representations***. Vol. 320. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2007, pp. 333–380.

[WW22] Hanneke Wiersema and Christian Wuthrich. *Integrality of twisted L-values of elliptic curves*. Doc. Math. 27 (2022), pp. 2041–2066.

[Wil06] Andrew Wiles. "The Birch and Swinnerton-Dyer conjecture". In: ***The millennium prize problems***. Clay Math. Inst., Cambridge, MA, 2006, pp. 31–41.

[Zha14] Wei Zhang. "The Birch–Swinnerton-Dyer conjecture and Heegner points: a survey". In: ***Current developments in mathematics 2013***. Int. Press, Somerville, MA, 2014, pp. 169–203.

[Zyw22] David Zywina. *On the surjectivity of* mod ℓ *representations associated to elliptic curves*. Bull. Lond. Math. Soc. 54.6 (2022), pp. 2404–2417.

(Bullach) Instituto de Ciencias Matemáticas, c/ Nicolás Cabrera 13-15, Campus de Cantoblanco UAM, 28049 Madrid, Spain.
Email address: dominik.bullach@icmat.es

(Honnor) St Paul's School, Lonsdale Road, London SW13 9JT, UK.