# Kolyvagin's result on the vanishing of $Ш(E/K)[p^\infty]$ and its consequences for anticyclotomic Iwasawa theory

**Ahmed Matar, Jan Nekovář**

Abstract: We discuss improvements of Kolyvagin's classical result about the vanishing of the $p$-primary part of the Tate–Šafarevič group of an elliptic curve $E$ (defined over $\mathbf{Q}$) over an imaginary quadratic field $K$ satisfying the Heegner hypothesis for which the basic Heegner point $y_K \in E(K)$ is not divisible by an odd prime $p$. Combining Kolyvagin's theorem with a new abstract Iwasawa-theoretical result, we deduce, under suitable assumptions, that similar vanishing holds for all layers in the anticyclotomic $\mathbf{Z}_p$-extension of $K$.

## 0. Introduction

**(0.1)** Let $E$ be an elliptic curve over $\mathbf{Q}$ of conductor $N$ and $K$ an imaginary quadratic field of discriminant $D_K$ in which all primes dividing $N$ split. Fix a modular parameterisation $\varphi : X_0(N) \longrightarrow E$ and an ideal $\mathcal{N} \subset O_K$ such that $\mathcal{O}_K/\mathcal{N} \simeq \mathbf{Z}/N\mathbf{Z}$. The basic Heegner point $y_K \in E(K)$ attached to these data is, by definition, the trace $y_K := \mathrm{Tr}_{H_1/K}(y_1)$ of the Heegner point of conductor one $y_1 := \varphi([\mathbf{C}/O_K \longrightarrow \mathbf{C}/\mathcal{N}^{-1}]) \in E(H_1)$ defined over the Hilbert class field $H_1$ of $K$.

**(0.2)** If $y_K \notin E(K)_{\mathrm{tors}}$ and $D_K \neq -3, -4$, Kolyvagin [K1, Thm. A] proved that the groups $E(K)/\mathbf{Z}y_K$ and $Ш(E/K)$ are finite, and that $\#Ш(E/K)$ divides $[E(K) : \mathbf{Z}y_K]^2$ multiplied by a product of several error terms. The $p$-primary parts of these error terms vanish in the following situation (each of the respective assumptions (a), (b) and (c) implies that the corresponding error term $a, b, c$ in [K1, Cor. 11, Cor. 12, Cor. 13] is relatively prime to $p$; the error term $d$ is equal to 1, since $p \neq 2$).

**(0.3) Theorem (Kolyvagin, special case of [K1, Cor. 13]).** *Assume that $D_K \neq -3, -4$ and that $p \neq 2$ is a prime number satisfying the following conditions.*
*(a) $\forall n_1, n_2 \geq 0 \quad H^1(K(E[p^{n_1+n_2}])/K, E[p^{n_1}]) = 0$.*
*(b) Neither of the $(\pm 1)$-eigenspaces $E[p]^\pm$ for the action of complex conjugation is stable under the action of $G_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Equivalently, the (mod $p$) Galois representation $\overline{\rho}_{E,p} : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}_{\mathbf{F}_p}(E[p]) \simeq GL_2(\mathbf{F}_p)$ is irreducible.*
*(c) $E(K)[p] = 0$.*
*If $y_K \notin E(K)_{\mathrm{tors}}$, then $E(K)/\mathbf{Z}y_K$ is finite and*

$$p^{m_0} Ш(E/K)[p^\infty] = 0, \qquad \#Ш(E/K)[p^\infty] \text{ divides } p^{2m_0},$$

*where $m_0 := \sup\{m \geq 0 \mid y_K \in p^m E(K)\}$ (thus $E(K) \otimes \mathbf{Z}_p \simeq \mathbf{Z}_p$ and $p^{m_0} = [E(K) \otimes \mathbf{Z}_p : \mathbf{Z}_p(y_K \otimes 1)]$).*

**(0.4)** For $p \neq 2$, the assumption (b) in Theorem 0.3 implies (c). Moreover, the assumptions (a), (b) and (c) are satisfied if $\overline{\rho}_{E,p}$ has "big image" (e.g., if it is surjective).

Gross [G] gave a self-contained account of Kolyvagin's proof of Theorem 0.3 in the simplest case when $\overline{\rho}_{E,p}$ is surjective and $m_0 = 0$. One step in the argument ([G, beginning of §9]) required an additional assumption $p \nmid D_K$.

**(0.5) Theorem ([G, Prop. 2.1, Prop. 2.3]).** *Assume that $D_K \neq -3, -4$ and that $p \nmid 2D_K$ is a prime number for which $\overline{\rho}_{E,p} : G_{\mathbf{Q}} \longrightarrow GL_2(\mathbf{F}_p)$ is surjective. If $y_K \notin pE(K)$, then $E(K) \otimes \mathbf{Z}_p = \mathbf{Z}_p y_K \simeq \mathbf{Z}_p$ and $Ш(E/K)[p^\infty] = 0$.*

**(0.6)** In [K2], Kolyvagin proved the following structure theorem for $Ш(E/K)[p^\infty]$, which refines Theorem 0.3 (under the "big image" assumption for the $p$-adic Galois representation $\rho_{E,p} : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}_{\mathbf{Z}_p}(T_p(E)) \simeq GL_2(\mathbf{Z}_p)$).

**(0.7) Theorem (Kolyvagin, [K2, Thm. C, Thm. D]).** *Assume that $D_K \neq -3, -4$ and that $p \neq 2$ is a prime number for which $\rho_{E,p} : G_{\mathbf{Q}} \longrightarrow GL_2(\mathbf{Z}_p)$ has "big image" (e.g., that $\rho_{E,p}$ is surjective). If $y_K \notin E(K)_{\mathrm{tors}}$, then*

$$Ш(E/K)[p^\infty] \simeq X \oplus X, \qquad X \simeq \bigoplus_{i \geq 0} \mathbf{Z}/p^{m_i - m_{i+1}}\mathbf{Z}, \qquad m_0 \geq m_1 \geq \cdots \geq m_\infty := \inf m_i,$$

*where $m_0$ is as in Theorem 0.3 and $m_i$ for $i > 0$ is defined in a similar way in terms of certain linear combinations of Heegner points of higher conductors. In particular,* $\#\text{Ш}(E/K)[p^\infty] = p^{2(m_0 - m_\infty)}$.

**(0.8)** The divisibility $\#X \mid p^{m_0}$ was reproved by Howard [H1, Thm. A] using the formalism of anticyclotomic Kolyvagin systems, under the assumptions that $\rho_{E,p}$ is surjective, $D_K \neq -3, -4$ and $p \nmid 2ND_K$.

**(0.9)** For $p \neq 2$, the condition (a) in Theorem 0.3 was studied in detail by Cha [Ch, Thm. 2], who showed that it is satisfied if $p \nmid D_K$, $p^2 \nmid N$ and $E(K)[p] = 0$, except when $p = 3$ and $\overline{\rho}_{E,3}(G_K) = \begin{pmatrix} \mathbf{F}_3^\times & \mathbf{F}_3 \\ 0 & 1 \end{pmatrix}$. Therefore the conclusions of Theorems 0.3 and 0.5 hold (for $D_K \neq -3, -4$) whenever $p \nmid 2D_K$, $p^2 \nmid N$ and $\overline{\rho}_{E,p}$ is irreducible. He also showed [Ch, Thm. 21, Rmk. 25] that the statement of Theorem 0.7 holds under the same assumptions.

**(0.10)** The authors of a collective article [GJPST] had made an attempt at generalising Cha's results. However, the cohomological calculations in [GJPST, Lemma 5.7, Lemma 5.9] and [GJPST, proof of Proposition 5.4] are incorrect (see [LW, Lemma 8]), the statement of [GJPST, Proposition 5.8] is correct but the proof is not, and the discussion of Kolyvagin's method (in the form presented in [G]) in [GJPST, §5] is seriously flawed. In particular, the assertion to the effect that the surjectivity of $\overline{\rho}_{E,p}$ in Theorem 0.5 can be replaced by the vanishing of the groups $H^i(K(E[p])/K, E[p])$ for $i = 1, 2$ and of $E'(K)[p]$ for all $\mathbf{Q}$-isogenies $E \longrightarrow E'$, is incorrect, for the following reason: the current state of the art requires an irreducibility assumption for $\overline{\rho}_{E,p}$ (or its restriction to $G_K$) in order to obtain, by Kolyvagin's method, an upper bound on the size of $\text{Ш}(E/K)[p^\infty]$ without any error terms. As a result, [GJPST, Thm. 3.7] remains unproved.

**(0.11)** Lawson and Wuthrich [LW] extended and simplified the cohomological calculations of [Ch], and corrected various mistakes from [GJPST]. In [LW, Thm 1, Thm 2], they gave a complete classification of pairs $(E, p)$ consisting of an elliptic curve $E$ over $\mathbf{Q}$ and a prime number $p \neq 2$ for which $H^1(\mathbf{Q}(E[p])/\mathbf{Q}, E[p]) \neq 0$ (and similarly for $H^1(\mathbf{Q}(E[p^n])/\mathbf{Q}, E[p^n]) \neq 0$, where $n > 1$ and $p > 3$). They also classified pairs $(E, p)$ for which $H^2(\mathbf{Q}(E[p])/\mathbf{Q}, E[p]) \neq 0$.

Their results imply that the condition (a) in Theorem 0.3 (for $p \neq 2$) is always satisfied if $\overline{\rho}_{E,p}$ is irreducible. Consequently, the conclusions of Theorems 0.3 and 0.7 hold (for $D_K \neq -3, -4$) if $\overline{\rho}_{E,p}$ is irreducible and $p \neq 2$.

However, the claims made in [LW, Thm. 14] about the validity of Theorem 0.3 in situations when (a) holds but $\overline{\rho}_{E,p}$ is reducible are unjustified, for reasons explained in 0.10.

We recall the methods of [Ch] and [LW] and prove a mild generalisation of some of their results in §5. We also prove the following variant of Theorem 0.5.

**(0.12) Theorem (= Theorem 6.7).** *Assume that $p \neq 2$ and that $E[p]$ is an irreducible $\mathbf{F}_p[G_\mathbf{Q}]$-module (which implies that $E(K)[p] = 0$).*
*(1) Assume that $(K, p) \neq (\mathbf{Q}(\sqrt{-3}), 3)$. If $y_K \notin pE(K)$, then*

$$E(K) \otimes \mathbf{Z}_p = \mathbf{Z}_p(y_K \otimes 1) \simeq \mathbf{Z}_p, \qquad \text{Ш}(E/K)[p^\infty] = 0.$$

*(2) Assume that $(K, p) = (\mathbf{Q}(\sqrt{-3}), 3)$; then $y_K \in 3E(K)$. If $3 \nmid a_3$, assume, in addition, that $\rho(G_K)$ is not a cyclic group of order four. If $y_K \notin 3^2E(K)$, then*

$$\mathbf{Z}_3 \simeq E(K) \otimes \mathbf{Z}_3 \supset 3E(K) \otimes \mathbf{Z}_3 = \mathbf{Z}_3(y_K \otimes 1), \qquad \text{Ш}(E/K)[3^\infty] = 0.$$

**(0.13)** We now turn to Iwasawa-theoretical results. Fix a prime number $p$ and denote by $K_\infty = \bigcup_{n \geq 1} K_n$ the anticyclotomic $\mathbf{Z}_p$-extension of $K$. In this case $\Gamma := \mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_p$, $K_n = K_\infty^{\Gamma_n}$, where $\Gamma_n = \Gamma^{p^n} \simeq p^n\mathbf{Z}_p$, and $\mathrm{Gal}(K_\infty/\mathbf{Q}) = \Gamma \rtimes \{1, c\}$, with complex conjugation $c$ acting on $\Gamma$ by $g \mapsto g^{-1}$. Denote by $\Lambda := \mathbf{Z}_p[[\Gamma]]$ the Iwasawa algebra of $\Gamma$.

**(0.14)** From now on until the end of Introduction we assume that $p \neq 2$ and that $E$ has good ordinary reduction at $p$. The Selmer module $\mathrm{Sel}_{p^\infty}(E/K_\infty) := \varinjlim_n \mathrm{Sel}_{p^\infty}(E/K_n)$ (resp. $S_p(E/K_\infty) := \varprojlim_n S_p(E/K_n)$) (see §1.4 for the notation) is a $\Lambda$-module of cofinite (resp. finite) type, of corank (resp. rank) equal to one, as predicted by one of Mazur's conjectures formulated in [Mz, §18]. This conjecture is a consequence of another conjecture of Mazur [Mz, §19] (proved independently by Cornut [Co1, Co2] and Vatsal [Va]) combined with an Euler system argument along the tower $K_\infty/K$ ([B, Thm. A] under some additional assumptions; the general case is proved in [N1, §2] together with [N3, Thm. 3.2]; see also [H1, Thm. B]). Another proof of [B, Thm. A], which had applications to the study of the anticyclotomic $\mu$-invariant, was given in [M, Thm. A].

In [B, Thm. B], Bertolini also proved a $\Lambda$-adic variant of Kolyvagin's annihilation result [K1, Cor. 12] for the torsion submodule of the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ (assuming the validity of Mazur's conjecture [Mz, §19]). This result was subsequently generalised by Howard [H1, Thm. B], who proved one half of a conjecture of Perrin-Riou [PR, Conj. B] for Heegner points along $K_\infty/K$, namely, a $\Lambda$-adic variant of Kolyvagin's result $\#X \mid p^{m_0}$ (in the notation of Theorem 0.7).

**(0.15)** The proofs of [B, Thm. B] and [H1, Thm. B] relied on fairly detailed arguments involving the Euler system and the Kolyvagin system of Heegner points along $K_\infty/K$, respectively. The main insight of the present work is that in the simplest case when $y_K \notin pE(K)$, one can obtain — under certain assumptions — precise information about the structure of the $\mathbf{Z}_p[\Gamma/\Gamma_n]$-modules $E(K_n) \otimes \mathbf{Q}_p/\mathbf{Z}_p$ and $Ш(E/K_n)[p^\infty]$ from Theorem 0.5 (and its variant Theorem 0.12) by purely Iwasawa-theoretical methods, combined with the norm relations for the Heegner points of $p$-power conductor, without applying any Euler system arguments along the tower $K_\infty/K$. The following results are proved in §4.

**(0.16) Theorem (= Theorem 4.8).** *If $p \neq 2$ is a prime number such that*
*(a) $E(K)[p] = 0$,*
*(b) $p \nmid N \cdot a_p \cdot (a_p - 1) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$,*
*(c) $y_K \notin E(K)_{\mathrm{tors}}$,*
*(d) $\mathrm{rk}_{\mathbf{Z}}\, E(K) = 1$ and $Ш(E/K)[p^\infty] = 0$,*
*then $Ш(E/K_\infty)[p^\infty] = 0$ and the Pontryagin dual of $E(K_\infty) \otimes \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Sel}_{p^\infty}(E/K_\infty)$ is a free module of rank one over $\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$.*

**(0.17) Theorem (= Theorem 4.9).** *If $p \neq 2$ is a prime number such that*
*(a) $E(K)[p] = 0$,*
*(b') $p \nmid N \cdot a_p \cdot (a_p - 1) \cdot (a_p - \eta_K(p)) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$,*
*(c') $y_K \notin pE(K)$,*
*(d) $\mathrm{rk}_{\mathbf{Z}}\, E(K) = 1$ and $Ш(E/K)[p^\infty] = 0$,*
*then, for every intermediate field $K \subset L \subset K_\infty$, $Ш(E/L)[p^\infty] = 0$ and the Pontryagin dual of $E(L) \otimes \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Sel}_{p^\infty}(E/L)$ is a free module of rank one over $\mathbf{Z}_p[[\mathrm{Gal}(L/K)]]$. For every integer $n \geq 0$, $\mathrm{rk}_{\mathbf{Z}}\, E(K_n) = p^n$, $Ш(E/K_n)[p^\infty] = 0$ and $E(K_n) \otimes \mathbf{Z}_p$ is generated over $\mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$ by the traces to $K_n$ of the Heegner points of $p$-power conductor.*

**(0.18)** Above, $a_p$ denotes the $p$-th coefficient of the $L$-function $L(E/\mathbf{Q}, s) = \sum_{n \geq 1} a_n n^{-s}$, the value $\eta_K(p)$ is equal to $1, -1, 0$, respectively, if $p$ splits, is inert, or is ramified in $K/\mathbf{Q}$, and $c_{\mathrm{Tam}}(E/\mathbf{Q}) = \prod_{\ell \mid N} c_{\mathrm{Tam},\ell}(E/\mathbf{Q})$ is the product of the local Tamagawa factors of $E$ at all primes of bad reduction.

**(0.19)** If $K = \mathbf{Q}(\sqrt{-3})$ and $p = 3$, the conditions (a) and (c') in Theorem 0.17 cannot be satisfied simultaneously, by Proposition 4.11 below. In general, (a) and (c') should imply both (d) and $p \nmid c_{\mathrm{Tam}}(E/\mathbf{Q})$ (see (6.2.1)).

**(0.20)** What is the role of the individual assumptions in Theorem 0.16 and Theorem 0.17? The condition (a) implies that $E(K_\infty)[p] = 0$. The assumption $p \nmid N \cdot a_p$ is equivalent to $E$ having good ordinary reduction at $p$, and the remaining part $p \nmid (a_p - 1) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$ of (b) ensures (when combined with (a)) that Mazur's control theorem holds along the tower $K_\infty/K$ without any error terms: $\mathrm{Sel}_{p^k}(E/K_n) \xrightarrow{\sim} \mathrm{Sel}_{p^k}(E/K_\infty)^{\Gamma_n}$ for all $k, n \geq 0$. The condition (d) implies that $\mathrm{Sel}_{p^\infty}(E/K) \simeq \mathbf{Q}_p/\mathbf{Z}_p$. Finally, the norm relations for the Heegner points of $p$-power conductor imply that, for a suitable non-zero element $m \in \mathbf{Z}_p$, the multiple $y_K \otimes m \in E(K) \otimes \mathbf{Z}_p$ is a universal norm from the projective system $\{E(K_n) \otimes \mathbf{Z}_p\}$, and the condition $p \nmid (a_p - 1) \cdot (a_p - \eta_K(p))$ ensures that $m \in \mathbf{Z}_p^\times$.

**(0.21)** One can combine Theorem 0.17 with the Euler system results over $K$ (but not over $K_\infty$) discussed in 0.1–0.11. Kolyvagin's result alluded to in 0.2 tells us that the condition $\mathrm{rk}_{\mathbf{Z}}\, E(K) = 1$ in Theorem 0.16(d) follows from (c), and therefore can be dropped. Likewise, the condition (d) in Theorem 0.17 follows from (c'), whenever the conclusions of Theorem 0.5 hold. Combining Theorem 0.5 (with weaker assumptions, supplied by [Ch], [LW] and Theorem 6.7(1)) with Theorem 0.17, we obtain the following result.

**(0.22) Theorem (= Theorem 6.9).** *If $p \neq 2$ is a prime number such that $E[p]$ is an irreducible $\mathbf{F}_p[G_{\mathbf{Q}}]$-module, $p \nmid N \cdot a_p \cdot (a_p - 1) \cdot (a_p - \eta_K(p)) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$ and $y_K \notin pE(K)$, then the conclusions of Theorem 0.17 hold.*

**(0.23)** The case $K = \mathbf{Q}(\sqrt{-3})$, $p = 3$ is different, as already mentioned in Theorem 0.12 and in 0.19. The point is that, if $E(K)[3] = 0$, then $y_K = 3z_K$, where $z_K \in E(K)$ is a linear combination of the traces to $K$ of the Heegner points of conductors 1 and $q$, for any prime $q \nmid 3N$ satisfying $a_q \not\equiv 1 + \eta_K(q) \pmod 3$ (there are infinitely many such primes $q$).

**(0.24) Theorem (= Theorem 6.10).** *Assume that $K = \mathbf{Q}(\sqrt{-3})$, $p = 3$, $E[3]$ is an irreducible $\mathbf{F}_3[G_{\mathbf{Q}}]$-module, $\rho(G_K)$ is not a cyclic group of order four and $3 \nmid a_3 \cdot (a_3 - 1) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$. If $y_K \notin 3^2 E(K)$, then the conclusions of Theorem 0.17 hold, with the following modification: each $E(K_n) \otimes \mathbf{Z}_3$ is generated over $\mathbf{Z}_3[\mathrm{Gal}(K_n/K)]$ by the traces to $K_\infty$ of the Heegner points of conductors dividing $3^\infty q$, for any prime $q$ as in 0.23.*

**(0.25)** Analogous results hold for anticyclotomic $\mathbf{Z}_p^m$-extensions and basic CM points on abelian varieties of $GL(2)$-type with real multiplication occurring as simple quotients of Jacobians of Shimura curves over totally real number fields. This will be discussed in a separate publication.

**(0.26)** Let us describe the contents of this article in more detail. The goal of §1-§3 is to prove two abstract results (Theorems 3.4 and 3.5) on Selmer groups of $\mathfrak{p}$-ordinary abelian varieties in dihedral Iwasawa theory. The framework is general enough to apply in the context of 0.25, not just in the situation involving classical Heegner points on elliptic curves. In §4 we recall the norm relations for Heegner points and combine them with Theorems 3.4 and 3.5 in order to deduce Theorems 0.16 and 0.17. In §5-§6 we give a proof of Kolyvagin's result on vanishing of $Ш(E/K)[p^\infty]$ in the form of Theorem 0.12. When combined with Theorems 0.16 and 0.17, this implies Theorems 0.22 and 0.24. Again, the general theory developed in §5 is applicable in the context of 0.25.

**Acknowledgements.** Some of the work on this article was carried out by the second named author when he was visiting Centre Interfacultaire Bernoulli (CIB) at Ecole Polytechnique Fédérale de Lausanne during the semester "Euler systems and special values of $L$-functions" in fall 2017, and when he was staying at Imperial College London as an ICL–CNRS fellow in spring 2018. He is grateful to both institutions for their generous support.

## 1. Generalities

**(1.1)** Throughout §1-§3,

- for any perfect field $k$, denote by $G_k = \mathrm{Gal}(\overline{k}/k)$ its absolute Galois group.
- For an integer $n \geq 1$ invertible in $k$, denote by $\chi_{n,k} : G_k \longrightarrow (\mathbf{Z}/n\mathbf{Z})^\times$ the cyclotomic character given by the action of $G_k$ on $\mu_n(\overline{k})$.
- $K$ is a number field.
- $Fr(v)$ will always denote the arithmetic Frobenius element.
- $p$ is a prime number; if $K$ is not totally imaginary, we assume that $p \neq 2$.
- $B$ is an abelian variety over $K$ with **good reduction** at all primes of $K$ above $p$; let $B^t$ be the dual abelian variety.
- If $v$ is a finite prime of a finite extension $L$ of $K$, denote by $B_v$ the Néron model of $B \otimes_K L_v$ over $O_{L_v}$, by $\widetilde{B}_v$ its special fibre (over the residue field $k(v)$ of $v$), and by $\pi_0(\widetilde{B}_v) = \widetilde{B}_v/\widetilde{B}_v^\circ$ the $G_{k(v)}$-module of its connected components.
- $M$ is a totally real number field with ring of integers $O_M$.
- We are given a ring morphism $i : O_M \longrightarrow \mathrm{End}(B)$ and an $O_M$-linear isogeny $\lambda : B \longrightarrow B^t$ which is symmetric in the sense that $\lambda = \lambda^t$. Above, we use a scheme-theoretic notation: the ring of endomorphisms of $B$ defined over a field $L$ containing $K$ is denoted by $\mathrm{End}(B \otimes_K L)$ (not by $\mathrm{End}_L(E)$).

Throughout, one can replace $O_M$ by any order in $M$ whose index in $O_M$ is prime to $p$, but the current setting is sufficient for the arithmetic applications we have in mind.

**(1.2)** The decomposition

$$O_M \otimes \mathbf{Z}_p = \prod_{\mathfrak{p}|p} O_{M_\mathfrak{p}}$$

(where $\mathfrak{p}$ runs through all primes of $M$ above $p$) induces decompositions

$$B[p^\infty] = \bigoplus_{\mathfrak{p}} B[\mathfrak{p}^\infty], \qquad T_p(B) = \bigoplus_{\mathfrak{p}} T_\mathfrak{p}(B).$$

Fix, once for all, a prime $\mathfrak{p} \mid p$ in $M$ and set

$$\mathcal{O} := O_{M_\mathfrak{p}}, \qquad \mathcal{K} := M_\mathfrak{p}, \qquad A := B[\mathfrak{p}^\infty], \qquad T := T_\mathfrak{p}(B).$$

Throughout §1-§3, we assume that

- $B$ has good **$\mathfrak{p}$-ordinary reduction** at each prime $v$ of $K$ above $p$ in the sense that

$$\mathrm{rk}_\mathcal{O}\, T_\mathfrak{p}(\widetilde{B}_v) = \frac{1}{2}\,\mathrm{rk}_\mathcal{O}\, T_\mathfrak{p}(B) \qquad (= \dim(B)/[M:\mathbf{Q}]).$$

  This condition is weaker than requiring $B$ to have good ordinary reduction at $v$ (which is equivalent to $B$ having good $\mathfrak{p}'$-ordinary reduction at $v$ for all $\mathfrak{p}' \mid p$ in $M$).

**(1.3) Pontryagin duality.** For any discrete or compact topological $\mathbf{Z}_p$-module $X$, let us denote by

$$D(X) := \mathrm{Hom}_{\mathrm{cont},\mathbf{Z}_p}(X, \mathbf{Q}_p/\mathbf{Z}_p)$$

the Pontryagin dual of $X$. In the special case when $X$ is a topological $\mathcal{O}$-module, so is $D(X)$, and there are canonical isomorphisms of $\mathcal{O}$-modules

$$D(X) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont},\mathcal{O}}(X, \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}, \mathbf{Q}_p/\mathbf{Z}_p)),$$
$$\mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}, \mathbf{Q}_p/\mathbf{Z}_p) \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}, \mathbf{Z}_p) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}, \mathbf{Z}_p) \otimes_\mathcal{O} \mathcal{K}/\mathcal{O},$$

where $\mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}, \mathbf{Z}_p)$ is a free $\mathcal{O}$-module of rank one. A choice of an isomorphism of $\mathcal{O}$-modules

$$\mathcal{O} \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathcal{O}, \mathbf{Z}_p) \tag{1.3.1}$$

is equivalent to choosing a generator $a \in \mathscr{D}^{-1}_{\mathcal{O}/\mathbf{Z}_p}$ of the inverse different, via the pairing

$$\mathcal{O} \times \mathcal{O} \longrightarrow \mathbf{Z}_p, \qquad (x, y) \mapsto \mathrm{Tr}_{\mathcal{K}/\mathbf{Q}_p}(axy). \tag{1.3.2}$$

As in [N2, (0.4.1)], we let

$$T^* := D(A), \qquad A^* := D(T).$$

The Weil pairing

$$(\ ,\ ) : T_p(B) \times T_p(B^t) \longrightarrow \mathbf{Z}_p(1)$$

is $\mathbf{Z}_p$-bilinear and $G_K$-equivariant. It satisfies $(\alpha x, y) = (x, \alpha^t y)$, for all $\alpha \in \mathrm{End}(B)$ (where $\alpha^t$ denotes the dual isogeny to $\alpha$). In particular, it induces an eponymous pairing

$$(\ ,\ ) : T_\mathfrak{p}(B) \times T_\mathfrak{p}(B^t) \longrightarrow \mathbf{Z}_p(1) \tag{1.3.3}$$

giving rise to isomorphisms of $\mathcal{O}[G_K]$-modules

$$D(A)(1) = T^*(1) = \mathrm{Hom}_{\mathbf{Z}_p}(T_\mathfrak{p}(B), \mathbf{Z}_p)(1) \xrightarrow{\sim} T_\mathfrak{p}(B^t), \qquad A^*(1) = D(T)(1) \xrightarrow{\sim} B^t[\mathfrak{p}^\infty].$$

Once we fix an isomorphism (1.3.1) via (1.3.2), we can pass from the Weil pairing (1.3.3) to its $\mathcal{O}$-bilinear version, namely

$$( \ , \ )_{\mathcal{O}} : T_{\mathfrak{p}}(B) \times T_{\mathfrak{p}}(B^t) = T \times T^*(1) \longrightarrow \mathcal{O}(1), \qquad (x,y) = \mathrm{Tr}_{\mathcal{K}/\mathbf{Q}_p}(a(x,y)_{\mathcal{O}}),$$

which induces an isomorphism of $\mathcal{O}[G_K]$-modules

$$T^*(1) = \mathrm{Hom}_{\mathcal{O}}(T_{\mathfrak{p}}(B), \mathcal{O})(1) \xrightarrow{\sim} T_{\mathfrak{p}}(B^t).$$

The symmetric isogeny $\lambda$ from (1.1) defines morphisms of $\mathcal{O}[G_K]$-modules

$$\lambda_* : T_{\mathfrak{p}}(B) \hookrightarrow T_{\mathfrak{p}}(B^t), \qquad B[\mathfrak{p}^\infty] \twoheadrightarrow B^t[\mathfrak{p}^\infty]$$

with finite cokernel and kernel, respectively. The Weil pairing attached to $\lambda$

$$( \ , \ )_{\mathcal{O},\lambda} : T_{\mathfrak{p}}(B) \times T_{\mathfrak{p}}(B) = T \times T \longrightarrow \mathcal{O}(1), \qquad (x,y)_{\mathcal{O},\lambda} := (x, \lambda_*(y))_{\mathcal{O}} \tag{1.3.4}$$

is skew-symmetric; in other words, $\lambda_* : T \longrightarrow T^*(1)$ satisfies $(\lambda_*)^*(1) = -\lambda_*$.

**(1.4) Classical Selmer groups.** For every finite extension $L/K$, $p$-power descent on $B$ over $L$ gives rise to the classical Selmer groups $\mathrm{Sel}_{p^k}(B/L) \subset H^1(L, B[p^k])$ sitting in the standard exact sequences

$$0 \longrightarrow B(L) \otimes \mathbf{Z}/p^k\mathbf{Z} \longrightarrow \mathrm{Sel}_{p^k}(B/L) \longrightarrow Ш(B/L)[p^k] \longrightarrow 0. \tag{1.4.1}$$

Their respective inductive and projective limits

$$\mathrm{Sel}_{p^\infty}(B/L) := \varinjlim_k \mathrm{Sel}_{p^k}(B/L) \subset H^1(L, B[p^\infty]), \qquad S_p(B/L) := \varprojlim_k \mathrm{Sel}_{p^k}(B/L) \subset H^1(L, T_p(B))$$

coincide with the corresponding Bloch–Kato Selmer groups

$$H^1_f(L, B[p^\infty]) \subset H^1(L, B[p^\infty]), \qquad H^1_f(L, T_p(B)) \subset H^1(L, T_p(B)),$$

by [BK, (3.11.1), (3.11.2)]. All groups in (1.4.1) and in the limit exact sequences

$$\begin{gathered} 0 \longrightarrow B(L) \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(B/L) \longrightarrow Ш(B/L)[p^\infty] \longrightarrow 0, \\ 0 \longrightarrow B(L) \otimes \mathbf{Z}_p \longrightarrow S_p(B/L) \longrightarrow T_p Ш(B/L)[p^\infty] \longrightarrow 0 \end{gathered}$$

are $O_M \otimes \mathbf{Z}_p$-modules. After tensoring with $\mathcal{O}$ over $O_M \otimes \mathbf{Z}_p$, we obtain exact sequences

$$0 \longrightarrow B(L) \otimes_{O_M} O_M/\mathfrak{p}^{ke} \longrightarrow \mathrm{Sel}_{\mathfrak{p}^{ke}}(B/L) \longrightarrow Ш(B/L)[\mathfrak{p}^{ke}] \longrightarrow 0 \tag{1.4.2}$$

(where $e = e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ above $p$) and

$$\begin{gathered} 0 \longrightarrow B(L) \otimes_{O_M} \mathcal{K}/\mathcal{O} \longrightarrow \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) \longrightarrow Ш(B/L)[\mathfrak{p}^\infty] \longrightarrow 0, \\ 0 \longrightarrow B(L) \otimes_{O_M} \mathcal{O} \longrightarrow S_{\mathfrak{p}}(B/L) \longrightarrow T_{\mathfrak{p}} Ш(B/L)[p^\infty] \longrightarrow 0. \end{gathered}$$

Again,

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) = H^1_f(L, B[\mathfrak{p}^\infty]) = H^1_f(L, A), \qquad S_{\mathfrak{p}}(B/L) = H^1_f(L, T_{\mathfrak{p}}(B)) = H^1_f(L, T).$$

The same discussion applies to $B^t$; one obtains

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(B^t/L) = H^1_f(L, B^t[\mathfrak{p}^\infty]) = H^1_f(L, A^*(1)), \qquad S_{\mathfrak{p}}(B^t/L) = H^1_f(L, T_{\mathfrak{p}}(B^t)) = H^1_f(L, T^*(1)).$$

If $L \subset \overline{K}$ is an arbitrary algebraic extension of $K$, we let

$$\mathrm{Sel}_{\mathfrak{p}^{ke}}(B/L) := \varinjlim_{F,\mathrm{res}} \mathrm{Sel}_{\mathfrak{p}^{ke}}(B/F) \qquad (k \in \mathbf{N} \cup \{\infty\}), \qquad S_{\mathfrak{p}}(B/L) := \varprojlim_{F,\mathrm{cor}} S_{\mathfrak{p}}(B/F),$$

where $F$ runs through all intermediate fields $K \subset F \subset L$ such that $[F:K] < \infty$.

**(1.5) Greenberg's Selmer groups.** Let $v \mid p$ be a prime of $K$ above $p$. As $B$ has good $\mathfrak{p}$-ordinary reduction at $v$, there are exact sequences of $\mathcal{O}[G_{K_v}]$-modules

$$0 \longrightarrow T_v^+ \longrightarrow T \longrightarrow T_v^- \longrightarrow 0, \qquad 0 \longrightarrow A_v^+ \longrightarrow A \longrightarrow A_v^- \longrightarrow 0 \tag{1.5.1}$$

in which

$$T_v^- = T_{\mathfrak{p}}(\widetilde{B}_v), \qquad A_v^- = \widetilde{B}_v[\mathfrak{p}^\infty],$$

and the Pontryagin dual of (1.5.1) is isomorphic to

$$0 \longrightarrow A^*(1)_v^+ \longrightarrow A^*(1) \longrightarrow A^*(1)_v^- \longrightarrow 0, \quad 0 \longrightarrow T^*(1)_v^+ \longrightarrow T^*(1) \longrightarrow T^*(1)_v^- \longrightarrow 0,$$

where

$$T^*(1)_v^- = T_{\mathfrak{p}}(\widetilde{B}_v^t), \qquad A^*(1)_v^- = \widetilde{B}_v^t[\mathfrak{p}^\infty].$$

In addition, $\lambda : B \longrightarrow B^t$ induces maps

$$T \hookrightarrow T^*(1), \qquad T_v^\pm \hookrightarrow T^*(1)_v^\pm, \qquad A \twoheadrightarrow A^*(1), \qquad A_v^\pm \twoheadrightarrow A^*(1)_v^\pm$$

with finite cokernel (for $T, T_v^\pm$) and kernel (for $A, A_v^\pm$), respectively.

Fix a finite set $S$ of primes of $K$ containing all archimedean primes, all primes above $p$ and all primes at which $B$ has bad reduction. If $L$ is a finite extension of $K$, let $L_S$ be the maximal algebraic extension of $L$ unramified outside primes above $S$; set $G_{L,S} := \mathrm{Gal}(L_S/L)$. Denote by $\Sigma_L$ (resp. $\Sigma'_L$) the set of all primes of $L$ above $p$ (resp. the set of all nonarchimedean primes of $L$ above $S \smallsetminus \Sigma_K$). For each $X = T, A, T^*(1), T^*(1)$, the Greenberg Selmer group over $L$ and its strict counterpart are defined, respectively, by

$$S_X(L) := \mathrm{Ker}\left( H^1(G_{L,S}, X) \longrightarrow \bigoplus_{v \in \Sigma_L} H^1(I_v, X_v^-) \oplus \bigoplus_{v \in \Sigma'_L} H^1(I_v, X) \right)$$

$$S_X^{\mathrm{str}}(L) := \mathrm{Ker}\left( H^1(G_{L,S}, X) \longrightarrow \bigoplus_{v \in \Sigma} H^1(G_{L_v}, X_v^-) \oplus \bigoplus_{v \in \Sigma'_L} H^1(I_v, X) \right),$$

where $I_v \subset G_{L_v} = \mathrm{Gal}(\overline{L}_v/L_v)$ denotes the inertia group at $v$. These groups do not depend on $S$, and the morphisms

$$S_T(L) \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O} \hookrightarrow S_A(L), \qquad S_{T^*(1)}(L) \otimes_{\mathcal{O}} \mathcal{K}/\mathcal{O} \hookrightarrow S_{A^*(1)}(L)$$

(as well as their strict counterparts) have finite cokernels.

**(1.6) Selmer complexes and extended Selmer groups.** In the notation of 1.5, the Selmer complex attached to $X = T, A, T^*(1), T^*(1)$ over $L$ is defined as

$$\widetilde{C}_f^\bullet(L, X) = \mathrm{Cone}\left( C^\bullet_{\mathrm{cont}}(G_{L,S}, X) \oplus \bigoplus_{v \in \Sigma_L \cup \Sigma'_L} U_v^+(X) \longrightarrow \bigoplus_{v \in \Sigma_L \cup \Sigma'_L} C^\bullet_{\mathrm{cont}}(G_{L_v}, X) \right)[-1],$$

where

$$U_v(X)^+ = \begin{cases} C^\bullet_{\mathrm{cont}}(G_{L_v}, X_v^+), & v \in \Sigma_L \\ C^\bullet_{\mathrm{cont}}(G_{L_v}/I_v, X^{I_v}), & v \in \Sigma'_L. \end{cases}$$

Up to a canonical quasi-isomorphism, $\widetilde{C}^{\bullet}_f(L,X)$ does not depend on $S$; its cohomology groups are denoted by $\widetilde{H}^i_f(L,X)$.

**(1.7) Comparison of Selmer groups.** For each $X = T, A, T^*(1), T^*(1)$, there is an exact sequence

$$0 \longrightarrow \widetilde{H}^0_f(L,X) \longrightarrow H^0(L,X) \longrightarrow \bigoplus_{v\in\Sigma_L} H^0(L_v, X_v^-) \longrightarrow \widetilde{H}^1_f(L,X) \longrightarrow S_X^{\mathrm{str}}(L) \longrightarrow 0,$$

by [N2, Lemma 9.6.3]. In addition, [N2, Lemma 9.6.7.3] implies that there are exact sequences

$$0 \longrightarrow S_T^{\mathrm{str}}(L) \longrightarrow S_{\mathfrak{p}}(B/L) \longrightarrow \bigoplus_{v\in\Sigma_L} H^1(L_v, T_v^-)_{\mathrm{tors}} \oplus \bigoplus_{v\in\Sigma'_L} H^1(L_v,T)/H^1_{ur}(L_v,T)$$

$$\begin{gathered} 0 \longrightarrow \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) \longrightarrow S_A^{\mathrm{str}}(L) \longrightarrow \\ \longrightarrow \bigoplus_{v\in\Sigma_L} \mathrm{Im}\left(H^1(L_v, A_v^+) \longrightarrow H^1(L_v,A)\right)/\mathrm{div} \oplus \bigoplus_{v\in\Sigma'_L} H^1_{ur}(L_v,A), \end{gathered}$$

in which

$$\begin{gathered} H^1(L_v, T_v^-)_{\mathrm{tors}} \xrightarrow{\sim} H^0(L_v, A_v^-)/\mathrm{div} = \widetilde{B}_v(k(v))[\mathfrak{p}^\infty] \\ D\left(\mathrm{Im}\left(H^1(L_v, A_v^+) \longrightarrow H^1(L_v,A)\right)/\mathrm{div}\right) \subseteq H^0(L_v, A^*(1)_v^-)/\mathrm{div} = \widetilde{B}^t_v(k(v))[\mathfrak{p}^\infty]. \end{gathered}$$

The same lemma implies that, for each $v \in \Sigma'_L$, the $\mathcal{O}$-modules $H^1(L_v,T)/H^1_{ur}(L_v,T)$ and $H^1_{ur}(L_v,A)$ have the same finite length, equal to the local Tamagawa factor $\mathrm{Tam}_v(T,\mathfrak{p})$ defined in 1.8 below.

Of course, one can replace $B$ by $B^t$, $T$ by $T^*(1)$ and $A$ by $A^*(1)$ in the above discussion.

**(1.8) Local Tamagawa factors.** In the notation of 1.6, if $v \nmid p$ is a finite prime of $L$, the local Tamagawa factor $\mathrm{Tam}_v(T,\mathfrak{p})$ is defined as in [N2, 7.6.10] (following [FoPR, Prop. 4.2.2(ii)]), namely

$$\mathrm{Tam}_v(T,\mathfrak{p}) := \ell_{\mathcal{O}}\left(H^1(I_v,T)_{\mathrm{tors}}^{Fr(v)=1}\right)$$

(where $Fr(v)$ is the arithmetic Frobenius at $v$ and $\ell_{\mathcal{O}}(Z)$ denotes the length of any $\mathcal{O}$-module $Z$). This is a non-negative integer (since the group $H^1(I_v,T)_{\mathrm{tors}} \simeq H^0(I_v,A)/\mathrm{div}$ is finite), equal to zero if $v \notin \Sigma'_L$.

It will be more convenient to use geometric notation; let us write

$$\mathrm{Tam}_v(B/L,\mathfrak{p}) := \mathrm{Tam}_v(T,\mathfrak{p}), \qquad \mathrm{Tam}(B/L,\mathfrak{p}) := \sum_{v\in\Sigma'_L} \mathrm{Tam}_v(B/L,\mathfrak{p}).$$

The equality

$$\mathrm{Tam}_v(T^*(1),\mathfrak{p}) = \mathrm{Tam}_v(T,\mathfrak{p}) \tag{1.8.1}$$

proved in [N2, 10.2.8] then implies that

$$\mathrm{Tam}_v(B^t/L,\mathfrak{p}) := \mathrm{Tam}_v(T^*(1),\mathfrak{p}) = \mathrm{Tam}_v(B/L,\mathfrak{p}), \qquad \mathrm{Tam}(B^t/L,\mathfrak{p}) = \mathrm{Tam}(B/L,\mathfrak{p}).$$

This cohomological definition agrees with the geometric one, namely, that

$$\mathrm{Tam}_v(B/L,\mathfrak{p}) := \ell_{\mathcal{O}}\left(\pi_0(\widetilde{B}_v)^{G_{k(v)}} \otimes_{O_M} \mathcal{O}\right). \tag{1.8.2}$$

In particular, if $M = \mathbf{Q}$, then $\mathfrak{p} = p$ and $\mathrm{Tam}_v(B/L,\mathfrak{p})$ is equal to the $p$-adic valuation of the usual local Tamagawa factor $c_{\mathrm{Tam},v}(B/L) = \#H^0(k(v), \pi_0(\widetilde{B}_v))$.

Note that (1.8.2) also implies (1.8.1), by the $G_{k(v)}$-equivariance and nondegeneracy of Grothendieck's monodromy pairing $\pi_0(\widetilde{B}_v) \times \pi_0(\widetilde{B}^t_v) \longrightarrow \mathbf{Q}/\mathbf{Z}$.

## 2. Comparison of Selmer groups, duality, control theorems

**(2.1) Conditions on $B$.** Given a finite extension $L/K$, consider the following conditions.

$(A1)_{B,L,\mathfrak{p}}$ There is an isomorphism of $\mathcal{O}[G_L]$-modules $j : T \xrightarrow{\sim} T^*(1)$ (where $T = T_{\mathfrak{p}}(B)$) such that $j^*(1) = -j$.
$(A2)_{B,L,\mathfrak{p}}$ $\mathrm{Tam}(B/L, \mathfrak{p}) = 0$ and $\bigoplus_{v\in\Sigma_L} \widetilde{B}_v(k(v))[\mathfrak{p}] = 0$.
$(A3)_{B,L,\mathfrak{p}}$ $B(L)[\mathfrak{p}] = 0$.
$(A4)_{B,L,\mathfrak{p}}$ $\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) \xrightarrow{\sim} \mathcal{K}/\mathcal{O}$ (which is equivalent to $D(\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L)) \xrightarrow{\sim} \mathcal{O}$).

**(2.2) Proposition.** *(1) The conditions $(A2)_{B,L,\mathfrak{p}}$ and $(A2)_{B^t,L,\mathfrak{p}}$ are equivalent.*
*(2) If $k \in \{3, 4\}$ and if the conditions $(A1)_{B,L,\mathfrak{p}}$ and $(Ak)_{B,L,\mathfrak{p}}$ hold, so does $(Ak)_{B^t,L,\mathfrak{p}}$.*
*(3) If $(A3)_{B,L,\mathfrak{p}}$ holds, then $\mathrm{Sel}_{\mathfrak{p}^{ke}}(B/L) = \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L)[\mathfrak{p}^{ke}]$ holds, for all $k \geq 1$.*
*(4) If $L'/L$ is a finite extension of $p$-power degree which is unramified at all primes of $L$ at which $B$ has bad reduction, then the conditions $(A2)_{B,L,\mathfrak{p}}$ and $(A2)_{B,L',\mathfrak{p}}$ are equivalent.*
*(5) If $L'/L$ is a finite Galois extension of $p$-power degree, then the conditions $(A3)_{B,L,\mathfrak{p}}$ and $(A3)_{B,L',\mathfrak{p}}$ are equivalent.*
*(6) If $\dim(B) = [M : \mathbf{Q}]$, then $(A1)_{B,L,\mathfrak{p}}$ holds, and the isomorphism $j : T \xrightarrow{\sim} T^*(1)$ induces isomorphisms of $\mathcal{O}[G_{L_v}]$-modules $X_v^\pm \xrightarrow{\sim} X^*(1)_v^\pm$, for $X = T, A$ and all $v \in \Sigma_L$.*

*Proof.* (1) Combine (1.8.1) with the fact that $\widetilde{B}_v(k(v))[\mathfrak{p}^\infty]$ and $\widetilde{B}_v^t(k(v))[\mathfrak{p}^\infty]$ have the same cardinality. The statement (2) is immediate, while (3) follows from (1.4.2). The statements (4) and (5) are consequences of the fact that, if a $p$-group $G$ acts on a finite set $X$, then $\#(X^G) \equiv \#(X) \pmod{p}$.

In the situation of (6), the given $O_M$-linear symmetric isogeny $\lambda = \lambda^t : B \longrightarrow B^t$ induces an isomorphism of $\mathcal{K}[G_K]$-modules $\lambda_* : T_{\mathfrak{p}}(B) \otimes_{\mathcal{O}} \mathcal{K} \xrightarrow{\sim} T_{\mathfrak{p}}(B^t) \otimes_{\mathcal{O}} \mathcal{K}$ and a $G_K$-equivariant, $\mathcal{O}$-bilinear, skew-symmetric pairing $\langle\ ,\ \rangle_{\mathcal{O},\lambda}$ from (1.3.4), which is non-degenerate when tensored with $\mathcal{K}$ and which satisfies $T_{\mathfrak{p}}(B^t) = \lambda_*\{y \in T_{\mathfrak{p}}(B) \otimes_{\mathcal{O}} \mathcal{K} \mid \forall x \in T_{\mathfrak{p}}(B)\ \ \langle x, y\rangle_{\mathcal{O},\lambda} \in \mathcal{O}\}$.

As $T = T_{\mathfrak{p}}(B)$ is a free $\mathcal{O}$-module of rank two, the matrix of the pairing $\langle\ ,\ \rangle_{\mathcal{O},\lambda}$ in any basis of $T$ over $\mathcal{O}$ is of the form $\begin{pmatrix} 0 & b \\ -b & 0 \end{pmatrix}$, for some $b \in \mathcal{O} \setminus \{0\}$. This implies that $T_{\mathfrak{p}}(B^t) = b^{-1}\lambda_*(T_{\mathfrak{p}}(B))$, hence $j := b^{-1} \circ \lambda_* : T_{\mathfrak{p}}(B) \xrightarrow{\sim} T_{\mathfrak{p}}(B^t)$ has the required property.

The maps $X_v^\pm \longrightarrow X^*(1)_v^\pm$ are isomorphisms, since $T_v^-$ is the unique quotient of $T$ which is free of rank one over $\mathcal{O}$ on which $I_v$ acts trivially.

**(2.3) Proposition.** *Let $L$ be a finite extension of $K$.*
*(1) If $(A2)_{B,L,\mathfrak{p}}$ holds, then*

$$\begin{aligned}
\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) &= H^1_f(L, A) = S^{\mathrm{str}}_A(L) = \widetilde{H}^1_f(L, A), && A = B[\mathfrak{p}^\infty] \\
\mathrm{Sel}_{\mathfrak{p}^\infty}(B^t/L) &= H^1_f(L, A^*(1)) = S^{\mathrm{str}}_{A^*(1)}(L) = \widetilde{H}^1_f(L, A^*(1)), && A^*(1) = B^t[\mathfrak{p}^\infty] \\
S_{\mathfrak{p}}(B/L) &= H^1_f(L, T) = S^{\mathrm{str}}_T(L) = \widetilde{H}^1_f(L, T), && T = T_{\mathfrak{p}}(B) \\
S_{\mathfrak{p}}(B^t/L) &= H^1_f(L, T^*(1)) = S^{\mathrm{str}}_{T^*(1)}(L) = \widetilde{H}^1_f(L, T^*(1)), && T^*(1) = T_{\mathfrak{p}}(B^t).
\end{aligned}$$

*(2) In general (without assuming any $(Ak)_{B,L,\mathfrak{p}}$), there are isomorphisms of $\mathcal{O}$-modules*

$$\begin{aligned}
D(\widetilde{H}^i_f(L, T)) &\simeq \widetilde{H}^{3-i}_f(L, A^*(1)) && (= 0 \text{ if } i \neq 1, 2, 3), \\
D(\widetilde{H}^i_f(L, A)) &\simeq \widetilde{H}^{3-i}_f(L, T^*(1)) && (= 0 \text{ if } i \neq 0, 1, 2).
\end{aligned}$$

*(3) If $(A2)_{B,L,\mathfrak{p}}$ holds, then*

$$\widetilde{H}^i_f(L, A) = \begin{cases} \text{a submodule of } B(L)[\mathfrak{p}^\infty], & i = 0 \\ \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L), & i = 1 \\ D(S_{\mathfrak{p}}(B^t/L)), & i = 2 \\ 0, & i \neq 0, 1, 2 \end{cases}$$

$$\widetilde{H}^i_f(L,T) = \begin{cases} S_{\mathfrak{p}}(B/L), & i=1 \\ D(\mathrm{Sel}_{\mathfrak{p}^\infty}(B^t/L)), & i=2 \\ \text{a quotient of } D(B^t(L)[\mathfrak{p}^\infty]), & i=3 \\ 0, & i \neq 1,2,3 \end{cases}$$

*(4) If $(A3)_{B,L,\mathfrak{p}}$ holds, then $\widetilde{H}^0_f(L,A) = 0 = \widetilde{H}^3_f(L,T^*(1))$. Dually, if $(A3)_{B^t,L,\mathfrak{p}}$ holds, then $\widetilde{H}^0_f(L,A^*(1)) = 0 = \widetilde{H}^3_f(L,T)$.*

*Proof.* The equalities of the various Selmer groups in (1) follow from the discussion in 1.7. The statement (2) is a consequence of [N2, Thm. 6.3.4, Prop. 6.7.7], while (3) is a combination of (1) and (2). Finally, (4) follows from (2) and the fact that $\widetilde{H}^0_f(L,A) \subset H^0(L,A)$.

**(2.4) Iwasawa theory.** Fix a Galois extension $K_\infty/K$ such that $\Gamma := \mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_p^d$ $(d \geq 1)$ and let $\Lambda := \mathcal{O}[[\Gamma]] = \varprojlim_F \mathcal{O}[\Gamma_F]$, where $F$ runs through all fields $K \subset F \subset K_\infty$ such that $[F:K] < \infty$, and $\Gamma_F := \mathrm{Gal}(F/K)$.

For every intermediate field $K \subset L \subset K_\infty$ (not necessarily of finite degree over $K$), let

$$\Gamma^L := \mathrm{Gal}(K_\infty/L), \qquad \Gamma_L := \mathrm{Gal}(L/K) = \Gamma/\Gamma^L, \qquad \Lambda_L := \mathcal{O}[[\Gamma_L]].$$

The corresponding Iwasawa-theoretical Selmer modules

$$\widetilde{H}^i_f(L,A) := \varinjlim_{F,\mathrm{res}} \widetilde{H}^i_f(F,A), \qquad \widetilde{H}^i_{f,\mathrm{Iw}}(L/K,T) := \varprojlim_{F,\mathrm{cor}} \widetilde{H}^i_f(F,T)$$

($K \subset F \subset L$, $[F:K] < \infty$) are $\Lambda_L$-modules of cofinite and finite type, respectively.

The standard involution $\iota : \Lambda_L \longrightarrow \Lambda_L$ is induced by the inverse map $\Gamma_L \longrightarrow \Gamma_L$, $\gamma \mapsto \gamma^{-1}$. For any $\Lambda_L$-module $N$ we denote by $N^\iota$ the $\Lambda_L$-module equal to $N$ as an $\mathcal{O}$-module, but on which every $r \in \Lambda_L$ acts as $\iota(r)$ does on $N$. Note that $\iota$ induces an isomorphism of $\Lambda_L$-modules $\iota : \Lambda_L \xrightarrow{\sim} \Lambda_L^\iota$.

This involution appears naturally when one compares Pontryagin duality between $\Lambda_L$-modules of finite type (compact) and cofinite type (discrete), defined by

$$D_{\Lambda_L}(N) := \mathrm{Hom}_{\mathrm{cont},\mathbf{Z}_p}(N, \mathbf{Q}_p/\mathbf{Z}_p), \quad (rf)(n) := f(rn) \quad (r \in \Lambda_L,\ f \in D_{\Lambda_L}(N),\ n \in N),$$

with Pontryagin duality for $\mathcal{O}$-modules with a continuous linear action of $\Gamma_L$: in this case

$$D(N) := \mathrm{Hom}_{\mathrm{cont},\mathbf{Z}_p}(N, \mathbf{Q}_p/\mathbf{Z}_p), \quad (\gamma \cdot f)(n) := f(\gamma^{-1}(n)) \quad (\gamma \in \Gamma_L,\ f \in D(N),\ n \in N).$$

In other words,

$$D_{\Lambda_L}(N) = D(N)^\iota.$$

**(2.5) Proposition.** *Assume that $K \subset L \subset K_\infty$ is an arbitrary intermediate field.*
*(1) In general (without assuming any $(Ak)_{B,L,\mathfrak{p}}$), there are isomorphisms of $\Lambda_L$-modules*

$$D_{\Lambda_L}(\widetilde{H}^i_{f,\mathrm{Iw}}(L/K,T)) \simeq \widetilde{H}^{3-i}_f(L,A^*(1))^\iota \qquad (= 0 \text{ if } i \neq 1,2,3),$$
$$D_{\Lambda_L}(\widetilde{H}^i_f(L,A)) \simeq \widetilde{H}^{3-i}_{f,\mathrm{Iw}}(L/K,T^*(1))^\iota \qquad (= 0 \text{ if } i \neq 0,1,2).$$

*(2) If $(A2)_{B,L,\mathfrak{p}}$ holds, then*

$$\widetilde{H}^i_f(L,A) = \begin{cases} \text{a submodule of } B(L)[\mathfrak{p}^\infty], & i=0 \\ \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L), & i=1 \\ D_{\Lambda_L}(S_{\mathfrak{p}}(B^t/L))^\iota, & i=2 \\ 0, & i \neq 0,1,2 \end{cases}$$

$$\widetilde{H}^i_{f,\mathrm{Iw}}(L/K,T) = \begin{cases} S_{\mathfrak{p}}(B/L), & i=1 \\ D_{\Lambda_L}(\mathrm{Sel}_{\mathfrak{p}^\infty}(B^t/L))^\iota, & i=2 \\ \text{a quotient of } D_{\Lambda_L}(B^t(L)[\mathfrak{p}^\infty])^\iota, & i=3 \\ 0, & i\neq 1,2,3 \end{cases}$$

*(3) (Exact control theorem) If $(A2)_{B,L,\mathfrak{p}}$ and $(A3)_{B,L,\mathfrak{p}}$ hold, then the canonical map*

$$\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) \xrightarrow{\sim} \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_\infty)^{\Gamma^L}$$

*is an isomorphism (idem if we replace everywhere $B$ by $B^t$).*
*(4) If $(A2)_{B,L,\mathfrak{p}}$ and $(A3)_{B,L,\mathfrak{p}}$ are satisfied, then there is an exact sequence of $\Lambda_L$-modules of cofinite type*

$$\begin{aligned} 0 \longrightarrow H^1(\Gamma^L, \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_\infty)) \longrightarrow D_{\Lambda_L}(S_{\mathfrak{p}}(B^t/L))^\iota \longrightarrow D_{\Lambda_L}(S_{\mathfrak{p}}(B^t/K_\infty)_{\Gamma^L})^\iota \\ \longrightarrow H^2(\Gamma^L, \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_\infty)) \longrightarrow 0 \end{aligned}$$

*(again, we can interchange everywhere $B$ with $B^t$).*
*(5) If $(A2)_{B,L,\mathfrak{p}}$ and $(A3)_{B,L,\mathfrak{p}}$ are satisfied, then there is an isomorphism of $\Lambda_L$-modules of finite type*

$$S_{\mathfrak{p}}(B/L) \xrightarrow{\sim} \mathrm{Hom}_{\Lambda_L}(D_{\Lambda_L}(\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L)), \Lambda_L)$$

*(as before, we can replace everywhere $B$ by $B^t$).*
*(6) If $(A2)_{B,L,\mathfrak{p}}$ and $(A3)_{B,L,\mathfrak{p}}$ are satisfied and if $\Gamma_L \simeq \mathbf{Z}_p^r$ $(0 \le r \le d)$, then*

$$\mathrm{rk}_{\Lambda_L} S_{\mathfrak{p}}(B/L) = \mathrm{rk}_{\Lambda_L} S_{\mathfrak{p}}(B^t/L) = \mathrm{cork}_{\Lambda_L} \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) = \mathrm{cork}_{\Lambda_L} \mathrm{Sel}_{\mathfrak{p}^\infty}(B^t/L).$$

*Proof.* (1), (2) Apply Proposition 2.3(2)-(3) over all intermediate fields $K \subset F \subset L$ such that $[F:K] < \infty$ (which is legitimate, thanks to Proposition 2.2(4)-(5)) and take the inductive (resp. the projective) limit.
(3),(4) In the spectral sequence from [N2, Prop. 8.10.12]

$$'\!E_2^{i,j} = H^i(\Gamma^L, \widetilde{H}^j_f(K_\infty, A)) \Longrightarrow \widetilde{H}^{i+j}_f(L, A)$$

(which is a consequence of the "exact control theorem for Selmer complexes" [N2, Prop. 8.10.1]) we have $'\!E_2^{i,j} = 0$ if $j \neq 1,2$, by (1) applied to $K_\infty$ and the fact that $B(K_\infty)[\mathfrak{p}] = 0$ (which follows from $(A3)_{B,K,\mathfrak{p}}$, by Proposition 2.2(5)).
(5) The duality theorem [N2, Thm. 8.9.12] applies in this case, giving rise to a spectral sequence

$$E_2^{i,j} = \mathrm{Ext}^i_{\Lambda_L}(\widetilde{H}^{3-j}_{f,\mathrm{Iw}}(L/K, T^*(1)), \Lambda_L)^\iota \Longrightarrow \widetilde{H}^{i+j}_{f,\mathrm{Iw}}(L/K,T)$$

satisfying $E_2^{i,j} = 0$ for $j \neq 1,2$ (as in the proof of (3) and (4)). Therefore

$$S_{\mathfrak{p}}(B/L) = \widetilde{H}^1_{f,\mathrm{Iw}}(L/K,T) \simeq E_2^{0,1} \simeq \mathrm{Hom}_{\Lambda_L}(D_{\Lambda_L}(\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L)), \Lambda_L).$$

(6) This follows from (5) and the fact that there exists a constant $C \geq 0$ such that, for every $k \geq 1$ and every finite extension $F/K$, the kernel and the cokernel of the map

$$\mathrm{Sel}_{\mathfrak{p}^k}(B/F) \longrightarrow \mathrm{Sel}_{\mathfrak{p}^k}(B^t/F)$$

induced by $\lambda : B \longrightarrow B^t$ is killed by $\mathfrak{p}^C$.
**(2.6) Notation.** For every field $K \subset L \subset K_\infty$ we are going to abbreviate as

$$0 \longrightarrow Z(B/L) \longrightarrow X(B/L) \longrightarrow Y(B/L) \longrightarrow 0 \qquad (2.6.1)$$

the terms in the exact sequence

$$0 \longrightarrow D_{\Lambda_L}(\text{Ш}(B/L)[\mathfrak{p}^\infty]) \longrightarrow D_{\Lambda_L}(\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L)) \longrightarrow D_{\Lambda_L}(B(L) \otimes_{O_M} \mathcal{K}/\mathcal{O}) \longrightarrow 0.$$

Proposition 2.5(3) tells us that, under the conditions $(A2)_{B,K,\mathfrak{p}}$ and $(A3)_{B,K,\mathfrak{p}}$, there are canonical isomorphisms of $\Lambda_L$-modules

$$X(B/K_\infty)_{\Gamma^L} \xrightarrow{\sim} X(B/L), \tag{2.6.2}$$

hence also

$$X(B/L')_{\mathrm{Gal}(L'/L)} \xrightarrow{\sim} X(B/L) \qquad (K \subset L \subset L' \subset K_\infty).$$

## 3. Freeness of compact Selmer groups and the vanishing of Ш$[\mathfrak{p}^\infty]$

**(3.1)** Consider another condition on $B$ and $K$.

$(A5)_{B,K}$ There exists a subfield $K^+ \subset K$ such that $[K : K^+] = 2$, $K_\infty/K^+$ is a Galois extension with Galois group $\Gamma^+ = \Gamma \rtimes \{1, c\}$, where $c^2 = 1$ and $\forall\gamma \in \Gamma \quad c\gamma c^{-1} = \gamma^{-1}$, and there exists an abelian variety $B^+$ over $K^+$ with good reduction at all primes of $K^+$ above $p$, equipped with a ring morphism $i^+ : O_M \longrightarrow \mathrm{End}(B^+)$ and a symmetric $O_M$-linear isogeny $\lambda^+ = (\lambda^+)^t : B^+ \longrightarrow (B^+)^t$, such that $B^+$ has good $\mathfrak{p}$-ordinary reduction at all primes of $K^+$ above $p$, and that the base change of $(B^+, i^+, \lambda^+)$ from $K^+$ to $K$ is isomorphic to $(B, i, \lambda)$.

**(3.2) Proposition.** *(1) If $(A5)_{B,K}$ holds, then*

$$\mathrm{cork}_{\mathcal{O}} \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K) \equiv \mathrm{cork}_{\Lambda_L} \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_\infty) \pmod 2,$$
$$\mathrm{cork}_{\mathcal{O}} \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K) \geq \mathrm{cork}_{\Lambda_L} \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_\infty).$$

*(2) If the conditions $(A2)_{B,K,\mathfrak{p}}$, $(A3)_{B,K,\mathfrak{p}}$ and $(A4)_{B,K,\mathfrak{p}}$ are satisfied, then, for every intermediate field $K \subset L \subset K_\infty$ such that $\Gamma_L = \mathrm{Gal}(L/K) \simeq \mathbf{Z}_p^r$ $(0 \leq r \leq d)$, $X(B/L) = D_{\Lambda_L}(\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L))$ is a cyclic $\Lambda_L$-module.*
*(3) If the conditions $(A2)_{B,K,\mathfrak{p}}$, $(A3)_{B,K,\mathfrak{p}}$, $(A4)_{B,K,\mathfrak{p}}$ and $(A5)_{B,K}$ are satisfied, then, for every intermediate field $K \subset L \subset K_\infty$, the $\Lambda_L$-modules $X(B/L)$ and $S_{\mathfrak{p}}(B/L)$ are free of rank one, the $\Lambda_L/\mathfrak{p}^{ke}$-module $D_{\Lambda_L}(\mathrm{Sel}_{\mathfrak{p}^{ke}}(B/L))$ is free of rank one (for every $k \geq 1$), and the canonical maps*

$$X(B/L')_{\mathrm{Gal}(L'/L)} \xrightarrow{\sim} X(B/L), \qquad S_{\mathfrak{p}}(B^t/L')_{\mathrm{Gal}(L'/L)} \xrightarrow{\sim} S_{\mathfrak{p}}(B^t/L)$$

*are isomorphisms of $\Lambda_L$-modules, if $K \subset L \subset L' \subset K_\infty$. In particular, if $[L : K] < \infty$, then*

$$\mathrm{rk}_{O_M} B(L) + \mathrm{cork}_{\mathcal{O}} \text{Ш}(B/L)[\mathfrak{p}^\infty] = [L : K].$$

*Proof.* (1) If $B = E$ is an elliptic curve, this is [N2, Prop. 10.7.19]. The general case follows from [N2, Thm. 10.7.17(iv)] (for $\chi = \chi' = 1$).
(2) $X(B/L)$ is a $\Lambda_L$-module of finite type satisfying $X(B/L)_{\Gamma_L} \xrightarrow{\sim} X(B/K) \xrightarrow{\sim} \mathcal{O}$, by (2.6.2) (for $L/K$ replacing $K_\infty/L$) and $(A4)_{B,K,\mathfrak{p}}$, respectively. If the image of $x \in X(B/L)$ generates $X(B/K)$ as an $\mathcal{O}$-module, then $(X(B/L)/\Lambda_L x)_{\Gamma_L} = 0$, hence $X(B/L) = \Lambda_L x$ by Nakayama's Lemma.
(3) It is enough to treat the case $L' = K_\infty$. According to (2) applied to $L = K_\infty$, we have $X(B/K_\infty) \xrightarrow{\sim} \Lambda/J$ for some ideal $J \subset \Lambda$. On the other hand, (1) together with $(A4)_{B,K,\mathfrak{p}}$ imply that $\mathrm{rk}_\Lambda X(B/K_\infty) = 1$, hence $J = 0$ and $X(B/K_\infty)$ is free of rank one over $\Lambda$. The control theorem (2.6.2) then yields $X(B/L) \xrightarrow{\sim} \Lambda_L$ as a $\Lambda_L$-module. The statement about $\mathrm{Sel}_{\mathfrak{p}^{ke}}(B/L)$ then follows from Proposition 2.2(3).

It remains to show that $S_{\mathfrak{p}}(B^t/K_\infty)_{\Gamma^L} \xrightarrow{\sim} S_{\mathfrak{p}}(B^t/L)$ is an isomorphism, which is equivalent, by Proposition 2.5(4), to the vanishing of $H^i(\Gamma^L, \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K_\infty))$ for $i = 1, 2$. We claim that the latter group vanishes for all $i > 0$. Indeed, its Pontryagin dual $H_i(\Gamma^L, X(B/K_\infty)) \simeq H_i(\Gamma^L, \Lambda)$ is the $i$-th homology group of the Koszul complex of $\Lambda$ with respect to the sequence $(\gamma'_1 - 1, \ldots, \gamma'_t - 1)$, where $\gamma'_1, \ldots, \gamma'_t$ is any basis of $\Gamma^L \simeq \mathbf{Z}_p^t$

over $\mathbf{Z}_p$. We can take $\gamma_i' = \gamma_i^{p^{n_i}}$ $(1 \leq i \leq t,\ n_i \geq 0)$, for a suitable basis $\gamma_1, \ldots, \gamma_d$ of $\Gamma$ over $\mathbf{Z}_p$. Therefore $\Lambda = \mathcal{O}[[X_1, \ldots, X_d]]$ $(X_i = \gamma_i - 1)$ and $\gamma_i' - 1 = (1+X_i)^{p^{n_i}} - 1$, which implies that $(\gamma_1' - 1, \ldots, \gamma_t' - 1)$ is a regular sequence in $\Lambda$, hence $H_i(\Gamma^L, \Lambda) = 0$ for $i > 0$.

**(3.3) Notation.** For an arbitrary algebraic extension $K'/K$, let us write

$$N_{K'/K}(B \otimes \mathcal{O}) := \varprojlim_{F,\mathrm{Tr}} (B(F) \otimes_{O_M} \mathcal{O}) \subset S_{\mathfrak{p}}(B/K'),$$

where $F$ runs through all intermediate fields $K \subset F \subset K'$ such that $[F : K] < \infty$.

We are going to consider the following conditions.

$(A6)_{B,K'/K,\mathfrak{p}}$ $\quad \mathrm{Im}(N_{K'/K}(B \otimes \mathcal{O}) \longrightarrow B(K) \otimes_{O_M} \mathcal{O}) \neq 0.$

$(A7)_{B,K'/K,\mathfrak{p}}$ $\quad \mathrm{Im}(N_{K'/K}(B \otimes \mathcal{O}) \longrightarrow B(K) \otimes_{O_M} \mathcal{O}/\mathfrak{p}) \neq 0.$

**(3.4) Theorem.** *Assume that the conditions $(A2)_{B,K,\mathfrak{p}}$, $(A3)_{B,K,\mathfrak{p}}$, $(A4)_{B,K,\mathfrak{p}}$, $(A5)_{B,K}$ and $(A6)_{B,K_\infty/K,\mathfrak{p}}$ are satisfied. Then, for every intermediate field $K \subset L \subset K_\infty$ such that $\Gamma_L = \mathrm{Gal}(L/K) \simeq \mathbf{Z}_p^r$ $(0 \leq r \leq d)$,*

$$Ш(B/L)[\mathfrak{p}^\infty] = 0, \qquad B(L) \otimes_{O_M} \mathcal{K}/\mathcal{O} = \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L)$$

*(the Pontryagin dual of the latter group being a free module of rank one over $\Lambda_L$).*

*Proof.* Induction on $r$. If $r = 0$, then $L = K$. In this case $B(K) \otimes_{O_M} \mathcal{O} \neq 0$ and $B(K)[\mathfrak{p}] = 0$ by $(A6)_{B,K_\infty/K,\mathfrak{p}}$ and $(A3)_{B,K,\mathfrak{p}}$, respectively. This means that $B(K) \otimes_{O_M} \mathcal{O} \simeq \mathcal{O}^m$ and $B(K) \otimes_{O_M} \mathcal{K}/\mathcal{O} \simeq (\mathcal{K}/\mathcal{O})^m$ for some $m \geq 1$. On the other hand, $B(K) \otimes_{O_M} \mathcal{K}/\mathcal{O} \subset \mathrm{Sel}_{\mathfrak{p}^\infty}(B/K) \simeq \mathcal{K}/\mathcal{O}$ (by $(A4)_{B,K,\mathfrak{p}}$); thus $m = 1$ and $Ш(B/K)[\mathfrak{p}^\infty] = 0$.

Assume that $r > 0$. In the notation of 2.6, we need to show that $Z(B/L) = 0$, which is equivalent to $X(B/L)/Z(B/L) = Y(B/L) = D_{\Lambda_L}(B(L) \otimes_{O_M} \mathcal{K}/\mathcal{O})$ not being $\Lambda_L$-torsion, since $X(B/L) \simeq \Lambda_L$, by Proposition 3.2(3). Note that the canonical map

$$B(F') \otimes_{O_M} \mathcal{K}/\mathcal{O} \longrightarrow (B(F) \otimes_{O_M} \mathcal{K}/\mathcal{O})^{\mathrm{Gal}(F/F')}$$

is injective, whenever $K \subset F' \subset F \subset K_\infty$ and $[F : K] < \infty$, since $B(K_\infty)[\mathfrak{p}] = 0$ (by Proposition 2.2(5) and $(A3)_{B,K,\mathfrak{p}}$).

If $r = 1$, write $L = \bigcup_{n \geq 1} K_n$, where $\mathrm{Gal}(K_n/K) \simeq \mathbf{Z}/p^n\mathbf{Z}$. If $Y(B/L)$ were $\Lambda_L$-torsion, it would be a free $\mathcal{O}$-module of finite type (since $Y(B/L)[\mathfrak{p}] = 0$), hence $B(L) \otimes_{O_M} \mathcal{O} = B(K_m) \otimes_{O_M} \mathcal{O}$ for some $m \geq 1$. This would imply that

$$\forall k \geq 0 \ \ \forall n \geq m \quad N_{K_{n+k}/K_n}(B(K_{n+k}) \otimes_{O_M} \mathcal{O}) \subset p^k(B(K_n) \otimes_{O_M} \mathcal{O}),$$

hence $N_{L/K}(B \otimes \mathcal{O}) = 0$, which contradicts $(A6)_{B,K_\infty/K,\mathfrak{p}}$.

Assume that $r > 1$. If $Y(B/L)$ were $\Lambda_L$-torsion, there would be $\gamma \in \Gamma_L \smallsetminus \Gamma_L^p$ such that $(\gamma - 1) \notin \mathrm{Supp}_{\Lambda_L}(Y(B/L))$. The fixed field $L' := L^{\gamma=1}$ satisfies $\Gamma_{L'} \simeq \mathbf{Z}_p^{r-1}$. By construction, $Y(B/L)/(\gamma-1)$ is a torsion module over $\Lambda_L/(\gamma - 1) = \Lambda_{L'}$, hence so is its quotient $Y(B/L')$; but this is false by the induction hypothesis.

**(3.5) Theorem.** *Assume that the conditions $(A2)_{B,K,\mathfrak{p}}$, $(A3)_{B,K,\mathfrak{p}}$, $(A4)_{B,K,\mathfrak{p}}$, $(A5)_{B,K}$ and $(A7)_{B,K_\infty/K,\mathfrak{p}}$ are satisfied.*
*(a) For every intermediate field $K \subset L \subset K_\infty$ the following statements hold.*

$$Ш(B/L)[\mathfrak{p}^\infty] = 0, \qquad B(L) \otimes_{O_M} \mathcal{K}/\mathcal{O} = \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L), \qquad N_{L/K}(B \otimes \mathcal{O}) = S_{\mathfrak{p}}(B/L)$$

*and both $S_{\mathfrak{p}}(B/L)$ and $D_{\Lambda_L}(\mathrm{Sel}_{\mathfrak{p}^\infty}(B/L))$ are free modules of rank one over $\Lambda_L = \mathcal{O}[[\mathrm{Gal}(L/K)]]$. In the special case when $[L : K] < \infty$, then $B(L) \otimes_{O_M} \mathcal{O} = S_{\mathfrak{p}}(B/L)$ is a free $\mathcal{O}$-module of rank $\mathrm{rk}_{O_M} B(L) = [L : K]$.*
*(b) If, in addition, $(A1)_{B,K,\mathfrak{p}}$ is satisfied, then the canonical maps*

$$N_{L'/K}(B \otimes \mathcal{O}) = S_{\mathfrak{p}}(B/L') \longrightarrow S_{\mathfrak{p}}(B/L) = N_{L/K}(B \otimes \mathcal{O})$$

*are surjective, for arbitrary intermediate fields $K \subset L \subset L' \subset K_\infty$. Furthermore, $S_\mathfrak{p}(B/L)$ is generated as a $\Lambda_L$-module by the image $x_L$ of any element $x \in N_{K_\infty/K}(B \otimes \mathcal{O})$ whose image $\overline{x}_K$ in $B(K) \otimes_{O_M} \mathcal{O}/\mathfrak{p}$ is non-zero.*

*Proof.* (a) Fix intermediate fields $K \subset L \subset L' \subset K_\infty$. For every finite extension $F/K$,

$$\mathrm{Cone}(\widetilde{C}^\bullet_f(F, X) \xrightarrow{\lambda_*} \widetilde{C}^\bullet_f(F, X^*(1))) \qquad (X = T, A)$$

is quasi-isomorphic to a complex of $\mathcal{O}/\mathfrak{p}^C$-modules, where $\mathfrak{p}^C \operatorname{Ker}(\lambda)(\overline{K})[\mathfrak{p}^\infty] = 0$. Therefore the kernel and cokernel of

$$\widetilde{H}^i_f(F, X) \longrightarrow \widetilde{H}^i_f(F, X^*(1)) \qquad (X = T, A)$$

is killed by $\mathfrak{p}^C$, for every $i$. Thus the same is true for the kernels and cokernels of the maps

$$S_\mathfrak{p}(B/L) \longrightarrow S_\mathfrak{p}(B^t/L), \qquad \mathrm{Sel}_{\mathfrak{p}^\infty}(B/L) \longrightarrow \mathrm{Sel}_{\mathfrak{p}^\infty}(B^t/L).$$

Combined with the freeness results and the isomorphisms in Proposition 3.2(3), this implies that the canonical map

$$j_{L'/L} : S_\mathfrak{p}(B/L')_{\mathrm{Gal}(L'/L)} \longrightarrow S_\mathfrak{p}(B/L)$$

is a morphism between two free $\Lambda_L$-modules of rank one, whose kernel and cokernel is killed by $\mathfrak{p}^C$. Therefore $\operatorname{Ker}(j_{L'/L}) = 0$ and the maps in the commutative diagram

$$\begin{array}{ccc} N_{L'/K}(B \otimes \mathcal{O})_{\mathrm{Gal}(L'/L)} & \xrightarrow{k_{L'/L}} & S_\mathfrak{p}(B/L')_{\mathrm{Gal}(L'/L)} \\ \Big\downarrow{\scriptstyle i_{L'/L}} & & \Big\downarrow{\scriptstyle j_{L'/L}} \\ N_{L/K}(B \otimes \mathcal{O}) & \xrightarrow{k_L} & S_\mathfrak{p}(B/L) \end{array}$$

satisfy

$$\operatorname{Ker}(j_{L'/L}) = 0 = \operatorname{Ker}(k_L), \qquad \mathfrak{p}^C \operatorname{Coker}(j_{L'/L}) = 0.$$

Moreover, $S_\mathfrak{p}(B/K) \xrightarrow{\sim} \mathcal{O}$ (by $(A4)_{B,K,\mathfrak{p}}$) and $\operatorname{Coker}(k_K \circ i_{L'/K}) = 0$, by $(A7)_{B,K_\infty/K,\mathfrak{p}}$. As a result, $j_{L'/K}$ is an isomorphism and

$$0 = \operatorname{Coker}(k_{L'/K}) = (S_\mathfrak{p}(B/L')/N_{L'/K}(B \otimes \mathcal{O}))_{\mathrm{Gal}(L'/K)},$$

which implies that

$$N_{L'/K}(B \otimes \mathcal{O}) = S_\mathfrak{p}(B/L') \simeq \Lambda_{L'} \tag{3.5.1}$$

(for arbitrary $K \subset L' \subset K_\infty$), by Nakayama's Lemma.

In the special case when $[L' : K] < \infty$, it follows from (3.5.1) that

$$B(L') \otimes_{O_M} \mathcal{O} = S_\mathfrak{p}(B/L'), \qquad \mathrm{rk}_{O_M} B(L') = \mathrm{rk}_\mathcal{O} S_\mathfrak{p}(B/L') = [L' : K].$$

As a result, both $X(B/L')$ and $Y(B/L')$ in the exact sequence (2.6.2) are free modules over $\mathcal{O}$ of the same rank $[L' : K]$, hence $Z(B/L') = 0$ and $Ш(B/L')[\mathfrak{p}^\infty] = 0$. This proves the Theorem in the special case when $[L : K] < \infty$. The general case follows by taking the inductive limit over all subfields of $L$ of finite degree over $K$.

(b) In this case the arguments in the proof of (a) go through if one replaces the map $\lambda_*$ by the map $j_*$ induced by the isomorphism $j : T_\mathfrak{p}(B) \xrightarrow{\sim} T_\mathfrak{p}(B^t)$ from $(A1)_{B,K,\mathfrak{p}}$. The constant $C$ is then replaced by zero, which means that the map $j_{L'/L} : S_\mathfrak{p}(B/L')_{\mathrm{Gal}(L'/L)} \longrightarrow S_\mathfrak{p}(B/L)$ is an isomorphism between two free $\Lambda_L$-modules of rank one. If $\overline{x}_K \neq 0$, then $S_\mathfrak{p}(B/K_\infty)/\Lambda x = 0$, by Nakayama's Lemma. It follows that $S_\mathfrak{p}(B/K_\infty) = \Lambda x$ and, after applying $j_{K_\infty/L}$, that $S_\mathfrak{p}(B/L) = \Lambda_L x_L$.

## 4. An application to Heegner points

**(4.1) Ring class fields.** Let $K$ be an imaginary quadratic field of discriminant $D_K$. Denote by $\eta_K : (\mathbf{Z}/|D_K|\mathbf{Z})^\times \longrightarrow \{\pm 1\}$ the primitive quadratic character attached to $K$. For each prime $p \nmid 2D_K$, we have $\eta_K(p) = \left(\frac{D_K}{p}\right)$; if $p \mid D_K$, then $\eta_K(p) = 0$.

For any integer $m \geq 1$, denote by $O_m := \mathbf{Z} + m\mathcal{O}_K \subset O_K$ the order of conductor $m$ in $K$ and by $H_m$ the ring class field of $K$ of conductor $m$ ($H_1$ is the Hilbert class field of $K$). The Galois groups of the intermediate extensions in the diagram

$$\mathbf{Q} = K^+ \hookrightarrow K \hookrightarrow H_1 \hookrightarrow H_m$$

are as follows.

$$G_m := \mathrm{Gal}(H_m/K) \simeq \mathrm{Pic}(O_m), \qquad \mathrm{Gal}(H_m/\mathbf{Q}) = G_m \rtimes \{1, c\}, \qquad \forall g \in G_m \;\; cgc^{-1} = g^{-1}$$

(where $c$ is complex conjugation) and there is an exact sequence

$$\frac{\mathcal{O}_K^\times}{\mathbf{Z}^\times} \longrightarrow \frac{(O_K \otimes \mathbf{Z}/m\mathbf{Z})^\times}{(\mathbf{Z}/m\mathbf{Z})^\times} \longrightarrow G_m \longrightarrow G_1 \longrightarrow 0.$$

The first group in this sequence is cyclic of order

$$u_K := \#(\mathcal{O}_K^\times/\mathbf{Z}^\times) = \begin{cases} 3, & D_K = -3 \\ 2, & D_K = -4 \\ 1, & D_K \neq -3, -4. \end{cases}$$

**(4.2) The anticyclotomic $\mathbf{Z}_p$-extension $K_\infty/K$.** For a fixed prime number $p$, the tower of fields

$$\mathbf{Q} = K^+ \hookrightarrow K \hookrightarrow H_1 \hookrightarrow H_p \hookrightarrow H_{p^2} \hookrightarrow \cdots \hookrightarrow H_{p^\infty} := \bigcup_{n \geq 0} H_{p^n}$$

has the following properties.

- $\forall n \geq 1 \quad \mathrm{Gal}(H_{p^{n+1}}/H_{p^n}) \simeq \mathbf{Z}/p\mathbf{Z}$.
- If $p \neq 2$, then $\mathrm{Gal}(H_{p^\infty}/H_p) \simeq \mathbf{Z}_p$.
- $\mathrm{Gal}(H_1/K) \simeq \mathrm{Pic}(O_K) = Cl_K$.
- $\mathrm{Gal}(H_p/H_1)$ is a cyclic group of order $u_K^{-1}(p - \eta_K(p))$.
- The torsion subgroup $\Delta := \mathrm{Gal}(H_{p^\infty}/K)_{\mathrm{tors}}$ is finite. Its fixed field $K_\infty := (H_{p^\infty})^\Delta$ satisfies $\mathrm{Gal}(K_\infty/K) \simeq \mathbf{Z}_p$ and $\mathrm{Gal}(K_\infty/\mathbf{Q}) = \mathrm{Gal}(K_\infty/K) \rtimes \{1, c\}$, as in (A5). Write $K_\infty = \bigcup_{n \geq 0} K_n$, where $\mathrm{Gal}(K_n/K) \simeq \mathbf{Z}/p^n\mathbf{Z}$.

**(4.3) Heegner points.** Assume that

- $E$ is an elliptic curve over $\mathbf{Q}$ of conductor $N$.
- $\varphi : X_0(N) \longrightarrow E$ is a modular parameterisation of $E$ (sending $i\infty$ to the origin) of the smallest degree.
- $K$ is an imaginary quadratic field satisfying the Heegner condition

(Heeg) all primes dividing $N$ split in $K/\mathbf{Q}$.

Fix an ideal $\mathcal{N} \subset O_K$ such that $O_K/\mathcal{N} \simeq \mathbf{Z}/N\mathbf{Z}$. If $m \geq 1$ is an integer such that $(m, N) = 1$, then $\mathcal{N}_m := \mathcal{N} \cap O_m$ is an invertible ideal of $O_m$ satisfying $O_m/\mathcal{N}_m \simeq \mathcal{N}_m^{-1}/O_m \simeq \mathbf{Z}/N\mathbf{Z}$.

The Heegner points of conductor $m$ on $X_0(N)$ and $E$, respectively, are defined as

$$x_m := [\mathbf{C}/O_m \longrightarrow \mathbf{C}/\mathcal{N}_m^{-1}] \in X_0(N)(H_m), \qquad y_m := \varphi(x_m) \in E(H_m)$$

(up to a sign, $y_m$ does not depend on the choice of $\mathcal{N}$). The basic Heegner point on $E$ is defined as

$$y_K := \mathrm{Tr}_{H_1/K}(y_1) \in E(K).$$

A general modular parameterisation $\varphi' : X_0(N) \longrightarrow E$ of $E$ (sending $i\infty$ to the origin) is obtained by composing $\varphi$ with a non-trivial element $a \in \mathrm{End}(E) = \mathbf{Z}$. The Heegner points $y'_m := \varphi'(x_m)$ corresponding to $\varphi'$ are therefore equal to $y'_m = a y_m$.

**(4.4) Norm relations.** Fix a prime number $p \nmid N$ and let $a_p := p + 1 - \#\widetilde{E}_p(\mathbf{F}_p)$. For any integer $m \geq 1$ relatively prime to $pN$, the Heegner points of conductors $mp^n$ on $E$ are related as follows [PR, 3.1, Prop. 1].

$$\forall n \geq 1 \qquad \mathrm{Tr}_{H_{mp^{n+1}}/H_{mp^n}}(y_{mp^{n+1}}) = a_p y_{mp^n} - y_{mp^{n-1}},$$

$$\exists\, \sigma \in \mathrm{Gal}(H_m/K) \qquad u_{K,m} \cdot \mathrm{Tr}_{H_{mp}/H_m}(y_{mp}) = \begin{cases} a_p y_m, & \text{if } \eta_K(p) = -1 \\ (a_p - \sigma) y_m, & \text{if } \eta_K(p) = 0 \\ (a_p - \sigma - \sigma^{-1}) y_m, & \text{if } \eta_K(p) = 1, \end{cases}$$

$$u_{K,m} = \begin{cases} u_K, & \text{if } m = 1, \\ 1, & \text{if } m > 1. \end{cases}$$

$$u_K \cdot \mathrm{Tr}_{H_p/K}(y_p) = (a_p - 1 - \eta_K(p)) y_K.$$

**(4.5) Universal norms in the $p$-ordinary case.** Assume that $E$ has good ordinary reduction at a prime number $p$ (which is equivalent to $p \nmid N \cdot a_p$). In this case the polynomial defining the Euler factor of $E$ at $p$ factors in $\mathbf{Z}_p[X]$ as

$$X^2 - a_p X + p = (X - \alpha_p)(X - \beta_p), \quad \alpha_p \in \mathbf{Z}_p^\times, \quad \beta_p \in p\mathbf{Z}_p^\times, \tag{4.5.1}$$

$$\alpha_p + \beta_p = a_p, \quad \alpha_p \beta_p = p. \tag{4.5.2}$$

In addition, $|\iota(\alpha_p)| = |\iota(\beta_p)| = \sqrt{p}$, for every embedding $\iota : \mathbf{Q}(\alpha_p) \hookrightarrow \mathbf{C}$.

Define, for every integer $n \geq 0$,

$$z_n := \alpha_p^{-n} y_{p^{n+1}} - \alpha_p^{-n-1} y_{p^n} \in E(H_{p^{n+1}}) \otimes \mathbf{Z}_p.$$

These elements are norm compatible, namely

$$\forall n \geq 1 \quad \mathrm{Tr}_{H_{p^{n+1}}/H_{p^n}}(z_n) = z_{n-1}. \tag{4.5.3}$$

In addition, the bottom element $z_0 = y_p - \alpha_p^{-1} y_0$ satisfies

$$u_K \cdot \mathrm{Tr}_{H_p/K}(z_0) = (a_p - 1 - \eta_K(p)) y_K - \alpha_p^{-1}(p - \eta_K(p)) y_K = (\alpha_p - 1)(1 - \alpha_p^{-1}\eta_K(p)) y_K. \tag{4.5.4}$$

**(4.6) Proposition.** *Assume that $p \nmid N \cdot a_p$.*
*(1) The element $(\alpha_p - 1)(1 - \alpha_p^{-1}\eta_K(p))\,(y_K \otimes 1) \in E(K) \otimes \mathbf{Z}_p$ is contained in*

$$u_K \cdot \mathrm{Im}(N_{H_{p^\infty}/K}(E \otimes \mathbf{Z}_p) \longrightarrow E(K) \otimes \mathbf{Z}_p) \subset u_K \cdot \mathrm{Im}(N_{K_\infty/K}(E \otimes \mathbf{Z}_p) \longrightarrow E(K) \otimes \mathbf{Z}_p).$$

*(2) If $v$ runs through all primes of $K$ above $p$, then*

$$\prod_{v \mid p} \#\widetilde{E}_p(k(v)) \equiv (1 - \alpha_p)(1 - \alpha_p \eta_K(p)) \pmod{p}.$$

*(3) If $a_p \not\equiv 1, \eta_K(p) \pmod p$, then $p \nmid \prod_{v|p} \#\widetilde{E}_p(k(v))$ and*

$$y_K \otimes 1 \in u_K \cdot \mathrm{Im}(N_{H_{p^\infty}/K}(E \otimes \mathbf{Z}_p) \longrightarrow E(K) \otimes \mathbf{Z}_p) \subset u_K \cdot \mathrm{Im}(N_{K_\infty/K}(E \otimes \mathbf{Z}_p) \longrightarrow E(K) \otimes \mathbf{Z}_p).$$

*Proof.* (1) This is a consequence of the norm relations (4.5.3) and (4.5.4).
(2) The term on the left hand side is equal to $(p+1-a_p)(p+1-\eta_K(p)a_p)$ if $\eta_K(p) \neq 0$, resp. to $p+1-a_p$ if $\eta_K(p) = 0$. The claim follows from the fact that $a_p \equiv \alpha_p \pmod p$.
(3) This is an immediate consequence of (1) and (2).

**(4.7)** We are now ready to combine the abstract Iwasawa-theoretical results of §1-§3 with the norm relations summarised in Proposition 4.6.

**(4.8) Theorem.** *If $p \neq 2$ is a prime number such that*
*(a) $E(K)[p] = 0$,*
*(b) $p \nmid N \cdot a_p \cdot (a_p - 1) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$,*
*(c) $y_K \notin E(K)_{\mathrm{tors}}$,*
*(d) $\mathrm{rk}_{\mathbf{Z}}\, E(K) = 1$ and $Ш(E/K)[p^\infty] = 0$,*
*then $Ш(E/K_\infty)[p^\infty] = 0$ and the Pontryagin dual of $E(K_\infty) \otimes \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Sel}_{p^\infty}(E/K_\infty)$ is a free module of rank one over $\mathbf{Z}_p[[\mathrm{Gal}(K_\infty/K)]]$.*

**(4.9) Theorem.** *If $p \neq 2$ is a prime number such that*
*(a) $E(K)[p] = 0$,*
*(b') $p \nmid N \cdot a_p \cdot (a_p - 1) \cdot (a_p - \eta_K(p)) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$,*
*(c') $y_K \notin pE(K)$,*
*(d) $\mathrm{rk}_{\mathbf{Z}}\, E(K) = 1$ and $Ш(E/K)[p^\infty] = 0$,*
*then, for every intermediate field $K \subset L \subset K_\infty$, $Ш(E/L)[p^\infty] = 0$ and the Pontryagin dual of $E(L) \otimes \mathbf{Q}_p/\mathbf{Z}_p = \mathrm{Sel}_{p^\infty}(E/L)$ is a free module of rank one over $\mathbf{Z}_p[[\mathrm{Gal}(L/K)]]$. For every integer $n \geq 0$, $\mathrm{rk}_{\mathbf{Z}}\, E(K_n) = p^n$, $Ш(E/K_n)[p^\infty] = 0$ and $E(K_n) \otimes \mathbf{Z}_p$ is generated over $\mathbf{Z}_p[\mathrm{Gal}(K_n/K)]$ by the traces of Heegner points of $p$-power conductor.*

*Proof.* Theorem 4.8 and Theorem 4.9 follow from Theorem 3.4 and Theorem 3.5, respectively, applied to $B = E$, $M = \mathbf{Q}$ and $\mathfrak{p} = p$. Indeed, the conditions $(A1)_{E,K,p}$ and $(A5)_{E,K}$ are immediate, $(A2)_{E,K,p}$, $(A3)_{E,K,p}$ and $(A4)_{E,K,p}$ follow from (b), (a) and (d), respectively. Finally, $(A6)_{E,K_\infty/K,p}$ (resp. $(A7)_{E,K_\infty/K,p}$) is a consequence of (c) and Proposition 4.6(1) (resp. of (b'), (c'), (d) and Proposition 4.6(3)).

**(4.10)** If $K = \mathbf{Q}(\sqrt{-3})$ and $p = 3$, then the conditions (a) and (c') in Theorem 4.9 can never be satisfied simultaneously. This is a special case of the following divisibility result, which is probably well known, but for which we have not found any reference.

**(4.11) Proposition.** *If a prime number $p$ divides $u_K$ (i.e., if $(K,p) = (\mathbf{Q}(i), 2)$ or $(\mathbf{Q}(\sqrt{-3}), 3)$, then $E(K)[p] \neq 0$ or $y_K \in pE(K)$. In particural, if $y_K \notin E(K)_{\mathrm{tors}}$, then the index $[E(K) : \mathbf{Z}y_K]$ is divisible by $p$.*

*Proof.* Assume that $E(K)[p] = 0$. According to Proposition 5.25, there are infinitely many prime numbers $q \nmid pN$ such that $p \nmid \widetilde{E}_q(\mathbf{F}_q) = q + 1 - a_q$. Any such $q$ satisfies $q \equiv \eta_K(q) \pmod{2u_K}$, and therefore $p \nmid (\eta_K(q) + 1 - a_q)$, since $p \mid u_K$. The last of the norm relations in 4.4

$$(a_q - 1 - \eta_K(q))y_K = u_K\, \mathrm{Tr}_{H_q/K}(y_q) \in u_K\, E(K) \subset pE(K)$$

then implies that $y_K \otimes 1 \in p(E(K) \otimes \mathbf{Z}_{(p)})$, hence $y_K \in pE(K)$.

**(4.12)** It may be worthwhile to reformulate the phenomenon encountered in Proposition 4.11 in more abstract terms, in the general situation of 4.3. Define the *group of Heegner points*

$$E(K)_{HP} \subset E(K)$$

to be the subgroup of $E(K)$ generated by the points

$$y_{K,m} := \mathrm{Tr}_{H_m/K}(y_m), \tag{4.12.1}$$

for all integers $m \geq 1$ relatively prime to $N$.

The norm relations in 4.4 imply, firstly, that $E(K)_{HP}$ is generated by $y_{K,1} = y_K$ and by the points $y_{K,q}$ (where $q$ runs through all primes not dividing $N$), and, secondly, that $u_K y_{K,q} \in \mathbf{Z} y_K$ for all such $q$. It follows that

$$u_K E(K)_{HP} \subset \mathbf{Z} y_K \subset E(K)_{HP};$$

in particular,

$$E(K)_{HP} = \mathbf{Z} y_K \qquad \text{if } u_K = 1.$$

Let us now consider the more interesting case $u_K \neq 1$, when $(K, u_K) = (\mathbf{Q}(i), 2)$ or $(\mathbf{Q}(\sqrt{-3}, 3)$. In either case $u_K = p$ is a prime dividing $D_K$, which implies that $p \nmid N$, and therefore $E$ has good reduction at $p$. In addition, $\chi_{p,K} = 1$ if $p = 3$ (and $\chi_{p,\mathbf{Q}} = 1$ if $p = 2$), where $\chi_{p,K}$ is the cyclotomic character defined in §1.1.

**(4.13) Proposition.** *Assume that $u_K = p > 1$ and $E(K)[p] \neq 0$.*
*(1) $E$ has good ordinary reduction at $p$, $\overline{\rho}_{E,p} = \begin{pmatrix} \chi_{p,\mathbf{Q}} & * \\ 0 & 1 \end{pmatrix}$ or $\begin{pmatrix} 1 & * \\ 0 & \chi_{p,\mathbf{Q}} \end{pmatrix}$ in some basis of $E[p]$, and $a_p \equiv 1 \pmod{p}$.*
*(2) For every prime $q$ not dividing $N$ we have $a_q - 1 - \eta_K(q) \equiv 0 \pmod{p}$.*
*(3) $\mathbf{Z} y_K \subset E(K)_{HP} \subset \mathbf{Z} y_K + E(K)[p]$.*

*Proof.* (1) The assumption $E(K)[p] \neq 0$ together with $\chi_{p,K} = 1$ imply that, in a suitable basis of $E[p]$, $\overline{\rho}_{E,p}|_{G_K} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. Therefore $\overline{\rho}_{E,p} = \begin{pmatrix} \alpha\chi_{p,\mathbf{Q}} & * \\ 0 & \alpha \end{pmatrix}$ for some character $\alpha : G_{\mathbf{Q}} \longrightarrow \mathrm{Gal}(K/\mathbf{Q}) \longrightarrow \{\pm 1\}$, which rules out the case of supersingular reduction at $p$, by [S1, Prop. 12].

If $p = 2$, then $\alpha = 1$ and $2 \nmid a_2$, for trivial reasons. If $p = 3$, then $\alpha = 1$ or $\alpha = \chi_{3,\mathbf{Q}}$. In either case, the semisimplification $\overline{\rho}_{E,3}^{ss}$ is isomorphic to $1 \oplus \chi_{3,\mathbf{Q}}$. On the other hand, $(\overline{\rho}_{E,3}|_{G_{\mathbf{Q}_3}})^{ss} \simeq \beta \oplus \beta\chi_{3,\mathbf{Q}_3}$ for an unramified character $G_{\mathbf{Q}_3}/I_3 \longrightarrow \{\pm 1\}$ such that $a_3 \equiv \beta(Fr(3)) \pmod{3}$; but $\beta = 1$ by the previous discussion.
(2) The case $q = p$ is treated in (1). If $q \nmid pN$, then $a_q = \mathrm{Tr}(\rho_{E,p}(Fr(q)) \equiv q + 1 \pmod{p}$, by (1). However, $q \equiv \eta_K(q) \pmod{p}$.
(3) For each prime $q \nmid N$, the point $y_{K,q} - ((a_q - 1 - \eta_K(q))/p) y_K$ lies in $E(K)[p]$, thanks to (2) and the norm relations in 4.4. In particular, $y_{K,q} \in \mathbf{Z} y_K + E(K)[p]$.

**(4.14) Proposition.** *Assume that $u_K = p > 1$ and $E(K)[p] = 0$.*
*(1) There are infinitely many primes $q \nmid pN$ satisfying $a_q - 1 - \eta_K(q) \not\equiv 0 \pmod{p}$.*
*(2) If $q$ is as in (1), then $y_K \in p(\mathbf{Z} y_K + \mathbf{Z} y_{K,q})$ and $E(K)_{HP} = \mathbf{Z} y_K + \mathbf{Z} y_{K,q} = \mathbf{Z} z_K$, where $z_K \in E(K)_{HP}$ does not depend on $q$ and satisfies $p z_K = y_K$.*
*(3) If $y_K \in E(K)_{\mathrm{tors}}$ is of order $m$, then $p \nmid m$ and $E(K)_{HP} = \mathbf{Z} y_K \simeq \mathbf{Z}/m\mathbf{Z}$.*
*(4) If $y_K \notin E(K)_{\mathrm{tors}}$, then $E(K)_{HP} \simeq \mathbf{Z}$ and $\mathbf{Z} y_K = p E(K)_{HP}$.*

*Proof.* (1) If $a_q - 1 - \eta_K(q) \equiv 0 \pmod{p}$ for all but finitely many primes $q \nmid pN$, then $\#\widetilde{E}_q(\mathbf{F}_q) = q + 1 - a_q \equiv q - \eta_K(q) \equiv 0 \pmod{p}$ for all such $q$, hence $E(\mathbf{Q}(\mu_p))[p] \neq 0$, by Proposition 5.25. This contradicts our assumption $E(K)[p] = 0$, since $K \supset \mathbf{Q}(\mu_p)$.
(2) The norm relation $p y_{K,q} = (a_q - 1 - \eta_K(q)) y_K$ together with $p \nmid (a_q - 1 - \eta_K(q))$ imply that $y_K \in p(\mathbf{Z} y_K + \mathbf{Z} y_{K,q})$. Fix a prime $q' \nmid qN$; then $p y_{K,q'} = (a_{q'} - 1 - \eta_K(q')) y_K$. There exists $n \in \mathbf{Z}$ such that $(a_q - 1 - \eta_K(q)) n \equiv a_{q'} - 1 - \eta_K(q') \pmod{p}$; then $p(y_{K,q'} - n y_{K,q}) \in \mathbf{Z} p y_K$, hence $y_{K,q'} - n y_{K,q} \in \mathbf{Z} y_K + E(K)[p] = \mathbf{Z} y_K$. Therefore $E(K)_{HP} = \mathbf{Z} y_K + \mathbf{Z} y_{K,q}$. Finally, there is a unique $z_K \in \mathbf{Z} y_K + \mathbf{Z} y_{K,q}$ such that $p z_K = y_K$; then $y_{K,q} = (a_q - 1 - \eta_K(q)) z_K$, hence $\mathbf{Z} y_K + \mathbf{Z} y_{K,q} = \mathbf{Z} z_K$.
(3), (4) This follows from (2) and $E(K)[p] = 0$.

**(4.15)** Let us now specialise to the case $K = \mathbf{Q}(\sqrt{-3})$ and $p = 3$. Assume, in addition, that $E(K)[3] = 0$. As we saw in the proofs of Propositions 4.11 and 4.14, there are infinitely many primes $q \nmid 3N$ such that

$$\#\widetilde{E}_q(\mathbf{F}_q) = q + 1 - a_q \not\equiv 0 \pmod{3},$$

thanks to Proposition 5.25 below. The point

$$y_{K,q} = \mathrm{Tr}_{H_q/K}(y_q) \in E(K)$$

satisfies

$$3y_{K,q} = (a_q - 1 - \eta_K(q))y_K$$

with $a_q - 1 - \eta_K(q) \equiv a_q - 1 - q \not\equiv 0 \pmod 3$, and therefore $y_K \in 3E(K)$.

Fix such a prime $q$. The discussion in §4.5-§4.9 needs to be modified as follows. Assume that $3 \nmid a_3$ and let, in the notation of (4.5.1) and (4.5.2), for every integer $n \geq 0$,

$$z_{n,q} := \alpha_3^{-n} y_{3^{n+1}q} - \alpha_3^{-n-1} y_{3^n q} \in E(H_{3^{n+1}q}) \otimes \mathbf{Z}_3.$$

These elements are again norm compatible

$$\forall n \geq 1 \quad \mathrm{Tr}_{H_{3^{n+1}q}/H_{3^n q}}(z_{n,q}) = z_{n-1,q}$$

and the bottom element $z_{0,q} = y_{3q} - \alpha_3^{-1} y_q \in H_{3q} \otimes \mathbf{Z}_3$ satisfies

$$\mathrm{Tr}_{H_{3q}/H_q}(z_{0,q}) = (a_3 - \sigma)y_q - 3\alpha_3^{-1} y_q \qquad (\sigma \in \mathrm{Gal}(H_q/K)),$$
$$\mathrm{Tr}_{H_{3q}/K}(z_{0,q}) = (a_3 - \sigma - \beta_3)\mathrm{Tr}_{H_q/K}(y_q) = (\alpha_3 - 1)y_{K,q}.$$

**(4.16) Proposition.** *Assume that $K = \mathbf{Q}(\sqrt{-3})$, $p = 3$, $E(K)[3] = 0$ and $3 \nmid a_3$. As in 4.15, fix a prime number $q \nmid 3N$ such that $3 \nmid (a_q - 1 - q)$ and define $y_{K,q} \in E(K)$ by (4.12.1).*
*(1) The element $(\alpha_3 - 1)(y_{K,q} \otimes 1) \in E(K) \otimes \mathbf{Z}_3$ is contained in*

$$\mathrm{Im}(N_{H_{3^\infty q}/K}(E \otimes \mathbf{Z}_3) \longrightarrow E(K) \otimes \mathbf{Z}_3) \subset \mathrm{Im}(N_{K_\infty/K}(E \otimes \mathbf{Z}_3) \longrightarrow E(K) \otimes \mathbf{Z}_3).$$

*(2) The only prime $v_3 = (\sqrt{-3})$ of $K$ above 3 satisfies*

$$\#\widetilde{E}_3(k(v_3)) = \#\widetilde{E}_3(\mathbf{F}_3) \equiv 1 - \alpha_3 \pmod 3.$$

*(3) If $a_3 \not\equiv 1 \pmod 3$, then $3 \nmid \#\widetilde{E}_3(k(v_3))$ and*

$$(y_{K,q} \otimes 1) \in \mathrm{Im}(N_{H_{3^\infty q}/K}(E \otimes \mathbf{Z}_3) \longrightarrow E(K) \otimes \mathbf{Z}_3) \subset \mathrm{Im}(N_{K_\infty/K}(E \otimes \mathbf{Z}_3) \longrightarrow E(K) \otimes \mathbf{Z}_3).$$

*Proof.* The statements (1) and (2) follow, respectively, from the norm relations in 4.15 and from the fact that $\#\widetilde{E}_3(\mathbf{F}_3) = 3 + 1 - a_3$. The statement (3) is a consequence of (1) and (2).

**(4.17) Theorem.** *If $K = \mathbf{Q}(\sqrt{-3})$, $p = 3$ and if*
*(a) $E(K)[3] = 0$,*
*(b') $3 \nmid a_3 \cdot (a_3 - 1) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$,*
*(c') $y_{K,q} \notin 3E(K)$ (for a fixed prime $q \nmid 3N$ satisfying $3 \nmid (a_q - 1 - q)$),*
*(d) $\mathrm{rk}_{\mathbf{Z}}\, E(K) = 1$ and $Ш(E/K)[3^\infty] = 0$,*
*then, for every intermediate field $K \subset L \subset K_\infty$, $Ш(E/L)[3^\infty] = 0$ and the Pontryagin dual of $E(L) \otimes \mathbf{Q}_3/\mathbf{Z}_3 = \mathrm{Sel}_{3^\infty}(E/L)$ is a free module of rank one over $\mathbf{Z}_3[[\mathrm{Gal}(L/K)]]$. For every integer $n \geq 0$, $\mathrm{rk}_{\mathbf{Z}}\, E(K_n) = 3^n$, $Ш(E/K_n)[3^\infty] = 0$ and $E(K_n) \otimes \mathbf{Z}_3$ is generated over $\mathbf{Z}_3[\mathrm{Gal}(K_n/K)]$ by the traces to $K_n$ of the Heegner points of conductors dividing $3^\infty q$.*

*Proof.* The proof of Theorem 4.9 applies, except that we use Proposition 4.16 instead of Proposition 4.6.

## 5. Vanishing of certain Galois cohomology groups (after [Ch] and [LW])

**(5.1)** One of the ingredients of Kolyvagin's method for obtaining upper bounds on the size of Selmer groups $\mathrm{Sel}_{p^n}(E/K) \subset H^1(K, E[p^n])$ in the situation of 4.3 is a passage to the extension $L_n := K(E[p^n])$ of $K$ over which the Galois action on $E[p^n]$ becomes trivial. The inflation-restriction sequence

$$0 \longrightarrow H^1(L_n/K, E[p^n]) \longrightarrow H^1(K, E[p^n]) \longrightarrow H^1(L_n, E[p^n])^{\mathrm{Gal}(L_n/K)} \longrightarrow H^2(L_n/K, E[p^n])$$

implies that such a passage entails no loss of information, provided that $H^1(L_n/K, E[p^n]) = 0$. Sufficient criteria for the vanishing of $H^i(L_n/K, E[p^n])$ were given in [Ch, Thm. 2] (for $i = 1$); a complete answer in the case $K = \mathbf{Q}$ was obtained in [LW, Thm. 1, Thm. 2] (for $i = 1, 2$). These questions were also considered, from a slightly different point of view, in [CS1, §5] and [CS2, §3].

In §5.2-§5.21 we recall the approach adopted in [Ch] and [LW], first in an abstract setting, then for $\mathfrak{p}$-power torsion in an abelian variety $B$ of $GL(2)$-type with real multiplication (which includes the case of elliptic curves). Unlike [Ch] and [LW], we are only interested in the "easy case" when $B[\mathfrak{p}]$ is an irreducible Galois module.

**(5.2)** Assume that we are given the following data:

- a prime number $p$,
- a finite extension $\mathcal{K}/\mathbf{Q}_p$, with ring of integers $\mathcal{O}$, uniformiser $\pi$ and residue field $k = \mathcal{O}/\pi$,
- a free $\mathcal{O}$-module $T$ of finite rank $r \geq 1$; set $\overline{T} := T/\pi$,
- a closed subgroup $G \subset \mathrm{Aut}_{\mathcal{O}}(T) \simeq GL_r(\mathcal{O})$.

The $\pi$-adic filtration on $T$ induces a filtration $G = G_0 \supset G_1 \supset G_2 \supset \cdots$ by open normal subgroups

$$G_n := \mathrm{Ker}(G \hookrightarrow \mathrm{Aut}_{\mathcal{O}}(T) \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T/\pi^n)),$$

which have the following properties:

- $G_0/G_1 \hookrightarrow \mathrm{Aut}_k(\overline{T}) \simeq GL_r(k)$,
- $\forall n \geq m \geq 1 \quad G_n/G_{m+n} \hookrightarrow \mathrm{End}_{\mathcal{O}}(\pi^n T/\pi^{m+n}) \simeq M_r(\mathcal{O}/\pi^m) \qquad (1 + \pi^n A \mapsto A \pmod{\pi^m})$,
- $\forall m, n \geq 1 \quad [G_m, G_n] \subset G_{m+n}$, which implies that the adjoint action of $g \in G/G_{m+n}$ on $G_n/G_{m+n}$ (given by $\mathrm{ad}(g)h := ghg^{-1}$) factors through $G/G_m$.

**(5.3)** We are interested in establishing sufficient criteria for the vanishing of the cohomology groups $H^1(G/G_n, T/\pi^m)$ (where $n \geq m \geq 1$). Firstly, dévissage implies that

$$\text{if } H^1(G/G_n, \overline{T}) = 0, \text{ then } \forall m \in \{1, \ldots, n\} \quad H^1(G/G_n, T/\pi^m) = 0. \tag{5.3.1}$$

Secondly, the inflation-restriction sequence for $G_n/G_{n+1} \lhd G/G_{n+1}$ (where $n \geq 1$)

$$0 \longrightarrow H^1(G/G_n, \overline{T}) \longrightarrow H^1(G/G_{n+1}, \overline{T}) \longrightarrow H^1(G_n/G_{n+1}, \overline{T})^{G/G_n} \tag{5.3.2}$$

has the following properties: $G_n/G_{n+1} \hookrightarrow \mathrm{End}_k(\overline{T})$ acts trivially on $\overline{T}$, the action of $G/G_n$ on $\overline{T}$ factors through $G/G_1 \hookrightarrow \mathrm{Aut}_k(\overline{T})$, and so does the adjoint action of $G/G_n$ on $\mathrm{End}_k(\overline{T})$ and its $\mathbf{F}_p[G/G_n]$-submodule $G_n/G_{n+1}$. As a result,

$$H^1(G_n/G_{n+1}, \overline{T})^{G/G_n} = \mathrm{Hom}_{\mathbf{F}_p}(G_n/G_{n+1}, \overline{T})^{G/G_1}. \tag{5.3.3}$$

Putting together (5.3.1)–(5.3.3), we obtain the following statement.

**(5.4) Proposition.** *Assume that* $n \geq 1$ *and that* $\forall n' \in \{1, \ldots, n-1\} \quad \mathrm{Hom}_{\mathbf{F}_p}(G_{n'}/G_{n'+1}, \overline{T})^{G/G_1} = 0$. *If* $H^1(G/G_1, \overline{T}) = 0$, *then* $\forall m \in \{1, \ldots, n\} \quad H^1(G/G_n, T/\pi^m) = 0$.

**(5.5)** It will be convenient to investigate the conditions in Proposition 5.4 in the following axiomatic setting. Throughout §5.5-§5.18,

- $p$ is a prime number,
- $k$ is a finite extension of $\mathbf{F}_p$, of degree $f = [k : \mathbf{F}_p]$,
- $V$ is a finite-dimensional $k$-vector space, of dimension $r \geq 1$,
- $H \subset GL(V) \simeq GL_r(k)$ is a subgroup,
- $W \subset \mathrm{End}_k(V) \simeq M_r(k)$ is an $\mathbf{F}_p[H]$-submodule (with respect to the adjoint action of $H$).
- Denote by $PH$ the image of $H$ under the projection $GL(V) \longrightarrow PGL(V)$.

In order to verify the assumptions of Proposition 5.4, we must be able to answer the following two questions (for $V = \overline{T}$, $H = G/G_1$ and $W = G_n/G_{n+1}$, where $n \geq 1$).

**Question (Q1):** When is $H^1(H, V) = 0$?
**Question (Q2):** When is $\mathrm{Hom}_{\mathbf{F}_p}(W, V)^H = 0$?

There is an extensive literature devoted to (Q1); see [Gu, Thm. A] for fairly general results (valid when $k$ is an arbitrary field of characteristic $p$ and $H$ is a finite subgroup of $GL(V)$).

As noted in [Ch], [LW] and [CS1, CS2], one can often deduce the vanishing statements in (Q1) and (Q2) by applying the following elementary observations.

(5.5.1) If $p \nmid \#H$, then $\forall i > 0 \quad H^i(H, V) = 0$.

(5.5.2) (Sah's Lemma [Sa, Prop. 2.7(b)]) If $M$ is a $k[H]$-module for which there exists a central element $z \in Z(H)$ acting on $M$ by a scalar $\lambda \in k^\times \smallsetminus \{1\}$, then $\forall i \geq 0 \quad H^i(H, M) = 0$.

**(5.6)** Following [Ch], [LW] and [CS1, CS2], we say that $H$ *contains a non-trivial homothety* if $H \cap Z(GL(V)) = H \cap k^\times \cdot \mathrm{id}_V \neq \{1\}$ (or, which is equivalent, that the projection $H \longrightarrow PH$ is not an isomorphism).

If $H$ contains a non-trivial homothety, Sah's Lemma implies that

$$\forall i \geq 0 \quad H^i(H, V) = 0 = H^i(H, \mathrm{Hom}_{\mathbf{F}_p}(W, V)).$$

In particular, the vanishing property in both questions (Q1) and (Q2) always holds.

**(5.7) Proposition.** *Assume that at least one of the following two conditions is satisfied.*
*(a)* $p \nmid \#H$;
*(b)* $V = \bigoplus V_i$ *is a direct sum of simple* $k[H]$*-modules of dimensions* $\dim_k(V_i) \leq (p+1)/2$.
*Then:*
*(1)* $\mathrm{End}_k(V)$ *is a semisimple* $k[H]$*-module.*
*(2)* $\mathrm{End}_k(V)$ *is a semisimple* $\mathbf{F}_p[H]$*-module.*
*(3) Every* $\mathbf{F}_p[H]$*-submodule* $W \subset \mathrm{End}_k(V)$ *is a direct summand.*
*(4) If* $\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V)^H = 0$, *then* $\mathrm{Hom}_{\mathbf{F}_p}(W, V)^H = 0$, *for every* $\mathbf{F}_p[H]$*-submodule* $W \subset \mathrm{End}_k(V)$.

*Proof.* The implications (2) $\Longrightarrow$ (3) $\Longrightarrow$ (4) and (a) $\Longrightarrow$ (1),(2) are automatic, and (2) follows from (1), since the Jacobson radical of $\mathbf{F}_p[H]$ is contained in the Jacobson radical of $k[H]$ ([FD, ch. 2, ex. 6, 50, 53(c)]). If $V = \bigoplus V_i$ is as in (b), so is its dual $V^* = \bigoplus V_i^*$. Semisimplicity of the $k[H]$-module $\mathrm{End}_k(V) = \bigoplus_{i,j} V_i^* \otimes V_j$ then follows from [S2, Cor. 1].

**(5.8)** In view of Proposition 5.7, it is natural to investigate (Q2) for $W = \mathrm{End}_k(V)$. In this case there is a non-degenerate $\mathbf{F}_p$-bilinear symmetric pairing

$$(\ ,\ ) : W \times W \longrightarrow \mathbf{F}_p, \qquad (A, B) := \mathrm{Tr}_{k/\mathbf{F}_p}(\mathrm{Tr}(AB)),$$

which is invariant under the adjoint action of $GL(V)$ and satisfies $(\lambda A, B) = (A, \lambda B)$, for all $\lambda \in k$. It induces, therefore, an isomorphism of $(k \otimes_{\mathbf{F}_p} k)[H]$-modules

$$W \otimes_{\mathbf{F}_p} V \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{F}_p}(W, V).$$

One can rewrite the tensor product on the left hand side in terms of the Galois group

$$\Delta := \mathrm{Gal}(k/\mathbf{F}_p) = \{\varphi^i \mid i \in \mathbf{Z}/f\mathbf{Z}\}, \qquad \varphi(a) = a^p,$$

as follows. The ring isomorphism

$$k \otimes_{\mathbf{F}_p} k \xrightarrow{\sim} \prod_{\sigma \in \Delta} k, \qquad a \otimes b \mapsto (\sigma \mapsto a\sigma(b))$$

induces an isomorphism of $(k \otimes_{\mathbf{F}_p} k)[H]$-modules

$$W \otimes_{\mathbf{F}_p} V \xrightarrow{\sim} \bigoplus_{\sigma \in \Delta} W \otimes_k V^{(\sigma)}, \qquad V^{(\sigma)} := V \otimes_{k,\sigma} k.$$

In concrete terms, if we fix a basis of $V$ over $k$, the (faithful) action $\rho : H \hookrightarrow GL(V) \simeq GL_r(k)$ of $H$ on $V$ gives rise to a twisted action $\rho^{(\sigma)} : H \hookrightarrow GL(V^{(\sigma)}) \simeq GL_r(k)$ given by $\rho^{(\sigma)} = \sigma \circ \rho$.

Using this language, the $k[H]$-module $W = \mathrm{End}_k(V)$ corresponds to the adjoint action $\mathrm{ad}(\rho) = \mathrm{Hom}_k(\rho, \rho) = \rho^* \otimes_k \rho : H \longrightarrow GL(W) \simeq GL_{r^2}(k)$, and

$$\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V) \xrightarrow{\sim} \bigoplus_{\sigma\in\Delta} \left(\mathrm{ad}(\rho) \otimes_k \rho^{(\sigma)}\right).$$

If $p \nmid \dim_k(V)$, then there is a decomposition $\mathrm{ad}(\rho) = \mathrm{ad}^\circ(\rho) \oplus k$, where $\mathrm{ad}^\circ(\rho) = \mathrm{End}^\circ_k(V) := \mathrm{End}_k(V)^{\mathrm{Tr}=0}$ and the trivial representation corresponds to the scalar endomorphisms $k \cdot \mathrm{id}_V$. Therefore

$$\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V) \xrightarrow{\sim} \left(\bigoplus_{\sigma\in\Delta} \rho^{(\sigma)}\right) \oplus \bigoplus_{\sigma\in\Delta} \left(\mathrm{ad}^\circ(\rho) \otimes_k \rho^{(\sigma)}\right)$$

if $p \nmid \dim_k(V)$. The previous discussion can be summed up as follows.

**(5.9) Proposition.** *If $\rho : H \hookrightarrow GL(V)$ denotes the (faithful) action of $H$ on $V$, then the condition $\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V)^H = 0$ is equivalent to $\forall \sigma \in \Delta \quad (\mathrm{ad}(\rho) \otimes_k \rho^{(\sigma)})^H = 0$. If $p \nmid \dim_k(V)$, the latter condition is equivalent to the conjunction of $\rho^H = 0$ and $\forall \sigma \in \Delta \quad (\mathrm{ad}^\circ(\rho) \otimes_k \rho^{(\sigma)})^H = 0$.*

**(5.10) A split dihedral example.** Assume that $p \neq 2$ and that $n > 1$ is an odd integer dividing $\# k^\times = p^f - 1$. Denote by $D_{2n}$ the dihedral group of order $2n$ and by $C_n \lhd D_{2n}$ its unique cyclic subgroup of order $n$. Fix an element $s \in D_{2n} \smallsetminus C_n$; then $s^2 = 1$ and $sgs^{-1} = g^{-1}$, for all $g \in C_n$.

For any character $\psi : C_n \longrightarrow k^\times$, the induced representation

$$I(\psi) := \mathrm{Ind}_{C_n}^{D_{2n}}(\psi) : D_{2n} \longrightarrow GL(V) \simeq GL_2(k)$$

has the following properties.

- In a suitable basis, $I(\psi)|_{C_n} = \begin{pmatrix} \psi & 0 \\ 0 & \psi^{-1} \end{pmatrix}, \; I(\psi)(s) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
- The image of $I(\psi)$ is contained in the normaliser $N(C)$ of a split Cartan subgroup $C \subset GL(V)$.
- $\det(I(\psi)) = \{\pm 1\} \subset k^\times$, $\det(I(\psi)|_{C_n}) = \{1\}$.
- $I(\psi) \simeq I(\psi) \otimes \mathrm{sgn} \simeq I(\psi^{-1}) \simeq I(\psi)^*$, where $\mathrm{sgn} : D_{2n} \longrightarrow D_{2n}/C_n \xrightarrow{\sim} \{\pm 1\}$.
- $I(\psi)$ is irreducible if and only if $\psi \neq 1$.
- $I(1) \simeq 1 \oplus \mathrm{sgn}$.
- $I(\psi_1) \otimes I(\psi_2) \simeq I(\psi_1\psi_2) \oplus I(\psi_1\psi_2^{-1})$.
- $\mathrm{ad}(I(\psi)) = I(\psi)^* \otimes I(\psi) \simeq I(\psi) \otimes I(\psi), \; \mathrm{ad}^\circ(I(\psi)) \simeq I(\psi^2) \oplus \mathrm{sgn}$.
- $\forall i \in \mathbf{Z}/f\mathbf{Z} \quad I(\psi)^{(\varphi^i)} = I(\psi^{p^i})$.
- $\mathrm{ad}^\circ(I(\psi)) \otimes I(\psi)^{(\varphi^i)} \simeq I(\psi^{p^i}) \oplus I(\psi^{p^i+2}) \oplus I(\psi^{p^i-2})$.
- $\dim_k I(\psi)^{C_n} = 2 \dim_k I(\psi)^{D_{2n}}$ is equal to 2 (resp. to 0) if $\psi = 1$ (resp. if $\psi \neq 1$).

**(5.11) A nonsplit dihedral example.** Let $k_2 \simeq \mathbf{F}_{p^{2f}}$ be a quadratic extension of $k$. Assume that $p \neq 2$ and that $n > 1$ is an odd integer dividing $\#(k_2^\times/k^\times) = p^f + 1$.

For any character $\psi' : C_n \longrightarrow \mathrm{Ker}(N_{k_2/k} : k_2^\times \longrightarrow k^\times) \subset k_2^\times$ we define

$$J(\psi') : D_{2n} \longrightarrow GL(V) \simeq GL_2(k)$$

as follows. Let $V = k_2$; the regular representation $j : k_2 = \mathrm{End}_{k_2}(V) \subset \mathrm{End}_k(V)$ identifies $k_2^\times$ with a nonsplit Cartan subgroup $C = j(k_2^\times) \subset GL(V)$ and $\mathrm{Ker}(N_{k_2/k} : k_2^\times \longrightarrow k^\times)$ with $C \cap SL(V)$. We let

$$J(\psi')|_{C_n} := j \circ \psi', \qquad J(\psi')(s) = s',$$

for any element $s' \in N(C)$ of the normaliser of $C$ with eigenvalues $\pm 1$. Explicitly, fix $\alpha \in k_2^\times$ such that $d := \alpha^2 \in k^\times$ and write $j$ in terms of the basis $1, \alpha$ of $k_2$ over $k$:

$$j(a+b\alpha) = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \qquad (a, b \in k).$$

We can then take $s' = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. The representation $J(\psi')$ has the following properties.

- $J(\tau \circ \psi') \simeq J(\psi')$, for any $\tau \in \mathrm{Gal}(k_2/k)$.
- Up to isomorphism, $J(\psi')$ does not depend on any choices.
- The image of $J(\psi')$ is contained in the normaliser $N(C)$ of a nonsplit Cartan subgroup $C \subset GL(V)$.
- $\det(J(\psi')) = \{\pm 1\} \subset k^\times$, $\det(J(\psi')|_{C_n}) = \{1\}$.
- $J(\psi') \otimes_k k_2 \simeq I(\psi')$ (where we consider $\psi'$ on the right hand side as a character $\psi' : C_n \longrightarrow k_2^\times$, and $I(\psi') : D_{2n} \longrightarrow GL_2(k_2)$).

**(5.12) Proposition.** *Assume that $p \neq 2$ and that $n > 1$ is an odd integer.*
*(1) If $n \mid (p^f - 1)$ and if the character $\psi : C_n \longrightarrow k^\times$ in 5.10 is injective, then the following properties of the representation $\rho := I(\psi) : D_{2n} \hookrightarrow GL(V) \simeq GL_2(k)$ are equivalent.*

$$\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V)^{C_n} \neq 0 \iff \mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V)^{D_{2n}} \neq 0 \iff$$
$$\exists \varepsilon \in \{\pm 1\}\ \exists i \in \mathbf{Z}/f\mathbf{Z}\ \ p^i \equiv 2\varepsilon \pmod n \iff \exists \varepsilon \in \{\pm 1\}\ \exists i \in \mathbf{Z}/f\mathbf{Z}\ \ p^i \equiv 2\varepsilon \pmod n \text{ and } n \mid ((2\varepsilon)^f - 1).$$

*(2) If $n \mid (p^f + 1)$ and if the character $\psi' : C_n \longrightarrow \mathrm{Ker}(N_{k_2/k})$ in 5.11 is injective, then the following properties of the representation $\rho := J(\psi') : D_{2n} \hookrightarrow GL(V) \simeq GL_2(k)$ are equivalent.*

$$\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V)^{C_n} \neq 0 \iff \mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k(V), V)^{D_{2n}} \neq 0 \iff$$
$$\exists i \in \mathbf{Z}/2f\mathbf{Z}\ \ p^i \equiv 2 \pmod n \iff \exists i \in \mathbf{Z}/2f\mathbf{Z}\ \ p^i \equiv 2 \pmod n \text{ and } n \mid (2^f - (-1)^i).$$

*Proof.* The first two equivalences in (1) follow from Proposition 5.9 combined with the discussion in 5.10; the third one from the fact that the congruences $p^i \equiv 2\varepsilon \pmod n$ and $p^f \equiv 1 \pmod n$ imply $(2\varepsilon)^f \equiv 1 \pmod n$. The statement (2) follows from the isomorphism $J(\psi') \otimes_k k_2 \simeq I(\psi')$ combined with (1) for the pair $(\psi', k_2)$.

**(5.13) Definition** Given a finite field $k \simeq \mathbf{F}_{p^f}$ of characteristic $p \neq 2$, we say that an odd integer $n > 1$ is *$k$-exceptional* if either $n \mid (p^f - 1)$ and the equivalent conditions in Proposition 5.12(1) are satisfied, or $n \mid (p^f + 1)$ and the equivalent conditions in Proposition 5.12(2) are satisfied. Such a $k$-exceptional integer must divide $2^f - 1$ or $2^f + 1$.

**Examples.** (1) If $k = \mathbf{F}_p$, then $n$ is $k$-exceptional if and only if $n = 3$ and $p \neq 3$.
(2) If $k = \mathbf{F}_{p^2}$, then $n$ is $k$-exceptional if and only if $n \in \{3, 5\}$ and $p \equiv \pm 2 \pmod n$.
(3) If $k = \mathbf{F}_{p^3}$, then $n$ is $k$-exceptional if and only if $n \in \{3, 7, 9\}$ and $p \equiv \pm 2, \pm 4 \pmod n$.

**(5.14)** From now on, we focus our attention on the case $\dim_k(V) = 2$. Recall Dickson's classification of subgroups $H \subset GL(V) \simeq GL_2(k)$ [Di, §260].

- If $p \mid \#H$, then either $H$ acts reducibly on $V$, or $H$ contains $SL(V')$, for some $\mathbf{F}_p$-vector subspace $V' \subset V$ such that $V' \otimes_{\mathbf{F}_p} k = V$.
- If $p \nmid \#H$, then either $H$ is contained in the normaliser $N(C)$ of a Cartan subgroup $C \subset GL(V)$ (which implies that $PH \subset PGL(V)$ is cyclic or dihedral), or $PH$ is isomorphic to $A_4, S_4$ or $A_5$.

The following Proposition gives a complete list of subgroups $H \subset GL_2(k)$ (for $p \neq 2$) acting irreducibly on $k^2$ and not containing a non-trivial homothety (cf. [Ch, Thm. 8], [LW, Lemma 4]).

**(5.15) Proposition.** *Assume that $\dim_k(V) = 2 \neq p$. If $H \subset GL(V)$ acts irreducibly on $V$ and does not contain a non-trivial homothety, then:*
*(1) There exists a Cartan subgroup $C \subset GL(V)$ such that $H \subset N(C)$; in particular, $p \nmid \#H$.*
*(2) The subgroup $H \cap C$ is contained in $C \cap SL(V)$; it is cyclic of order $n > 2$, where $2 \nmid n$ and $n$ divides $\#C/\#k^\times = \#k \mp 1$.*
*(3) If $H \not\subset C$ (which is automatic if $C$ is split), then $H$ is isomorphic to the dihedral group $D_{2n}$ of order $2n$, and $\det(H) = \{\pm 1\} \subset k^\times$.*

*[In concrete terms, $H$ is isomorphic either to $D_{2n}$ or to $C_n$, and its action on $V$ is given by $I(\psi)$ (if $H \simeq D_{2n}$) or $J(\psi')$ (if $H \simeq D_{2n}$ or $C_n$), for an injective character $\psi$ resp. $\psi'$.]*
*(4) Conversely, if $H \subset GL(V)$ is a subgroup satisfying (1)–(2) for some Cartan subgroup $C \subset GL(V)$ and if $H \not\subset C$ if $C$ is split, then $H$ acts irreducibly on $V$ and does not contain a non-trivial homothety.*
*(5) If $k = \mathbf{F}_3$, then no such $H$ exists.*

*Proof.* The irreducibility assumption together with the absence of non-trivial homothety in $H$ imply, by Dickson's classification, that $p \nmid \#H$ and that $H \simeq PH$ is cyclic, dihedral or isomorphic to $A_4, S_4$ or $A_5$. However, the representation theory of $H$ over $\overline{\mathbf{F}}_p$ is the same as over $\mathbf{C}$, since $p \nmid \#H$. The groups $A_4, S_4, A_5$ do not admit a faithful representation into $GL_2(\mathbf{C})$, therefore there is no such a representation into $GL_2(\overline{\mathbf{F}}_p)$, which leaves us only with the cases $H \simeq PH \simeq C_n$ or $D_{2n}$, for some integer $n \geq 1$. In particular, $H \subset N(C)$ for some Cartan subgroup $C \subset GL(V)$ and $H \cap k^\times \cdot \mathrm{id}_V = \{\mathrm{id}_V\}$, which implies that $H \cap C \simeq P(H \cap C) \subset C/k^\times \cdot \mathrm{id}_V$ is cyclic of order $n > 2$ (by irreducibility), where $n \mid \#(C/k^\times \cdot \mathrm{id}_V)$.

If $C \simeq k_2^\times$ is nonsplit, then $n \mid (p^f + 1)$ and, for each $a \in H \cap C$, $\det(a) = N_{k_2/k}(a) = a^{p^f+1} = 1$.

If $C$ is split, then $n \mid (p^f - 1)$ and $H \not\subset C$. For fixed $s \in H \smallsetminus (H \cap C)$ and any $a \in H \cap C$, $(as)^2 = a(sas^{-1}) = \det(a)\,\mathrm{id}_V \in H \cap C \cap k^\times \cdot \mathrm{id}_V = \{\mathrm{id}_V\}$, hence $\det(a) = 1$.

In either case, the cyclic group $H \cap C$ is contained in $C \cap SL(V)$. Its order $n > 1$ is odd, since the only element of order two in $C \cap SL(V)$ is $-\mathrm{id}_V \notin H$.

The above discussion implies that the pair $(H, \rho : H \hookrightarrow GL(V))$ is of the form $(C_n, J(\psi')|_{C_n}), (D_{2n}, I(\psi))$ or $(D_{2n}, J(\psi'))$, where $I(\psi)$ (resp. $J(\psi')$) is as in 5.10 (resp. 5.11), with $\psi$ (resp. $\psi'$) injective. In each of these three cases $H$ acts irreducibly on $V$ and does not contain a non-trivial homothety. This proves parts (1)–(4) of the proposition. Finally, (5) follows from the fact that there is no odd $n > 2$ dividing $3 \pm 1$.

**(5.16) Theorem ([CS1, Thm. 9] if $k = \mathbf{F}_p$).** *Assume that $\dim_k(V) = 2 \neq p$ and that $H$ acts semisimply on $V$.*
*(1) $\forall i > 0 \quad H^i(H, V) = 0$.*
*(2) If $H$ acts irreducibly on $V$, then the following conditions are equivalent.*
*(a) For every $\mathbf{F}_p$-submodule $W \subset \mathrm{End}_k(V)$, $\mathrm{Hom}_{\mathbf{F}_p}(W, V)^H = 0$.*
*(b) $\mathrm{Hom}_{\mathbf{F}_p}(\mathrm{End}_k^\circ(V), V)^H = 0$.*
*(c) The pair $(H, \rho : H \hookrightarrow GL(V))$ is not of the form*

$$(C_n, J(\psi')|_{C_n}), \qquad (D_{2n}, I(\psi)), \qquad (D_{2n}, J(\psi')),$$

*for any $k$-exceptional $n > 1$.*

*Proof.* (1) It is enough to assume that $p \mid \#H$, which rules out the reducible semisimple case, when $H$ is contained in a split Cartan subgroup. By Dickson's classification, $H$ contains $SL(V')$, which in turn contains the homothety $-1 \in k^\times \smallsetminus \{1\}$; we conclude by Sah's Lemma.
(2) If $H$ contains a non-trivial homothety, (a), (b) and (c) are satisfied. If $H$ does not contain a non-trivial homothety, then $p \nmid \#H$, by Proposition 5.15(1). The irreducibility assumption implies that $(V^{(\sigma)})^H = 0$, for all $\sigma \in \mathrm{Gal}(k/\mathbf{F}_p)$. Therefore (b) is equivalent to the same statement with $\mathrm{End}_k^\circ(V)$ replaced by $\mathrm{End}_k(V)$. The equivalence (a) $\iff$ (b) then follows from the case (a) of Proposition 5.7, and the equivalence (b) $\iff$ (c) from Proposition 5.12 combined with Proposition 5.15.

**(5.17) Theorem.** *In the situation of 5.2, assume that $p \neq 2 = r$, that the group $G_0/G_1$ acts irreducibly on the $k$-vector space $\overline{T}$, and that $G_0/G_1$ is not isomorphic to $C_n$ or $D_{2n}$, for any $k$-exceptional odd integer $n > 1$. Then*

$$\forall m_1 \geq m_2 \geq 1 \quad H^1(G/G_{m_1}, T/\pi^{m_2}T) = 0.$$

*Proof.* Combine Theorem 5.16 with Proposition 5.4.

**(5.18) Corollary.** *Assume that $p \neq 2 = r$ and that $G_0/G_1$ acts irreducibly on the $k$-vector space $\overline{T}$. If at least one of the conditions (a)–(g) below holds, then*

$$\forall m_1 \geq m_2 \geq 1 \quad H^1(G/G_{m_1}, T/\pi^{m_2}T) = 0.$$

*(a)* $\det(G_0/G_1) \not\subset \{\pm 1\} \subset k^\times$.
*(b)* $\det(G_0/G_1) = \{\pm 1\} \subset k^\times$ *and* $G_0/G_1$ *is not isomorphic to* $D_{2n}$*, for any* $k$*-exceptional odd integer* $n > 1$.
*(c)* $\det(G_0/G_1) = \{1\} \subset k^\times$ *and* $G_0/G_1$ *is not isomorphic to* $C_n$*, for any* $k$*-exceptional odd integer* $n > 1$.
*(d)* $\det(G_0/G_1) = \mathbf{F}_p^\times$ *and* $p > 3$.
*(e)* $k = \mathbf{F}_p$ *and* $p = 3$.
*(f)* $k = \mathbf{F}_p$, $p > 3$ *and* $G_0/G_1 \not\simeq A_3, S_3$.
*(g)* $k = \mathbf{F}_p$ *and* $\det(G_0/G_1) = \mathbf{F}_p^\times$.

**(5.19)** Consider the following geometric situation:

- $p \neq 2$ is a prime number,
- $K$ is a field of characteristic different from $p$,
- $M$ is a totally real number field,
- $\mathfrak{p} \mid p$ is a prime of $M$ above $p$; let $\mathcal{K} := M_\mathfrak{p}$, $\mathcal{O} := O_\mathcal{K}$, $k := \mathcal{O}/\mathfrak{p}$;
- $B$ is an abelian variety over $K$ of dimension $\dim(B) = [M : \mathbf{Q}]$, equipped with a ring morphism $i : O_M \longrightarrow \mathrm{End}(B)$ and a symmetric $O_M$-linear isogeny $\lambda = \lambda^t : B \longrightarrow B^t$; let $T := T_\mathfrak{p}(B)$ be as in (1.2).

In this case $T$ is a free $\mathcal{O}$-module of rank $r = 2$. Denote by $G \subset \mathrm{Aut}_\mathcal{O}(T) \simeq GL_2(\mathcal{O})$ the image of the Galois representation $\rho_{B,\mathfrak{p}} : G_K \longrightarrow \mathrm{Aut}_\mathcal{O}(T)$. In the notation of 5.2, we have $T/\mathfrak{p}^n = B[\mathfrak{p}^n]$ (in particular, $\overline{T} = B[\mathfrak{p}]$), $G/G_n = \mathrm{Gal}(K(B[\mathfrak{p}^n])/K) \subset \mathrm{Aut}_\mathcal{O}(T/\mathfrak{p}^n) \simeq GL_2(\mathcal{O}/\mathfrak{p}^n)$ and $G_0/G_1$ is the image of the residual Galois representation $\overline{\rho}_{B,\mathfrak{p}} : G_K \longrightarrow \mathrm{Aut}_k(B[\mathfrak{p}]) \simeq GL_2(k)$. The Weil pairing attached to $\lambda$ implies that $\det(\rho_{B,\mathfrak{p}}) : G_K \longrightarrow \mathcal{O}^\times$ is given by the $p$-adic cyclotomic character, hence $\det(\overline{\rho}_{B,\mathfrak{p}}) = \chi_{p,K} : G_K \longrightarrow \mathbf{F}_p^\times \subset k^\times$ is the (mod $p$) cyclotomic character. Applying Theorem 5.17 and Corollary 5.18 in this situation, we obtain the following results.

**(5.20) Theorem.** *In the situation of 5.19, assume that* $B[\mathfrak{p}]$ *is an irreducible* $k[G_K]$*-module, and that* $\overline{\rho}_{B,\mathfrak{p}}(G_K) \subset GL_2(k)$ *is not isomorphic to* $C_n$ *or* $D_{2n}$*, for any* $k$*-exceptional odd integer* $n > 1$*. Then*

$$\forall m_1 \geq m_2 \geq 1 \quad H^1(K(B[\mathfrak{p}^{m_1}])/K, B[\mathfrak{p}^{m_2}]) = 0.$$

**(5.21) Corollary.** *Assume that* $B[\mathfrak{p}]$ *is an irreducible* $k[G_K]$*-module. If at least one of the conditions (a)–(g') below holds, then*

$$\forall m_1 \geq m_2 \geq 1 \quad H^1(K(B[\mathfrak{p}^{m_1}])/K, B[\mathfrak{p}^{m_2}]) = 0.$$

*(a)* $\chi_{p,K}(G_K) \not\subset \{\pm 1\} \subset \mathbf{F}_p^\times$.
*(a')* $K \supset \mathbf{Q}$ *and* $\mathbf{Q}(\mu_p)^+ \not\subset K$.
*(a")* $K$ *is an imaginary quadratic field and* $p > 3$.
*(b)* $\chi_{p,K}(G_K) = \{\pm 1\} \subset \mathbf{F}_p^\times$ *and* $\overline{\rho}_{B,\mathfrak{p}}(G_K)$ *is not isomorphic to* $D_{2n}$*, for any* $k$*-exceptional odd integer* $n > 1$.
*(b')* $\mathbf{Q}(\mu_p)^+ \subset K$, $\mathbf{Q}(\mu_p) \not\subset K$ *and* $\overline{\rho}_{B,\mathfrak{p}}(G_K)$ *is not isomorphic to* $D_{2n}$*, for any* $k$*-exceptional odd integer* $n > 1$.
*(c)* $\chi_{p,K}(G_K) = \{1\} \subset \mathbf{F}_p^\times$ *and* $\overline{\rho}_{B,\mathfrak{p}}(G_K)$ *is not isomorphic to* $C_n$*, for any* $k$*-exceptional odd integer* $n > 1$.
*(c')* $\mathbf{Q}(\mu_p) \subset K$ *and* $\overline{\rho}_{B,\mathfrak{p}}(G_K)$ *is not isomorphic to* $C_n$*, for any* $k$*-exceptional odd integer* $n > 1$.
*(d)* $\chi_{p,K}(G_K) = \mathbf{F}_p^\times$ *and* $p > 3$.
*(d')* $K \supset \mathbf{Q}$, $K \cap \mathbf{Q}(\mu_p) = \mathbf{Q}$ *and* $p > 3$.
*(e)* $k = \mathbf{F}_p$ *and* $p = 3$.
*(e')* $K$ *is an imaginary quadratic field and* $k = \mathbf{F}_p$.
*(f)* $k = \mathbf{F}_p$, $p > 3$ *and* $\overline{\rho}_{B,\mathfrak{p}}(G_K) \not\simeq A_3, S_3$.
*(g)* $k = \mathbf{F}_p$ *and* $\chi_{p,K}(G_K) = \mathbf{F}_p^\times$.
*(g')* $K \supset \mathbf{Q}$, $K \cap \mathbf{Q}(\mu_p) = \mathbf{Q}$ *and* $k = \mathbf{F}_p$.

**(5.22)** If $M = \mathbf{Q}$, then $\mathfrak{p} = p$, $\mathcal{K} = \mathbf{Q}_p$, $\mathcal{O} = \mathbf{Z}_p$ and $B = E$ is an elliptic curve. In this case much more precise results were proved in [Ch, Thm. 2] and [LW, Thm. 11], under suitable assumptions on $K$.

We now prove several auxiliary results that will be needed in §6 (Proposition 5.25 was already used in the proofs of Propositions 4.11 and 4.14).

**(5.23) Proposition.** *Let $V$ be a two-dimensional vector space over a field $k$.*
*(1) If $G \subset GL(V)$ is a subgroup satisfying $\forall g \in G \quad \det(1-g \mid V) = 0$, then there exists a one-dimensional subspace $W \subset V$ such that $W^G \neq 0$ or $(V/W)^G \neq 0$. Equivalently, there exists a basis of $V$ in which $G \subset H_1 := \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ or $G \subset H_2 := \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.*
*(2) If $G \subset GL(V)$ is a subgroup satisfying $\forall g \in G \quad \mathrm{Tr}(g-1 \mid V) = 0$ and if the characteristic of $k$ is not equal to 2, then there exists a one-dimensional subspace $W \subset V$ such that $W^G = W$ and $(V/W)^G = V/W$. Equivalently, there exists a basis of $V$ in which $G \subset \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.*

*Proof.* (1) The eigenvalues of any $g \in G$ are equal to 1 and $\det(g)$. In particular, if $g \in G \cap SL(V)$, then $g$ is unipotent and $\mathrm{Tr}(g) = 2$, $\det(g) = 1$.

If $\#(G \cap SL(V)) > 1$, then there exists a basis of $V$ in which $g_0 := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$. If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \cap SL(V)$, then $ad - bc = 1$ and $a + d = \mathrm{Tr}(g) = 2 = \mathrm{Tr}(g_0 g) = a + c + d$, which implies that $c = 0$, and both eigenvalues of $g$ are equal to $a = d = 1$; thus $G \cap SL(V) \subset H_1 \cap H_2$ and $G \subset \{g \in GL(V) \mid g g_0 g^{-1} \subset H_1 \cap H_2\} = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. This means that $G$ is contained in the union of the subgroups $H_1$ and $H_2$ of $GL(V)$, and therefore is contained in one of them.

If the group $G \cap SL(V)$ is trivial, then $\det : G \xrightarrow{\sim} \det(G) \subset k^\times$ is an isomorphism and $G$ is abelian. As a result, for each $g \in G \smallsetminus \{\mathrm{id}_V\}$, the direct sum decomposition $V = V^{g=1} \oplus V^{g=\det(g)}$ is $G$-stable, hence $G \subset H_1' \cup H_2'$, where $H_1' := \begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$ and $H_2' := \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$. Again, this implies that $G \subset H_1'$ or $G \subset H_2'$.
(2) For each $g \in G$ we have $2\det(1-g \mid V) = \mathrm{Tr}(g-1)\mathrm{Tr}(g) - \mathrm{Tr}(g^2-1) = 0$. Part (1) then implies that there exists $i \in \{1,2\}$ such that $G \subset H_i^{\mathrm{Tr}=2} = H_1 \cap H_2$.

**(5.24) Corollary.** *Assume that, in the situation of 5.2, $r = 2$ and $Y \subset G$ is a subset that maps surjectively on $G_0/G_1$.*
*(1) If $\forall g \in Y \ \det(1-g \mid T) \equiv 0 \pmod{\pi}$, then there is a basis of $\overline{T}$ in which $G_0/G_1 \subset \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ or $G_0/G_1 \subset \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$.*
*(2) If $p \neq 2$ and $\forall g \in Y \ \mathrm{Tr}(g-1 \mid T) \equiv 0 \pmod{\pi}$, then there is a basis of $\overline{T}$ in which $G_0/G_1 \subset \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.*

**(5.25) Proposition.** *If, in the situation of 5.19, $K$ is a number field and there exists a finite set $S$ of finite primes of $K$ (containing all primes above $p$ and all primes at which $B$ has bad reduction) such that*

$$\forall v \notin S \quad \#\widetilde{B}_v(k(v)) \equiv 0 \pmod{p},$$

*then $\overline{\rho}_{B,\mathfrak{p}}$ is isomorphic to $\begin{pmatrix} 1 & * \\ 0 & \chi_{p,K} \end{pmatrix}$ or $\begin{pmatrix} \chi_{p,K} & * \\ 0 & 1 \end{pmatrix}$. In particular, $B(K(\mu_p))[\mathfrak{p}] \neq 0$.*

*Proof.* For each $v \notin S$,

$$\det_{\mathcal{O}}(1 - Fr(v) \mid T_{\mathfrak{p}}(B)) = \#\widetilde{B}_v(k(v)) \equiv 0 \pmod{\mathfrak{p}}.$$

The statement of the proposition follows from Corollary 5.24(1) applied to $T = T_{\mathfrak{p}}(B)$, $G = \mathrm{Im}(G_K \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T))$ and $Y = \{Fr(v) \mid v \notin S\}$ (which maps surjectively on $G_0/G_1 = \mathrm{Im}(G_K \longrightarrow \mathrm{Aut}_k(B[\mathfrak{p}]))$, by the Čebotarev density theorem for $K(B[\mathfrak{p}])/K$).

**(5.26) Proposition.** *Let $E$ be an elliptic curve over $\mathbf{Q}$ of conductor $N$ and $K$ a quadratic field of discriminant $D_K$ relatively prime to $N$. Let $\rho := \overline{\rho}_{E,p} : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}_{\mathbf{F}_p}(E[p]) \simeq GL_2(\mathbf{F}_p)$, for a prime number $p \neq 2$.*
*(1) The field $L := \mathbf{Q}(E[p])$ has the following property:*

$$\rho(G_{\mathbf{Q}}) \neq \rho(G_K) \iff L \cap K = K \iff D_K = p^* := (-1)^{(p-1)/2} p.$$

*(2) If $\rho$ is irreducible, so is $\rho|_{G_K}$.*
*(3) If $\rho|_{G_K}$ is irreducible, but not absolutely irreducible, then $p = 3$, $K = \mathbf{Q}(\sqrt{-3})$, $E$ has good ordinary reduction at 3, $\rho(G_K)$ is a cyclic group of order 4 and $\rho(G_{\mathbf{Q}})$ is a dihedral group of order 8.*

*Proof.* (1) We have $\rho(G_{\mathbf{Q}}) \xrightarrow{\sim} \mathrm{Gal}(L/\mathbf{Q})$ and $\mathrm{Gal}(L/L \cap K) \simeq \mathrm{Gal}(KL/K) \xrightarrow{\sim} \rho(G_K)$, which yields the first equivalence in (1). A prime number $\ell$ is unramified in $K/\mathbf{Q}$ if and only if $\ell \nmid D_K$; it is unramified in $L/\mathbf{Q}$ if $\ell \nmid pN$. As $(N, D_K) = 1$, the equality $L \cap K = K$ implies that $\{\ell \mid D_K\} \subset \{\ell \mid D_K\} \cap \{\ell \mid pN\} \subset \{p\}$, hence $D_K = p^*$. Conversely, $\mathbf{Q}(\sqrt{p^*}) \subset \mathbf{Q}(\mu_p) \subset L$.
(2) If $\rho$ is irreducible but $\rho|_{G_K}$ is not, then $\rho|_{G_K}$ is semisimple (since $G_K$ is a normal subgroup of $G_{\mathbf{Q}}$) and its image is contained in a split Cartan subgroup $C_s$ of $GL_2(\mathbf{F}_p)$. Moreover, $\rho(G_{\mathbf{Q}}) \neq \rho(G_K)$, hence $D_K = p^*$ and $p \nmid N$, which means that $E$ has good reduction at $p$.

If the reduction at $p$ is supersingular, then $\rho(G_{\mathbf{Q}_p}) = N(C_{ns})$ is the normaliser of a nonsplit Cartan subgroup $C_{ns}$ of $GL_2(\mathbf{F}_p)$, by [S1, Prop. 12]. In particular, $\#\rho(G_K)$ is a multiple of $\#N(C_{ns})/2 = p^2 - 1 > (p-1)^2 = \#C_s \geq \#\rho(G_K)$, which is impossible.

If the reduction at $p$ is ordinary, then the restriction of $\rho$ to the inertia group $I_p \subset G_{\mathbf{Q}_p}$ is given by $\begin{pmatrix} \chi_{p,\mathbf{Q}_p} & * \\ 0 & 1 \end{pmatrix}$, by [S1, Prop. 11]. On the other hand, $\rho|_{G_K} = \alpha \oplus \alpha^c$, where $\alpha : G_K \longrightarrow \mathbf{F}_p^\times$ is a character and $\alpha^c(g) := \alpha(\tilde{c} g \tilde{c}^{-1})$, for any $\tilde{c} \in G_{\mathbf{Q}} \smallsetminus G_K$. Consequently, the restrictions to the inertia group $I_{\mathfrak{p}} \subset G_{K_{\mathfrak{p}}}$ (where $\mathfrak{p} \mid p$ is the only prime of $K$ above $p$) satisfy $\{\alpha|_{I_{\mathfrak{p}}}, \alpha^c|_{I_{\mathfrak{p}}}\} = \{\chi_{p,K_{\mathfrak{p}}}|_{I_{\mathfrak{p}}}, 1\}$. As a result, $\chi_{p,K_{\mathfrak{p}}}|_{I_{\mathfrak{p}}} = 1$, which implies that $\chi^2_{p,\mathbf{Q}_p}(I_p) = 1$, $p = 3$ and $K = \mathbf{Q}(\sqrt{-3})$. In this case $\chi_{3,K} = 1$, hence $\rho(G_K) \subset C_s \cap SL_2(\mathbf{F}_3) = \{\pm I\}$. As $\rho(G_{\mathbf{Q}})$ contains $\rho(\tilde{c}) \sim \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, we have $\rho(G_{\mathbf{Q}}) \simeq (\mathbf{Z}/2\mathbf{Z})^a$ for some $a \leq 2$, which contradicts the irreducibility of $\rho$.
(3) Firstly, $\rho(G_K)$ is contained in $C_{ns}$ but not in $C_{ns} \cap C_s = \mathbf{F}_p^\times \cdot I$. Secondly, $\rho(G_{\mathbf{Q}})$ contains $\rho(\tilde{c}) \notin C_{ns}$, hence $\rho(G_{\mathbf{Q}}) \neq \rho(G_K)$; thus $D_K = p^*$ and $E$ has good reduction at $p$.

If the reduction at $p$ is supersingular, then

$$\#\rho(G_K) = \#\rho(G_{\mathbf{Q}})/2 \geq \#\rho(G_{\mathbf{Q}_p})/2 = \#C_{ns} \geq \#\rho(G_K).$$

It follows that $\rho(G_K) = C_{ns}$ and $\det \rho(G_K) = N_{\mathbf{F}_{p^2}/\mathbf{F}_p}(\mathbf{F}_{p^2}^\times) = \mathbf{F}_p^\times$, which is equivalent to $\mathbf{Q}(\mu_p) \cap K = \mathbf{Q}$, but this is not true.

If the reduction at $p$ is ordinary, then the restriction of $\rho$ to $I_p$ is of the form $\begin{pmatrix} \chi_{p,\mathbf{Q}_p} & * \\ 0 & 1 \end{pmatrix} \subset C_{ns}$, which implies again that $\chi_{p,K_{\mathfrak{p}}}|_{I_{\mathfrak{p}}} = 1$, $p = 3$, $K = \mathbf{Q}(\sqrt{-3})$ and $\chi_{3,K} = 1$, hence $\rho(G_K)$ is contained in $C_{ns} \cap SL_2(\mathbf{F}_3)$, which is a cyclic group of order 4. On the other hand, $\#\rho(G_K) > 2$, by the irreducibility of $\rho|_{G_K}$, which implies the statements about the structure of $\rho(G_K)$ and $\rho(G_{\mathbf{Q}})$.

**(5.27) Genus theory of quadratic fields.** Let $K$ be a quadratic field, $R = \{q \mid D_K\}$ the set of prime numbers ramified in $K/\mathbf{Q}$, $C$ the strict ideal class group of $K$, $H$ the strict Hilbert class field of $K$ (the maximal abelian extension of $K$ unramified over $K$ at all finite primes) and $K_{\mathrm{gen}} := H \cap \mathbf{Q}^{ab}$ the genus field of $K$. The Galois groups in the tower $\mathbf{Q} \hookrightarrow K \hookrightarrow K_{\mathrm{gen}} \hookrightarrow H$ are as follows.

$$G := \mathrm{Gal}(H/K) \simeq C, \qquad G_+ := \mathrm{Gal}(H/\mathbf{Q}) \text{ satisfies } \forall g_+ \in G_+ \smallsetminus G \ \forall g \in G \ \ g_+^2 \in G, \quad g_+ g g_+^{-1} = g^{-1}$$
$$\mathrm{Gal}(H/K_{\mathrm{gen}}) = [G_+, G_+] = G^2 \simeq C^2, \qquad \mathrm{Gal}(K_{\mathrm{gen}}/K) \simeq C/C^2.$$

There is a unique factorisation

$$D_K = \prod_{q \in R} D_q, \qquad D_q \equiv 0, 1 \pmod 4, \qquad |D_q| = \text{ a power of } q$$

(if $q \neq 2$, then $D_q = q^* := (-1)^{(q-1)/2} q$). In terms of this factorisation,

$$K_{\mathrm{gen}} = \mathbf{Q}(\{\sqrt{D_q}\}_{q \in R})$$

is the compositum of the quadratic fields $K(q) := \mathbf{Q}(\sqrt{D_q})$, for all $q \in R$.

**(5.28) Proposition.** *For each $q \in R$, the compositum $H(q)$ of all subfields of $H$ unramified over $\mathbf{Q}$ outside $q\infty$ is equal to*

$$H(q) = \begin{cases} H, & \text{if } R = \{q\} \\ K(q), & \text{if } R \neq \{q\}. \end{cases}$$

*Proof.* The case $R = \{q\}$ is immediate. Assume that $R \neq \{q\}$. For each $q' \in R \smallsetminus \{q\}$ and each prime $v$ in $H$ above $q'$, the inertia subgroup $I_v \subset \mathrm{Gal}(H/\mathbf{Q}) = G_+$ is of the form $I_v = \{1, h_v\}$, where $h_v^2 = 1$ and $h_v \neq G$. By definition, $H(q)$ is the fixed field of the subgroup $G(q) \subset G$ generated by the $I_v$, for all $q' \in R \smallsetminus \{q\}$ and $v \mid q'$. If $g \in G$, then $g h_v g^{-1} \in I_{g(v)}$ and $g^2 = g h_v g^{-1} h_v^{-1} \in G(q)$; thus $G^2 \subset G(q)$ and $H(q) \subset K_{\mathrm{gen}}$, but the only subfields of $K_{\mathrm{gen}}$ unramified over $\mathbf{Q}$ outside $q\infty$ are $\mathbf{Q}$ and $K(q)$.

**(5.29)** For an arbitrary quadratic field $K$, its ring class field $H_n$ of conductor $n \geq 1$ is an abelian extension of $K$ characterised by the fact that the reciprocity map of class field theory induces an isomorphism

$$K_+^\times \backslash \widehat{K}^\times / \widehat{O}_n^\times \xrightarrow{\sim} \mathrm{Gal}(H_n/K),$$

where $\widehat{K} = K \otimes \widehat{\mathbf{Z}}$, $\widehat{O}_n = (\mathbf{Z} + nO_K) \otimes \widehat{\mathbf{Z}}$ and $K_+^\times \subset K^\times$ is the subgroup of elements that are positive under all real embeddings $K \hookrightarrow \mathbf{R}$. For $n = 1$, $H_1$ is the strict Hilbert class field of $K$. In general, $H_n$ is a Galois extension of $\mathbf{Q}$ and

$$\forall g \in \mathrm{Gal}(H_n/K) \quad \forall g_+ \in \mathrm{Gal}(H_n/\mathbf{Q}) \smallsetminus \mathrm{Gal}(H_n/K) \qquad g_+^2 \in \mathrm{Gal}(H_n/K), \quad g_+ g g_+^{-1} = g^{-1}.$$

In particular, $\mathrm{Gal}(H_n/\mathbf{Q})^{ab} \xrightarrow{\sim} (\mathbf{Z}/2\mathbf{Z})^a$ for some $a \geq 0$.

**(5.30)** In the situation of 5.2, assume that we are given surjective morphisms $G_{\mathbf{Q}} \xrightarrow{\rho} G \xrightarrow{\chi} \mathbf{Z}_p^\times$ whose composition is the cyclotomic character, and a surjective $\mathcal{O}$-bilinear pairing $\langle \ , \ \rangle : T \times T \longrightarrow \mathcal{O}$ satisfying

$$\forall g \in G \quad \forall x, y \in T \qquad \langle gx, gy \rangle = \chi(g) \langle x, y \rangle.$$

For each $m \geq 1$, let $\rho_m$ be the composition $\rho_m : G_{\mathbf{Q}} \longrightarrow G \longrightarrow G/G_m \hookrightarrow \mathrm{Aut}_{\mathcal{O}/\pi^m}(T/\pi^m)$ and define $L_m := \mathbf{Q}(T/\pi^m T) = \overline{\mathbf{Q}}^{\mathrm{Ker}(\rho_m)}$.

By definition, if $g \in G_m$ ($m \geq 1$), then $(g-1)T \subset \pi^m T$ and

$$\forall x, y \in T \quad (\chi(g) - 1)\langle x, y \rangle = \langle gx, gy \rangle - \langle x, y \rangle = \langle (g-1)x, gy \rangle + \langle x, (g-1)y \rangle \in \pi^m \mathcal{O},$$

hence $\chi(g) \in 1 + \pi^m \mathcal{O}$, by the surjectivity of $\langle \ , \ \rangle$. This implies that

$$\forall m \geq 1 \quad L_m = \mathbf{Q}(T/\pi^m T) \supset \mathbf{Q}(\mu_{p^t}),$$

where $t$ is the smallest integer such that $t \geq m/e$ and $e := \mathrm{ord}_\pi(p)$ is the ramification index of $\mathcal{K}/\mathbf{Q}_p$. In particular,

$$L_\infty := \bigcup_{m \geq 1} L_m \supset \mathbf{Q}(\mu_{p^\infty}).$$

**(5.31) Proposition.** *Assume that we are in the situation of 5.30 with $p \neq 2$, that $K$ is a quadratic field of discriminant $D_K$ and that $\rho : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}_{\mathcal{O}}(T)$ is unramified outside $pN\infty$ (i.e., that $L_\infty/K$ is unramified*

*outside $pN\infty$). Fix $m, n \geq 1$.*
*(1) For every algebraic extension $F/\mathbf{Q}$ we have $(T/\pi^m T)^{G_F} = (T/\pi^m T)^{G_{F \cap L_m}}$.*
*(2) If $L_m \subset H_n$, then $p = 3$, $1 \leq m \leq e$ and $3 \mid nD_K$.*
*(3) If $(n, pN) = 1$, then $KL_\infty \cap H_n = KL_\infty \cap H_1$.*
*(4) If $(N, D_K) = 1$, then the extension $(L_\infty \cap H_1)/\mathbf{Q}$ is unramified outside $p\infty$.*
*(5) If $(pN, D_K) = 1$, then $L_\infty \cap H_1 = \mathbf{Q}$.*
*(6) If $(N, D_K) = 1$ and $D_K = p^* := (-1)^{(p-1)/2}$, then $K \subset L_1$.*
*(7) If $(N, D_K) = 1$, $p \mid D_K$ and $D_K \neq p^*$, then $L_\infty \cap H_1 = \mathbf{Q}(\sqrt{p^*}) = L_1 \cap H_1$ and $L_\infty \cap K = \mathbf{Q}$.*
*(8) If $(N, D_K) = 1$, $D_K = p^*$ and $r = \mathrm{rk}_{\mathcal{O}}(T) = 2$, then $\overline{T}^{G_{H_1}} = \overline{T}^{G_K}$.*

*Proof.* (1) This is true by the definition of $L_m$.
(2) If $t$ is the smallest integer such that $t \geq m/e$, then $L_m \subset H_n$ implies that $\mathbf{Q}(\mu_{p^t}) \subset L_m \cap \mathbf{Q}^{ab} \subset H_n \cap \mathbf{Q}^{ab} =$ a compositum of quadratic fields unramified outside $nD_K\infty$. Therefore $\varphi(p^t) \leq 2$, $p = 3$, $t = 1$ and $3 \mid nD_K$.
(3) The extension $KL_\infty/K$ (resp. $H_n/K$) is unramified outside $\{v \mid pN\infty\}$ (resp. $\{v \mid n\infty\}$); thus $(KL_\infty \cap H_n)/K$ is an abelian extension unramified at all finite places, so it must be contained in $H_1$.
(4) The extension $L_\infty/\mathbf{Q}$ (resp. $H_1/\mathbf{Q}$) is unramified outside $\{\ell \mid pN\infty\}$ (resp. $\{\ell \mid D_K\infty\}$); thus $(L_\infty \cap H_1)/\mathbf{Q}$ is unramified outside $p\infty$.
(5) In this case $(L_\infty \cap H_1)/\mathbf{Q}$ is unramified outside $\infty$, so $L_\infty \cap H_1 = \mathbf{Q}$.
(6) $K = K(p) := \mathbf{Q}(\sqrt{p^*}) \subset \mathbf{Q}(\mu_p) \subset L_1$.
(7) The quadratic field $K(p) = \mathbf{Q}(\sqrt{p^*})$ is contained in both $\mathbf{Q}(\mu_p) \subset L_1$ and in $H_1$ (by genus theory); thus $K(p) \subset L_1 \cap H_1 \subset L_\infty \cap H_1$. On the other hand, (4) tells us that $L_\infty \cap H_1$ is contained in $H(p)$, but $H(p) = K(p)$ in our case, by Proposition 5.28.
(8) If $p = 3$, then $K = \mathbf{Q}(\sqrt{-3}) = H_1$. If $p > 3$, then $L_1 \not\subset H_1$ by (2), which means that $d := \dim_k \overline{T}^{G_{H_1}} \leq 1$. There is nothing to prove if $d = 0$. If $d = 1$, then $\mathrm{Gal}(L_1 \cap H_1/\mathbf{Q})$ acts on the line $\overline{T}^{G_{H_1}} = \overline{T}^{G_{L_1 \cap H_1}}$ by a character $\alpha : \mathrm{Gal}(L_1 \cap H_1/\mathbf{Q}) \longrightarrow \mathrm{Gal}(L_1 \cap H_1/\mathbf{Q})^{ab} \longrightarrow k^\times$. However, $\mathrm{Gal}(L_1 \cap H_1/\mathbf{Q})^{ab}$ is a quotient of $\mathrm{Gal}(H_1/\mathbf{Q})^{ab} = \mathrm{Gal}(K_{\mathrm{gen}}/\mathbf{Q}) = \mathrm{Gal}(K/\mathbf{Q})$, which means that $G_K$ acts on $\overline{T}$ by $\begin{pmatrix} 1 & * \\ 0 & \chi_{p,K} \end{pmatrix}$. As $\chi_{p,K} \neq 1$ for $p > 3$, it follows that $\overline{T}^{G_K} = \overline{T}^{G_{H_1}}$, as claimed.

## 6. Kolyvagin's result on the vanishing of Ш$(E/K)[p^\infty]$

**(6.1)** Throughout §6, let:

- $E$ be an elliptic curve over $\mathbf{Q}$ of conductor $N$,
- $\varphi : X_0(N) \longrightarrow E$ a modular parameterisation of $E$ sending $i\infty$ to the origin,
- $K$ an imaginary quadratic field in which all primes dividing $N$ split,
- $\mathcal{N}$ an ideal of $O_K$ such that $O_K/\mathcal{N} \simeq \mathbf{Z}/N\mathbf{Z}$.

As in 4.3, these data determine the Heegner points $y_m \in E(H_m)$ on $E$, defined over the ring class fields $H_m$ of conductors $m \geq 1$ relatively prime to $N$, and the basic Heegner point $y_K = \mathrm{Tr}_{H_1/K}(y_1)$.

**(6.2)** If $y_K \notin E(K)_{\mathrm{tors}}$ (and $D_K \neq -3, -4$), then the groups $E(K)/\mathbf{Z}y_K$ and Ш$(E/K)$ are finite ([K1, Thm. A]) and the Néron–Tate height of $y_K$ is given by the formula of Gross and Zagier [GZ, Thm. V.2.1] (Gross and Zagier considered only the case when $D_K$ is odd; for even $D_K$ the corresponding formula is a special case of [Z, Thm. 1.2.1]). Combining their formula with the conjecture of Birch and Swinnerton-Dyer, Gross and Zagier observed [GZ, Conj. V.2.2] that, if $y_K \notin E(K)_{\mathrm{tors}}$, then the conjecture of Birch and Swinnerton-Dyer for $E$ over $K$ holds if and only if

$$[E(K) : \mathbf{Z}y_K] \stackrel{?}{=} (\#\text{Ш}(E/K))^{1/2}\, u_K\, c_{\mathrm{Tam}}(E/\mathbf{Q})\, c_{\mathrm{Manin}}(\varphi), \tag{6.2.1}$$

where $c_{\mathrm{Tam}}(E/\mathbf{Q}) = \prod_{\ell \mid N} c_{\mathrm{Tam},\ell}(E/\mathbf{Q})$ is the product of all non-archimedean local Tamagawa factors of $E$ over $\mathbf{Q}$, $u_K = \#(O_K^\times/\mathbf{Z}^\times)$ and $c_{\mathrm{Manin}}(\varphi) \in \mathbf{Z}_{>0}$ is the Manin constant for $\varphi$.

Recall that, for any elliptic curve $E'$ defined over any number field $K'$, the Cassels–Tate pairing on the finite abelian group $Ш(E'/K')/\mathrm{div}$ with values in $\mathbf{Q}/\mathbf{Z}$ is alternating and non-degenerate, which implies that $Ш(E'/K')/\mathrm{div}$ is of the form $X \oplus X$, for some maximal isotropic subspace $X$. In particular, $\#(Ш(E'/K')/\mathrm{div}) = (\#X)^2$ is a square.

In §0.8-§0.9 we discussed Kolyvagin's results on a conjectural divisibility

$$\text{if } y_K \notin E(K)_{\mathrm{tors}}, \text{ then } \quad [E(K) : \mathbf{Z}y_K]/(\#Ш(E/K))^{1/2} \in \mathbf{Z}_{(p)}, \tag{6.2.2}$$

for a fixed prime $p \neq 2$. Jetchev [J, Thm. 1.1] proved, under suitable assumptions, a sharpening of (6.2.2) in the following form:

$$\text{if } y_K \notin E(K)_{\mathrm{tors}}, \text{ then } \quad \forall \ell \mid N \quad [E(K) : \mathbf{Z}y_K]/((\#Ш(E/K))^{1/2} c_{\mathrm{Tam},\ell}(E/\mathbf{Q})) \in \mathbf{Z}_{(p)}, \tag{6.2.3}$$

in line with (6.2.1).

**(6.3)** The simplest case of the expected divisibility (6.2.2) is the following statement:

$$\text{if } y_K \notin pE(K) + E(K)_{\mathrm{tors}}, \text{ then } E(K) \otimes \mathbf{Z}_p = \mathbf{Z}_p(y_K \otimes 1) \simeq \mathbf{Z}_p \text{ and } Ш(E/K)[p^\infty] = 0 \tag{6.3.1}$$

(if $E(K)[p] = 0$, then $pE(K) + E(K)_{\mathrm{tors}} = pE(K)$). As recalled in §0.3-§0.4, (6.3.1) was deduced by Kolyvagin [K1] from his more general annihilation result [K1, Cor. 13] under the assumption that $p \neq 2$, $u_K = 1$ and $\rho := \overline{\rho}_{E,p} : G_{\mathbf{Q}} \longrightarrow \mathrm{Aut}_{\mathbf{F}_p}(E[p]) \simeq GL_2(\mathbf{F}_p)$ has "large image".

A more direct exposition of Kolyvagin's proof of (6.3.1) in the case when $p \nmid 2D_K$ and $\rho$ is surjective was given by Gross [G, Proposition 2.1, Proposition 2.3]. It turns out that the arguments in [G] are valid under weaker assumptions, as we are now going to explain. We begin by extracting from [G] the conditions on $E$, $K$ and $p$ used in the proof. After that we show that only one of them (an irreducibility assumption) really matters.

**(6.4) Proposition ([G, Prop. 2.1, Prop. 2.3 and its proof].** *If $p \neq 2$ is a prime number and if the conditions (C1)–(C6) below are satisfied, then the implication (6.3.1) holds.*
*(C1) $u_K = 1$ (i.e., $D_K \neq -3, -4$).*
*(C2) For each $n \geq 1$ relatively prime to $pND_K$, $E(H_n)[p] = 0$.*
*(C3) $E(\mathbf{Q})[p] = 0$.*
*(C4) For $i = 1, 2$, $\quad H^i(K(E[p])/K, E[p]) = 0$.*
*(C5) The restriction of $\rho = \overline{\rho}_{E,p}$ to $G_K$ is absolutely irreducible.*
*(C6) Neither of the two subgroups $E[p]^\pm \subset E[p]$ (:= the $(\pm1)$-eigenspaces for the action of complex conjugation) contains a non-zero $G_K$-stable subgroup (equivalently, $\rho$ is irreducible).*

*Proof.* The conditions (C1) and (C2) are used in [G, §3-§5] in order to construct Kolyvagin's derivative classes and establish their basic properties, and (C3) is needed in the proof of [G, Prop. 6.2(1)] for $v \mid N$. In the general discussion in [G, §7-§8], no additional conditions are needed. Things begin to get more interesting in [G, §9]. The condition (C4) implies the statement of [G, Prop. 9.1] (the proof of which relied on the assumption that $p \nmid D_K$; this was not stated explicitly in [G, Prop. 2.1, Prop. 2.3]). The irreducibility conditions (C5) and (C6) are used, respectively, in the proofs of [G, Prop. 9.3] and [G, Prop. 9.5(2)] (note that the proof of [G, Prop. 9.3] relies on the fact that $\mathrm{End}_{\mathbf{F}_p[G_K]}(E[p]) = \mathbf{F}_p$). The rest of the proof in [G, §9-§10] goes through unchanged.

**(6.5) Proposition.** *For any prime number $p \neq 2$, the conditions (C2), (C3), (C4) and (C6) in Proposition 6.4 follow from (C5). Therefore the implication (6.3.1) holds if $p \neq 2$, $D_K \neq -3, -4$ and $E[p]$ is an absolutely irreducible $\mathbf{F}_p[G_K]$-module (the latter condition implies that $E(K)[p] = 0$).*

*Proof.* The implication (C5) $\Longrightarrow$ (C6) is straightforward, and (C3) follows from (C6) and the fact that $\dim_{\mathbf{F}_p} E(\mathbf{Q})[p] \leq 1$. The implication (C5) $\Longrightarrow$ (C2) is a special case of Proposition 5.31(8). Finally, (C4) follows from Sah's Lemma (5.5.2) and the fact that $\rho(G_K) \subset GL_2(\mathbf{F}_p)$ contains a non-trivial homothety (by Proposition 5.15, since $\#\det(\rho(G_K)) = \#\chi_{p,K}(G_K) > 2$ for $p > 3$).

**(6.6)** We are now ready to reprove (and slightly extend) the refinement of Kolyvagin's result on (6.3.1) established by Cha [Ch, the case $m = 0$ of Thm. 21].

**(6.7) Theorem.** *Assume that $p \neq 2$ and that $E[p]$ is an irreducible $\mathbf{F}_p[G_{\mathbf{Q}}]$-module (which implies that $E(K)[p] = 0$).*
*(1) Assume that $(K,p) \neq (\mathbf{Q}(\sqrt{-3}), 3)$. If $y_K \notin pE(K)$, then*

$$E(K) \otimes \mathbf{Z}_p = \mathbf{Z}_p(y_K \otimes 1) \simeq \mathbf{Z}_p, \qquad Ш(E/K)[p^\infty] = 0.$$

*(2) Assume that $(K,p) = (\mathbf{Q}(\sqrt{-3}), 3)$; then $y_K \in 3E(K)$. If $3 \nmid a_3$, assume, in addition, that $\rho(G_K)$ is not a cyclic group of order four. If $y_K \notin 3^2E(K)$, then*

$$\mathbf{Z}_3 \simeq E(K) \otimes \mathbf{Z}_3 \supset 3E(K) \otimes \mathbf{Z}_3 = \mathbf{Z}_3(y_K \otimes 1), \qquad Ш(E/K)[3^\infty] = 0.$$

*Proof.* According to Proposition 5.26, the assumptions imply that $E[p]$ is an absolutely irreducible $\mathbf{F}_p[G_K]$-module. If $u_K = 1$, the statement follows from Proposition 6.5. It remains to consider the two fields $K = \mathbf{Q}(i)$ and $K = \mathbf{Q}(\sqrt{-3})$, when $u_K = 2$ and $u_K = 3$, respectively. We distinguish two separate cases.
**Case 1:** $p \nmid u_K$ (equivalently, either $K = \mathbf{Q}(i)$ and $p > 2$, or $K = \mathbf{Q}(\sqrt{-3})$ and $p > 3$).
We modify the constructions in [G] as follows. For any square-free integer $n$ we let $H'_n$ to be the compositum inside $H_n$ of the ring class fields $H_\ell$, where $\ell$ runs through all prime numbers dividing $n$. The Galois group $G_n := \mathrm{Gal}(H'_n/H_1)$ is then canonically isomorphic to $\prod_{\ell|n} G_\ell$, where $G_\ell = \mathrm{Gal}(H_\ell/H_1)$ is a cyclic group of order $\#(G_\ell) = (\ell - \eta_K(\ell))/u_K$. If, in addition, $(n,N) = 1$, we define $y_n := \mathrm{Tr}_{H_n/H'_n}(\varphi(x_n)) \in E(H'_n)$.

One considers only square-free products $n$ of Kolyvagin primes $\ell$ satisfying [G, (3.1)-(3.2)]. For each such an $\ell$ fix a generator $\sigma_\ell \in G_\ell$ and define $D_n := \prod_{\ell|n} D_\ell \in \mathbf{Z}[G_n]$, where each $D_\ell$ is defined as in [G, §3], except that $\ell + 1$ is replaced by $\#(G_\ell) = (\ell+1)/u_K$. The norm relation [G, 3.7(1)] is replaced by $u_K \mathrm{Tr}_\ell(y_{\ell m}) = a_\ell \cdot y_m$ (which implies that [G, 3.6] still holds, since $p \nmid u_K$); the congruence relation [G, 3.7(2)] does not change.

The points $P_n \in E(H'_n)$ are defined as in [G, (4.1)], except that we replace $H_n$ (denoted by $K_n$ in [G]) by $H'_n$. The vanishing statement $E(H_n)[p] = 0$ of [G, 4.3] (i.e., (C2) in Proposition 6.4) still holds, by Proposition 6.5.

Kolyvagin's classes $c(n) \in H^1(K, E[p])$ are then defined by $\mathrm{res}_{H'_n/K}(c(n)) = \delta_n[P_n] \in H^1(H'_n, E[p])$ (hence $c(1) = \delta y_K$). These classes (and their images $d(n) \in H^1(K,E)[p]$) have all the properties listed in [G, §6-§7] (except that $H_n$ needs to be replaced by $H'_n$). In the formula [G, p. 246, l. 2] one needs to replace $Q_n$ by $u_K Q_n$, but this is harmless for the argument proving the key statement [G, 6.2(2)], since $p \nmid u_K$.

The rest of the proof goes through as in the situation considered in Proposition 6.4.
**Case 2:** $p \mid u_K$ (equivalently, $K = \mathbf{Q}(\sqrt{-3})$ and $p = u_K = 3$).
According to Proposition 4.14(1), there exist infinitely many primes $q \nmid 3N$ satisfying $3 \nmid (q + 1 - a_q)$ (which is equivalent to $3 \nmid (\eta_K(q) + 1 - a_q)$); fix once for all such a prime $q$.

Consider square-free products $n$ of primes $\ell \nmid 3Nq$ satisfying Kolyvagin's condition [G, (3.2)] (which implies that $\eta_K(\ell) = -1$, by [G, (3.3)]). For each such $n$ we consider the point $y_n := \varphi(x_{qn}) \in E(H_{qn})$. The Galois group $G_n := \mathrm{Gal}(H_{qn}/H_q)$ is canonically isomorphic to $\prod_{\ell|n} G_\ell$, and each $G_\ell$ is cyclic of order $\ell+1$. We define $D_n$ and $\mathrm{Tr}_\ell$ as in [G, §3]. The statements of [G, 3.6-3.7] and the definition of $P_n$ in [G, (4.1)] are unchanged, except that each $H_n$ (denoted by $K_n$ in [G]) needs to be replaced by $H_{qn}$ (so that $P_n \in E(H_{qn})$). One obtains again classes $c(n) \in H^1(K, E[p])$ and $d(n) \in H^1(K,E)[p])$, with $c(1) = \delta y_{K,q}$. They have all the properties listed in [G, §6-§7], except that $H_n$ needs to be replaced by $H_{qn}$.

The rest of the proof goes through as in the situation considered in Proposition 6.4, except that $y_K$ in [G, §9-§10] needs to be replaced by $y_{K,q}$, and $P_\ell \in H_\ell$ in [G, §10] by $P_\ell \in H_{q\ell}$. The conclusion is that $\mathrm{Sel}_3(E/K) = (\mathbf{Z}/3\mathbf{Z}) \cdot \delta y_{K,q}$, which is equivalent to $Ш(E/K)[3^\infty] = 0$ and $E(K) \otimes \mathbf{Z}_3 = \mathbf{Z}_3(y_{K,q} \otimes 1) \simeq \mathbf{Z}_3$, since $E(K)[3] = 0$. In particular, $E(K) \otimes \mathbf{Z}_3 = E(K)_{HP} \otimes \mathbf{Z}_3 \simeq \mathbf{Z}_3$, which implies that $\mathbf{Z}_3(y_K \otimes 1) = 3E(K) \otimes \mathbf{Z}_3$, by Proposition 4.14(4).

**(6.8)** Combining Theorem 6.7 with Theorems 4.9 and 4.17, respectively, we obtain the following results.

**(6.9) Theorem.** *Assume that $p \neq 2$, $E[p]$ is an irreducible $\mathbf{F}_p[G_{\mathbf{Q}}]$-module and $p \nmid N \cdot a_p \cdot (a_p - 1) \cdot (a_p - \eta_K(p)) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$. If $y_K \notin pE(K)$, then the conclusions of Theorem 4.9 hold.*

**(6.10) Theorem.** *Assume that $K = \mathbf{Q}(\sqrt{-3})$, $p = 3$, $E[3]$ is an irreducible $\mathbf{F}_3[G_{\mathbf{Q}}]$-module, $\rho(G_K)$ is not a cyclic group of order four and $3 \nmid a_3 \cdot (a_3 - 1) \cdot c_{\mathrm{Tam}}(E/\mathbf{Q})$. If $y_K \notin 3^2E(K)$, then the conclusions of*

*Theorem 4.17 hold, with the following modification: each $E(K_n) \otimes \mathbf{Z}_3$ is generated over $\mathbf{Z}_3[\mathrm{Gal}(K_n/K)]$ by the traces to $K_\infty$ of the Heegner points of conductors dividing $3^\infty q$, for any prime $q$ as in 0.23.*

## References


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

[BK] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, in: The Grothendieck Festschrift I, Progress in Mathematics **86**, Birkhäuser, Boston, Basel, Berlin, 1990, pp. 333–400.

[Ch] B. Cha, *Vanishing of some cohomology groups and bounds for the Shafarevich–Tate groups of elliptic curves*, J. of Number Theory **111** (2005), 154–178.

[CS1] M. Çiperiani, J. Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups I: The Bashmakov problem for elliptic curves over* $\mathbf{Q}$, Comp. Math. **149** (2013), 729–753.

[CS2] M. Çiperiani, J. Stix, *Weil-Châtelet divisible elements in Tate-Shafarevich groups II: On a question of Cassels*, J. reine angew. Math. **700** (2015), 175–207.

[Co1] C. Cornut, *Reduction de Familles de points CM*, thesis, 2000.

[Co2] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495–523.

[Di] L.E. Dickson, *Linear groups: With an exposition of the Galois field theory*, Dover, New York, 1958.

[FD] B. Farb, R.K. Dennis, *Noncommutative Algebra*, Graduate Texts in Math. **144**, Springer, Berlin, 1993.

[FoPR] J.-M. Fontaine, B. Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L*, in: Motives (Seattle, 1991), Proc. Symp. in Pure Math. **55/I**, American Math. Society, Providence, Rhode Island, 1994, pp. 599–706.

[GJPST] G. Grigorov, A. Jorza, S. Patrikis, W.A. Stein, C. Tarnita, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Math. of Comp. **78** (2009), No. 268, 2397–2425.

[G] B.H. Gross, *Kolyvagin's work on modular elliptic curves*, in: $L$-functions and arithmetic (Durham, 1989; J. Coates, M.J. Taylor, eds.), LMS Lect. Note Ser. **153**, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

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

[Gu] R.M. Guralnick, *Small representations are completely reducible*, J. of Algebra **220** (1999), 531–541.

[H1] B. Howard, *The Heegner point Kolyvagin system*, Comp. Math. **140** (2004), 1439–1472.

[J] D. Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Comp. Math. **144** (2008), 811–826.

[K1] V. A. Kolyvagin, *Euler systems*, in: The Grothendieck Festschrift, vol. II, Progress in Math. **87**, Birkhäuser, Boston, Basel, Berlin, 1990, pp. 435–483.

[K2] V. A. Kolyvagin, *On the structure of Shafarevich–Tate groups*, in: Proc. USA–USSR Symposium on Algebraic Geometry, Chicago, 1989, Lect. Notes in Math. **1479**, Springer, Berlin, 1991, pp. 94–121.

[LW] T. Lawson, C. Wuthrich, *Vanishing of some Galois cohomology groups for elliptic curves*, in: Elliptic curves, modular forms and Iwasawa theory (in honour of John H. Coates' 70th birthday, Cambridge 2015; eds. D. Loeffler, S.L. Zerbes), Springer Proc. in Math. and Stat. **188**, Springer, 2016, pp. 373–399.

[Ma] A. Matar, *Selmer groups and Anticyclotomic $\mathbf{Z}_p$-extensions*, Math. Proc. Camb. Phil. Soc. **161** (2016), 409–433.

[Mz] B. Mazur, *Modular curves and arithmetic*, in: Proc. ICM 1983 (Warsaw), Vol. 1, PWN, Warsaw, 1984, pp. 185–211.

[N1] J. Nekovář, *On the parity of Selmer groups II*, C. R. Acad. Sci. Paris, Sér. I Math. **332** (2001), no. 2, 99–104.

[N2] J. Nekovář, *Selmer complexes*, Astérisque **310** (2006), Soc. Math. de France, Paris.

[N3] J. Nekovář, *The Euler system method for CM points on Shimura curves*, in: $L$-functions and Galois representations (Durham, July 2004), LMS Lect. Note Ser. **320**, Cambridge Univ. Press, 2007, pp. 471–547.

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

[Sa] C.-H. Sah, *Automorphisms of finite groups*, J. of Algebra **10** (1968), 47–68.

[S1] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[S2] J.-P. Serre, *Sur la semisimplicité des produits tensoriels de représentations de groupes*, Invent. Math. **116** (1994), 513–530.

[Va] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), 549–566.

[Z] S.-W. Zhang, *Gross–Zagier formula for $GL_2$*, Asian J. Math. **5** (2001), 183–290.

Ahmed Matar, Department of Mathematics, University of Bahrain, P.O. Box 32038, Sukhair, Bahrain

Jan Nekovář, Sorbonne Université, Campus Pierre et Marie Curie, Institut de Mathématiques de Jussieu, Théorie des Nombres, Case 247, 4 place Jussieu, 75252 Paris cedex 05, France