SOLVABLE POINTS ON GENUS ONE CURVES

MIRELA ÇIPERIANI and ANDREW WILES

Abstract

A genus one curve defined over $\mathbb{Q}$ which has points over $\mathbb{Q}_p$ for all primes p may not have a rational point. It is natural to study the classes of $\mathbb{Q}$-extensions over which all such curves obtain a global point. In this article, we show that every such genus one curve with semistable Jacobian has a point defined over a solvable extension of $\mathbb{Q}$.

Contents

0. Introduction

One of the great discoveries of the nineteenth century is that equations of degree 5 or more need not be solvable. To put this another way, such an equation need not have

DUKE MATHEMATICAL JOURNAL
Vol. 142, No. 3, © 2008 DOI 10.1215/00127094-2008-010
Received 15 May 2006. Revision received 18 July 2007.
2000 *Mathematics Subject Classification*. Primary 14G05; Secondary 14H45, 14H52, 11R34, 11R23.
Wiles's work supported in part by a National Science Foundation grant and the Clay Mathematics Institute.

roots in a solvable extension of the field of coefficients. One can ask the same question about polynomials in two variables.

Let X denote a smooth geometrically irreducible projective curve of genus g defined over a field F. Pál [P] has proved that every curve X of genus g has a point defined over some solvable extension of the base field F for each $g \in \{0, 2, 3, 4\}$. This makes one wonder if there are any curves where this does not hold. This is also addressed in Pál's article [P], where he constructs curves that have no solvable points. Pál is able to construct a curve with this property for every genus g either greater than or equal to 40 or $g \in \{6, 8, 10, 11, 15, 16, 20, 21, 22, 25, 26, 27, 28, 29, 30, 31, 32, 34, 35, 36, 37, 38\}$. These curves are defined over local fields F such that the absolute Galois group of the residue field of F has quotients isomorphic to S_5, $PSL_3(\mathbb{F}_2)$, and $PSL_3(\mathbb{F}_3)$. This condition does not hold for completions of number fields. Therefore, the question of whether a curve X of genus g defined over a number field has solvable points remains open for all $g \notin \{0, 2, 3, 4\}$.

We are interested in studying the case of genus one curves defined over the rational numbers. A curve C of genus one defined over $\mathbb{Q}$ has a Jacobian, $E = \operatorname{Jac} C$, also defined over $\mathbb{Q}$. The L-series of the Jacobian of C, which we also write $L(E, s)$, has analytic continuation to the whole complex plane by the theorems of [Wi] extended by [BCDT]. This is a consequence of E being modular, that is, covered by the modular curve by a finite map $\pi : X_0(N) \to E$ for some positive integer N. The minimal such N is called the conductor of E. Here $L(E, s)$ is defined as an Euler product

$$\prod_{p|N}(1 - a_p p^{-s})^{-1} \cdot \prod_{p\nmid N}(1 - a_p p^{-s} + p^{1-2s})^{-1},$$

where $a_p = 1 + p - \#E(\mathbb{F}_p)$ for $p \nmid N$ and $a_p = -1, +1,$ or 0 for $p|N$. The precise values of a_p are given in [S1, §2.4], and $L(E, s)$ is then equal to the L-series of a new form of level N.

In §1, we prove the following theorem.

THEOREM 0.0.1
Suppose that
(a) $L(E, s)$ *has a zero of order* 0 *or* 1 *at* $s = 1$; *and*
(b) $C(\mathbb{Q}_p) \neq \emptyset$ *for all* p.
Then C *has a point over a solvable extension of* $\mathbb{Q}$.

We note that while our method allows us to put some local restrictions on the extension, for example, that it is unramified at a given finite set of primes not dividing N, it does not allow us to pick an extension that is totally real. Such a condition would perhaps be useful in possible applications to base change (see [T]) if such results extended to cover higher genus. The reason that we are unable to make points over totally real fields is that we use the system of Heegner points on $X_0(N)$, and these are defined over abelian extensions of imaginary quadratic fields, and thus not usually over totally real fields. However, the method does suggest that such a result can be true since conjectures of Darmon [D] lead one to suppose the existence of similar systems of points on elliptic curves defined over abelian extensions of real quadratic fields.

We now give a brief idea of the proof of Theorem 0.0.1. The curves C of genus one satisfying condition Theorem 0.0.1(a) and $\operatorname{Jac} C = E$ are classified by $Ш = Ш(E/\mathbb{Q})$, the Tate-Shafarevich group of E. The principal homogeneous space C has a point over a solvable extension if and only if the corresponding class in Ш splits over a solvable extension. As Ш is a torsion group, it is therefore enough to prove that all classes of p-power order have this property for each prime p. Moreover, under condition (a) of Theorem 0.0.1, Kolyvagin has shown that this group is finite. Its p^n-torsion fits into the exact sequence

$$0 \longrightarrow E(\mathbb{Q})/p^n E(\mathbb{Q}) \xrightarrow{\phi} H^1_{\mathrm{Sel}}(\overline{\mathbb{Q}}/\mathbb{Q}, E_{p^n}) \longrightarrow Ш_{p^n} \longrightarrow 0,$$

where the central term is the Selmer group, which is defined as a subgroup of classes c of $H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E_{p^n})$ satisfying

$$H^1_{\mathrm{Sel}}(\overline{\mathbb{Q}}/\mathbb{Q}, E_{p^n}) = \left\{ c \in H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E_{p^n}) : c_\ell \in \operatorname{im}\phi_\ell,\ \forall\, \ell \right\}.$$

Here ϕ_ℓ is the local connecting homomorphism $E(\mathbb{Q}_\ell)/p^n E(\mathbb{Q}_\ell) \to H^1(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell, E_{p^n})$. In terms of $H^1_{\mathrm{Sel}}(\overline{\mathbb{Q}}/\mathbb{Q}, E_{p^n})$, we need only show that the restriction of this group is in the image of ϕ after a solvable extension.

Kolyvagin [Ko1] has given a construction of ramified classes in $H^1(\overline{\mathbb{Q}}/\mathbb{Q}, E_{p^n})$. These classes split (i.e., appear in the image of ϕ) over some solvable extension. Our main argument is the development of the principle described in [Wi, Introduction], that if one can construct enough ramified classes, then the unramified classes are already contained in the group generated by those ramified classes.

Neither condition (a) nor (b) of Theorem 0.0.1 seems to be essential. In §2, we remove condition (a) of Theorem 0.0.1 to obtain the main result of this article, Theorem 0.0.2.

THEOREM 0.0.2
Let C *be a curve of genus one defined over* $\mathbb{Q}$ *so that*
(a) $E = \operatorname{Jac} C$ *is semistable; and*
(b) $C(\mathbb{Q}_p) \neq \emptyset$ *for all* p.
Then C *has a point over a solvable extension of* $\mathbb{Q}$.

The proof of Theorem 0.0.2 is also based on the principle that is described above, but its statement as well as its application become more complicated if condition (a) of Theorem 0.0.1 does not hold. It is for this reason that we have chosen to dedicate §1 to the proof of Theorem 0.0.1. There are two new issues that appear in the case when $L(\mathrm{E}, s)$ has a zero of order greater than 1 at $s = 1$:

(i) the Heegner point that we can construct in E(K) for some imaginary quadratic field K is always a torsion point; and

(ii) the Tate-Shafarevich group is not known to be finite.

The first issue is overcome by constructing points defined over a sequence of extensions of K and using results that guarantee that we eventually construct a point that is not torsion. More precisely, we consider the anticyclotomic $\mathbb{Z}_p$-extension of K, and we construct Heegner points $\alpha_n \in \mathrm{E}(\mathrm{K}_n)$ (defined in §2.3), where $\mathrm{Gal}(\mathrm{K}_n/\mathrm{K}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Cornut [C] and Vatsal [V] have both shown that there exists an n such that α_n is of infinite order. In order to use the points α_n, we need to consider $\mathrm{H}^1(\overline{\mathrm{K}_n}/\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, where m_n is an integer greater than n instead of the group $\mathrm{H}^1(\overline{\mathrm{K}}/\mathrm{K}, \mathrm{E}_{p^n})$, which is what we use when we assume that condition (a) of Theorem 0.0.1 holds. This passage solves one problem and creates another. We can now construct nontrivial cohomology classes in $\mathrm{H}^1(\overline{\mathrm{K}_n}/\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, assuming that n is big enough, but we can certainly not ensure that we have constructed the whole Selmer group $\mathrm{H}^1_{\mathrm{Sel}}(\overline{\mathrm{K}_n}/\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$.

In attempting to resolve this new issue, we treat $\mathrm{H}^1(\overline{\mathrm{K}_n}/\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ as a module over the ring $(\mathbb{Z}/p^{m_n}\mathbb{Z})[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})]$. At this stage, the situation appears even more complicated because we do not really understand the structure of this new module that we choose to consider. In addition, the issue that the Tate-Shafarevich group is not known to be finite is still present. All these problems are fixed by an idea that is similar to one described in [Wi] and [TW]. We consider some carefully chosen submodules of $\mathrm{H}^1(\overline{\mathrm{K}_n}/\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ containing $\mathrm{H}^1_{\mathrm{Sel}}(\overline{\mathrm{K}_n}/\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ which vary depending on n, and we allow n to grow. We now have an infinite sequence of modules out of which we choose a subsequence of modules that are compatible with each other when treated as abstract $(\mathbb{Z}/p^{m_n}\mathbb{Z})[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})]$-modules. This allows us to formally put them together into a module $\mathscr{M}$ over the ring

$$\varprojlim_n (\mathbb{Z}/p^{m_n}\mathbb{Z})[\mathrm{Gal}(\mathrm{K}_n/\mathrm{K})].$$

We can now hope to overcome the second issue (ii) because the module $\mathscr{M}$ contains $\mathrm{H}^1_{\mathrm{Sel}}(\overline{\mathrm{K}}/\mathrm{K}, \mathrm{E}_{p^\infty})$. Our construction ensures that $\mathscr{M}$ has a very nice structure, which makes it possible for us to generalize the principle that is described above and used in proving Theorem 0.0.1.

The last step of the proof involves making sure that we are able to construct the ramified classes that are needed in order to apply our generalized principle. As we have already mentioned, Kolyvagin's construction of ramified classes in [Ko1, §1] uses rational primes. If the primes are chosen to construct ramified classes in $\mathrm{H}^1(\overline{\mathrm{K}_n}/\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, one cannot construct anything new in $\mathrm{H}^1(\overline{\mathrm{K}}_{n+1}/\mathrm{K}_{n+1}, \mathrm{E}_{p^{m_{n+1}}})$ using the same primes. So, we are forced to choose new primes for every level n. This is the reason why the submodules of $H^1(\overline{K_n}/K_n, E_{p^{m_n}})$ which we consider cannot be chosen in a naturally compatible way. In addition, the fact that the cohomology classes that we construct ramify at primes that change depending on n makes it harder to see if these classes become nontrivial as n grows. In order to bypass this difficulty, we keep track of what we are constructing in a way that does not depend on the specific prime where the class is ramified but only on the Frobenius of this prime. This cannot be done for all the ramified classes that we construct, but the information that we manage to extract allows us to complete our argument without actually constructing the whole module $\mathscr{M}$.

Because the proof in the general case is rather intricate, we have decided to present the case of rank at most 1 separately in §1. Although this incurs some repetition, and although many of the results in §1 are well known or can be proved more quickly by citing results from the literature, we believe that a detailed exposition of our approach in this much simpler case makes the reading of §2 much easier. In particular, both Kolyvagin [Ko3] and McCallum [M] have shown that the subgroup of $H^1(\overline{K}/K, E)$ generated by Kolyvagin's classes contains the Tate-Shafarevich group in the case when the analytic rank of E/K is 1. This result is equivalent to the statement of Theorem 0.0.1. McCallum's account, which is based on Kolyvagin's original approach, cannot be generalized to the higher-rank case because it uses the nondegeneracy of the Cassels pairing which in turn depends on the finiteness of the Tate-Shafarevich group. Kolyvagin [Ko2] has also considered the higher-rank case and has proved similar partial results assuming that at least one of the classes that he constructs in $H^1(\overline{K}/K, E)$ is nontrivial. This assumption remains a conjecture in the case when the analytic rank of $E/\mathbb{Q}$ is greater than one.

In a sequel to this article, we hope to remove the hypotheses of Theorem 0.0.2, at least if E has nonintegral j-invariant.

Notation. In the article, we frequently write $\varinjlim$ (resp., $\varprojlim$) for $\varinjlim_n$ (resp., $\varprojlim_n$) as all our limits are taken over n.

1. Rank at most 1

1.1. Unramified under ramified principle

Let E be an elliptic curve over $\mathbb{Q}$. Associated to E is its L-series $L(E, s)$. We call the order of its vanishing at $s = 1$ the *analytic rank* of E over $\mathbb{Q}$. A similar definition applies to a number field F other than $\mathbb{Q}$ for which the L-series $L(E/F, s)$ of the curve over F has analytic continuation. In particular, this applies to abelian extensions of $\mathbb{Q}$. We assume throughout §1 that E has analytic rank over $\mathbb{Q}$ equal to zero or 1. By a theorem proved independently by [BFH, Introduction, Theorem] and

[MM, Corollary to Theorem 2], the work of Waldspurger [W] in the case when the analytic rank of $E/\mathbb{Q}$ is 1, we can find an imaginary quadratic field K with discriminant $D_K \neq -3, -4$ so that

(i) the analytic rank of E over K is 1; and

(ii) every prime dividing N, the conductor of E, splits in K.

From the fundamental work of Gross and Zagier [GZ, §1.6], it follows that the Heegner point, which we review in §1.2, yields a point of infinite order over K. Kolyvagin [Ko1, Corollary C] has shown that, in addition, E(K) has rank 1 and $Ш = Ш(E/K)$ is finite.

It is enough to prove Theorem 0.0.1 for genus one curves C that correspond to elements of p-power order in $Ш(E/\mathbb{Q})$, where p is a prime. Hence, fix a prime p from now on. We also assume throughout the article that $\mathrm{Gal}(K(E_p)/K)$ is not solvable since the restriction of $H^1_{\mathrm{Sel}}(\overline{\mathbb{Q}}/\mathbb{Q}, E_{p^n})$ splits over an abelian extension of $\mathbb{Q}(E_{p^n})$, and $\mathrm{Gal}(\mathbb{Q}(E_{p^n})/\mathbb{Q})$ is solvable if and only if $\mathrm{Gal}(K(E_p)/K)$ is solvable. In particular, we assume for the rest of the article that $p > 3$ and $E(K)_p = 0$. It is then known that the natural image of this Galois group in $\mathrm{PGL}_2(\mathbb{F}_p)$ is either the full group or isomorphic to A_5 (see [S2, Proposition 16]). In §1, we give conditions on a set Q of auxiliary primes so that for k sufficiently large, $H^1_{\mathrm{Sel}}(K, E_{p^k})$ is contained in the subgroup of $H^1(K, E_{p^k})$ generated by

(a) the image of E(K); and

(b) the classes that are Selmer outside Q and are ramified at a nonempty subset of primes in Q.

1.1.1

Let ν be a prime of K, and denote by K_ν, k_ν, and $\mathcal{O}_\nu$ the corresponding local field, residue field, and local ring of integers, respectively. Consider the group $E(K_\nu)/p^m E(K_\nu)$ for some $m \in \mathbb{N}$.

LEMMA 1.1.1

Let $\wp$ be a prime of K which divides p and $m \in \mathbb{N}$. Then we have

$$\#\big(E(K_\wp)/p^m\big) = \#E(K_\wp)_{p^m} \cdot \#\big(E^1(K_\wp)/p^m\big),$$

where $E^1(K_\wp)$ is the group of points of $E(K_\wp)$ which map to zero when E is reduced modulo p.

Proof

Let G be an abelian group, and set

$$\chi_{p^m}(G) := \#G_{p^m}/\#(G/p^m G).$$

It is known that χ_{p^m} is multiplicative on short exact sequences and trivial on finite groups.

Since $\mathrm{E}(\mathrm{K}_\wp)$ is an extension of a finite group by $\mathrm{E}^1(\mathrm{K}_\wp)$, we have

$$\chi_{p^m}\big(\mathrm{E}(\mathrm{K}_\wp)\big) = \chi_{p^m}\big(\mathrm{E}^1(\mathrm{K}_\wp)\big).$$

Then the fact that $\mathrm{E}^1(\mathrm{K}_\wp)_{p^m} = 0$ implies that

$$\#\big(\mathrm{E}(\mathrm{K}_\wp)/p^m\big) = \#\mathrm{E}(\mathrm{K}_\wp)_{p^m} \cdot \#\big(\mathrm{E}^1(\mathrm{K}_\wp)/p^m\big). \qquad \square$$

In the next lemma, we prove a similar result for the other primes.

LEMMA 1.1.2
Let ν be a prime of K *relatively prime to* p *and* $m \in \mathbb{N}$ *so that* $\mathrm{E}(\mathrm{K}_\nu)_{p^\infty} = \mathrm{E}(\mathrm{K}_\nu)_{p^m}$. *Then the inclusion of* $\mathrm{E}(\mathrm{K}_\nu)_{p^m}$ *in* $\mathrm{E}(\mathrm{K}_\nu)$ *gives rise to the canonical isomorphism*

$$\mathrm{E}(\mathrm{K}_\nu)/p^m\mathrm{E}(\mathrm{K}_\nu) \simeq \mathrm{E}(\mathrm{K}_\nu)_{p^m}.$$

Proof
Since $\mathrm{E}(\mathrm{K}_\nu)_{p^\infty} = \mathrm{E}(\mathrm{K}_\nu)_{p^m}$, the inclusion of $\mathrm{E}(\mathrm{K}_\nu)_{p^m}$ into $\mathrm{E}(\mathrm{K}_\nu)/p^m\mathrm{E}(\mathrm{K}_\nu)$ is injective. So, in order to prove that these two groups are equal, we need only show that their sizes are equal. As in Lemma 1.1.1, we have

$$\chi_{p^m}\big(\mathrm{E}(\mathrm{K}_\nu)\big) = \chi_{p^m}\big(\mathrm{E}^1(\mathrm{K}_\nu)\big).$$

Since ν does not divide p, we know that $\mathrm{E}^1(\mathrm{K}_\nu)$ is a p-divisible group. This implies that $\chi_{p^m}(\mathrm{E}^1(\mathrm{K}_\nu)) = 1$. Hence, $\chi_{p^m}(\mathrm{E}(\mathrm{K}_\nu)) = 1$ and $\#(\mathrm{E}(\mathrm{K}_\nu)/p^m) = \#\mathrm{E}(\mathrm{K}_\nu)_{p^m}$, as required. $\square$

1.1.2
Let y be a generator of the free part of E(K). Denote by Σ the set of primes of K which divide p together with those where E has bad reduction. We choose $k \in \mathbb{N}$ so that

(1) p^{k-1} annihilates the p-primary part of $Ш = Ш(\mathrm{E}/\mathrm{K})$; and
(2) $\mathrm{E}(\mathrm{K}_\lambda)_{p^\infty} = \mathrm{E}(\mathrm{K}_\lambda)_{p^k}$ for all $\lambda \in \Sigma$.

Suppose that $\Sigma' = \Sigma \cup \{\lambda_0\}$, where $\lambda_0 \notin \Sigma$ is a prime of K such that $\mathrm{E}(\mathrm{K}_{\lambda_0})_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_{\lambda_0}})_{p^{2k}}$ and y is not divisible by p in $\mathrm{E}(\mathrm{K}_{\lambda_0})$.

Suppose that Q is a set of primes of $\mathbb{Q}$ with the following properties for $q \in \mathrm{Q}$:

(i) q remains inert in $\mathrm{K}/\mathbb{Q}$;
(ii) $q \notin \Sigma'$;
(iii) $\mathrm{E}(\mathrm{K}_q)_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_q})_{p^k}$; and

(iv) $H^1_{\mathrm{Sel}}(K, E_{p^k}) \hookrightarrow \prod_{q\in Q} H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k})$, where K_q^{unr} denotes the maximal unramified extension of K_q.

Denote by $K_{\Sigma'\cup Q}$ (resp., $K_{\Sigma'}$) the maximal extension of K which is unramified outside $\Sigma'\cup Q$ (resp., Σ'). Define

$$L_\nu = \begin{cases} H^1(K_\nu^{\mathrm{unr}}/K_\nu, E_{p^{2k}}), & \nu \in Q, \\ H^1(K_\nu, E_{p^{2k}}), & \nu \in \Sigma'. \end{cases}$$

Then we set

$$H^1{}_{L}(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) := \{s \in H^1(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) \mid s_\nu \in L_\nu \text{ for } \nu \in \Sigma'\cup Q\},$$
$$H^1{}_{L_Q}(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) := \{s \in H^1(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) \mid s_\nu \in L_\nu \text{ for } \nu \in \Sigma'\}.$$

Thus L_Q denotes that no local conditions are imposed at the primes of Q but that the same conditions are imposed on primes in Σ' as were imposed for L. Similarly, $H^1_{\mathrm{Sel}_Q}(K_{\Sigma'\cup Q}/K, E_{p^{2k}})$ denotes classes with the Selmer condition at primes of Σ' but no condition at the primes of Q.

Denote by L_ν^* the exact annihilator of L_ν in the nondegenerate pairing

$$H^1(K_\nu, E_{p^{2k}}) \times H^1(K_\nu, E_{p^{2k}}) \to \mathbb{Q}_p/\mathbb{Z}_p. \tag{1}$$

Then, as above, we have

$$H^1{}_{L^*}(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) = \{s \in H^1(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) \mid s_\nu \in L_\nu^* \text{ for } \nu \in \Sigma'\cup Q\}.$$

LEMMA 1.1.3
The group $H^1{}_{L^*}(K_{\Sigma'\cup Q}/K, E_{p^{2k}})$ *is contained in the Selmer group* $H^1_{\mathrm{Sel}}(K, E_{p^k})$.

Proof
By properties of local duality (see [Mi, Theorem 2.6]), we know that

$$L_\nu^* = \begin{cases} H^1(K_\nu^{\mathrm{unr}}/K_\nu, E_{p^{2k}}), & \nu \in Q, \\ 0, & \nu \in \Sigma'. \end{cases}$$

This implies that $H^1{}_{L^*}(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) \subset H^1_{\mathrm{Sel}}(K, E_{p^{2k}})$. Since $Ш_{p^{2k}} = Ш_{p^k}$ by assumption (1) in §1.1.2, we have an exact sequence

$$0 \longrightarrow H^1_{\mathrm{Sel}}(K, E_{p^k}) \longrightarrow H^1_{\mathrm{Sel}}(K, E_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^{2k}\mathbb{Z})(p^k y) \longrightarrow 0, \tag{2}$$

where $(\mathbb{Z}/p^{2k}\mathbb{Z})(p^k y)$ is the subgroup of $H^1_{\mathrm{Sel}}(K, E_{p^{2k}})$ generated by $p^k y$. We can easily see that all we need to prove is that

$$(\mathbb{Z}/p^{2k}\mathbb{Z})y \cap H^1{}_{L^*}(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) = 0.$$

Lemma 1.1.2 tells us that $\mathrm{E}(\mathrm{K}_{\lambda_0})/p^{2k}\mathrm{E}(\mathrm{K}_{\lambda_0}) = \mathrm{E}(\mathrm{K}_{\lambda_0})_{p^{2k}}$. This and the properties of λ_0 imply that in $\mathrm{E}(\mathrm{K}_{\lambda_0})$, we have

$$y = p^{2k}y' + e_{p^{2k}}, \qquad \text{where } y' \in \mathrm{E}(\mathrm{K}_{\lambda_0}) \text{ and } e_{p^{2k}} \in \mathrm{E}(\mathrm{K}_{\lambda_0})_{p^{2k}} - \mathrm{E}(\mathrm{K}_{\lambda_0})_{p^{2k-1}}.$$

Then $p^i y \in \mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}})$ only if $p^i y = p^{2k}y''$ for some $y'' \in \mathrm{E}(\mathrm{K}_{\lambda_0})$. Finally, the fact that $e_{p^{2k}} \in \mathrm{E}(\mathrm{K}_{\lambda_0})_{p^{2k}} - \mathrm{E}(\mathrm{K}_{\lambda_0})_{p^{2k-1}}$ allows us to conclude that $i \geq 2k$. This implies that

$$(\mathbb{Z}/p^{2k}\mathbb{Z})y \cap \mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) = 0$$

and concludes our proof. □

LEMMA 1.1.4
The group $\mathrm{H}^1{}_{\mathrm{L}^*_{\mathrm{Q}}}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}})$ *is isomorphic to* $\mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}})$ *under the natural inclusion map.*

Proof
The exactness of the sequence

$$0 \to \mathrm{H}^1{}_{\mathrm{L}^*_{\mathrm{Q}}}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q\in\mathrm{Q}} \mathrm{L}_q \tag{3}$$

implies that $\mathrm{H}^1{}_{\mathrm{L}^*_{\mathrm{Q}}}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \simeq \mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}})$ if and only if the map

$$\mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q\in\mathrm{Q}} \mathrm{L}_q \tag{4}$$

is zero.

Using Lemma 1.1.3, as well as the last property of the set Q, we get the commutative diagram

$$\begin{array}{ccccc}
\mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}) \\
 & \searrow & \uparrow & & \uparrow \\
 & & \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) & \hookrightarrow & \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k})
\end{array}$$

So, in order to prove that the map (4) is zero, it suffices to show that the right-hand-side vertical map is zero.

We know that $\mathrm{E}_{p^{2k}}(\overline{\mathrm{K}}_q) = \mathrm{E}_{p^{2k}}(\mathrm{K}_q^{\mathrm{unr}})$, and therefore, the exactness of

$$0 \longrightarrow \mathrm{E}_{p^k}(\mathrm{K}_q^{\mathrm{unr}}) \longrightarrow \mathrm{E}_{p^{2k}}(\mathrm{K}_q^{\mathrm{unr}}) \xrightarrow{p^k} \mathrm{E}_{p^k}(\mathrm{K}_q^{\mathrm{unr}}) \longrightarrow 0$$

implies the exactness of

$$
\begin{array}{l}
0 \longrightarrow E_{p^k}(K_q) \longrightarrow E_{p^{2k}}(K_q) \xrightarrow{p^k} E_{p^k}(K_q) \longrightarrow H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}) \longrightarrow H^1(K_q^{\mathrm{unr}}/K_q, E_{p^{2k}}) \\
\hfill \downarrow \\
\hfill H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}).
\end{array}
$$

The third property of the primes $q \in Q$ tells us that $E_{p^{2k}}(K_q) = E_{p^k}(K_q)$, and therefore, this reduces to the sequence

$$0 \longrightarrow E_{p^k}(K_q) \longrightarrow H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}) \longrightarrow H^1(K_q^{\mathrm{unr}}/K_q, E_{p^{2k}}) \longrightarrow H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}).$$

Since we also know that $H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}) \simeq E(K_q)/p^k E(K_q)$, Lemma 1.1.2 allows us to conclude that $H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}) \simeq E(K_q)_{p^k}$ and, therefore, that the map

$$H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}) \to H^1(K_q^{\mathrm{unr}}/K_q, E_{p^{2k}}) \text{ is zero for all } q \in Q. \tag{5}$$

This concludes the proof of the lemma. □

PROPOSITION 1.1.5
The following sequence is exact:

$$0 \longrightarrow H^1{}_{L}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longrightarrow H^1{}_{L_Q}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longrightarrow \prod_{q \in Q} H^1(K_q, E_{p^{2k}})/L_q \longrightarrow 0.$$

Proof
The only part of this sequence which is not obviously exact is the last map. So, we need only show that

$$H^1{}_{L_Q}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longrightarrow \prod_{q \in Q} H^1(K_q, E_{p^{2k}})/L_q \tag{6}$$

is surjective.

Consider the beginning of the exact sequence of Cassels, Poitou, and Tate (see [Mi, §1, Theorem 4.20]):

$$
\begin{array}{l}
0 \longrightarrow H^1{}_{L}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longrightarrow H^1{}_{L_Q}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longrightarrow \prod_{q \in Q} H^1(K_q, E_{p^{2k}})/L_q \\
\hfill \downarrow \psi \\
\hfill H^2(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longleftarrow H^1{}_{L^*}(K_{\Sigma' \cup Q}/K, \widehat{E_{p^{2k}}})
\end{array}
$$

where $\widehat{M} = \mathrm{Hom}(M, \mathbb{Q}_p/\mathbb{Z}_p)$. It follows that the map (6) is surjective if and only if $\psi = 0$, which is equivalent to the following map being zero:

$$H^1{}_{L^*}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \to \prod_{q \in Q} L_q.$$

This follows from Lemma 1.1.4 since $H^1{}_{L_Q^*}(K_{\Sigma' \cup Q}/K, E_{p^{2k}})$ is the kernel of the above map. □

Using the definition of the local conditions L_λ, we see that

$$H^1{}_{L}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) = H^1(K_{\Sigma'}/K, E_{p^{2k}}),$$
$$H^1{}_{L_Q}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) = H^1(K_{\Sigma' \cup Q}/K, E_{p^{2k}}).$$

Then Proposition 1.1.5 gives us the exact sequence

$$0 \longrightarrow H^1(K_{\Sigma'}/K, E_{p^{2k}}) \longrightarrow H^1(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longrightarrow \textstyle\prod_{q \in Q} H^1(K_q, E_{p^{2k}})/L_q \longrightarrow 0. \tag{7}$$

The second and third properties of the primes in Q together with Lemma 1.1.2 imply that for $q \in Q$,

$$L_q^* = L_q = H^1(K_q^{\mathrm{unr}}/K_q, E_{p^{2k}}) \simeq E(K_q)/p^{2k}E(K_q) \simeq E(K_q)_{p^k} \simeq \mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^k\mathbb{Z}.$$

Then using the nondegeneracy of the pairing (1), we conclude that

$$H^1(K_q, E_{p^{2k}})/L_q \simeq \mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^k\mathbb{Z}. \tag{8}$$

Moreover, one can understand the structure of the full group $H^1(K_q, E_{p^{2k}})$ by considering the sequence

$$0 \longrightarrow E(\overline{K}_q)_{p^k} \longrightarrow E(\overline{K}_q)_{p^{2k}} \xrightarrow{\times p^k} E(\overline{K}_q)_{p^k} \longrightarrow 0,$$

which gives rise to

$$0 \longrightarrow E(K_q)_{p^k} \longrightarrow H^1(K_q, E_{p^k}) \longrightarrow H^1(K_q, E_{p^{2k}})$$

as $E(K_q)_{p^k} = E(K_q)_{p^{2k}}$. By the above identifications, we can then deduce that

$$H^1(K_q, E)_{p^k} \simeq H^1(K_q, E_{p^k})/H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k}) \subseteq H^1(K_q, E_{p^{2k}}).$$

The groups $H^1(K_q, E)_{p^k} \subseteq H^1(K_q, E)_{p^{2k}}$ have the same size since their duals are isomorphic to $E(K_q)_{p^k}$ and $E(K_q)_{p^{2k}}$, respectively, by pairing (1). So, we have

$$H^1(K_q, E_{p^{2k}})/H^1(K_q^{\mathrm{unr}}/K_q, E_{p^{2k}}) \subseteq H^1(K_q, E_{p^{2k}}).$$

It is then clear that

$$\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}}) \simeq \big(\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}})\big) \oplus \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}).$$

We show that when we restrict the above cohomology groups to the Selmer condition for $\lambda \in \Sigma'$, we end up missing exactly one generator of $\prod_{q\in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q$.

PROPOSITION 1.1.6
The cokernel of the last map in the exact sequence

$$0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q$$

is cyclic of order p^k.

Proof
Recall our notation that Sel_Q imposes no local condition at primes in Q and the unramified one at the prime λ_0. Set $\mathrm{W} = \prod_{\lambda\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k})$, where $\mathrm{Sel}_\lambda(p^{2k})$ denotes the image of $\mathrm{E}(\mathrm{K}_\lambda)/p^{2k}\mathrm{E}(\mathrm{K}_\lambda)$ in $\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})$. Using the exact sequence (7), we now apply the snake lemma to the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{H}^1(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \mathrm{H}^1(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow & & \\
0 & \longrightarrow & \mathrm{W} & \longrightarrow & \mathrm{W} & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

We get

$$\begin{array}{ccccc}
0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q & \\
 & & & \downarrow & \\
0 \longleftarrow & \operatorname{coker}\phi_2 & \xleftarrow{\gamma_0} & \operatorname{coker}\phi_1 &
\end{array} \tag{9}$$

Seeing the maps ϕ_1 and ϕ_2 as part of the corresponding exact sequences of Cassels, Poitou, and Tate, we have

$$\begin{array}{ccccc}
\mathrm{H}^1(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \xrightarrow{\phi_1} & \prod_{\lambda\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_1} & \mathrm{H}^1_{\mathrm{Sel}^*}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})} \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \xrightarrow{\phi_2} & \prod_{\lambda\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_2} & \mathrm{H}^1_{(\mathrm{Sel}_\mathrm{Q})^*}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})}
\end{array} \tag{10}$$

Now, we need to study the maps ψ_i since $\operatorname{coker}\phi_i \simeq \operatorname{im}\psi_i$ for $i = 1, 2$.

We start by proving that $\mathrm{Sel}_\lambda(p^{2k}) = \mathrm{Sel}^*_\lambda(p^{2k})$ for $\lambda \in \Sigma$. We know that $\mathrm{Sel}_\lambda(p^{2k}) \supset \mathrm{Sel}^*_\lambda(p^{2k})$ for all λ (see [B, Proposition 9]). Since $\#\mathrm{E}(\overline{\mathrm{K}}_\lambda)_{p^{2k}} = p^{4k}$, a result of Tate about the local Euler-Poincaré characteristic (see [Mi, §1, Theorem 2.8]) implies that $\#\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}}) = [\mathcal{O}_\lambda : p^{4k}\mathcal{O}_\lambda] \cdot (\#\mathrm{E}(\mathrm{K}_\lambda)_{p^{2k}})^2$. We also know that $\mathrm{E}^1(\mathrm{K}_\wp) \simeq \mathcal{O}_\wp$ for $\wp | p$. Therefore, Lemmas 1.1.1 and 1.1.2 imply that $\#\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}}) = (\#\mathrm{Sel}_\lambda(p^{2k}))^2$. Finally, the nondegeneracy of pairing (1) implies that $\#\mathrm{Sel}_\lambda(p^{2k}) = \#\mathrm{Sel}^*_\lambda(p^{2k})$ for all $\lambda \in \Sigma$, which proves our claim.

Furthermore, since $\mathrm{Sel}_\lambda(p^{2k}) = \mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_\lambda/\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})$ for all $\lambda \notin \Sigma$ and, by [Mi, Theorem 2.6], $\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_\lambda/\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})$ is its own exact annihilator in pairing (1), we conclude that

$$\mathrm{Sel}_\lambda(p^{2k}) = \mathrm{Sel}^*_\lambda(p^{2k}) \quad \text{for all } \lambda.$$

Therefore, we have

$$\mathrm{H}^1_{\mathrm{Sel}^*}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \qquad \text{and} \qquad \mathrm{H}^1_{(\mathrm{Sel}_\mathrm{Q})^*}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}),$$

where $\mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ is the subgroup of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ consisting of classes that are locally trivial at primes in Q.

We know that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ maps to $\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_q/\mathrm{K}_q, \mathrm{E}_{p^k})$ under the localization map for $q \in \mathrm{Q}$. Then (5) implies that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ maps to zero in $\mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_q/\mathrm{K}_q, \mathrm{E}_{p^{2k}})$ for all $q \in \mathrm{Q}$, and therefore,

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \subset \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}).$$

We show that these two groups are equal. The fourth property of the set Q implies via Lemma 1.1.2 that there exists a prime $q_0 \in \mathrm{Q}$ such that $y \neq py'$ in $\mathrm{E}(\mathrm{K}_{q_0})$. Then $y = p^{2k}y' + e_{p^k}$, where $y' \in \mathrm{E}(\mathrm{K}_{q_0})$ and $e_{p^k} \in \mathrm{E}(\mathrm{K}_{q_0})_{p^k} - \mathrm{E}(\mathrm{K}_{q_0})_{p^{k-1}}$. We see that $p^i y \in \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ if and only if $i \geq k$, and therefore,

$$(\mathbb{Z}/p^{2k}\mathbb{Z})y \cap \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = (\mathbb{Z}/p^{2k}\mathbb{Z})p^k y,$$

which implies that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) = \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$, as in the proof of Lemma 1.1.3.

So, the right-hand-side square of (10) may be viewed as

$$\begin{array}{ccc} \prod_{\lambda \in \Sigma'} \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_1} & \mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})} \\ \big\downarrow & & \big\downarrow \\ \prod_{\lambda \in \Sigma'} \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_2} & \mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^k})} \end{array}$$

and the map $\gamma : \mathrm{im}\,\psi_1 \to \mathrm{im}\,\psi_2$ is simply the restriction of an element of $\mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})}$ to $\mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^k})}$. We are now going to show that $\ker\gamma \simeq \mathbb{Z}/p^k\mathbb{Z}$.

In order to improve our understanding of the maps ψ_1 and ψ_2, we consider the following compatible nondegenerate pairings for $\lambda \in \Sigma'$:

$$\begin{array}{ccccc} \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \times & \mathrm{Sel}_\lambda(p^{2k}) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p \\ \Big\downarrow{\scriptstyle \psi_1} & & \Big\uparrow{\scriptstyle \mathrm{Res}_\lambda} & & \\ \widehat{\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})} & \times & \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p \end{array}$$

where $\mathrm{Res}_\lambda : \mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})$.

We know that $p^k \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) = 0$, and consequently, the order of every element of $\operatorname{im} \psi_2$ divides p^k. We aim to construct an element $s \in \operatorname{im} \psi_1$ of order p^{2k} because then $p^k s \in \ker \gamma$ and has order p^k.

Consider $\mathrm{Res}_{\lambda_0}(y)$. We know that $\mathrm{Res}_{\lambda_0}(y)$ is of order p^{2k} because y is not divisible by p in $\mathrm{E}(\mathrm{K}_{\lambda_0})$, and $\mathrm{E}(\mathrm{K}_{\lambda_0})_{p^\infty} = \mathrm{E}_{p^{2k}}$. It follows that there exists an element $s_{\lambda_0} \in \mathrm{H}^1(\mathrm{K}_{\lambda_0}, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_{\lambda_0}(p^{2k})$ which pairs with $\mathrm{Res}_{\lambda_0}(y)$ to give a generator of $\mathbb{Z}/p^{2k}\mathbb{Z}$. This implies that $\psi_1(s_{\lambda_0})$ has order p^{2k}.

So, we have now shown that the kernel of the map γ contains an element of order p^k, namely, $p^k \psi_1(s_{\lambda_0})$. Since, by (2),

$$0 \longrightarrow \mathbb{Z}/p^k\mathbb{Z} \longrightarrow \widehat{\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})} \longrightarrow \widehat{\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})} \longrightarrow 0, \qquad (11)$$

we conclude that $\ker \gamma \simeq \mathbb{Z}/p^k\mathbb{Z}$, which also shows that $\ker \gamma_0 \simeq \mathbb{Z}/p^k\mathbb{Z}$ in (9), and this completes the proof of Proposition 1.1.6. □

We are now ready to prove a theorem according to which the subgroup of $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$ generated by enough classes ramified in Q together with the cohomology classes coming from E(K) contains the Selmer group $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$. Since the elements of the Selmer group are unramified at primes in Q, the following theorem can be viewed as a materialization of the unramified-under-ramified principle.

THEOREM 1.1.7

(i) *The group* $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})$ *is isomorphic to* $(\mathbb{Z}/p^k\mathbb{Z})^{2t}$, *where* t *denotes the cardinality of* Q.

(ii) *The Selmer group* $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ *is contained in the subgroup of* $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})$ *generated by the image of* y *and any subset* $\mathrm{S} \subseteq \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})$ *with the following property:*

(∗) *the image of* S *in* $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})/\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ *generates a subgroup* $\langle \overline{\mathrm{S}} \rangle$ *satisfying* $\mathrm{rank}_{\mathbb{Z}/p\mathbb{Z}} \langle \overline{\mathrm{S}} \rangle / p \langle \overline{\mathrm{S}} \rangle = 2t - 1$.

Proof
Since $Ш_{p^k} = Ш_{p^{k-1}}$, we can write

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \simeq \mathbb{Z}/p^k\mathbb{Z} \times \mathbb{Z}/p^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{m_{2t-1}}\mathbb{Z},$$

where each $m_i < k$. Let us consider the map

$$\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}}). \tag{12}$$

We know that the kernel of this map $\mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$.

By our analysis of the groups $\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})$ in the paragraph preceding Proposition 1.1.6, we know that

$$\prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}}) = \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}) \oplus \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}).$$

The fact that $\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q \simeq (\mathbb{Z}/p^k\mathbb{Z})^2$ for each $q \in \mathrm{Q}$ by (8), together with Proposition 1.1.6, implies that

$$0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^{2t-1} \longrightarrow 0. \tag{13}$$

Therefore, the image of $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ in

$$\prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}})$$

is isomorphic to $(\mathbb{Z}/p^k\mathbb{Z})^{2t-1}$. Moreover, by the sequence (2), we know that the image of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ in $\prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}})$ is isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$. This implies that the image of the map (12) contains a subgroup isomorphic to $(\mathbb{Z}/p^k\mathbb{Z})^{2t}$. By size considerations, we now see that the map (12) gives rise to the exact sequence

$$0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \longrightarrow \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^{2t} \longrightarrow 0. \tag{14}$$

Let us now compute the size of the group $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})$. We know that

$$\mathrm{H}^1_{\mathrm{Sel}^*}(\mathrm{K}, \mathrm{E}_{p^k}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \hookrightarrow \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k}),$$

which implies that $\mathrm{H}^1_{(\mathrm{Sel}_\mathrm{Q})^*}(\mathrm{K}, \mathrm{E}_{p^k}) = \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k}) = 0$. Then, as in [Wi, Proposition 1.6], it follows that

$$\#\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k}) = p^{2k} \prod_{q \in \mathrm{Q}} \#\mathrm{E}(\mathrm{K}_q)_{p^k} \prod_{\lambda \in \Sigma} \frac{\#\mathrm{E}(\mathrm{K}_\lambda)_{p^k}}{[\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^k}) : \mathrm{Sel}_\lambda(p^k)]}. \tag{15}$$

The third property of the elements of Q implies that $\#E(K_q)_{p^k} = p^{2k}$. As we have seen in the proof of Proposition 1.1.6, the group $\mathrm{Sel}_\lambda(p^k)$ is its own exact annihilator under the pairing (1). This implies that

$$\#H^1(K_\lambda, E_{p^k}) = \big(\#\mathrm{Sel}_\lambda(p^k)\big)^2.$$

Moreover, since $E^1(K_\wp) \simeq \mathcal{O}_\wp$, by Lemma 1.1.1 and 1.1.2 we have

$$\#\mathrm{Sel}_\wp(p^k) = [\mathcal{O}_\wp : p^k\mathcal{O}_\wp] \cdot \big(\#E(K_\lambda)_{p^k}\big)$$

and

$$\#\mathrm{Sel}_\lambda(p^k) = \#E(K_\lambda)_{p^k} \quad \text{for } \lambda \in \Sigma \setminus \{\wp | p\}.$$

It follows that

$$\prod_{\lambda \in \Sigma\setminus\{\wp|p\}} \frac{\#E(K_\lambda)_{p^k}}{[H^1(K_\lambda, E_{p^k}) : \mathrm{Sel}_\lambda(p^k)]} = 1$$

and

$$\prod_{\lambda \in \{\wp|p\}} \frac{\#E(K_\lambda)_{p^k}}{[H^1(K_\lambda, E_{p^k}) : \mathrm{Sel}_\lambda(p^k)]} = \prod_{\lambda \in \{\wp|p\}} \frac{1}{[\mathcal{O}_\wp : p^k\mathcal{O}_\wp]} = p^{-2k}.$$

Hence, we conclude that $\#H^1_{\mathrm{Sel}_Q}(K, E_{p^k}) = p^{2kt}$.

Then the exact sequence (14) implies that as a group,

$$H^1_{\mathrm{Sel}_Q}(K, E_{p^{2k}}) \simeq \mathbb{Z}/p^{2k}\mathbb{Z} \times \mathbb{Z}/p^{k+m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{k+m_{2t-1}}\mathbb{Z}$$

because otherwise, $H^1_{\mathrm{Sel}_Q}(K, E_{p^k})$, viewed as the kernel of multiplication by p^k in $H^1_{\mathrm{Sel}_Q}(K, E_{p^{2k}})$, is of order greater than p^{2kt}. Hence, we have

$$H^1_{\mathrm{Sel}_Q}(K, E_{p^k}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^{2t}. \tag{16}$$

We now prove the second part of this theorem. Let $S \subseteq H^1_{\mathrm{Sel}_Q}(K, E_{p^k})$ have the property that its image in $H^1_{\mathrm{Sel}_Q}(K, E_{p^k})/H^1_{\mathrm{Sel}}(K, E_{p^k})$ generates a subgroup $\langle \overline{S} \rangle$ satisfying $\mathrm{rank}_{\mathbb{Z}/p\mathbb{Z}} \langle \overline{S} \rangle / p\langle \overline{S} \rangle = 2t - 1$. Using this assumption and (16), we can see that

$$H^1_{\mathrm{Sel}_Q}(K, E_{p^k})[p] \subseteq \langle y, S \rangle$$

and

$$\langle y, S \rangle \cap H^1_{\mathrm{Sel}}(K, E_{p^k}) = \langle y, pS \rangle \cap H^1_{\mathrm{Sel}}(K, E_{p^k}),$$

where $p\mathrm{S}$ denotes the subset of $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})$ consisting of p-multiples of elements in S. Let $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ so that $ps \in \langle y, \mathrm{S}\rangle$. It follows that $ps \in \langle y, p\mathrm{S}\rangle$, which implies that

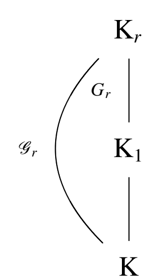
$$s \in \langle y, \mathrm{S}\rangle + \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})[p] \subseteq \langle y, \mathrm{S}\rangle.$$

We can then conclude that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \subseteq \langle y, \mathrm{S}\rangle$. □

Remark 1.1.8
The conclusion that $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^{2t}$ can also be reached more simply by computing the size of $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_p)$ in addition to the size of $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})$ as above. (We thank the referees for pointing out to us that such an argument is used in [MR].) We have chosen this longer way of presenting the result because this was our original proof through which we understood how this idea can be generalized and what its limitations are. In particular, it motivated our arguments in the anomalous and supersingular cases.

1.2. Kolyvagin cohomology classes
1.2.1
In this section, using Kolyvagin's method, we make an explicit construction of cohomology classes. Most of this section is a slight adaptation of the work of Kolyvagin described in [Gr] and in [R].

Let $\mathcal{O}_\mathrm{K}$ denote the ring of integers of K. For $r \in \mathbb{N}$ prime to N, the conductor of the elliptic curve E, we can consider $x_r = (\mathbb{C}/\mathcal{O}_r, \mathbb{C}/\mathcal{N}_r) \in \mathrm{X}_0(\mathrm{N})$, where $\mathcal{O}_r = \mathbb{Z} + r\mathcal{O}_\mathrm{K}$, $\mathrm{N}\mathcal{O}_\mathrm{K} = \mathcal{N} \cdot \overline{\mathcal{N}}$, and $\mathcal{N}_r = \mathcal{N} \cap \mathcal{O}_r$. We fix a parametrization $\pi : \mathrm{X}_0(\mathrm{N}) \to \mathrm{E}$ which maps the cusp ∞ to the origin of E, and then we define the Heegner point $y_r = \pi(x_r) \in \mathrm{E}(\mathrm{K}_r)$, where K_r is the ring class field of conductor r over K. We have to consider the following field extensions and Galois groups:



Suppose now that $r = \prod \ell_i$, where $\ell_i \neq \ell_j$ for $i \neq j$, $(r, p\mathrm{N}) = 1$, and the ℓ_i are all inert in $\mathrm{K}/\mathbb{Q}$. Then $G_\ell = \langle \sigma_\ell \rangle$ is cyclic of order $\ell + 1$ (recall that D_K, the discriminant of $\mathrm{K}/\mathbb{Q}$, satisfies $\mathrm{D}_\mathrm{K} \leq -5$), and $G_r = \prod_{\ell | r} G_\ell$.

We define an element D_r of the group ring $\mathbb{Z}[G_r]$ as the product of certain elements D_ℓ of $\mathbb{Z}[G_\ell]$ for ℓ dividing r. Let $D_\ell = \sum_{i=1}^{\ell} i\sigma_\ell^i$. Notice that if $\mathrm{Tr}_\ell = \sum_{\sigma \in G_\ell} \sigma$, then D_ℓ satisfies the equality

$$(\sigma_\ell - 1) \cdot D_\ell = \ell + 1 - \mathrm{Tr}_\ell. \tag{17}$$

Let S be a set of representatives of $\mathcal{G}_r/G_r$, and then define $P_r = \sum_{\sigma \in S} \sigma(D_r y_r)$, where $D_r = \prod_{\ell | r} D_\ell$. We use this same set S in order to define P_m for all $m|r$.

Since E has analytic rank 1 over K, we know that $y_{\mathrm{K}} = P_1$ has infinite order and that E(K) has rank 1. Fix a prime $p \neq 2, 3$, and let p^{k_o} be the smallest power of p which annihilates the p-part of $H^1(\mathrm{K}_\nu^{\mathrm{unr}}/\mathrm{K}_\nu, \mathrm{E}(\mathrm{K}_\nu^{\mathrm{unr}}))$ for all primes ν. This group is trivial if E has good reduction at ν and is finite for all ν. Finally, we choose $k, v \in \mathbb{N}$ so that

(1) p^{k-1} annihilates the p-primary part of Ш(E/K);

(2) $\mathrm{E}(\mathrm{K}_\lambda)_{p^\infty} = \mathrm{E}(\mathrm{K}_\lambda)_{p^k}$ for all $\lambda \in \Sigma$;

(3) $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_{p^{k+1}})/\mathrm{K}(\mathrm{E}_{p^k}))$, seen as a subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^{k+1}\mathbb{Z})$, consists of all matrices of the form

$$\begin{pmatrix} 1 + p^k a & p^k b \\ p^k c & 1 + p^k d \end{pmatrix} \quad \text{for } a, b, c, d \in \mathbb{Z}/p\mathbb{Z},$$

and Serre has shown that the index of $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_{p^n})/\mathrm{K})$ in $\mathrm{GL}(2, \mathbb{Z}/p^n\mathbb{Z})$ is bounded by a constant that depends only on E and K, implying that the above condition is satisfied for almost all k; and

(4) p^{k-v} divides y_{K} exactly in E(K) and $k_o < v$. (This last condition is needed in order for the cohomology classes that we construct to remain ramified even after multiplication by p^{k_o}.)

Notice that the first two conditions allow us to use the principle of §1.1, while the third is useful in making sure that the set Q of primes that we choose in this section is such that $\mathrm{E}(\mathrm{K}_q)_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}}_q)_{p^k}$.

We now assume that the primes ℓ dividing r, which were chosen to be inert in $\mathrm{K}/\mathbb{Q}$, also split completely in $\mathrm{K}(\mathrm{E}_{p^k})/\mathrm{K}$. We ensure this by choosing primes ℓ so that $\mathrm{Frob}_\ell(\mathrm{K}(\mathrm{E}_{p^k})/\mathbb{Q}) = \tau$, where τ denotes complex conjugation. Since $\mathrm{Frob}_\ell(\mathbb{Q}(\mathrm{E}_{p^k})/\mathbb{Q}) = \tau$, by comparing the characteristic polynomial of $\mathrm{Frob}_\ell(\mathbb{Q}(\mathrm{E}_{p^k})/\mathbb{Q})$ and that of τ in E_{p^k}, we see that

$$a_\ell \equiv \ell + 1 \equiv 0 \pmod{p^k}, \tag{18}$$

where $\ell + 1 - a_\ell$ is the number of points of E over the finite field $\mathbb{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$. Let λ be the prime of K above ℓ. For the proof of the following proposition giving the standard properties of Heegner points, we refer to [Gr, proof of Proposition 3.7].

PROPOSITION 1.2.1
Suppose that $r = m\ell$. *Then*

(a) $\mathrm{Tr}_\ell y_r = a_l \cdot y_m$ *in* $\mathrm{E}(\mathrm{K}_m)$*;*

(b) λ *is unramified in* K_m/K *and totally ramified in* $\mathrm{K}_\ell/\mathrm{K}$*; and*

(c) $y_r \equiv \mathrm{Frob}(\lambda_m)(y_m)$ *(mod* λ_r*), where* λ_m *is a prime of* K_m *dividing* ℓ *and* λ_r *is the unique prime of* K_r *dividing* λ_m.

PROPOSITION 1.2.2
The natural image $[P_r]$ *of* P_r *in* $\mathrm{E}(\mathrm{K}_r)/p^k\mathrm{E}(\mathrm{K}_r)$ *is fixed by* $\mathscr{G}_r$.

Proof
We first prove that the image $[D_r y_r]$ of $D_r y_r$ in $\mathrm{E}(\mathrm{K}_r)/p^k\mathrm{E}(\mathrm{K}_r)$ is fixed by G_r. Since $G_r = \prod_{l|r} G_\ell$, and $G_\ell = \langle\sigma_\ell\rangle$, it suffices to prove that $[D_r y_r]$ is fixed by σ_ℓ for all $\ell|r$. We have

$$\begin{aligned}(\sigma_\ell - 1)D_r y_r &= (\sigma_\ell - 1)D_\ell D_m y_r = (\ell + 1 - \mathrm{Tr}_\ell)D_m y_r \\ &= (\ell + 1)D_m y_r + D_m(\mathrm{Tr}_\ell y_r) \\ &= (\ell + 1)D_m y_r + D_m(a_\ell y_m) \in p^k\mathrm{E}(\mathrm{K}_r),\end{aligned}$$

by (18).
Therefore, $(\sigma_\ell - 1)[D_r y_r] = 0$.

By the definition of P_r, we now see that $[P_r] = \mathrm{tr}_{\mathrm{K}_1/\mathrm{K}}[D_r y_r]$. Hence, $[P_r]$ is fixed by $\mathscr{G}_r$. □

Now, we consider the commutative diagram

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & \mathrm{H}^1\big(\mathrm{K}_r/\mathrm{K}, \mathrm{E}(\mathrm{K}_r)\big)_{p^k} & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \\
0 & \longrightarrow & \mathrm{E}(\mathrm{K})/p^k\mathrm{E}(\mathrm{K}) & \xrightarrow{\phi} & \mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k}) & \longrightarrow & \mathrm{H}^1(\mathrm{K}, \mathrm{E})_{p^k} & \longrightarrow & 0 \\
 & & \downarrow & & {\scriptstyle \mathrm{Res}}\downarrow\wr & & {\scriptstyle \mathrm{Res}}\downarrow & & \\
0 & \longrightarrow & \big(\mathrm{E}(\mathrm{K}_r)/p^k\mathrm{E}(\mathrm{K}_r)\big)^{\mathscr{G}_r} & \xrightarrow{\phi_r} & \mathrm{H}^1(\mathrm{K}_r, \mathrm{E}_{p^k})^{\mathscr{G}_r} & \longrightarrow & \mathrm{H}^1(\mathrm{K}_r, \mathrm{E})_{p^k}^{\mathscr{G}_r} & &
\end{array} \qquad (19)$$

Note that $\mathrm{Res} : \mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k}) \to \mathrm{H}^1(\mathrm{K}_r, \mathrm{E}_{p^k})^{\mathscr{G}_r}$ is an isomorphism since $\mathrm{E}(\mathrm{K}_r)_{p^k}$ is assumed to be zero. (This is because we are assuming that $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_p)/\mathrm{K})$ is not solvable.)

Using the fact that $[P_r] \in (\mathrm{E}(\mathrm{K}_r)/p^k\mathrm{E}(\mathrm{K}_r))^{\mathcal{G}_r}$, Kolyvagin defines the cohomology class $c(r)$ to be the unique element of $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$ such that $\mathrm{Res}(c(r)) = \phi_r([P_r])$. Let $d(r)$ be the image of $c(r)$ in $\mathrm{H}^1(\mathrm{K}, \mathrm{E})_{p^k}$. As observed by McCallum in [Gr, §4], $c(r)$ can be represented by the 1-cocycle

$$c(r)(\sigma) = \sigma\Big(\frac{P_r}{p^k}\Big) - \frac{P_r}{p^k} - \frac{(\sigma - 1)P_r}{p^k}, \quad \sigma \in \mathrm{Gal}(\overline{\mathrm{K}}/\mathrm{K}),$$

where P_r/p^k is a fixed p^kth-root of P_r in $\mathrm{E}(\overline{\mathrm{K}})$, and $((\sigma - 1)P_r)/p^k$ is a uniquely defined element of $\mathrm{E}(\mathrm{K}_r)$ since $(\sigma - 1)P_r \in p^k\mathrm{E}(\mathrm{K}_r)$ and $\mathrm{E}(\mathrm{K}_r)_{p^k}$ is trivial. We also define $\tilde{d}(r) \in \mathrm{H}^1(\mathrm{K}_r/\mathrm{K}, \mathrm{E}(\mathrm{K}_r))_{p^k} = \mathrm{H}^1(\mathcal{G}_r, \mathrm{E}(\mathrm{K}_r))_{p^k}$ to be the preimage of $d(r)$ under the inflation map. Then it follows that

$$\tilde{d}(r)(\sigma) = -\frac{(\sigma - 1)P_r}{p^k} \quad \text{for } \sigma \in \mathcal{G}_r.$$

1.2.2

PROPOSITION 1.2.3

The classes $c(r)$ and $d(r)$ satisfy the following:

(1) *the class $c(r) \in \mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$ is trivial if and only if $P_r \in p^k\mathrm{E}(\mathrm{K}_r)$; and*

(2) *the classes $d(r) \in \mathrm{H}^1(\mathrm{K}, \mathrm{E})_{p^k}$ and $\tilde{d}(r) \in \mathrm{H}^1(\mathcal{G}_r, \mathrm{E}(\mathrm{K}_r))_{p^k}$ are trivial if and only if $P_r \in p^k\mathrm{E}(\mathrm{K}_r) + \mathrm{E}(\mathrm{K})$.*

Proof

This follows from the definitions of the above cohomology classes and the commutative diagram (19). □

The group $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \{1, \tau\}$ acts on $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$. Since p is odd, $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$ splits as the direct sum of the two eigenspaces for the action of τ. Let $-\epsilon$ be the sign of the functional equation of the L-function of E over $\mathbb{Q}$. For the proofs of the next two propositions, we refer to [Gr, proof of Propositions 5.3, 5.4].

PROPOSITION 1.2.4

There exists $\sigma \in \mathcal{G}_r$ such that $y_r^\tau = \epsilon y_r^\sigma +$ (torsion) in $\mathrm{E}(\mathrm{K}_r)$, where σ depends on the choice of complex conjugation τ.

PROPOSITION 1.2.5

(1) *The class $[P_r]$ lies in the ($\epsilon_r = \epsilon(-1)^{f_r}$)-eigenspace of $(\mathrm{E}(\mathrm{K}_r)/p^k\mathrm{E}(\mathrm{K}_r))^{\mathcal{G}_r}$ under the action of τ, where f_r denotes the number of primes dividing r.*

(2) *The cohomology class $c(r)$ lies in the ϵ_r-eigenspace for τ in $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$.*

Recall that $r = m\ell$, and recall that λ is the unique prime of K which divides ℓ. Let $\mathbb{F}_\lambda$ be the residue field of K at λ. Since we assumed that λ splits completely in $\mathrm{K}(\mathrm{E}_{p^k})/\mathrm{K}$, it follows that $\mathrm{E}(\mathbb{F}_\lambda)_{p^k} = (\mathbb{Z}/p^k\mathbb{Z})^2$.

Now, τ has eigenvalues ± 1 on $\mathrm{E}(\mathbb{F}_\lambda)_{p^k}$, and since its determinant is -1, it follows that

$$\mathrm{E}(\mathbb{F}_\lambda)^{\pm}_{p^k} \simeq \mathbb{Z}/p^k\mathbb{Z}. \tag{20}$$

For the primes ℓ that we have chosen, we also know that

$$\begin{aligned} \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E})_{p^k} &\simeq \mathrm{E}(\mathrm{K}_\lambda)/p^k\mathrm{E}(\mathrm{K}_\lambda) \simeq \mathrm{E}(\mathbb{F}_\lambda)/p^k\mathrm{E}(\mathbb{F}_\lambda) \\ &\simeq \mathrm{E}(\mathbb{F}_\lambda)_{p^k} \simeq \mathrm{E}(\mathrm{K}_\lambda)_{p^k} \simeq (\mathbb{Z}/p^k\mathbb{Z})^2. \end{aligned} \tag{21}$$

PROPOSITION 1.2.6

The classes $d(r)$ have the following local properties:

(1) *the class $p^{k_o}d(r)_\nu \in \mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E})_{p^k}$ is trivial at the archimedean place $\nu = \infty$ and at the finite places ν of* K *which do not divide r; and*

(2) *for any $1 \le i \le k$, $p^{k-i}d(r)_\lambda = 0$ in $\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E})_{p^k}$ if and only if $P_m \in p^i\mathrm{E}(\mathrm{K}_\lambda)$, where $r = m\ell$ and λ is the prime of* K *above ℓ.*

Proof

(1) If $\nu = \infty$, then $\mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E})_{p^k}$ is trivial and, therefore, so is $d(r)_\nu$. If ν is a finite place that does not divide r, then in (19) we have the fact that $d(r)$ is the inflation of a class from K_r/K and, hence, is unramified at ν. By the definition of k_0, $p^{k_o}d(r)_\nu$ is then trivial.

(2) Let K_{λ_m} be the localization of K_m at λ_m, and let K_{λ_r} be the localization of K_r at λ_r. We know that $\tilde{d}(r)_\lambda \in \mathrm{H}^1(\mathrm{K}_{\lambda_r}/\mathrm{K}_\lambda, \mathrm{E})_{p^k}$ is represented by the cocycle $\sigma \mapsto -((\sigma - 1)P_r)/p^k$ for $\sigma \in \mathrm{Gal}(\mathrm{K}_{\lambda_r}/\mathrm{K}_\lambda)$. Since $\mathrm{K}_{\lambda_m} = \mathrm{K}_\lambda$, and λ_m is totally ramified in $\mathrm{K}_{\lambda_r}/\mathrm{K}_{\lambda_m}$, it follows that $\mathrm{Gal}(\mathrm{K}_{\lambda_r}/\mathrm{K}_\lambda) \simeq \mathrm{Gal}(\mathrm{K}_{\lambda_r}/\mathrm{K}_{\lambda_m}) \simeq G_\ell$. Let E^1 be the subgroup of E which maps to the identity of the reduction of E modulo ℓ. Since E^1 is a pro-ℓ group, and $\ell \ne p$, $\mathrm{H}^1(G_\ell, \mathrm{E}^1(\mathrm{K}_{\lambda_r}))_{p^k} = 0$. It follows that $\mathrm{H}^1(\mathrm{K}_{\lambda_r}/\mathrm{K}_\lambda, \mathrm{E})_{p^k}$ injects into

$$\mathrm{H}^1\big(G_\ell, \mathrm{E}(\mathbb{F}_{\lambda_r})\big)_{p^k} = \mathrm{H}^1\big(G_\ell, \mathrm{E}(\mathbb{F}_\lambda)\big)_{p^k} = \mathrm{Hom}\big(G_\ell, \mathrm{E}(\mathbb{F}_\lambda)_{p^k}\big)$$

since $\mathbb{F}_{\lambda_r} = \mathbb{F}_\lambda$, G_ℓ acts trivially on $\mathrm{E}(\mathbb{F}_\lambda)$ and $\mathrm{Hom}(G_\ell, \mathrm{E}(\mathbb{F}_\lambda)_{p^k}) = \mathrm{Hom}(G_\ell, \mathrm{E}(\mathbb{F}_\lambda))_{p^k}$. Then the fact that G_ℓ is cyclic and generated by σ_ℓ implies that

$$p^{k-i}d(r)_\lambda = 0 \text{ if and only if } p^{k-i}\tilde{d}(r)(\sigma_\ell) \equiv 0 \pmod{\lambda_r}. \tag{22}$$

Now, we evaluate $\tilde{d}(r)(\sigma_\ell) \pmod{\lambda_r}$:

$$\begin{aligned}\tilde{d}(r)(\sigma_\ell) &= -\frac{(\sigma_\ell - 1)P_r}{p^k}\\ &= -\frac{(\sigma_\ell - 1)\sum_{\sigma\in S}\sigma(D_r y_r)}{p^k} = -\frac{\sum_{\sigma\in S}\sigma D_m(\sigma_\ell - 1)D_\ell y_r}{p^k}\\ &= -\frac{\sum_{\sigma\in S}\sigma D_m((\ell+1)y_r - \mathrm{Tr}_\ell y_r)}{p^k},\end{aligned}$$

by (17),

$$= \sum_{\sigma\in S}\sigma D_m\Big(\frac{a_\ell}{p^k}y_m - \frac{\ell+1}{p^k}y_r\Big),$$

by Proposition 1.2.1(1),

$$\equiv \sum_{\sigma\in S}\sigma D_m\Big(\frac{a_\ell}{p^k} - \frac{(\ell+1)\mathrm{Frob}(\lambda_m)}{p^k}\Big)y_m \pmod{\lambda_r},$$

by Proposition 1.2.1(3).

Let $\sigma \in \mathscr{G}_m$. Then since $\mathrm{Frob}(\sigma^{-1}\lambda_m) = \sigma^{-1}\,\mathrm{Frob}(\lambda_m)\sigma$ and

$$\frac{a_\ell}{p^k}y_m - \frac{\ell+1}{p^k}y_r \equiv \frac{a_\ell - (\ell+1)\,\mathrm{Frob}(\sigma^{-1}\lambda_m)}{p^k}y_m \pmod{\sigma^{-1}\lambda_r},$$

it follows that

$$\sigma\Big(\frac{a_\ell}{p^k}y_m - \frac{\ell+1}{p^k}y_r\Big) \equiv \frac{a_\ell - (\ell+1)\,\mathrm{Frob}(\lambda_m)}{p^k}\sigma y_m \pmod{\lambda_r}.$$

Then we have

$$\begin{aligned}\tilde{d}(r)(\sigma_\ell) &\equiv \sum_{\sigma\in S}\sigma D_m\Big(\frac{a_\ell - (\ell+1)\,\mathrm{Frob}(\lambda_m)}{p^k}\Big)y_m \pmod{\lambda_r}\\ &\equiv \frac{a_\ell - (\ell+1)\,\mathrm{Frob}(\lambda_m)}{p^k}P_m \pmod{\lambda_r}.\end{aligned}$$

Recall that P_m lies in the ϵ_m-eigenspace for $\mathrm{Frob}_\ell = \tau$ on $\mathrm{E}(\mathbb{F}_\lambda)/p^k\mathrm{E}(\mathbb{F}_\lambda)$. We know the size of the $+1$-eigenspace for τ on $\mathrm{E}(\mathbb{F}_\lambda)$,

$$\#\mathrm{E}(\mathbb{F}_\lambda)^+ = \ell + 1 - a_\ell.$$

In addition, since $\#\mathrm{E}(\mathbb{F}_\lambda) = 1 + \ell^2 - \alpha_\ell^2 - \overline{\alpha}_\ell^2 = (1+\ell)^2 - a_\ell^2$, where $\alpha_\ell + \overline{\alpha}_\ell = a_\ell$ and $\alpha_\ell\overline{\alpha}_\ell = \ell$, it follows that

$$\#\mathrm{E}(\mathbb{F}_\lambda)^- = 2^\varepsilon(\ell + 1 + a_\ell), \quad \text{where } \varepsilon \in \{0, \pm 1\}.$$

Then using the cyclicity of the p-part of $\mathrm{E}(\mathbb{F}_\lambda)^{\pm}$, we see that the kernel of multiplication of $\mathrm{E}(\mathbb{F}_\lambda)^{\pm}$ by $2^{\varepsilon}\big((a_\ell - (\ell+1)\,\mathrm{Frob}(\lambda_m))/p^i\big)$ is $p^i\mathrm{E}(\mathbb{F}_\lambda)^{\pm}$ for any $1 \le i \le k$. This implies that $2^{\varepsilon} p^{(k-i)}\tilde{d}(r)(\sigma_\ell) \equiv 0$ modulo λ_r if and only if $P_m \in p^i\mathrm{E}(\mathbb{F}_\lambda)$, which is equivalent to $P_m \in p^i\mathrm{E}(\mathrm{K}_{\lambda_m})$ because E^1 is p-divisible. Moreover, since p is odd, it follows that

$$p^{k-i}\tilde{d}(r)(\sigma_\ell) \equiv 0 \pmod{\lambda_r} \text{ if and only if } P_m \in p^i\mathrm{E}(\mathrm{K}_{\lambda_m}).$$

This result, taken together with (22), allows us to conclude that

$$p^{k-i}d(r)_\lambda = 0 \quad \text{if and only if } P_m \in p^i\mathrm{E}(\mathrm{K}_{\lambda_m}) \text{ for any } 1 \le i \le k. \qquad \square$$

1.3. Choosing the set of auxiliary primes Q

Recall that the auxiliary primes $q \in \mathrm{Q}$ are required to have the following properties:

(i) q remains inert in $\mathrm{K}/\mathbb{Q}$;

(ii) $q \notin \Sigma'$;

(iii) $\mathrm{E}(\mathrm{K}_q)_{p^\infty} = \mathrm{E}_{p^k}$; and

(iv) $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \hookrightarrow \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k})$, where $\mathrm{K}_q^{\mathrm{unr}}$ denotes the maximal unramified extension of K_q.

In this section, we prove the existence of a set of primes with these properties and give a method for constructing such a set.

1.3.1

We start by showing how we can choose the primes of Q so that

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \hookrightarrow \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k}).$$

Let $\mathrm{L}_k = \mathrm{K}(\mathrm{E}_{p^k})$, let $\mathscr{G}_k = \mathrm{Gal}(\mathrm{L}_k/\mathrm{K})$, and consider the exact sequence

$$0 \longrightarrow \mathrm{H}^1(\mathscr{G}_k, \mathrm{E}_{p^k}) \longrightarrow \mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k}) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(\mathrm{L}_k, \mathrm{E}_{p^k})^{\mathscr{G}_k} \longrightarrow \mathrm{H}^2(\mathscr{G}_k, \mathrm{E}_{p^k}). \qquad (23)$$

PROPOSITION 1.3.1
We have $\mathrm{H}^1(\mathscr{G}_k, \mathrm{E}_{p^k}) = 0$ *for all* $k \in \mathbb{N}$.

Proof
We have two cases. If $\mathscr{G}_1 = \mathrm{Gal}(\mathrm{K}(\mathrm{E}_p)/\mathrm{K})$ has order divisible by p, then since it is assumed not solvable, a result of Serre [S2, Proposition 15], shows that $\overline{\mathscr{G}_1}$, the image of $\mathscr{G}_1$ in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, contains $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Since the determinant is a cyclotomic character, we deduce that $\overline{\mathscr{G}_1}$ intersects nontrivially with the center Z of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Pick a lift δ of an element of $\overline{\mathscr{G}_1} \cap \mathrm{Z}$ to the center of $\mathrm{GL}_2(\mathbb{Z}_p)$. Then there exists

$m \in \mathbb{N}$ such that $\delta^{p^m} \in \operatorname{im}(\operatorname{Gal}(\overline{\mathrm{K}}/\mathrm{K}) \to \mathrm{GL}_2(\mathbb{Z}_p))$ since this image is open by a theorem of Serre [S2, §4.4, Theorem 3] and such that δ^{p^m} projects to an element of $\mathscr{G}_k$ of order prime to p. Now, consider the inflation-restriction sequence with respect to the subgroup $\langle \delta^{p^m} \rangle$ of $\mathscr{G}_k$, and observe that $(\mathrm{E}_{p^k})^{\langle \delta^{p^m} \rangle} = 0$. The proposition follows.

In the remaining case, where the image of $\mathscr{G}_1$ in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ is isomorphic to A_5, we can assume that $p > 5$ since the case $p = 5$ is taken care of by the preceding argument. So, suppose now that $p > 5$. It follows that $\mathrm{H}^1(\mathscr{G}_1, \mathrm{E}_p) = 0$ in this case. Notice that it is sufficient to prove that $\mathrm{H}^1(\mathscr{G}_k, \mathrm{E}_p) = 0$ since by using induction, we can deduce that $\mathrm{H}^1(\mathscr{G}_k, \mathrm{E}_{p^k}) = 0$ for all $k \in \mathbb{N}$. By examining the inflation-restriction sequence with respect to the subgroup $\mathrm{H}_1 = \ker : \mathscr{G}_k \to \mathscr{G}_1$, this time we see that it is enough to show that $\mathrm{H}^1(\mathrm{H}_1, \mathrm{E}_p)^{\mathscr{G}_1} = 0$. To verify this, it is enough to show that $\mathrm{H}^1(\mathrm{H}_1, \mathrm{E}_p)^{\langle \delta \rangle} = 0$ for $\delta \in \mathscr{G}_1$, which maps to an element of order 5 in $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.

Let us first assume that $p - 1$ is prime to 5, which in particular allows us to pick a lifting of δ to an element of order 5 of $\mathscr{G}_k$. It then follows that $\langle \delta \rangle$ injects into $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. The eigenvalues of δ on E_p are given by ζ and ζ^{-1} for some 5th-root of unity ζ. (The determinant is 1 on δ as A_5 is not solvable.) Since H_1 acts trivially on E_p, the elements of $\mathrm{H}^1(\mathrm{H}_1, \mathrm{E}_p)^{\langle \delta \rangle}$ are just δ-invariant homomorphisms. Then we claim that H_1 has a filtration by δ-invariant abelian groups of exponent p, on which the action of δ has eigenvalues in the set $\{1, \zeta^2, \zeta^{-2}\}$. To check this, it is enough to verify a similar statement for $\ker : \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ under the action of an element δ of order 5 of $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$. Here the filtration is the usual one by normal subgroups of level $1, \ldots, k$, and the subquotients are abelian groups of exponent p. In this case, the result is easily verified using the fact that the eigenvalues of δ in the adjoint representation of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ are in the set $\{1, \zeta^2, \zeta^{-2}\}$. It follows that $\mathrm{H}^1(\mathrm{H}_1, \mathrm{E}_p)^{\langle \delta \rangle} = 0$, and this completes the proof of the case when 5 does not divide $p - 1$.

If $p - 1$ is divisible by 5, let x and y denote the eigenvalues of δ on E_p. We can assume that $x^5 = y^5 = a \in (\mathbb{Z}/p)^* - \{1\}$ since the case when $x^5 = y^5 = 1$ is the same as the one treated in the previous paragraph. It follows that $y = x\zeta$, where $\zeta^5 = 1$. Finally, the fact that $\{x, x\zeta\} \cap \{1, \zeta, \zeta^{-1}\} = \varnothing$ concludes the proof of this lemma by the same argument as above. □

COROLLARY 1.3.2

The restriction map $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k}) \longrightarrow \operatorname{Hom}_{\mathscr{G}_k}(\operatorname{Gal}(\mathrm{L}_k^{\mathrm{ab}}/\mathrm{L}_k), \mathrm{E}_{p^k})$*, where* $\mathrm{L}_k^{\mathrm{ab}}$ *denotes the maximal abelian extension of* L_k*, is injective.*

Proof

This follows immediately from diagram (23) and Proposition 1.3.1. □

Corollary 1.3.2 gives us the $\mathscr{G}_k$-pairing

$$\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k}) \times \operatorname{Gal}(\mathrm{L}_k^{\mathrm{ab}}/\mathrm{L}_k) \longrightarrow \mathrm{E}_{p^k}. \tag{24}$$

Let M be the fixed field of the subgroup of $\mathrm{Gal}(L_k^{ab}/L_k)$ which pairs to zero with the finite subgroup $H^1_{Sel}(K, E_{p^k})$ of $H^1(K, E_{p^k})$. Then we have a nondegenerate $\mathcal{G}_k$-pairing

$$H^1_{Sel}(K, E_{p^k}) \times \mathrm{Gal}(M/L_k) \longrightarrow E_{p^k}. \tag{25}$$

Let $H = \mathrm{Gal}(M/L_k)$. The element τ of $\mathrm{Gal}(L_k/\mathbb{Q})$ acts on H. We extend τ to a complex conjugation in $\mathrm{Gal}(M/\mathbb{Q})$. The nondegeneracy of the pairing (25) implies, in particular, that H has p-power and, hence, odd order. So, H splits as a direct sum of the eigenspaces for the action of τ, $H = H^+ \oplus H^-$. Furthermore,

$$H^+ = H^{\tau+1} := \left\{\tau h \tau^{-1} h = (\tau h)^2 \,:\, h \in H\right\}. \tag{26}$$

PROPOSITION 1.3.3

Let $s \in H^1_{Sel}(K, E_{p^k})$. Then the following are equivalent:

(1) $s = 0$;

(2) $[s, \rho] = 0$ *for all* $\rho \in H$, *where* $[\,,\,]$ *denotes the pairing (25); and*

(3) $[s, \rho] = 0$ *for all* $\rho \in H^+$.

Proof

It is obvious that (1) $\Rightarrow$ (2) $\Rightarrow$ (3). The nondegeneracy of pairing (25) implies that (2) $\Rightarrow$ (1). We show that (3) $\Rightarrow$ (2).

Let $s = s^+ + s^-$, where $s^\pm \in H^1_{Sel}(K, E_{p^k})^\pm$. We may view s^+ and s^-, via (25), as elements of $\mathrm{Hom}_{\mathcal{G}_k}(H, E_{p^k})$. Since $s^\pm(H^+) \subseteq E^\pm_{p^k}$, $s(H^+) = 0$ implies that $s^\pm(H^+) = 0$. Consequently, $s^\pm(H) = s^\pm(H^-) \subseteq E^\mp_{p^k}$. We know that E_p is an irreducible $\mathcal{G}_k$-module because we have assumed that $\mathrm{Gal}(K(E_p)/K)$ is not solvable. Since $s^\pm(H)$ is a $\mathcal{G}_k$-module, it follows that either $s^\pm(H) \supset E_p$ or $s^\pm(H) = 0$. Then as $E_p \not\subseteq E^\pm_{p^k}$, we deduce that $s^\pm(H) = 0$, and consequently, $s(H) = 0$. □

PROPOSITION 1.3.4

If $s \in H^1_{Sel}(K, E_{p^k})$, $\rho \in \mathrm{Gal}(M/L_k)$, and λ is a prime of K not contained in Σ, then the following are equivalent:

(1) $[s, \rho] = 0$ *for some* ρ *in the conjugacy class of* Frob_λ;

(2) $[s, \mathrm{Frob}_\lambda] = 0$ *for all* ρ *in the conjugacy class of* Frob_λ; *and*

(3) $s_\lambda = 0$ *in* $H^1(K_\lambda, E_{p^k})$.

Proof

By hypothesis, s_λ is in the image of $E(K_\lambda)/p^k E(K_\lambda)$ since it is in the Selmer group, say, $s_\lambda = \mathrm{im}(P_\lambda)$. Then $[s, \rho] = (P_\lambda/p^k)^{\rho-1}$. It follows that $[s, \rho] = 0$ if and only if $P_\lambda \in p^k E(L_{k,\tilde{\lambda}}) = p^k E(K_\lambda)$, where $\tilde{\lambda}$ is the prime of L_k above λ to which ρ is associated. □

COROLLARY 1.3.5
Suppose that $\langle h_1 \dots h_t \rangle = \mathrm{H}^+$, *and let* $\mathrm{Q} = \{\ell_1, \dots, \ell_t\}$ *be a set of* t *rational primes so that* $\tau h_i' \in \mathrm{Frob}_{\ell_i}(\mathrm{M}/\mathbb{Q})$, *where* $(\tau h_i')^2 = h_i$ *for each* i. *Then the natural map*

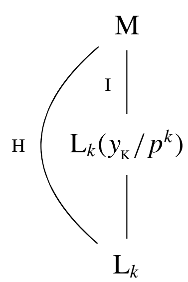
$$\phi_{\mathrm{Q}} : \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \longrightarrow \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k})$$

is injective.

Proof
Suppose that s is in the kernel of ϕ_{Q}. Then by Proposition 1.3.4, $[s, \mathrm{Frob}_{\lambda_i}] = 0$, where λ_i is the unique prime of K above ℓ_i for each i. Then $[s, h_i] = 0$ for each i, and so $[s, \mathrm{H}^+] = 0$. Thus $s = 0$, by Proposition 1.3.3. □

1.3.2
We now show how to ensure that the auxiliary primes $q \in \mathrm{Q}$ have the property that $\mathrm{E}(\mathrm{K}_q)_{p^{k+1}} = \mathrm{E}(\overline{\mathrm{K}}_q)_{p^k}$.

By Proposition 1.2.4, the point y_{K} belongs to $\mathrm{E}(\mathrm{K})^{\pm} + \mathrm{E}(\mathrm{K})_{\mathrm{tors}}$, and therefore, by diagram (19), the class $\phi(y_{\mathrm{K}})$ lies in $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})^{\pm}$. We denote by I the subgroup of H which pairs to zero with the subgroup of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ generated by $\phi(y_{\mathrm{K}})$, and we denote by $\mathrm{L}_k(y_{\mathrm{K}}/p^k)$ the subfield of M fixed by I. Then we have



(27)

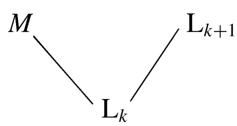
Since $\phi(y_{\mathrm{K}}) \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})^{\pm}$, we see that I is fixed by τ. Let I^+ be the $+1$-eigenspace of I for the action of τ. We observe, as we did in the case of H, that $\mathrm{I}^+ = \mathrm{I}^{\tau+1}$.

LEMMA 1.3.6
We have $\mathrm{H}/\mathrm{I} \simeq \mathrm{E}_{p^v}$, *and consequently,* $(\mathrm{H}/\mathrm{I})^+ \simeq \mathrm{H}^+/\mathrm{I}^+ \simeq \mathbb{Z}/p^v\mathbb{Z}$.

Proof
We know that $\phi(y_{\mathrm{K}}) \in \mathrm{Hom}_{\mathscr{G}_k}(\mathrm{H}, \mathrm{E}_{p^k})$, and we know that $\ker(\phi(y_{\mathrm{K}})) = \mathrm{I}$. Recall that y_{K} is exactly divisible by p^{k-v}, and therefore, $\langle \phi(y_{\mathrm{K}}) \rangle = \mathbb{Z}/p^v\mathbb{Z}$. This implies that

$\mathrm{im}(\phi(y_{\mathrm{K}})) \subseteq \mathrm{E}_{p^v}$. We show that $\mathrm{im}(\phi(y_{\mathrm{K}})) = \mathrm{E}_{p^v}$. If $\mathrm{im}(\phi(y_{\mathrm{K}})) \subseteq \mathrm{E}_{p^{v-1}}$, then by the nondegeneracy of pairing (25), it would follow that $p^{v-1} \cdot \phi(y_{\mathrm{K}}) = 0$, which is a contradiction. If $\mathrm{im}(\phi(y_{\mathrm{K}})) \neq \mathrm{E}_{p^k}$, then $\mathrm{im}(p^{v-1}\phi(y_{\mathrm{K}})) \subsetneq \mathrm{E}_p$. But this is impossible since the image of $p^{v-1}\phi(y_{\mathrm{K}})$ is a $\mathscr{G}_k$-submodule of E_p, and the action is irreducible since we have assumed that $\mathscr{G}_1$ is not solvable. Since $\ker(\phi(y_{\mathrm{K}})) = \mathrm{I}$, it follows that $\mathrm{H}/\mathrm{I} \simeq \mathrm{E}_{p^v}$, and consequently, $(\mathrm{H}/\mathrm{I})^+ \simeq (\mathrm{E}_{p^v})^+ \simeq \mathbb{Z}/p^v\mathbb{Z}$. □

Consider the following two extensions of L_k:



(28)

We know that $\mathrm{Gal}(\mathrm{L}_{k+1}/\mathrm{L}_k)$ is a p-torsion group. By the nondegeneracy of pairing (25), we have

$$\mathrm{Gal}(\mathrm{M}/\mathrm{L}_k)/p\,\mathrm{Gal}(\mathrm{M}/\mathrm{L}_k) \simeq \mathrm{E}_p \oplus \mathrm{E}_{p^{\delta_2}} \oplus \cdots \oplus \mathrm{E}_{p^{\delta_{2t}}}$$

as a $\mathscr{G}_1$-module, where $\delta_i \in \{0, 1\}$. On the other hand, the action of $\mathscr{G}_k$ on $\mathrm{Gal}(\mathrm{L}_{k+1}/\mathrm{L}_k)$ factors through $\mathscr{G}_1$, and as a $\mathscr{G}_1$-module

$$\mathrm{Gal}(\mathrm{L}_{k+1}/\mathrm{L}_k) \subseteq \mathsf{Ad}^0_\rho \oplus 1, \tag{29}$$

where Ad^0_ρ denotes the restriction to trace-zero matrices of the adjoint representation of $\rho : \mathscr{G}_1 \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. This already shows that the two extensions in (28) are disjoint. We claim that (29) is also an isomorphism, as follows from assumption (3) on k in §1.2.1. We need this to know that there are elements of $\mathrm{Gal}(\mathrm{L}_{k+1}/\mathrm{L}_k)$ with no fixed points on $\mathrm{E}_{p^{k+1}} - \mathrm{E}_{p^k}$.

Now, pick elements $h_1, \ldots, h_t \in \mathrm{H}^+ - \mathrm{I}^+$ so that $\{h_1, \ldots, h_t\}$ is a minimal set of generators of H^+ and so that each $\overline{h}_i$ has maximal order in $\mathrm{H}^+/\mathrm{I}^+$. Then each $h_i = (\tau h_i')^2$ for $h_i' \in \mathrm{H}$ by (26). We can extend each $\tau h_i'$ to an element of $\mathrm{Gal}(\mathrm{ML}_{k+1}/\mathbb{Q})$ in such a way that its restriction to $\mathrm{Gal}(\mathrm{L}_{k+1}/\mathrm{L}_k)$ has no fixed points in $\mathrm{E}_{p^{k+1}} - \mathrm{E}_{p^k}$. Finally, we can choose primes $\ell_i \in \mathbb{Q}$ for $i = 1, \ldots, t$ so that

$$\tau h_i' \in \mathrm{Frob}_{\ell_i}(\mathrm{ML}_{k+1}/\mathbb{Q}).$$

It then follows that

(i) $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ maps injectively to $\prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k})$ for $\mathrm{Q} = \{\ell_1, \ldots, \ell_t\}$;

(ii) $\mathrm{E}(\mathrm{K}_{\lambda_i})_{p^{k+1}} = \mathrm{E}(\overline{\mathrm{K}}_{\lambda_i})_{p^k}$, where λ_i is the unique prime of K above ℓ_i; and

(iii) each $h_i = (\tau h_i')^2$ has maximal order in $\mathrm{H}^+/\mathrm{I}^+$.

1.4. Construction of ramified classes

In this section, we construct the ramified cohomology classes that are needed to apply the principle of §1.1. To do this, we need a slight refinement of the results of §1.3.

PROPOSITION 1.4.1

Let $\tau h \in \mathrm{Frob}_\ell(\mathrm{M}/\mathbb{Q})$*, where* $h \in \mathrm{H}$ *and* λ *is the unique prime of* K *dividing* ℓ*. Then* $p^i d(\ell)_\lambda = 0$ *in* $\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E})_{p^k}$ *if and only if* $(h^{1+\tau})^{p^i} \in \mathrm{I}^+$.

Proof

Since $\tau h \in \mathrm{Frob}_\ell(\mathrm{M}/\mathbb{Q})$, we have $h^{\tau+1} \in \mathrm{Frob}_\lambda(\mathrm{M}/\mathrm{K})$. By Proposition 1.2.6, we know that $p^i d(\ell)_\lambda = 0$ in $\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E})_{p^k}$ if and only if $y_{\mathrm{K}} = P_1 \in p^{k-i}\mathrm{E}(\mathrm{K}_\lambda)$, which is equivalent to $p^i \phi(y_{\mathrm{K}})_\lambda = 0$. It then follows from Proposition 1.3.4 that

$$p^i d(\ell)_\lambda = 0 \quad \text{in } \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E})_{p^k} \iff [p^i\phi(y_{\mathrm{K}}), h^{\tau+1}] = [\phi(y_{\mathrm{K}}), (h^{\tau+1})^{p^i}] = 0.$$

By the definition of I and the fact that $h^{\tau+1} \in \mathrm{H}^+$, $[\phi(y_{\mathrm{K}}), (h^{\tau+1})^{p^i}] = 0$ is equivalent to $(h^{\tau+1})^{p^i} \in \mathrm{I}^+$. □

We now refine the construction of §1.3 slightly. Suppose that we have chosen generators $h_1, \ldots, h_t$ of H^+ as in the last paragraph of §1.3. Let us now fix $\ell = \ell_1$ so that $\tau h_1' \in \mathrm{Frob}_\ell(\mathrm{ML}_{k+1}/\mathbb{Q})$. Since $\langle \bar{h}_1 \rangle = \mathrm{H}^+/\mathrm{I}^+$, by Lemma 1.3.6 $h = (\tau h_1')^2$ is of order p^v in H/I. Therefore, Proposition 1.4.1 implies that $p^v c(\ell) \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$, while $p^{v-1}c(\ell) \notin \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$.

Consider $\mathrm{L}_k(p^v c(\ell))$ and $\mathrm{L}_k(p^{v-1}c(\ell))$, the field extensions of L_k which are fixed by the subgroups pairing to zero in (24) with $p^v c(\ell)$ and $p^{v-1}c(\ell)$, respectively. The extension

$$\begin{array}{c} \mathrm{L}_k\big(p^{v-1}c(\ell)\big) \nsubseteq \mathrm{M} \\ \Big| \\ \mathrm{L}_k\big(p^{v}c(\ell)\big) \subseteq \mathrm{M} \end{array}$$

is ramified at ℓ because $p^{v-1}c(\ell)$ is ramified at this prime, and

$$\mathrm{Gal}\big(\mathrm{L}_k(p^{v-1}c(\ell))/\mathrm{L}_k(p^v c(\ell))\big) \simeq \mathrm{E}_p.$$

So, we have the following.

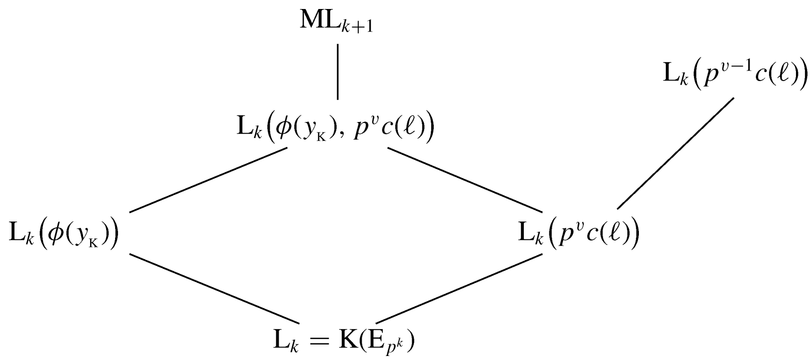
(1) The Galois groups $\mathrm{Gal}\big(\mathrm{ML}_{k+1}/\mathrm{L}_k(p^v c(\ell))\big)$ and $\mathrm{Gal}\big(\mathrm{L}_k(p^{v-1}c(\ell))/\mathrm{L}_k(p^v c(\ell))\big)$ are $\mathscr{G}_k$-modules. (In each case, the natural action of $\mathrm{Gal}\big(\mathrm{L}_k(p^v c(\ell))/\mathrm{K}\big)$ factors through $\mathscr{G}_k$.)

(2) $\mathrm{Gal}\big(\mathrm{L}_k(p^{v-1}c(\ell))/\mathrm{L}_k(p^v c(\ell))\big) \simeq \mathrm{E}_p$ is an irreducible $\mathscr{G}_k$-module (since $\mathscr{G}_1$ is assumed to be not solvable).

(3) The extension $ML_{k+1}/L_k(p^v c(\ell))$ is unramified outside pN since the elements of the Selmer group as well as p-power torsion points are unramified at primes of good reduction which do not divide p. Moreover, $(p\mathrm{N}, \ell) = 1$.

The above imply that ML_{k+1} and $L_k(p^{v-1}c(\ell))$ are disjoint over $L_k(p^v c(\ell))$.

At this point, we need to consider the tower of field extensions:



Choose $g \in \mathrm{Gal}\big(L_k(p^{v-1}c(\ell))/L_k(p^v c(\ell))\big)$ so that $g^{\tau+1} \neq 1$. Let $\ell_2, \ldots, \ell_t$ be primes of $\mathbb{Q}$ so that

(1) $\tau h_i' \in \mathrm{Frob}_{\ell_i}(ML_{k+1}/\mathbb{Q})$ if $p^v c(\ell)(h_i) \neq 0$; and

(2) $\tau h_i' \in \mathrm{Frob}_{\ell_i}(ML_{k+1}/\mathbb{Q})$ and $\tau g \in \mathrm{Frob}_{\ell_i}\big(L_k(p^{v-1}c(\ell))/\mathbb{Q}\big)$ if $p^v c(\ell)(h_i) = 0$ (since we can choose h_i' so that $p^v c(\ell)(h_i') = 0$ by applying the construction of (26) while replacing H by $\mathrm{Gal}\big(ML_{k+1}/L_k(p^v c(\ell))\big)$.

Consider the cohomology classes $c(\ell_i)$ for $i = 1, \ldots, t$ and $c(\ell\ell_i)$ for $i = 2, \ldots, t$, where $\ell_1 = \ell$. Proposition 1.4.1 implies that since $H^+/I^+ \simeq \mathbb{Z}/p^v\mathbb{Z}$ and h_i is maximal, $d(\ell_i)$ has order p^v in $H^1(K_{\lambda_i}, E)_{p^k}$. Then since $v > k_0$, Proposition 1.2.6 allows us to conclude that

(1) $p^{k_o} d(\ell_i)_\nu = 0$ in $H^1(K_\nu, E)_{p^k}$ for all primes $\nu \neq \lambda_i$;

(2) $p^{k_o} d(\ell_i)_{\lambda_i} \neq 0$ in $H^1(K_{\lambda_i}, E)_{p^k}$ for $i \geq 1$;

(3) $p^{k_o} d(\ell\ell_i)_\nu = 0$ in $H^1(K_\nu, E)_{p^k}$ for all primes $\nu \neq \lambda, \lambda_i$, Proposition 1.2.6(1); and

(4) $p^{k_o} d(\ell\ell_i)_{\lambda_i} \neq 0$ in $H^1(K_{\lambda_i}, E)_{p^k}$ for $i \geq 2$. By Proposition 1.2.6(2), $p^{k_o} d(\ell\ell_i)_{\lambda_i} \neq 0$ in $H^1(K_{\lambda_i}, E)_{p^k}$ if and only if $P_\ell \notin p^{k-k_0}E(K_{\lambda_i})$, which is equivalent to $p^{k_o} c(\ell)_{\lambda_i} \neq 0$. We know that $p^{v-1}c(\ell)_{\lambda_i} \neq 0$ because of the way we have chosen $\ell_2, \ldots, \ell_t$. Since $k_0 \leq v-1$, it follows that $p^{k_o} c(\ell)_{\lambda_i} \neq 0$. So, we can conclude that $p^{k_o} d(\ell\ell_i)_{\lambda_i} \neq 0$ in $H^1(K_{\lambda_i}, E)_{p^k}$.

Furthermore, the classes $p^{k_o} c(\ell_i), p^{k_o} c(\ell\ell_j) \in H^1_{\mathrm{Sel}_Q}(K, E_{p^k})$ lie in different eigenspaces of $H^1(K, E_{p^k})$ for the action of τ, and consequently, even if $i = j$, their images in $H^1(K^{\mathrm{unr}}_{\lambda_i}, E_{p^k})$ are not multiples of one another.

1.5 Conclusion

In §1.4, we have chosen a set of auxiliary primes Q that satisfy all the properties for auxiliary primes that are required in Theorem 1.1.7(ii). In addition, we have also constructed a set of $2t-1$ ($t = \#\mathrm{Q}$) ramified classes $c_1, \ldots, c_{2t-1}$ so that if

$$a_1c_1 + \cdots + a_{2t-1}c_{2t-1} = 0 \qquad \text{in } \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{H}^1_{\mathrm{Sel}}\mathrm{K}, \mathrm{E}_{p^k}) \text{ for } a_i \in \mathbb{Z},$$

then $a_i \equiv 0 \pmod p$ for $i \geq 1$ because all the c_i are ramified classes, and the ones that belong to the same eigenspace of $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$ for the action of τ have relatively prime ramification.

Consequently, Theorem 1.1.7 allows us to see that the cohomology classes that we have constructed together with $y \in \mathrm{E}(\mathrm{K})$ generate a subgroup of $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$ containing $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$. Finally, since we have allowed any $p \geq 5$ and Kolyvagin's cohomology classes come from points of E defined over solvable extensions of $\mathbb{Q}$, we have the following.

THEOREM 1.5.1

Every element of $\text{Ш}(\mathrm{E}/\mathrm{K})$ *becomes trivial after a base change by a solvable extension of* $\mathbb{Q}$.

Theorem 0.0.1 of the introduction follows as $\text{Ш}(\mathrm{E}/\mathbb{Q})$ classifies curves of genus one whose Jacobian is E and which have points in all the local fields.

2. General rank case

2.1. Local results

In this section, we let K be any number field. Let ν be a prime of K, and denote by K_ν, k_ν, and $\mathcal{O}_\nu$ the corresponding local field, residue field, and local ring of integers, respectively. Consider the group $\mathrm{E}(\mathrm{K}_\nu)/p^m\mathrm{E}(\mathrm{K}_\nu)$ for some $m \in \mathbb{N}$.

Let $\wp$ be a prime of K which divides p, and let $\mathrm{E}^1(\mathrm{K}_\wp)$ be the group of points of $\mathrm{E}(\mathrm{K}_\wp)$ which map to zero when E is reduced modulo p.

LEMMA 2.1.1

If $\#\mathrm{E}^1(\mathrm{K}_\wp)_{p^\infty} = 0$*, then we have*

$$\#\big(\mathrm{E}(\mathrm{K}_\wp)/p^m\big) = \#\mathrm{E}(\mathrm{K}_\wp)_{p^m} \cdot \#\big(\mathrm{E}^1(\mathrm{K}_\wp)/p^m\big).$$

Proof

The proof of this lemma is exactly the same as the proof of Lemma 1.1.1. □

If ν is a prime of K which does not divide p, we know that $E^1(K_\nu)_p = 0$ and $E^1(K_\nu)/p^m E^1(K_\nu) = 0$. Since the proof of Lemma 2.1.1 does not use the fact that $\wp$ divides p, we also have the following lemma.

LEMMA 2.1.2
Let ν be a prime of K relatively prime to p and $m \in \mathbb{N}$; then

$$\#E(K_\nu)/p^m E(K_\nu) = \#E(K_\nu)_{p^m}.$$

We now prove an additional result for the primes of K which do not divide p.

LEMMA 2.1.3
Suppose that $E(K_\nu)_{p^\infty} = E(K_\nu)_{p^m}$, where ν is a prime of K relatively prime to p and $m \in \mathbb{N}$. Then we have $E(K_\nu)_{p^m} \simeq E(K_\nu)/p^m E(K_\nu)$ under the natural inclusion.

Proof
Since $E(K_\nu)_{p^\infty} = E(K_\nu)_{p^m}$, the inclusion of $E(K_\nu)_{p^m}$ into $E(K_\nu)/p^m E(K_\nu)$ is injective. Lemma 2.1.2 implies that these two groups have the same size and are, therefore, isomorphic. □

2.2. The structure at the base level
Let p be a prime of good ordinary reduction, and let K be an imaginary quadratic extension of $\mathbb{Q}$. We want to understand the structure of the Selmer group $H^1_{\mathrm{Sel}}(K, E_{p^k})$.

2.2.1
In this section, we assume that p is a prime of good ordinary nonanomalous reduction; that is, the reduction of E modulo p has trivial p-torsion over the residue field of $\mathbb{Q}$ at p.

We now fix the number field K to be an imaginary quadratic extension of $\mathbb{Q}$ of discriminant $D_K \neq -3, -4$ so that the conductor N of E splits and p ramifies in $K/\mathbb{Q}$. Denote by Σ the set of primes of K, where E has bad reduction together with $\wp$, the unique prime of K which divides p.

We continue to assume that $\mathrm{Gal}(K(E_p)/K)$ is not solvable. Hence, we know that the natural image of this Galois group in $\mathrm{PGL}_2(\mathbb{F}_p)$ is either the full group or is isomorphic to A_5 (see [S2, Proposition 16]).

Since $H^1_{\mathrm{Sel}}(K, E_{p^\infty})$ is finitely generated, we know that

$$H^1_{\mathrm{Sel}}(K, E_{p^\infty}) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^r \oplus (\text{finite abelian group})$$

for some $r \in \mathbb{N}$. Choose $k \in \mathbb{N}$ so that $p^{k-1} H^1_{\mathrm{Sel}}(K, E_{p^\infty}) = H^1_{\mathrm{Sel}}(K, E_{p^\infty})^{\mathrm{div}}$, the p-divisible subgroup of $H^1_{\mathrm{Sel}}(K, E_{p^\infty})$. Let $s_1, \ldots, s_r \in H^1_{\mathrm{Sel}}(K, E_{p^{2k}})$ be generators of

$H^1_{Sel}(K, E_{p^\infty})^{div}_{p^{2k}}$, the p^{2k}-torsion of $H^1_{Sel}(K, E_{p^\infty})^{div}$. It follows that each s_i has order p^{2k}.

Suppose that Q is a set of primes of $\mathbb{Q}$ with the following properties for $q \in Q$:

(i) q is inert in $K/\mathbb{Q}$;

(ii) $q \notin \Sigma$;

(iii) $E(K_q)_{p^\infty} = E(\overline{K_q})_{p^k}$; and

(iv) $H^1_{Sel}(K, E_{p^k}) \hookrightarrow \prod_{q\in Q} H^1(K_q^{unr}/K_q, E_{p^k})$, where K_q^{unr} denotes the maximal unramified extension of K_q.

Then we suppose that $\Sigma' = \Sigma \cup \{\lambda_i \mid 1 \le i \le r\}$, where $\{\lambda_i \mid 1 \le i \le r\}$ is a set of primes of K not in $\Sigma \cup Q$ such that

(a) $E(K_\lambda)_{p^\infty} = E(\overline{K_\lambda})_{p^{2k}}$ for all $\lambda \in \{\lambda_i \mid 1 \le i \le r\}$; and

(b) the local cohomology class $(s_i)_{\lambda_j}$ has order p^{2k} if $i = j$ and is trivial if $i \ne j$.

As in §1, $K_{\Sigma' \cup Q}$ (resp., $K_{\Sigma'}$) denotes the maximal extension of K which is unramified outside $\Sigma' \cup Q$ (resp., Σ'). Recall that

$$L_\nu = \begin{cases} H^1(K_\nu^{unr}/K_\nu, E_{p^{2k}}), & \nu \in Q, \\ H^1(K_\nu, E_{p^{2k}}), & \nu \in \Sigma'. \end{cases}$$

As before, L_ν^* and Sel_ν^* denote the exact annihilators, respectively, of L_ν and Sel_ν in the pairing

$$H^1(K_\nu, E_{p^{2k}}) \times H^1(K_\nu, E_{p^{2k}}) \to \mathbb{Q}_p/\mathbb{Z}_p. \tag{30}$$

We now have the following lemma, which is very similar to Lemma 1.1.3. The key difference lies in the fact that r may not be 1 in this case.

LEMMA 2.2.1

The group $H^1{}_{L^*}(K_{\Sigma'\cup Q}/K, E_{p^{2k}})$ *is contained in* $H^1_{Sel}(K, E_{p^k})$.

Proof

By properties of local duality, we know that

$$L_\nu^* = \begin{cases} H^1(K_\nu^{unr}/K_\nu, E_{p^{2k}}), & \nu \in Q, \\ 0, & \nu \in \Sigma'. \end{cases}$$

This implies that $H^1{}_{L^*}(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) \subset H^1_{Sel}(K, E_{p^{2k}})$. By the choice of k so that $p^{k-1}H^1_{Sel}(K, E_{p^\infty}) = H^1_{Sel}(K, E_{p^\infty})^{div}$, we have an exact sequence

$$0 \longrightarrow H^1_{Sel}(K, E_{p^k}) \longrightarrow H^1_{Sel}(K, E_{p^{2k}}) \xrightarrow{p^k} \prod_{i=1}^r (\mathbb{Z}/p^{2k}\mathbb{Z})p^k s_i \longrightarrow 0. \tag{31}$$

We observe that

$$p^k \mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \subseteq \langle s_1, \ldots, s_r \rangle$$

by our choice of classes $s_1, \ldots, s_r$, and all we have to show is that the left-hand side is actually zero. This follows from the assumption that there exists $\lambda \in \Sigma' \setminus \Sigma$ such that $p^{2k-1} s_\lambda \neq 0$ in $\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})$, as this implies that

$$\langle s_1, \ldots, s_r \rangle \cap \mathrm{H}^1{}_{\mathrm{L}^*}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) = 0$$

and concludes our proof. □

PROPOSITION 2.2.2
The following sequence is exact:

$$0 \longrightarrow \mathrm{H}^1{}_{\mathrm{L}}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \mathrm{H}^1{}_{\mathrm{L}_\mathrm{Q}}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}})$$

$$\longrightarrow \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q \longrightarrow 0.$$

Proof
The proof of this proposition is the same as that of Lemma 1.1.5. The assumption that E/K has analytic rank 1 enters the proof of Lemma 1.1.5 only through the use of Lemma 1.1.3, which in the general rank case is substituted by the same result proved in Lemma 2.2.1. □

Observe that

$$\mathrm{H}^1{}_{\mathrm{L}}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}})$$

and

$$\mathrm{H}^1{}_{\mathrm{L}_\mathrm{Q}}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}).$$

Consequently, Proposition 2.2.2 gives us the exact sequence

$$0 \longrightarrow \mathrm{H}^1(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \mathrm{H}^1(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}})$$
$$\longrightarrow \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q \longrightarrow 0.$$

The second and third properties of the primes in Q and Lemma 2.1.3 imply that for $q \in \mathrm{Q}$,

$$\mathrm{L}_q^* = \mathrm{L}_q = \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}) \simeq \mathrm{E}(\mathrm{K}_q)/p^{2k}\mathrm{E}(\mathrm{K}_q) \simeq \mathrm{E}(\mathrm{K}_q)_{p^k} \simeq \mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^k\mathbb{Z}.$$

Then using the nondegeneracy of the pairing (30), we conclude that

$$\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q \simeq \mathbb{Z}/p^k\mathbb{Z} \oplus \mathbb{Z}/p^k\mathbb{Z}. \tag{32}$$

We now show that when we restrict the above cohomology groups to the Selmer condition for $\lambda \in \Sigma'$, we end up missing exactly r generators of $\prod_{q\in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q$.

PROPOSITION 2.2.3
The cokernel of the last map in the exact sequence

$$0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}_{\Sigma'\cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q$$

is isomorphic to $(\mathbb{Z}/p^k\mathbb{Z})^r$.

Proof
The following proof is essentially the same as the proof of Proposition 1.1.6, except that in this case, we may have $r \neq 1$.

Recall our notation that Sel_Q imposes no local condition at primes in Q. Set $W = \prod_{\nu\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\nu(p^{2k})$, where $\mathrm{Sel}_\nu(p^{2k})$ denotes the image of $\mathrm{E}(\mathrm{K}_\nu)/p^{2k}\mathrm{E}(\mathrm{K}_\nu)$ in $\mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}_{p^{2k}})$. By applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{H}^1(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \mathrm{H}^1(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow & & \\
0 & \longrightarrow & \mathrm{W} & \longrightarrow & \mathrm{W} & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

we get

$$\begin{array}{ccccccc}
0 \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q & \\
 & & & & & \downarrow & \\
 & 0 & \longleftarrow & \operatorname{coker}\phi_2 & \xleftarrow{\ \gamma_0\ } & \operatorname{coker}\phi_1 &
\end{array} \tag{33}$$

Seeing the maps ϕ_1 and ϕ_2 as part of the corresponding exact sequences of Cassels, Poitou, and Tate, we have

$$\begin{array}{ccccc}
\mathrm{H}^1(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \xrightarrow{\phi_1} & \prod_{\nu\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\nu(p^{2k}) & \xrightarrow{\psi_1} & \mathrm{H}^1_{\mathrm{Sel}^*}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})} \\
\downarrow & & \downarrow & & \downarrow \\
\mathrm{H}^1(\mathrm{K}_{\Sigma'\cup\mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) & \xrightarrow{\phi_2} & \prod_{\nu\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\nu(p^{2k}) & \xrightarrow{\psi_2} & \mathrm{H}^1_{(\mathrm{Sel}_\mathrm{Q})^*}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})}
\end{array} \tag{34}$$

Now, we need to study the maps ψ_i since $\operatorname{coker}\phi_i \simeq \operatorname{im}\psi_i$ for $i = 1, 2$.

As we saw in the proof of Proposition 1.1.6, $\mathrm{Sel}_\nu(p^{2k}) = \mathrm{Sel}^*_\nu(p^{2k})$ for all ν. Therefore, we have

$$\mathrm{H}^1_{\mathrm{Sel}^*}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \quad \text{and} \quad \mathrm{H}^1_{(\mathrm{Sel}_\mathrm{Q})^*}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}),$$

where $\mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ is the subgroup of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ consisting of classes that are locally trivial at primes in Q.

We know that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ maps to $\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k})$ under the localization map for $q \in \mathrm{Q}$. Then by property (iii) of the prime $q \in \mathrm{Q}$, we have the map

$$\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^k}) \to \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}) \text{ is zero for all } q \in \mathrm{Q}.$$

This implies that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ maps to zero in $\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}})$ for all $q \in \mathrm{Q}$, and therefore,

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \subset \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}).$$

We show that these two groups are equal. Let $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ be an element of order p^{2k}. Property (iv) of the set Q implies that there exists a prime $q \in \mathrm{Q}$ such that the localization of $p^{2k-1}s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ at the prime q, $p^{2k-1}s_q \neq 0$ in $\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^k})$. Since $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$, there exists $y' \in \mathrm{E}(\mathrm{K}_q)$ such that $s_q(\sigma) = \sigma(y'/p^{2k}) - y'/p^{2k}$. It follows that $y' \neq py''$ in $\mathrm{E}(\mathrm{K}_q)$, and Lemma 2.1.3 implies that $y' = p^{2k}y'' + e_{p^k}$, where $y'' \in \mathrm{E}(\mathrm{K}_q)$ and $e_{p^k} \in \mathrm{E}(\mathrm{K}_q)_{p^k} - \mathrm{E}(\mathrm{K}_q)_{p^{k-1}}$. We then see that $p^i s \in \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ if and only if $i \geq k$, which is equivalent to $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \supset \mathrm{H}^1_{\mathrm{Sel}^\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$.

So, the right-hand-side square of (34) may be viewed as

$$\begin{array}{ccc}
\prod_{\nu\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\nu(p^{2k}) & \xrightarrow{\psi_1} & \mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})} \\
\downarrow & & \downarrow \\
\prod_{\nu\in\Sigma'} \mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\nu(p^{2k}) & \xrightarrow{\psi_2} & \mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^{k}})}
\end{array}$$

and the map $\gamma : \mathrm{im}\psi_1 \to \mathrm{im}\psi_2$ is simply the restriction of an element of $\mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})}$ to $\mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^k})}$. We now show that $\ker\gamma \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$.

In order to better understand the maps ψ_1 and ψ_2, we consider the following compatible nondegenerate pairings for $\nu \in \Sigma'$:

$$\begin{array}{ccccc}
\mathrm{H}^1(\mathrm{K}_\nu, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\nu(p^{2k}) & \times & \mathrm{Sel}_\nu(p^{2k}) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p \\
\psi_1 \downarrow & & \uparrow \mathrm{Res}_\nu & & \\
\mathrm{H}^1_{\mathrm{Sel}}\widehat{(\mathrm{K}, \mathrm{E}_{p^{2k}})} & \times & \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) & \longrightarrow & \mathbb{Q}_p/\mathbb{Z}_p
\end{array}$$

We know that $p^k \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) = 0$, and consequently, the order of every element of $\operatorname{im}\psi_2$ divides p^k. We aim to construct a subgroup of $\operatorname{im}\psi_1$ isomorphic to $(\mathbb{Z}/p^{2k}\mathbb{Z})^r$ because then $p^k s \in \ker\gamma$ for all $s \in \operatorname{im}\psi_1$ of order p^{2k}.

We have ensured that for each $s \in \{s_1, \dots, s_r\}$, there is a corresponding prime $\lambda \in \Sigma' - \Sigma$ so that $p^{2k-1}s_\lambda \neq 0$ in $\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})$. Consider $\mathrm{Res}_\lambda(s)$. The cohomology class $\mathrm{Res}_\lambda(s)$ is of order p^{2k}. It follows that there exists an element $s^*_\lambda \in \mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k})$ which pairs with $\mathrm{Res}_\lambda(s)$ to give a generator of $\mathbb{Z}/p^{2k}\mathbb{Z}$. Consequently, we see that $\psi_1(s^*_\lambda)$ has order p^{2k}. Furthermore, property (b) of $\lambda \in \Sigma' - \Sigma$ implies that $\psi_1(s^*_\lambda)(s') = 0$ for all $s' \in \{s_1, \dots, s_r\} \setminus \{s\}$. It then follows that

$$\langle \psi_1(s^*_\lambda) \mid s \in \{s_1, \dots, s_r\}\rangle \simeq (\mathbb{Z}/p^{2k}\mathbb{Z})^r.$$

Since, by (31),

$$0 \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^r \longrightarrow \widehat{\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}})} \longrightarrow \widehat{\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})} \longrightarrow 0, \qquad (35)$$

we conclude that $\ker\gamma \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$, which also shows that $\ker\gamma_0 \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$ in (33). This completes the proof of the proposition. □

PROPOSITION 2.2.4
The group $\mathrm{H}^1_{\mathrm{Sel_Q}}(\mathrm{K}, \mathrm{E}_{p^k})$ *is isomorphic to* $(\mathbb{Z}/p^k\mathbb{Z})^{2t}$, *where* $t = \#\mathrm{Q}$.

Proof
This is a generalization of Theorem 1.1.7(i).

Since $p^{k-1}\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^\infty}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^\infty})^{\mathrm{div}}$, we can write

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^r \times \mathbb{Z}/p^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{m_{2t-r}}\mathbb{Z},$$

where each $m_i < k$. Let us consider the map

$$\mathrm{H}^1_{\mathrm{Sel_Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}}). \qquad (36)$$

The fact that $\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{L}_q \simeq (\mathbb{Z}/p^k\mathbb{Z})^2$ for each $q \in \mathrm{Q}$ by (32), together with Proposition 2.2.3, implies that

$$0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \mathrm{H}^1_{\mathrm{Sel_Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^{2t-r} \longrightarrow 0. \qquad (37)$$

Just as in the proof of Theorem 1.1.7(i), we use sequences (35) and (37) to see that

$$\operatorname{im}\Big(\mathrm{H}^1_{\mathrm{Sel_Q}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}, \mathrm{E}_{p^{2k}})\Big) \simeq (\mathbb{Z}/p^k\mathbb{Z})^{2t-r}$$

and

$$\mathrm{im}\Big(\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q \in \mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}})\Big) \simeq (\mathbb{Z}/p^k\mathbb{Z})^r.$$

Consequently, the map (36) gives rise to the exact sequence

$$0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_{\Sigma'}/\mathrm{K}, \mathrm{E}_{p^k}) \longrightarrow \mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^{2t} \longrightarrow 0.$$

Since we also know that $\#\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k}) = p^{2kt}$, it follows that

$$\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^{2k}}) \simeq (\mathbb{Z}/p^{2k}\mathbb{Z})^r \times \mathbb{Z}/p^{k+m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{k+m_{2t-r}}\mathbb{Z},$$

and hence,

$$\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}_{\Sigma' \cup \mathrm{Q}}/\mathrm{K}, \mathrm{E}_{p^k}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^{2t}. \qquad \square$$

2.2.2

In this section, we assume that p is a prime of good ordinary anomalous reduction (i.e., the reduction of E modulo p has nontrivial p-torsion over the residue field of $\mathbb{Q}$ at p) and that it is inert in $\mathrm{K}/\mathbb{Q}$. In this case, instead of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$, we must consider a bigger subgroup of $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^k})$. The reason for this is that in the anomalous case, the Selmer condition is not well behaved under taking invariants in a $\mathbb{Z}_p$-tower (see §2.3.2). The only difference between $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^k})$ and this new group lies at the local condition at $\wp$, the only prime of K lying above p.

Let $\mathrm{Sel}'_\wp(p^k)$ be a subgroup of $\mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^k})$ so that

(i) $\mathrm{Sel}_\wp(p^k) \subseteq \mathrm{Sel}'_\wp(p^k)$; and

(ii) $\#(\mathrm{Sel}'_\wp(p^k)/\mathrm{Sel}_\wp(p^k))$ is bounded by a constant that does not depend on k.

The group $\mathrm{Sel}'_\wp(p^k)$ is defined in §2.3.2. Consider the exact sequence

$$0 \longrightarrow \mathrm{E}(\mathrm{K}_\wp)_{p^k} \longrightarrow \mathrm{E}(\mathrm{K}_\wp)_{p^k+1} \longrightarrow \mathrm{E}(\mathrm{K}_\wp)_p \longrightarrow \mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^k}) \xrightarrow{\varphi_k} \mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^{k+1}}).$$

As we see in §2.3.2, $\mathrm{Sel}'_\wp(p^k) = \varphi_k^{-1}\mathrm{Sel}'_\wp(p^{k+1})$, and the size of the group $\mathrm{Sel}'_\wp(p^k)/\mathrm{Sel}_\wp(p^k)$ does not decrease as $k \to \infty$.

In addition to the condition that $p^{k-1}\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^\infty}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^\infty})^{\mathrm{div}}$, in the case when p is a prime of good ordinary anomalous reduction, we also assume that

$$p^k > \#\big(\mathrm{Sel}'_\wp(p^k)/\mathrm{Sel}_\wp(p^k)\big).$$

It follows in the same way that $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^{2t}$, where $t = \#\mathrm{Q}$. In addition, we have $\mathrm{H}^1_{\mathrm{Sel}_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k}) \subseteq \mathrm{H}^1_{\mathrm{Sel}'_\mathrm{Q}}(\mathrm{K}, \mathrm{E}_{p^k})$, and by computing the sizes of these two groups, we see that

$$\#\mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}}}(\mathrm{K}, \mathrm{E}_{p^k})/\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}}}(\mathrm{K}, \mathrm{E}_{p^k}) = \#\mathrm{Sel}'_{\wp}(p^k)/\#\mathrm{Sel}_{\wp}(p^k).$$

We have then proved the following proposition.

PROPOSITION 2.2.5
The group $\mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}}}(\mathrm{K}, \mathrm{E}_{p^k})$ *is isomorphic to* $(\mathbb{Z}/p^k)^{2t} \oplus \mathrm{N}_{\mathrm{Q}}$, *where* N_{Q} *is a finite group of order bounded independently of* k.

2.3. Generalized unramified-under-ramified principle
Let us consider $\widetilde{\mathrm{K}}_\infty = \bigcup_{n \geq 1} \mathrm{K}[p^n]$, where $\mathrm{K}[p^n]$ denotes the ring class field of K of conductor p^n. Then the group $\mathrm{Gal}(\widetilde{\mathrm{K}}_\infty/\mathrm{K})$ is isomorphic to $\mathbb{Z}_p \times \Delta$, where Δ is a finite abelian group. The unique $\mathbb{Z}_p$-extension contained in $\widetilde{\mathrm{K}}_\infty$ is denoted by K_∞ and called the anticyclotomic $\mathbb{Z}_p$-extension. Let K_n be the subextension of K_∞ of degree p^n over K, and denote by $\mathrm{K}[p^{k(n)}]$ the minimal ring class field of p-power conductor containing K_n. (Throughout this section, we use K_n in this sense. Note that in §1, we write K_r for the ring class field of conductor r, but this should not cause any confusion.) The motivation for using the anticyclotomic $\mathbb{Z}_p$-extension is that we can construct cohomology classes, which are introduced in §2.5.1.

2.3.1
In this section, we consider the case where p is a prime of good ordinary nonanomalous reduction. Recall that in this case, we choose the extension $\mathrm{K}/\mathbb{Q}$ so that p ramifies (see §2.2.1).

Choose n_0 so that

(1) $p^{n_0-1}\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^\infty}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^\infty})^{\mathrm{div}}$; and

(2) $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_{p^{n+1}})/\mathrm{K}(\mathrm{E}_{p^n}))$, viewed as a subgroup of $\mathrm{GL}(2, \mathbb{Z}/p^{n+1}\mathbb{Z})$, consists of all matrices of the form

$$\begin{pmatrix} 1 + p^n a & p^n b \\ p^n c & 1 + p^n d \end{pmatrix} \quad \text{for } a, b, c, d \in \mathbb{Z}/p\mathbb{Z}$$

for all $n \geq n_0$. Serre [S2] has shown that the index of $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_{p^k})/\mathrm{K})$ in $\mathrm{GL}(2, \mathbb{Z}/p^k\mathbb{Z})$ is finite and depends only on E and K. This implies that condition (2) is satisfied for some big-enough n_0. (Recall that we are assuming that E does not have complex multiplication.)

We fix any $n \geq n_0$ and consider the Selmer group $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, where $m_n \geq n$, the sequence $\{m_n\}_{n \in \mathbb{N}}$ is strictly increasing, and $\mathrm{E}(\mathrm{K}_{\nu_n})_{p^\infty} \subset \mathrm{E}(\mathrm{K}_{\nu_n})_{p^{m_n}}$ for all primes $\nu_n | \mathrm{N}$ of K_n, where K_{ν_n} denotes the completion of K_n at ν_n.

Suppose that Q_n is a set of primes of $\mathbb{Q}$ with the following properties for $q \in \mathrm{Q}_n$:

(i) q is inert in $\mathrm{K}/\mathbb{Q}$;

(ii) $q \notin \Sigma$;

(iii) $\mathrm{E}(\mathrm{K}_{q_n})_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_{q_n}})_{p^{m_n}}$, where q_n denotes any prime of K_n above q and K_{q_n} is the completion of K_n at q_n; and

(iv) $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{q \in \mathrm{Q}_n} \mathrm{H}^1(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}})$, where $\mathrm{H}^1(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}}) := \bigoplus_{q_n|q} \mathrm{H}^1(\mathrm{K}_{q_n}^{\mathrm{unr}}/\mathrm{K}_{q_n}, \mathrm{E}_{p^{m_n}})$ and $\mathrm{K}_{q_n}^{\mathrm{unr}}$ denotes the maximal unramified extension of K_{q_n}.

Denote by G_m the Galois group $\mathrm{Gal}(\mathrm{K}_m/\mathrm{K})$, and denote by t the number of rational primes in Q_n. (A similar notational remark applies to G_m, as was made earlier for K_n. In §1, G_m was $\mathrm{Gal}(\mathrm{K}_m/\mathrm{K}_1)$, and K_m referred to the ring class field of conductor m.) When choosing Q_n, we ensure that its size does not depend on n.

PROPOSITION 2.3.1

The following holds for all $m \le n$ and $k \le m_n$:

$$\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_m, \mathrm{E}_{p^k}) = \#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t}.$$

Proof

We know that

$$\mathrm{H}^1_{\mathrm{Sel}^*}(\mathrm{K}_m, \mathrm{E}_{p^k}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_m, \mathrm{E}_{p^k}) \subset \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{q \in \mathrm{Q}_n} \mathrm{H}^1\big(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}}\big),$$

which implies that $\mathrm{H}^1_{(\mathrm{Sel}_{\mathrm{Q}_n})^*}(\mathrm{K}_m, \mathrm{E}_{p^k}) = \mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n}}(\mathrm{K}_m, \mathrm{E}_{p^k}) \subset \mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) = 0$. Then, as in [Wi, Proposition 1.6], we have

$$\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_m, \mathrm{E}_{p^k}) = p^{2kp^m} \prod_{q \in \mathrm{Q}_n} \#\mathrm{E}\big(\mathrm{K}_m(q)\big)_{p^k} \prod_{\nu_m | \nu \in \Sigma} \frac{\#\mathrm{E}(\mathrm{K}_{\nu_m})_{p^k}}{[\mathrm{H}^1(\mathrm{K}_{\nu_m}, \mathrm{E}_{p^k}) : \mathrm{Sel}_{\nu_m}(p^k)]},$$

where $\mathrm{E}(\mathrm{K}_m(q))_{p^k} = \bigoplus_{q_m|q} \mathrm{E}(\mathrm{K}_{q_m})_{p^k}$.

Using the fact that $k \le m_n$, the properties of the elements of Q_n imply that $\mathrm{E}(\mathrm{K}_{q_m})_{p^k} = (\mathbb{Z}/p^k\mathbb{Z})^2$, and therefore, $\mathrm{E}(\mathrm{K}_m(q))_{p^k} \simeq (\mathbb{Z}/p^k\mathbb{Z}[G_m])^2$.

Using the fact that $\mathrm{Sel}_{\nu_m}(p^k)$ is its own exact annihilator under the pairing (30) for all primes ν_m of K_m (see the proof of Proposition 1.1.6), we deduce that

$$\#\mathrm{H}^1(\mathrm{K}_{\nu_m}, \mathrm{E}_{p^k}) = \big(\#\mathrm{Sel}_{\nu_m}(p^k)\big)^2 \quad \text{for all } \nu_m.$$

Lemma 2.1.2 implies that

$$\#\mathrm{Sel}_{\nu_m}(p^k) = \#\mathrm{E}(\mathrm{K}_{\nu_m})_{p^k} \quad \text{for } \nu_m | \nu \in \Sigma \setminus \{p\},$$

and consequently,

$$\prod_{\nu_m|\nu\in\Sigma\setminus\{p\}} \frac{\#\mathrm{E}(\mathrm{K}_{\nu_m})_{p^k}}{[\mathrm{H}^1(\mathrm{K}_{\nu_m},\mathrm{E}_{p^k}):\mathrm{Sel}_{\nu_m}(p^k)]} = 1.$$

Since $\mathrm{E}^1(\mathrm{K}_{\wp_m}) \simeq \mathcal{O}_{\wp_m}$, by Lemma 2.1.1 we know that $\#\mathrm{Sel}_{\wp_m}(p^k) = [\mathcal{O}_{\wp_m} : p^k\mathcal{O}_{\wp_m}] \cdot \#\mathrm{E}(\mathrm{K}_{\wp_m})_{p^k}$. It then follows that

$$\prod_{\wp_m|p} \frac{\#\mathrm{E}(\mathrm{K}_{\wp_m})_{p^k}}{[\mathrm{H}^1(\mathrm{K}_{\wp_m},\mathrm{E}_{p^k}):\mathrm{Sel}_{\wp_m}(p^k)]} = \prod_{\wp_m|p} \frac{1}{[\mathcal{O}_{\wp_m} : p^k\mathcal{O}_{\wp_m}]} = p^{-2kp^m}.$$

We can now conclude that

$$\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_m,\mathrm{E}_{p^k}) = \prod_{q\in\mathrm{Q}_n} \#\mathrm{E}\big(\mathrm{K}_m(q)\big)_{p^k} = \#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t},$$

where $t = \#\mathrm{Q}_n$. □

PROPOSITION 2.3.2

The following is true for all $n \geq n_0$:

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K},\mathrm{E}_{p^{m_n}}) \simeq (\mathbb{Z}/p^{m_n}\mathbb{Z})^{2t}.$$

Proof

This statement follows from Proposition 2.2.4 if we can show that Q_n satisfies the properties of the set Q stated in §2.2.1. The elements of Q_n are chosen to be rational primes of good reduction and different from p which are inert in $\mathrm{K}/\mathbb{Q}$. Furthermore, since elements of the set Q_n split completely in K_n/K, it follows that

$$\mathrm{E}(\mathrm{K}_q)_{p^\infty} = \mathrm{E}(\mathrm{K}_{q_n})_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_q})_{p^{m_n}}.$$

Therefore, the only property that remains to be verified is that the primes of Q_n control $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K},\mathrm{E}_{p^{m_n}})$ or, equivalently, that $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K},\mathrm{E}_{p^{m_n}}) \to \prod_{q\in\mathrm{Q}_n}\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q,\mathrm{E}_{p^{m_n}})$ is injective. This last property follows from the fact that we are assuming that $\mathrm{E}(\mathrm{K}_n)_{p^\infty} = 0$, which implies that

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K},\mathrm{E}_{p^{m_n}}) \hookrightarrow \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n,\mathrm{E}_{p^{m_n}}),$$

and consequently,

$$\mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n}}(\mathrm{K},\mathrm{E}_{p^{m_n}}) \hookrightarrow \mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n}}(\mathrm{K}_n,\mathrm{E}_{p^{m_n}}) = 0.$$

Since $\mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n}}(\mathrm{K},\mathrm{E}_{p^{m_n}}) = \ker\big(\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K},\mathrm{E}_{p^{m_n}}) \to \prod_{q\in\mathrm{Q}_n}\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q,\mathrm{E}_{p^{m_n}})\big)$, this concludes the proof of the proposition. □

We now relate the groups $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ to each other as n grows.

PROPOSITION 2.3.3
The following holds for all $m \leq n$:

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m} = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_m, \mathrm{E}_{p^{m_n}}).$$

Proof
We know that $\mathrm{E}(\mathrm{K}_n)_p = 0$, and consequently,

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m} \subset \mathrm{H}^1(\mathrm{K}_m, \mathrm{E}_{p^{m_n}}).$$

We need to compute the image of $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m}$ in $\mathrm{H}^1(\mathrm{K}_{\nu_m}, \mathrm{E}_{p^{m_n}})$ for all primes ν_m of K_m.

Let ν_m be a prime of K_m of good reduction which does not divide any of the elements of $\mathrm{Q}_n \cup \{p\}$, and let ν_n be a prime of K_n dividing ν_m. Since $\mathrm{Sel}_{\nu_n}(p^{m_n}) = \mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{\nu_n}/\mathrm{K}_{\nu_n}, \mathrm{E}_{p^{m_n}})$, it follows that the image of $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m}$ in $\mathrm{H}^1(\mathrm{K}_{\nu_m}, \mathrm{E}_{p^{m_n}})$ is unramified, or equivalently, it lies in $\mathrm{Sel}_{\nu_m}(p^{m_n})$.

Let us now consider primes ν_m of K_m, where E has bad reduction. Our choice of m_n (such that $\mathrm{E}(\mathrm{K}_{\nu_n})_{p^\infty} \subset \mathrm{E}_{p^{m_n}}$) and Lemma 2.1.2 together imply that $\mathrm{E}(\mathrm{K}_{\nu_n})/p^{m_n} = \mathrm{E}(\mathrm{K}_{\nu_n})_{p^{m_n}}$. Since

$$\left(\mathrm{E}(\mathrm{K}_{\nu_n})/p^{m_n}\right)^{G_n/G_m} = \left(\mathrm{E}(\mathrm{K}_{\nu_n})_{p^{m_n}}\right)^{G_n/G_m} = \mathrm{E}(\mathrm{K}_{\nu_m})_{p^{m_n}} = \mathrm{E}(\mathrm{K}_{\nu_m})/p^{m_n},$$

we see that the image of $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m}$ in $\mathrm{H}^1(\mathrm{K}_{\nu_m}, \mathrm{E}_{p^{m_n}})$ lies in $\mathrm{Sel}_{\nu_m}(p^{m_n})$.

Finally, we must consider the primes $\wp_m | p$. We start by studying $\varinjlim_k \mathrm{E}(\mathrm{K}_{\wp_m})/p^k$. We show that

$$\left(\varinjlim_k \mathrm{E}(\mathrm{K}_{\wp_n})/p^k\right)^{G_n/G_m} = \varinjlim_k \mathrm{E}(\mathrm{K}_{\wp_m})/p^k, \quad \forall n \geq m.$$

We have the exact sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{E}^1(\mathrm{K}_{\wp_n})_{p^\infty} &\longrightarrow \mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty} \\ &\longrightarrow \widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})_{p^\infty} \longrightarrow \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}^1_{p^\infty}) \xrightarrow{\epsilon_n} \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty}), \end{aligned} \tag{38}$$

where $\widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})$ denotes the points of $\widetilde{\mathrm{E}}$ over the residue field of $\mathrm{K}_{\wp_n}$. Greenberg [G, Theorem 2.8] has shown that $\varinjlim_k \mathrm{E}(\mathrm{K}_{\wp_n})/p^k = \mathrm{im}\,\epsilon_n$ if p is a prime of ordinary nonanomalous reduction.

Since $\mathrm{Gal}(\mathrm{K}_{\wp_n}/\mathbb{Q}_p)$ is a dihedral group and $\mathrm{E}^1(\mathrm{K}_\wp) \simeq \mathcal{O}_\wp$, it follows that $\mathrm{E}^1(\mathrm{K}_{\wp_n})_{p^\infty} = \mathrm{E}^1(\mathrm{K}_\wp)_{p^\infty} = 0$. Recall that since we are assuming that E has good ordinary reduction at p, the action of $\mathrm{Gal}(\overline{\mathrm{K}_\wp}/\mathrm{K}_\wp)$ has the form $\begin{pmatrix} \chi\epsilon & * \\ 0 & \chi^{-1} \end{pmatrix}$, where χ is an unramified character and ϵ is the cyclotomic character. This implies that $\mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}^1_{p^\infty}) = \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}^1_{p^\infty})^{G_n/G_m}$. Furthermore, $\widetilde{\mathrm{E}}(\mathrm{K}_\wp)_{p^\infty} = 0$, and hence, $\widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})_{p^\infty} = 0$. Consequently, we have

$$\operatorname{im}\epsilon_m = (\operatorname{im}\epsilon_n)^{G_n/G_m} \qquad \text{and} \qquad \mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty} = \mathrm{E}(\mathrm{K}_\wp)_{p^\infty} = 0.$$

We now show that $\mathrm{E}(\mathrm{K}_{\wp_m})/p^k = (\mathrm{E}(\mathrm{K}_{\wp_n})/p^k)^{G_n/G_m}$. Since $\mathrm{E}(\mathrm{K}_{\wp_n})_{p^k} = 0$, we may conclude that $\mathrm{E}(\mathrm{K}_{\wp_m})/p^k$ maps injectively into $(\mathrm{E}(\mathrm{K}_{\wp_n})/p^k)^{G_n/G_m}$, and we may conclude that the maps $\psi_{k,r}$ used to define the direct limit $\varinjlim_k \mathrm{E}(\mathrm{K}_{\wp_n})/p^k$ are injective:

$$0 = \mathrm{E}(\mathrm{K}_{\wp_n})_{p^r}/p^k\mathrm{E}(\mathrm{K}_{\wp_n})_{p^{k+r}} \longrightarrow \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^k}) \xrightarrow{\psi_{k,r}} \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^{k+r}}).$$

Let $s \in (\mathrm{E}(\mathrm{K}_{\wp_n})/p^k)^{G_n/G_m} - (\mathrm{E}(\mathrm{K}_{\wp_m})/p^k)$. Since

$$\left(\varinjlim_k \mathrm{E}(\mathrm{K}_{\wp_n})/p^k\right)^{G_n/G_m} = \varinjlim_k \mathrm{E}(\mathrm{K}_{\wp_m})/p^k,$$

it follows that $\psi_{k,r}(s) = 0$ or $s \in \mathrm{E}(\mathrm{K}_{\wp_m})/p^{k+r}$ for some $r \geq 1$. In the first case, $s = 0$ since $\psi_{k,r}(s)$ is injective. In the second case, we know that $p^k s = 0$, which implies that $s \in \mathrm{E}(\mathrm{K}_{\wp_m})/p^k$.

We can now conclude that $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m} = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_m, \mathrm{E}_{p^{m_n}})$. □

Let $\mathrm{R}_n := \mathbb{Z}/p^{m_n}\mathbb{Z}[G_n]$, and let $\mathrm{R}_n^\tau := \mathbb{Z}/p^{m_n}\mathbb{Z}[G_n \rtimes \langle\tau\rangle]$, where τ is an element of $\mathrm{Gal}(\mathrm{K}_\infty/\mathbb{Q})$ such that $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}) = \langle\tau\rangle$. We now consider the R_n^τ-modules

$$\mathrm{X}(k, n) = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_k}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \quad \text{for all } n \leq k.$$

We inductively choose an infinite subsequence of $\mathrm{X}_n \in \{\mathrm{X}(k, n) \mid k \geq n\}$ by requiring its elements to be compatible in the following way. (This is motivated by the construction in [TW].)

The elements of the set $\mathscr{S}_{n_0} = \{\mathrm{X}(k, n_0) \mid k \geq n_0\}$ are finite $\mathrm{R}^\tau_{n_0}$-modules. It then follows that infinitely many $\mathrm{X}(k, n_0)$ have the same $\mathrm{R}^\tau_{n_0}$-module structure. We choose one element of this infinite compatible subset and denote it by

$$\mathrm{X}_{n_0} = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k_{n_0}}}}(\mathrm{K}_{n_0}, \mathrm{E}_{p^{m_{n_0}}}).$$

We now consider the set

$$\mathscr{S}_{n_0+1} = \left\{\mathrm{X}(k, n_0+1) \,\middle|\, k \geq n_0+1 \text{ and } \mathrm{X}(k, n_0) \simeq \mathrm{X}_{n_0} \text{ as } \mathrm{R}^\tau_{n_0}\text{-modules}\right\}.$$

The elements of $\mathscr{S}_{n_0+1}$ are finite $\mathrm{R}^\tau_{n_0+1}$-modules, and therefore, infinitely many of them have the same $\mathrm{R}^\tau_{n_0+1}$-module structure. We choose one element of this infinite compatible subset and denote it by X_{n_0+1}.

We continue this process to obtain an infinite compatible sequence of modules X_n. Set $\Gamma = \mathrm{Gal}(K_\infty/K)$, and then define the $\mathbb{Z}_p[[\Gamma]]$-module

$$\mathscr{M} := \varinjlim_{n \geq n_0} X_n,$$

where the maps are chosen inductively as above. (The maps are not defined in any natural way on cohomology groups.)

Let $\widehat{\mathscr{M}}$ denote the Pontryagin dual of the module $\mathscr{M}$. We view $\widehat{\mathscr{M}}$ as a Λ-module, where $\Lambda = \mathbb{Z}_p[[T]]$ and T acts on $\mathscr{M}$ through $\gamma - 1$, where $\Gamma = \langle \gamma \rangle$.

THEOREM 2.3.4
The Λ-module $\widehat{\mathscr{M}}$ is isomorphic to Λ^{2t}.

Proof
By Proposition 2.3.3, we know that $H^1_{\mathrm{Sel}_{Q_{k_n}}}(K_n, E_{p^{m_n}})^{G_n} = H^1_{\mathrm{Sel}_{Q_{k_n}}}(K, E_{p^{m_n}})$. One can then see that

$$H^1_{\mathrm{Sel}_{Q_{k_n}}}(K, E_p) = H^1_{\mathrm{Sel}_{Q_{k_n}}}(K, E_{p^{m_n}})[p] = H^1_{\mathrm{Sel}_{Q_{k_n}}}(K_n, E_{p^{m_n}})^{G_n}[p],$$

and consequently,

$$H^1_{\mathrm{Sel}_{Q_{k_n}}}(K, E_p) \simeq \mathscr{M}[T, p] \quad \text{for all } n \geq n_0.$$

This implies that

$$\widehat{\mathscr{M}}/(p, T) \simeq \widehat{H^1_{\mathrm{Sel}_{Q_{k_n}}}(K, E_p)} \quad \text{for any } n \geq n_0.$$

Since, as a Λ-module, $\widehat{\mathscr{M}}$ has the same number of generators as $\widehat{\mathscr{M}}/(p, T)$, Proposition 2.3.2 implies that $\widehat{\mathscr{M}}$ has $2t$ generators. It then follows that there is a surjective map

$$\psi : \Lambda^{2t} \to \widehat{\mathscr{M}}.$$

In order to show that ψ is an injection, we consider $\widehat{\mathscr{M}}/(p^k, (1+T)^{p^m} - 1)$. On the one hand, we know that

$$\Lambda^{2t}/\big(p^k, (1+T)^{p^m} - 1\big) \simeq (\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t}.$$

On the other hand,

$$\widehat{\mathscr{M}}/\big(p^k, (1+T)^{p^m} - 1\big) \simeq \widehat{H^1_{\mathrm{Sel}_{Q_{k_n}}}(K_m, E_{p^k})} \quad \text{for any } n \geq m \text{ and } n_0 \leq k \leq m_n.$$

Proposition 2.3.1 implies that $\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k_n}}}(\mathrm{K}_m, \mathrm{E}_{p^k}) = \#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t}$, and consequently,

$$\#\Lambda^{2t}/\big(p^k, (1+\mathrm{T})^{p^m}-1\big) = \#\widehat{\mathscr{M}}/\big(p^k, (1+\mathrm{T})^{p^m}-1\big).$$

It follows that $\ker\psi \subset (p^k, (1+\mathrm{T})^{p^m}-1)$. Since k and m are not bounded, we have shown that $\ker\psi = 0$, which concludes the proof of the theorem. □

2.3.2

In this section, we define the group $\mathrm{Sel}'_{\wp_n}(p^k) \subseteq \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^k})$ and understand the structure of $\mathrm{H}^1_{\mathrm{Sel}'}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ as n varies in the case where p is a prime of good ordinary anomalous reduction. Notice that since p is inert in $\mathrm{K}/\mathbb{Q}$, $\mathrm{Gal}(\mathrm{K}_{\wp_n}/\mathbb{Q}_p)$ is a dihedral group, and consequently, $\mathrm{E}^1(\mathrm{K}_{\wp_n})_p = \mathrm{E}^1(\mathrm{K}_{\wp})_p = 0$. Since $\widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})_{p^\infty} = \widetilde{\mathrm{E}}(\mathrm{K}_{\wp_{k_0}})_{p^\infty}$ for some $k_0 \in \mathbb{N}$, it follows that $\mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty} = \mathrm{E}(\mathrm{K}_{\wp_{k_0}})_{p^\infty}$.

We start by defining $\mathrm{Sel}'_{\wp_n}(p^\infty) \subseteq \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty})$. Let us consider the exact sequence

$$0 \longrightarrow \mathrm{H}^1\big(\mathrm{K}_{\wp_n}/\mathrm{K}_{\wp_m}, \mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty}\big) \longrightarrow \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}_{p^\infty}) \xrightarrow{\psi_{n,m}} \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty}).$$

The group $\mathrm{Sel}'_{\wp_n}(p^\infty)$ should have the following properties:

(i) $\mathrm{Sel}_{\wp_m}(p^\infty) \subseteq \mathrm{Sel}'_{\wp_m}(p^\infty)$;

(ii) $\psi_{n,m}^{-1}\big((\mathrm{Sel}'_{\wp_n}(p^\infty))^{G_n/G_m}\big) = \mathrm{Sel}'_{\wp_m}(p^\infty)$; and

(iii) the size of the group $\mathrm{Sel}'_{\wp_m}(p^\infty)/\mathrm{Sel}_{\wp_m}(p^\infty)$ is bounded independently of m.

Greenberg [G, Theorem 2.6] has shown that $\mathrm{Sel}_{\wp_n}(p^\infty) = (\mathrm{im}\,\epsilon_n)_{\mathrm{div}}$, where ϵ_n is the natural map in the exact sequence

$$0 \longrightarrow \mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty} \longrightarrow \widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})_{p^\infty} \longrightarrow \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}^1_{p^\infty}) \xrightarrow{\epsilon_n} \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty}). \tag{39}$$

We set

$$\mathrm{Sel}'_{\wp_m}(p^\infty) := \bigcup_{n\geq m} \psi_{n,m}^{-1}(\mathrm{im}\,\epsilon_n)^{G_n/G_m},$$

and we prove that this subgroup of $\mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}_{p^\infty})$ satisfies the required properties.

The result of Greenberg that we mentioned above implies that $\mathrm{Sel}_{\wp_m}(p^\infty) \subseteq \mathrm{Sel}'_{\wp_m}(p^\infty)$. Property (ii) translates to saying that

$$\psi_{n,m}^{-1}\Big(\bigcup_{k\geq n}\psi_{k,n}^{-1}(\mathrm{im}\,\epsilon_k)^{G_k/G_n}\Big)^{G_n/G_m} = \bigcup_{k\geq m}\psi_{k,m}^{-1}(\mathrm{im}\,\epsilon_k)^{G_k/G_m} \quad \text{for all } n \geq m.$$

Since $\ker\psi_{n,m} \subseteq \ker\psi_{k,m}$ for any $k \geq n \geq m$, all we need to show is that $\psi_{k,n}(\mathrm{im}\,\epsilon_n) \subseteq \mathrm{im}\,\epsilon_k$ for any triple $k \geq n \geq m$. This is clear because one can see easily that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{E}(\mathrm{K}_{\wp_k})_{p^\infty} & \longrightarrow & \widetilde{\mathrm{E}}(\mathrm{K}_{\wp_k})_{p^\infty} & \longrightarrow & \mathrm{H}^1(\mathrm{K}_{\wp_k}, \mathrm{E}^1_{p^\infty}) & \xrightarrow{\epsilon_k} & \mathrm{H}^1(\mathrm{K}_{\wp_k}, \mathrm{E}_{p^\infty}) \\ & & \uparrow & & \uparrow & & \uparrow & & \uparrow \psi_{k,n} \\ 0 & \longrightarrow & \mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty} & \longrightarrow & \widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})_{p^\infty} & \longrightarrow & \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}^1_{p^\infty}) & \xrightarrow{\epsilon_n} & \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty}) \end{array}$$

is commutative.

We now need to prove that property (iii) holds. Since Greenberg [G, Theorem 2.8] has shown that $\#(\operatorname{im}\epsilon_m/\mathrm{Sel}_{\wp_m}(p^\infty)) \le \#\widetilde{\mathrm{E}}(\mathrm{K}_\wp)_{p^\infty}$, we can concentrate on bounding $\#(\mathrm{Sel}'_{\wp_m}(p^\infty)/\operatorname{im}\epsilon_m)$. Applying the snake lemma to sequence (39), we get

$$\begin{array}{ccccc} \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}^1_{p^\infty})^{G_n/G_m} & \xrightarrow{\epsilon_n} & (\operatorname{im}\epsilon_n)^{G_n/G_m} & \longrightarrow & \big(\widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})_{p^\infty}/\mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty}\big)/\operatorname{im}(g^{p^m}-1) \\ \uparrow & & \uparrow \psi_{n,m} & & \\ \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}^1_{p^\infty}) & \xrightarrow{\epsilon_m} & \operatorname{im}\epsilon_m & \longrightarrow & 0 \end{array}$$

where $\langle g^{p^m}\rangle = G_n/G_m$.

Since $\mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}^1_{p^\infty})^{G_n/G_m} = \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}^1_{p^\infty})$, it follows that

$$(\operatorname{im}\epsilon_n)^{G_n/G_m}/\psi_{n,m}(\operatorname{im}\epsilon_m) \hookrightarrow \big(\widetilde{\mathrm{E}}(\mathrm{K}_{\wp_n})_{p^\infty}/\mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty}\big)/\operatorname{im}(g^{p^m}-1),$$

which implies that

$$\#\big(\psi_{n,m}^{-1}(\operatorname{im}\epsilon_n)^{G_n/G_m}/\operatorname{im}\epsilon_m\big) \le \#\ker\psi_{n,m}\cdot\#\big(\widetilde{\mathrm{E}}(\mathrm{K}_{\wp_{k_0}})_{p^\infty}\big).$$

Fixing $m_0 > k_0$ so that $\mathrm{E}(\mathrm{K}_{\wp_{k_0}})_{p^\infty} = \mathrm{E}(\mathrm{K}_{\wp_{k_0}})_{p^{m_0}}$, we deduce that

$$\ker\psi_{n,m} \subseteq \mathrm{H}^1\big(\mathrm{K}_{\wp_{m+m_0}}/\mathrm{K}_{\wp_m}, \mathrm{E}(\mathrm{K}_{\wp_{k_0}})_{p^\infty}\big),$$

and therefore,

$$\#\big(\mathrm{Sel}'_{\wp_m}(p^\infty)/\operatorname{im}\epsilon_m\big) \le \#\mathrm{H}^1\big(\mathrm{K}_{\wp_{m+m_0}}/\mathrm{K}_{\wp_m}, \mathrm{E}(\mathrm{K}_{\wp_{k_0}})_{p^\infty}\big)\cdot\#\big(\widetilde{\mathrm{E}}(\mathrm{K}_\wp)_{p^\infty}/\mathrm{E}(\mathrm{K}_\wp)_{p^\infty}\big).$$

Finally, we see that the size of $\mathrm{Sel}'_{\wp_m}(p^\infty)/\mathrm{Sel}_{\wp_m}(p^\infty)$ is bounded from above by

$$\#\big(\widetilde{\mathrm{E}}(\mathrm{K}_\wp)_{p^\infty}\big)^2\cdot\#\mathrm{H}^1\big(\mathrm{K}_{\wp_{m+m_0}}/\mathrm{K}_{\wp_m}, \mathrm{E}(\mathrm{K}_{\wp_{k_0}})_{p^\infty}\big).$$

This concludes the proof of property (iii).

Let us consider the sequence

$$\begin{aligned} 0 \longrightarrow \mathrm{E}(\mathrm{K}_{\wp_m})_{p^k} &\longrightarrow \mathrm{E}(\mathrm{K}_{\wp_m})_{p^\infty} \longrightarrow \mathrm{E}(\mathrm{K}_{\wp_m})_{p^\infty} \\ &\longrightarrow \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}_{p^k}) \xrightarrow{\phi_{m,k}} \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}_{p^\infty}), \end{aligned}$$

and define $\mathrm{Sel}'_{\wp_m}(p^k) := \phi_{m,k}^{-1}(\mathrm{Sel}'_{\wp_m}(p^\infty))$. The exact sequence

$$0 \longrightarrow \mathrm{H}^1\big(\mathrm{K}_{\wp_n}/\mathrm{K}_{\wp_m}, \mathrm{E}(\mathrm{K}_{\wp_n})_{p^k}\big) \longrightarrow \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}_{p^k}) \xrightarrow{\psi_{n,m}^k} \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^k})$$

allows us to compare $(\mathrm{Sel}'_{\wp_n}(p^k))^{G_n/G_m}$ and $\mathrm{Sel}'_{\wp_m}(p^k)$.

We show that

(i) $\mathrm{Sel}_{\wp_m}(p^k) \subseteq \mathrm{Sel}'_{\wp_m}(p^k)$;

(ii) $(\psi_{n,m}^k)^{-1}(\mathrm{Sel}'_{\wp_n}(p^k))^{G_n/G_m} = \mathrm{Sel}'_{\wp_m}(p^k)$; and

(iii) the size of the group $\mathrm{Sel}'_{\wp_m}(p^k)/\mathrm{Sel}_{\wp_m}(p^k)$ is bounded independently of m and k.

We know that $\mathrm{Sel}_{\wp_m}(p^\infty) \subseteq \mathrm{Sel}'_{\wp_m}(p^\infty)$. Since $\mathrm{Sel}_{\wp_m}(p^k) = \phi_{m,k}^{-1}(\mathrm{Sel}_{\wp_m}(p^\infty))$, it follows that $\mathrm{Sel}_{\wp_m}(p^k) \subseteq \mathrm{Sel}'_{\wp_m}(p^k)$.

Our next aim is to show that $(\psi_{n,m}^k)^{-1}(\mathrm{Sel}'_{\wp_n}(p^k))^{G_n/G_m} \subset \mathrm{Sel}'_{\wp_m}(p^k)$ since the opposite inclusion is obvious. We can see that

$$\big(\mathrm{Sel}'_{\wp_n}(p^k)\big)^{G_n/G_m} = \big[\phi_{n,k}^{-1}\big(\mathrm{Sel}'_{\wp_n}(p^\infty)\big)\big]^{G_n/G_m} \subset \phi_{n,k}^{-1}\big[\big(\mathrm{Sel}'_{\wp_n}(p^\infty)\big)^{G_n/G_m}\big].$$

Notice that the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}_{p^k}) & \xrightarrow{\phi_{m,k}} & \mathrm{H}^1(\mathrm{K}_{\wp_m}, \mathrm{E}_{p^\infty}) \\ \downarrow{\scriptstyle \psi_{n,m}^k} & & \downarrow{\scriptstyle \psi_{n,m}} \\ \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^k})^{G_n/G_m} & \xrightarrow{\phi_{n,k}} & \mathrm{H}^1(\mathrm{K}_{\wp_n}, \mathrm{E}_{p^\infty})^{G_n/G_m} \end{array}$$

Furthermore, we know that $\psi_{n,m}^{-1}(\mathrm{Sel}'_{\wp_n}(p^\infty))^{G_n/G_m} = \mathrm{Sel}'_{\wp_m}(p^\infty)$. We can then deduce that

$$\begin{aligned} (\psi_{n,m}^k)^{-1}\big(\mathrm{Sel}'_{\wp_n}(p^k)\big)^{G_n/G_m} &\subseteq (\psi_{n,m}^k)^{-1}\phi_{n,k}^{-1}\big[\big(\mathrm{Sel}'_{\wp_n}(p^\infty)\big)^{G_n/G_m}\big] \\ &= \phi_{m,k}^{-1}\psi_{n,m}^{-1}\big[\big(\mathrm{Sel}'_{\wp_n}(p^\infty)\big)^{G_n/G_m}\big] \\ &= \phi_{m,k}^{-1}\mathrm{Sel}'_{\wp_m}(p^\infty) = \mathrm{Sel}'_{\wp_m}(p^k). \end{aligned}$$

We now show that the size of the group $\mathrm{Sel}'_{\wp_m}(p^k)/\mathrm{Sel}_{\wp_m}(p^k)$ is bounded independently of m and k. Let $s \in \mathrm{Sel}'_{\wp_m}(p^k)$ be such that

$$\bar{s} \in \big(\mathrm{Sel}'_{\wp_m}(p^k)/\mathrm{Sel}_{\wp_m}(p^k)\big) - \{0\}.$$

Consider $\phi_{m,k}(s)$. If $\phi_{m,k}(s) \in \mathrm{Sel}_{\wp_m}(p^\infty)$, then $s \in \mathrm{Sel}_{\wp_m}(p^k) = \phi_{m,k}^{-1}\mathrm{Sel}_{\wp_m}(p^\infty)$, contradicting our assumption. It follows that $\phi_{m,k}(s) \notin \mathrm{Sel}_{\wp_m}(p^\infty)$, and therefore, $\phi_{m,k}(s) \in \mathrm{Sel}'_{\wp_m}(p^\infty)/\mathrm{Sel}_{\wp_m}(p^\infty)$, which implies that

$$\#\big(\mathrm{Sel}'_{\wp_m}(p^k)/\mathrm{Sel}_{\wp_m}(p^k)\big) \le \#\big(\mathrm{Sel}'_{\wp_m}(p^\infty)/\mathrm{Sel}_{\wp_m}(p^\infty)\big).$$

This concludes the proof of the properties on $\mathrm{Sel}'_{\wp_n}(p^k)$.

Let us choose Q_n so that it satisfies the first set of properties (i) – (iii) that we required in the beginning of §2.3.1 and so that

$$H^1_{\mathrm{Sel}'}(K_n, E_{p^{m_n}}) \hookrightarrow \prod_{q \in Q_n} H^1\big(K_n(q)^{\mathrm{unr}}/K_n(q), E_{p^{m_n}}\big).$$

In addition to the conditions that we have already put on n_0, in the case when p is a prime of good ordinary anomalous reduction, we also require that

$$\#\big(\mathrm{Sel}'_{\wp_m}(p^\infty)/\mathrm{Sel}_{\wp_m}(p^\infty)\big) \le p^{n_0} \quad \text{for all } m \in \mathbb{N}.$$

We then know that for all $n \ge 0$ and $k > n_0$,

$$\#H^1_{\mathrm{Sel}'_{Q_n}}(K_n, E_{p^k})/\#H^1_{\mathrm{Sel}_{Q_n}}(K_n, E_{p^k}) = \#\big(\mathrm{Sel}'_{\wp_n}(p^k)/\mathrm{Sel}_{\wp_n}(p^k)\big) \le p^{n_0}.$$

Since, in the proofs of Propositions 2.3.1 and 2.3.2, we have not assumed that p is nonanomalous or even ordinary, we have

$$\#H^1_{\mathrm{Sel}'_{Q_n}}(K_m, E_{p^k}) = \#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t} \cdot \#\big(\mathrm{Sel}'_{\wp_n}(p^k)/\mathrm{Sel}_{\wp_n}(p^k)\big) \tag{40}$$

for all $m \le n$ and $n_0 \le k \le m_n$, and

$$\#H^1_{\mathrm{Sel}'_{Q_n}}(K, E_{p^{m_n}}) = \#(\mathbb{Z}/p^{m_n}\mathbb{Z})^{2t} \cdot \#\big(\mathrm{Sel}'_{\wp}(p^{m_n})/\mathrm{Sel}_{\wp}(p^{m_n})\big) \quad \text{for all } n \ge n_0. \tag{41}$$

We now come to the reason for which we need to consider $H^1_{\mathrm{Sel}'}(K_n, E_{p^{m_n}})$ instead of $H^1_{\mathrm{Sel}}(K_n, E_{p^{m_n}})$. As in the proof of Proposition 2.3.3, we can see easily that

$$H^1_{\mathrm{Sel}'_{Q_n \cup \{p\}}}(K_n, E_{p^{m_n}})^{G_n/G_m} = H^1_{\mathrm{Sel}'_{Q_n \cup \{p\}}}(K_m, E_{p^{m_n}}).$$

Since we have ensured that $(\psi^{m_n}_{n,m})^{-1}(\mathrm{Sel}'_{\wp_n}(p^{m_n}))^{G_n/G_m} = \mathrm{Sel}'_{\wp_m}(p^{m_n})$, the following result holds true.

PROPOSITION 2.3.5
We have $H^1_{\mathrm{Sel}'_{Q_n}}(K_n, E_{p^{m_n}})^{G_n/G_m} = H^1_{\mathrm{Sel}'_{Q_n}}(K_m, E_{p^{m_n}})$ *for all* $m \le n$.

Let us consider the module $\mathscr{M}_a$ that is constructed in the same way as in the ordinary nonanomalous case by using $H^1_{\mathrm{Sel}'_{Q_k}}(K_m, E_{p^{m_n}})$ for $k \ge n$ instead of $H^1_{\mathrm{Sel}_{Q_k}}(K_m, E_{p^{m_n}})$. In this case, the structure theorem is the following.

THEOREM 2.3.6
The Λ*-module* $\widehat{\mathscr{M}}_a$ *is pseudoisomorphic to* Λ^{2t}.

Proof
Let s_0 denote the number of generators of $\mathrm{N_Q}$ defined in Proposition 2.2.5. Consequently, the number of generators of $\widehat{\mathscr{M}}_a$ is $2t + s_0$. By the structure theorem for finitely generated Λ-modules, we have an exact sequence of the form

$$0 \longrightarrow \mathrm{F}_1 \longrightarrow \widehat{\mathscr{M}}_a \longrightarrow \Lambda^d \oplus \Lambda/f_1 \oplus \cdots \oplus \Lambda/f_r \longrightarrow \mathrm{F}_2 \longrightarrow 0,$$

where $f_i \in \Lambda$, F_i is a finite group and $r, d \in \mathbb{N}$.

Proposition 2.3.5 implies that

$$\widehat{\mathscr{M}}_a/\big(p^k, (1+T)^{p^m} - 1\big) \simeq \mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_{k_n}}}\widehat{(\mathrm{K}_m, \mathrm{E}_{p^k})} \quad \text{for any } n \geq m \text{ and } n_0 \leq k \leq m_n,$$

and by (40), we know that

$$\#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t} \leq \#\mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_n}}(\mathrm{K}_m, \mathrm{E}_{p^k}) \leq \#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t} \cdot p^{n_0}.$$

It follows that $d = 2t$, and $\Lambda/f_i = 0$ for all i. This concludes the proof. □

2.4. Choosing the auxiliary Q_n
2.4.1
In this section, we assume that E has good ordinary reduction at p. Recall that the auxiliary primes $q \in \mathrm{Q}_n$ are required to have the following properties:

(i) q is inert in $\mathrm{K}/\mathbb{Q}$;
(ii) $q \notin \Sigma$;
(iii) $\mathrm{E}(\mathrm{K}_{q_n})_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_{q_n}})_{p^{m_n}}$, where q_n denotes any prime of K_n above q; and
(iv) $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{q \in \mathrm{Q}_n} \mathrm{H}^1(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}})$, where $\mathrm{H}^1(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}}) = \bigoplus_{q_n | q} \mathrm{H}^1(\mathrm{K}^{\mathrm{unr}}_{q_n}/\mathrm{K}_{q_n}, \mathrm{E}_{p^{m_n}})$ and $\mathrm{K}^{\mathrm{unr}}_{q_n}$ denotes the maximal unramified extension of K_{q_n}.

We prove the existence of a set of primes with these properties and give a method for constructing such a set. Let us start by showing how we can choose the primes of Q_n so that

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{q \in \mathrm{Q}_n} \mathrm{H}^1\big(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}}\big).$$

The kernel of the above map is $\mathrm{H}^1_{\mathrm{Sel}\mathrm{Q}_n}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$. This group is trivial if and only if its invariants under G_n are trivial. Since $\mathrm{H}^1_{\mathrm{Sel}\mathrm{Q}_n}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n} = \mathrm{H}^1_{\mathrm{Sel}\mathrm{Q}_n}(\mathrm{K}, \mathrm{E}_{p^{m_n}})$ by Proposition 2.3.3, we aim to find Q_n so that $\mathrm{H}^1_{\mathrm{Sel}\mathrm{Q}_n}(\mathrm{K}, \mathrm{E}_{p^{m_n}}) = 0$.

Let $\mathrm{L}_n = \mathrm{K}(\mathrm{E}_{p^{m_n}})$, $\mathscr{G}_n = \mathrm{Gal}(\mathrm{L}_n/\mathrm{K})$, and consider the exact sequence

$$0 \longrightarrow \mathrm{H}^1(\mathscr{G}_n, \mathrm{E}_{p^{m_n}}) \longrightarrow \mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^{m_n}}) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(\mathrm{L}_n, \mathrm{E}_{p^{m_n}})^{\mathscr{G}_n}. \tag{42}$$

Since $\mathrm{H}^1(\mathscr{G}_n, \mathrm{E}_{p^{m_n}}) = 0$ for all n (see Proposition 1.3.1), the above diagram implies that

$$\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^{m_n}}) \hookrightarrow \mathrm{H}^1(\mathrm{L}_n, \mathrm{E}_{p^{m_n}})^{\mathscr{G}_n} = \mathrm{Hom}_{\mathscr{G}_n}\big(\mathrm{Gal}(\overline{\mathrm{L}}_n/\mathrm{L}_n), \mathrm{E}_{p^{m_n}}\big).$$

We then have the $\mathscr{G}_n$-pairing

$$\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^{m_n}}) \times \mathrm{Gal}(\overline{\mathrm{L}}_n/\mathrm{L}_n) \longrightarrow \mathrm{E}_{p^{m_n}}. \tag{43}$$

Let M_n be the fixed field of the subgroup of $\mathrm{Gal}(\overline{\mathrm{L}}_n/\mathrm{L}_n)$ which pairs to zero with the finite subgroup $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}})$ of $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^{m_n}})$. Consequently, the $\mathscr{G}_n$-pairing,

$$\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}}) \times \mathrm{Gal}(\mathrm{M}_n/\mathrm{L}_n) \longrightarrow \mathrm{E}_{p^{m_n}}, \tag{44}$$

is nondegenerate.

Let $\mathrm{H}_n = \mathrm{Gal}(\mathrm{M}_n/\mathrm{L}_n)$. The element $\tau \in \mathrm{Gal}(\mathrm{L}_n/\mathbb{Q})$ denotes a complex conjugation; it acts on H_n. We extend τ to a complex conjugation in $\mathrm{Gal}(\mathrm{M}_n/\mathbb{Q})$, and we may assume that these choices are compatible as n varies. The nondegeneracy of pairing (44) implies, in particular, that H_n has odd order. So, H_n splits as a direct sum of the eigenspaces for the action of τ, $\mathrm{H}_n = \mathrm{H}_n^+ \oplus \mathrm{H}_n^-$. Furthermore,

$$\mathrm{H}_n^+ = \mathrm{H}_n^{\tau+1} = \big\{\tau^{-1} h \tau h = (\tau h)^2 : h \in \mathrm{H}_n\big\}. \tag{45}$$

PROPOSITION 2.4.1
Let $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}})$. *Then the following are equivalent:*
(1) $s = 0$;
(2) $[s, \rho] = 0$ *for all* $\rho \in \mathrm{H}_n$, *where* $[\,,\,]$ *denotes pairing (44); and*
(3) $[s, \rho] = 0$ *for all* $\rho \in \mathrm{H}_n^+$.

Proof
See Proposition 1.3.3. □

Since the minimal number of generators of H_n^+ does not depend on n, Proposition 2.4.1 implies that we can choose $h_1, \ldots, h_t \in \mathrm{H}_n^+$ so that $\mathrm{H}_n^+ = \langle h_1, \ldots, h_t \rangle$ and

$$[s, h_i] = s(h_i) = 0, \quad \forall i \in \{1, \ldots, t\} \Rightarrow s = 0, \tag{46}$$

for any $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}}) = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n}$.

PROPOSITION 2.4.2
If $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}})$, $\rho \in \mathrm{Gal}(\mathrm{M}_n/\mathrm{L}_n)$, *and* λ *is a prime of* K *not contained in* Σ *such that* $\mathrm{Frob}_\lambda(\mathrm{L}_n/\mathrm{K}) = \{g\rho g^{-1} : g \in \mathscr{G}_n\}$, *then the following are equivalent:*
(1) $[s, \sigma] = 0$ *for some* $\sigma \in \mathrm{Frob}_\lambda(\mathrm{M}_n/\mathrm{K})$;
(2) $[s, \sigma] = 0$ *for all* $\sigma \in \mathrm{Frob}_\lambda(\mathrm{M}_n/\mathrm{K})$; *and*
(3) $s_\lambda = 0$ *in* $\mathrm{H}^1(\mathrm{K}_\lambda, \mathrm{E}_{p^{m_n}})$.

Proof
See [Gr, Proposition 9.6] or Proposition 1.3.4. □

PROPOSITION 2.4.3
Suppose that $\mathrm{H}_n^+ = \langle h_1, \dots, h_t \rangle$, *and let* $\mathrm{Q}_n = \{\ell_1, \dots, \ell_t\}$ *be a set of t primes in* $\mathbb{Q}$ *so that* $\mathrm{Frob}_{\ell_i}(\mathrm{M}_n/\mathbb{Q}) = \tau h_i'$, *where* $(\tau h_i')^2 = h_i \in \mathrm{H}_n^+$ *for each i. Then the natural map*

$$\phi_{\mathrm{Q}_n} : \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \longrightarrow \prod_{q \in \mathrm{Q}_n} \mathrm{H}^1\big(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}}\big)$$

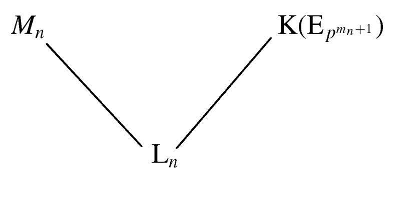
is injective.

Proof
Suppose that $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n} = \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^{m_n}})$ is in the kernel of ϕ_{Q_n}. Then by Proposition 2.4.2, $[s, \mathrm{Frob}_\lambda] = 0$ for each λ a prime of K above $\ell \in \{\ell_1, \dots, \ell_t\}$. So, we have $[s, h_i] = 0$ for each i, and consequently, $[s, \mathrm{H}_n^+] = 0$. Thus $s = 0$ by Proposition 2.4.1. It follows that $\mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n} = 0$, which is equivalent to $\mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) = 0$ and concludes the proof. □

By choosing the set Q_n in this way, we make sure that its size does not depend on n.

2.4.2
We now show how to ensure that the auxiliary primes $q \in \mathrm{Q}_n$ have the property that $\mathrm{E}(\mathrm{K}_{q_n})_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_{q_n}})_{p^{m_n}}$. Since any rational prime different from p which is inert in $\mathrm{K}/\mathbb{Q}$ splits completely in $\mathrm{K}[p^m]$ for any m, it follows that $\mathrm{E}(\mathrm{K}_{q_n})_{p^\infty} = \mathrm{E}(\mathrm{K}(q))_{p^\infty}$. (Here we have written $\mathrm{K}(q)$ for the completion of K at q to avoid confusion with K_n, the nth-layer of the anticyclotomic $\mathbb{Z}_p$-extension, defined at the beginning of §2.3. In §1, $\mathrm{K}(q)$ was written in the more standard way as K_q.)

Consider the following two extensions of L_n:



These extensions of L_n are disjoint (see §1.3.2). Assumption (2) on n_0 (in §2.3.1) implies that there are elements of $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_{p^{m_n+1}})/\mathrm{L}_n)$ with no fixed points on $\mathrm{E}_{p^{m_n+1}}/\mathrm{E}_{p^{m_n}}$.

Now, pick elements $h_1, \ldots, h_t \in \mathrm{H}_n^+$ so that $\mathrm{H}_n^+ = \langle h_1, \ldots, h_t \rangle$. Then each $h_i = (\tau h_i')^2$ for some $h_i' \in \mathrm{H}_n$ by (45). We can extend each $\tau h_i'$ to an element of $\mathrm{Gal}(\mathrm{M}_n\mathrm{K}(\mathrm{E}_{p^{m_n+1}})/\mathbb{Q})$ in such a way that the restriction of $(\tau h_i')^2$ to $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_{p^{m_n+1}})/\mathrm{L}_n)$ has no fixed points in $\mathrm{E}_{p^{m_n+1}}/\mathrm{E}_{p^{m_n}}$. Finally, we can choose primes $\ell_i \in \mathbb{Q}$ for $i = 1, \ldots, t$ so that

$$\mathrm{Frob}_{\ell_i}\left(\mathrm{M}_n\mathrm{K}(\mathrm{E}_{p^{m_n+1}})/\mathbb{Q}\right) = \tau h_i'.$$

It then follows that:

(i) $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{q\in \mathrm{Q}_n} \mathrm{H}^1(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}})$ for $\mathrm{Q}_n = \{\ell_1, \ldots, \ell_t\}$; and

(ii) $\mathrm{E}(\mathrm{K}_{\lambda_n})_{p^\infty} = \mathrm{E}(\overline{\mathrm{K}_{\lambda_n}})_{p^{m_n}}$, where λ_n is any prime of K_n above $\ell \in \mathrm{Q}_n$.

Remark 2.4.4

In the case when p is a prime of good ordinary anomalous reduction, the process of choosing the set Q_n is exactly the same, except that the Selmer condition must be replaced by the less-restrictive Sel'.

2.5. *Construction of cohomology classes*

2.5.1

We have chosen K so that N, the conductor of E, splits in $\mathrm{K}/\mathbb{Q}$, $\mathrm{N} = \mathscr{N}\bar{\mathscr{N}}$. For any positive integer $\mathfrak{f}$ prime to N, we can consider $x_\mathfrak{f} = (\mathbb{C}/\mathscr{O}_\mathfrak{f}, \mathbb{C}/\mathscr{N}_\mathfrak{f}) \in \mathrm{X}_0(\mathrm{N})$, where $\mathscr{O}_\mathfrak{f}$ denotes the order of K of conductor $\mathfrak{f}$ and $\mathscr{N}_\mathfrak{f} = \mathscr{N} \cap \mathscr{O}_\mathfrak{f}$. Fixing a parametrization $\pi : \mathrm{X}_0(\mathrm{N}) \longrightarrow \mathrm{E}$ which maps the cusp at ∞ to the origin of E, we define the Heegner point $y_\mathfrak{f} = \pi(x_\mathfrak{f})$. The Heegner point $y_\mathfrak{f}$ is defined over the ring class field of K of conductor $\mathfrak{f}$, $\mathrm{K}[\mathfrak{f}]$. Then we define α_n to be the trace of $y_{p^{k(n)}}$ from $\mathrm{K}[p^{k(n)}]$ to K_n.

We now describe a natural generalization of Kolyvagin's cohomology classes to ring class fields (following [BD]). Let r be a squarefree product of primes $\ell | r$ satisfying the following conditions:

(i) ℓ is relatively prime to $p\mathrm{ND}_\mathrm{K}$; and

(ii) $\mathrm{Frob}_\ell(\mathrm{K}(\mathrm{E}_{p^{m'_{n'}}})/\mathbb{Q}) = \tau$.

Let $k_0 \le n \le n'$, where $\mathrm{K}_{k_0} = \mathrm{K}_\infty \cap \mathrm{K}[1]$. Then we denote by $\mathrm{K}_n[r]$ the maximal subextension of $\mathrm{K}_n\mathrm{K}[r]$ which is a p-primary extension of K_n. We now define $\alpha_n(r)$ to be the trace of $y_{rp^{k(n)}}$ over $\mathrm{K}[rp^{k(n)}]/\mathrm{K}_n[r]$. (Recall that $k(n)$ was defined at the beginning of §2.3).

Let $\mathsf{G}_{n,r} = \mathrm{Gal}(\mathrm{K}_n[r]/\mathrm{K}_n[r] \cap \mathrm{K}_n\mathrm{K}[1])$, and let $\mathsf{G}_{n,\ell} = \mathrm{Gal}(\mathrm{K}_n[\ell]/\mathrm{K}_n[\ell] \cap \mathrm{K}_n\mathrm{K}[1])$. By class field theory, $\mathsf{G}_{n,r} = \prod_{\ell | r} \mathsf{G}_{n,\ell}$, and $\mathsf{G}_{n,\ell} \simeq \mathbb{Z}/p^{n_\ell}\mathbb{Z}$ for $n_\ell = p^{\mathrm{ord}_p(\ell+1)}$. Consider $D_\ell := \sum_{i=1}^{n_\ell} i\sigma_\ell^i \in \mathbb{Z}/p^{m_n}\mathbb{Z}[\mathsf{G}_{n,\ell}]$, and consider $D_r := \prod_{\ell | r} D_\ell \in \mathbb{Z}/p^{m_n}\mathbb{Z}[\mathsf{G}_{n,r}]$ (with $D_1 := 1$). One can then show that $D_r\alpha_n(r)$ belongs to $(\mathrm{E}(\mathrm{K}_n[r])/p^{m_n})^{\mathsf{G}_{n,r}}$ (see [BD, Lemma 3.3]). It follows that

$$\mathrm{tr}_{(\mathrm{K}_n[r]\cap \mathrm{K}_n\mathrm{K}[1])/\mathrm{K}_n} D_r\alpha_n(r) \in \big(\mathrm{E}(\mathrm{K}_n[r])/p^{m_n}\big)^{\mathcal{G}_{n,r}},$$

where $\mathcal{G}_{n,r} = \mathrm{Gal}(\mathrm{K}_n[r]/\mathrm{K}_n)$. We now consider the commutative diagram

$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
 & & & & & & \mathrm{H}^1(\mathrm{K}_n[r]/\mathrm{K}_n, \mathrm{E})_{p^{m_n}} & & \\
 & & & & & & \downarrow{\scriptstyle \mathrm{Inf}} & & \\
0 & \longrightarrow & \mathrm{E}(\mathrm{K}_n)/p^{m_n}\mathrm{E}(\mathrm{K}_n) & \xrightarrow{\phi} & \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) & \longrightarrow & \mathrm{H}^1(\mathrm{K}_n, \mathrm{E})_{p^{m_n}} & \longrightarrow & 0 \\
 & & \downarrow & & {\scriptstyle \mathrm{Res}}\downarrow\wr & & {\scriptstyle \mathrm{Res}}\downarrow & & \\
0 & \longrightarrow & \big(\mathrm{E}(\mathrm{K}_n[r])/p^{m_n}\big)^{\mathcal{G}_{n,r}} & \xrightarrow{\phi_r} & \mathrm{H}^1(\mathrm{K}_n[r], \mathrm{E}_{p^{m_n}})^{\mathcal{G}_{n,r}} & \longrightarrow & \mathrm{H}^1(\mathrm{K}_n[r], \mathrm{E})_{p^{m_n}}^{\mathcal{G}_{n,r}} & &
\end{array} \tag{47}$$

Let $c_n(r) \in \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ be so that

$$\phi_r\big(\mathrm{tr}_{(\mathrm{K}_n[r]\cap \mathrm{K}_n\mathrm{K}[1])/\mathrm{K}_n} D_r\alpha_n(r)\big) = \mathrm{Res}\big(c_n(r)\big),$$

and let $d_n(r)$ be the image of $c_n(r)$ in $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E})_{p^{m_n}}$. In particular, $\mathrm{Res}(c_n(1)) = \phi_1(\alpha_n)$. These generalized Kolyvagin cohomology classes have the following properties.

(1) Let $-\epsilon$ denote the sign of the functional equation of the L-function of $\mathrm{E}/\mathbb{Q}$, and let f_r be the number of prime divisors of r. After extending τ to a complex conjugation in $\mathrm{Gal}(\mathrm{K}_\infty/\mathbb{Q})$, we see that τ acts on α_n and $\tau\alpha_n = \epsilon g^{i_{n,1}}\alpha_n + \beta_n$ with $\beta_n \in \mathrm{E}(\mathrm{K}_n)_{\mathrm{tors}}$, g a generator of $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})$, and $i_{n,1} \in \{0, \dots, p^n - 1\}$. Moreover, the complex conjugation τ acts on $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, and we can deduce that $\tau c_n(r) = \epsilon_r g^{i_{n,r}} c_n(r)$, where $\epsilon_r = (-1)^{f_r}\epsilon$ and $i_{n,r} \in \{0, \dots, p^n - 1\}$.

(2) If v is a rational prime that does not divide r, then $d_n(r)_{v_n} = 0$ in $\mathrm{H}^1(\mathrm{K}_{v_n}, \mathrm{E})_{p^{m_n}}$ for all primes of K_n $v_n|v$.

(3) Let $\mathrm{H}^1(\mathrm{K}_n(\ell), \mathrm{E}_{p^{m_n}}) := \prod_{\lambda_n|\ell} \mathrm{H}^1(\mathrm{K}_{\lambda_n}, \mathrm{E}_{p^{m_n}})$, and define res_ℓ to be the localization map

$$\mathrm{res}_\ell : \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \to \mathrm{H}^1\big(\mathrm{K}_n(\ell), \mathrm{E}_{p^{m_n}}\big).$$

Recall that $\mathrm{E}(\mathrm{K}_n(\ell))/p^{m_n} = \prod_{\lambda_n|\ell} \mathrm{E}(\mathrm{K}_{\lambda_n})/p^{m_n}$. Then if $\ell|r$, there exists a G_n-equivariant and τ-antiequivariant isomorphism

$$\psi_\ell : \mathrm{H}^1\big(\mathrm{K}_n(\ell), \mathrm{E}\big)_{p^{m_n}} \to \mathrm{E}\big(\mathrm{K}_n(\ell)\big)/p^{m_n}$$

such that $\psi_\ell(\mathrm{res}_\ell\, d_n(r)) = \mathrm{res}_\ell(c_n(r/\ell))$.

(4) We have $R_n\alpha_n \subset R_{n+1}\alpha_{n+1}$. In addition, $R_n c_n(r) \subset R_{n+1}c_{n+1}(r)$, and consequently, $R_n d_n(r) \subset R_{n+1}d_{n+1}(r)$.

Let us start by showing that $R_n\alpha_n \subset R_{n+1}\alpha_{n+1}$. Since we have assumed that $p > 3$ ramifies in $\mathrm{Gal}(K/\mathbb{Q})$, $K[p^n]/K[1]$ is cyclic of order p^n. Therefore, $k(n) = n - k_0$ for $n \geq k_0$, and $k(n) = 0$ for $n \leq k_0$, where p^{k_0} is the order of the Galois group of the intersection of the maximal $\mathbb{Z}_p$-extension of K with the Hilbert class field of K, over K. Perrin-Riou [Pe, §3.3, Lemma 2] has shown that for any $r \in \mathbb{N}$ prime to p, we have

$$a_p y_{rp^{n+1}} = y_{rp^n} + \mathrm{tr}_{K[rp^{n+2}]/K[rp^{n+1}]} y_{rp^{n+2}} \quad \text{for } n \geq 0,$$
$$(a_p - g)y_r = \mathrm{tr}_{K[rp]/K[r]} y_{rp} \quad \text{for some } g \in \mathrm{Gal}(K[r]/K),$$

where $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Setting $r = 1$, this implies that

$$a_p\alpha_{n+1} = \alpha_n + \mathrm{tr}_{K_{n+2}/K_{n+1}}\alpha_{n+1} \quad \text{for } n \geq k_0,$$
$$(a_p - g)\alpha_{k_0} = \mathrm{tr}_{K_{k_0+1}/K_{k_0}}\alpha_{k_0+1} \quad \text{for some } g \in \mathrm{Gal}(K_{k_0}/K_0).$$

Since $a_p(a_p - 1) \not\equiv 0 \pmod p$, $a_p - g$ is invertible in $\mathbb{Z}_p[G_{k_0}]$ for any $g \in G_{k_0} = \mathrm{Gal}(K_{k_0}/K_0)$. This proves that $R_n\alpha_n \subset R_{n+1}\alpha_{n+1}$ for $n = k_0$. This result is trivial for $n < k_0$ since $\alpha_n = \mathrm{tr}_{K_{k_0}/K_n}\alpha_{k_0}$ for all $n < k_0$. Let us now assume that $\alpha_n = u\,\mathrm{tr}_{K_{n+1}/K_n}\alpha_{n+1}$ for some $u \in \mathbb{Z}_p[G_n]$. We can then see that

$$\mathrm{tr}_{K_{n+2}/K_{n+1}}\alpha_{n+2} = a_p\alpha_{n+1} - \alpha_n = (a_p - u\,\mathrm{tr}_{K_{n+1}/K_n}\alpha_{n+1})\alpha_{n+1}.$$

This implies that $R_{n+1}\alpha_{n+1} \subset R_{n+2}\alpha_{n+2}$ and concludes our argument.

The proof that $R_n c_n(r) \subset R_{n+1}c_{n+1}(r)$ is very similar. It suffices to notice that $\mathrm{Gal}(K[rp^{k(n)}]/K_n[r])$, $\mathrm{Gal}(K_n[r]/K_n)$, and consequently, $D_r := \prod_{\ell | r} D_\ell$ do not depend on n for $n \geq k_0$.

2.5.2

We now choose the first element of the set Q_n satisfying the required properties and such that the module of ramified cohomology classes which we can construct using this prime is big enough at every level in a sense that becomes clear later.

Let us consider the module $R_n\alpha_n$, which we view as a submodule of $H^1_{\mathrm{Sel}}(K_n, E_{p^{m_n}})$. We know that $R_n\alpha_n$ is an R_{n+1}-submodule of $R_{n+1}\alpha_{n+1}$. This allows us to construct the direct limit of the modules $R_n\alpha_n$.

THEOREM 2.5.1

The Heegner module $\widehat{\varinjlim_n R_n\alpha_n}$ *is not a torsion* Λ*-module.*

Proof
Let $\mathfrak{a}_n$ be the ideal of Λ so that $\mathrm{R}_n\alpha_n \simeq \Lambda/\mathfrak{a}_n$. Denote by $\mathfrak{m}$ the maximal ideal of Λ. Since $\Lambda/\mathfrak{a}_n[\mathfrak{m}]$ is a subgroup of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_p)$, we can see that $\Lambda/\mathfrak{a}_n[\mathfrak{m}]$ is bounded independently of n, and, consequently, so is $\widehat{\Lambda/\mathfrak{a}_n}/\mathfrak{m}$. This implies that $\varprojlim \widehat{\Lambda/\mathfrak{a}_n}$ is a finitely generated module. If $\varprojlim \widehat{\Lambda/\mathfrak{a}_n}$ is torsion, then there exists $f \in \Lambda$ such that $f(\widehat{\Lambda/\mathfrak{a}_n}) = 0$ for all n. Let $\iota : \Lambda \longrightarrow \Lambda$ be the automorphism induced by $(1+T) \mapsto (1+T)^{-1}$. It follows that $f^\iota \in \mathfrak{a}_n$ for all n.

Let us consider

$$\bigcup_{m \geq n_0} \mathrm{R}_m\alpha_n \in \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^\infty}).$$

We can see that f^ι annihilates $\bigcup_{m\geq n_0} \mathrm{R}_m\alpha_n$ for every n. Since Cornut [C] and Vatsal [V] have both shown that for n big enough, α_n is nontorsion, we know that $\bigcup_{m\geq n_0} \mathrm{R}_m\alpha_n$ is a nontrivial submodule of $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^\infty})$ for almost all n.

Let us assume that for infinitely many $k \geq n$, there exists $r_k \in \mathbb{N}$ prime to p such that $r_k\alpha_k$ and $r_k\alpha_{k+1}$ are defined over K_k. This implies that

$$pr_k\alpha_{k+1} = \mathrm{tr}_{\mathrm{K}_{k+1}/\mathrm{K}_k} r_k\alpha_{k+1} = f_k r_k \alpha_k$$

for some invertible element $f_k \in \Lambda$, and consequently, α_k is divisible by p. The assumption that this happens for infinitely many $k \geq n$ implies that α_n is p-divisible in $\mathrm{E}(\mathrm{K}_\infty)$. Since $\mathrm{E}(\mathrm{K}_\infty)_p = 0$, it follows easily that α_n is p-divisible in $\mathrm{E}(\mathrm{K}_n)$ and, hence, torsion for all n. (If $\alpha_n = p^i\gamma_n$ with $\gamma_n \in \mathrm{E}(\mathrm{K}_{n+r})$, say, then $p^i(\gamma_n - g_0\gamma_n) = 0$ for all $g_0 \in \mathrm{Gal}(\mathrm{K}_{n+r}/\mathrm{K}_n)$, whence $\gamma_n \in \mathrm{E}(\mathrm{K}_n)$.) This contradicts the results of Cornut and Vatsal.

Since we are assuming that $\mathrm{E}(\mathrm{K}_\infty)_p = 0$, we have shown that

$$g^{p^{n-1}}\alpha_n - \alpha_n \in \mathrm{E}(\mathrm{K}_n) - \mathrm{E}(\mathrm{K}_n)_{\mathrm{tors}}$$

for almost all n. It follows that there exists $r_\circ$ such that

$$g^{p^{n-1}}\alpha_n - \alpha_n \notin p^{r_\circ}\mathrm{E}(\mathrm{K}_n).$$

This implies that the image of $g^{p^{n-1}}\alpha_n - \alpha_n$ in $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^\infty})$ is infinite, and consequently, so is the image of $\mathbb{Z}\alpha_n \otimes \mathbb{Q}_p/\mathbb{Z}_p$ in $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^\infty})/\mathrm{H}^1(\mathrm{K}_{n-1}, \mathrm{E}_{p^\infty})$.

Let

$$\xi_n = \frac{(T+1)^{p^n} - 1}{(T+1)^{p^{n-1}} - 1} \in \Lambda.$$

Then if ξ_n is coprime to f^ι, there exists a k such that $p^k \in (f^\iota, \xi_n)$. This implies that p^k annihilates the image of $\bigcup_{m \geq n_0} \mathrm{R}_m \alpha_n$ in $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^\infty})/\mathrm{H}^1(\mathrm{K}_{n-1}, \mathrm{E}_{p^\infty})$, which is false. It follows that ξ_n and f^ι have a common factor for almost all n, and hence, $f = 0$. □

In order to control the size of the module of ramified cohomology classes which we construct, we need to use our knowledge of $\varinjlim \mathrm{R}_n \alpha_n$.

For each $h_n \in \mathrm{Gal}(\overline{\mathrm{L}_n}/\mathrm{K}_n\mathrm{L}_n) \subseteq \mathrm{Gal}(\overline{\mathrm{L}_n}/\mathrm{L}_n)$, we define a new R_n-module $[\mathrm{R}_n\alpha_n](h_n)$ as

$$[\mathrm{R}_n\alpha_n](h_n) := \left\{ \sum_{i=1}^{i=p^n} [(g^{-i}c)(h_n)] \cdot g^i \text{ such that } c \in \mathrm{R}_n\alpha_n \right\} \subseteq \mathrm{Hom}_{\mathrm{sets}}(G_n, \mathrm{E}_{p^{m_n}}),$$

where $G_n = \langle g \rangle$ and $[(g^{-i}c)(h_n)] \in \mathrm{E}_{p^{m_n}}$ is simply the evaluation of the class $g^{-i}c$ at $h_n \in \mathrm{Gal}(\overline{\mathrm{K}_n(\mathrm{E}_{p^{m_n}})}/\mathrm{K}_n(\mathrm{E}_{p^{m_n}}))$. The action of G_n on this module is the one induced from the standard action on $\mathrm{Hom}_{\mathrm{sets}}(G_n, \mathrm{E}_{p^{m_n}})$, namely, by multiplication on G_n, $(gf)(g_1) = f(gg_1)$. The map $\mathrm{R}_n\alpha_n \to [\mathrm{R}_n\alpha_n](h_n)$ is seen to be an R_n-module homomorphism. By picking a basis for $\mathrm{E}_{p^{m_n}}$, we may view the right-hand side as ${\mathrm{R}_n}^2$ and, hence, $[\mathrm{R}_n\alpha_n](h_n)$ as a submodule of ${\mathrm{R}_n}^2$.

Let $(h_n)_{n\in\mathbb{N}} \in \mathrm{Gal}(\overline{\mathrm{L}_\infty}/\mathrm{L}_\infty)$, where $h_n \in \mathrm{Gal}(\overline{\mathrm{L}_n}/\mathrm{K}_n\mathrm{L}_n)$. Noticing that the diagram

$$\begin{array}{ccc} \mathrm{R}_n\alpha_n & \longrightarrow & [\mathrm{R}_n\alpha_n](h_n) \\ \downarrow & & \downarrow \\ \mathrm{R}_{n+1}\alpha_{n+1} & \longrightarrow & [\mathrm{R}_{n+1}\alpha_{n+1}](h_{n+1}) \end{array}$$

is commutative, we deduce that we have the map

$$\psi : \varinjlim_n \mathrm{R}_n\alpha_n \to \varinjlim_n [\mathrm{R}_n\alpha_n](h_n).$$

By choosing the basis of $\mathrm{E}_{p^{m_n}}$ compatibly as n grows, we view $\varinjlim [\mathrm{R}_n\alpha_n](h_n)$ as a Λ-submodule of $\hat{\Lambda}^2$.

We now analyze the image of ψ. Theorem 2.5.1 implies the existence of a nonzero map

$$\phi : \hat{\Lambda} \to \varinjlim_n \mathrm{R}_n\alpha_n.$$

Now, τ acts on $\mathrm{R}_n\alpha_n$ and $\varinjlim \mathrm{R}_n\alpha_n$. Since $\phi^\tau - \phi$ and $\phi^\tau + \phi$ cannot be zero simultaneously, we can assume that ϕ lies in one of the eigenspaces for the action of complex conjugation τ. Let $s_0 \in (\mathrm{im}(\phi)^\Gamma)^{\mathrm{div}}[p] - \{0\}$. Observe that since $\phi^\tau = \pm\phi$, $s_0 \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_p)$ is an eigenvector for the action of τ on $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_p)$.

PROPOSITION 2.5.2
If $s_0(h_n) \neq 0$ for all n, then the image of the map ψ has nontrivial corank.

Proof
Since we have chosen $h_n \in \mathrm{Gal}(\mathrm{M}_n/\mathrm{L}_n)$ so that $s_0(h_n) \neq 0$ for all n, we know that $\mathrm{im}(\psi \circ \phi) \neq 0$. We have the chain of Λ-modules

$$\widehat{\mathrm{im}(\psi \circ \phi)} \subseteq \widehat{\mathrm{im}(\phi)} \subseteq \Lambda.$$

Since all nonzero submodules of Λ have rank 1, it follows that $\mathrm{im}(\psi \circ \phi)$ and, consequently, $\mathrm{im}(\psi)$ have nontrivial corank. □

We now choose compatible $h_n \in \mathrm{Gal}(\mathrm{M}_n/\mathrm{L}_n)^+$ (where $+$ denotes the $+1$-eigenspace for the action of complex conjugation τ) so that $(h_n)_{n\in\mathbb{N}} \in \mathrm{Gal}(\mathrm{M}_\infty/\mathrm{L}_\infty)$ and $s_0(h_n) \neq 0$. Then we fix a sequence of primes $\ell_n \in \mathbb{Q}$ so that $\tau h'_n \in \mathrm{Frob}_{\ell_n}(\mathrm{M}_n/\mathbb{Q})$, where $(\tau h'_n)^2 = h_n$.

We now establish the connection between the modules $\mathrm{res}_{\ell_n}(\mathrm{R}_n\alpha_n)$ and $[\mathrm{R}_n\alpha_n](h_n)$. Let $\mathrm{L}_{n,k} = \mathrm{K}_n(\mathrm{E}_{p^k})$, let $\mathscr{G}_{n,k} = \mathrm{Gal}(\mathrm{L}_{n,k}/\mathrm{K}_n)$, and consider the exact sequence

$$0 \longrightarrow \mathrm{H}^1(\mathscr{G}_{n,k}, \mathrm{E}_{p^k}) \longrightarrow \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^k}) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(\mathrm{L}_{n,k}, \mathrm{E}_{p^k})^{\mathscr{G}_{n,k}}. \tag{48}$$

In order to show that the restriction map in the above diagram is injective, we start by proving the following lemma.

LEMMA 2.5.3
The extensions $\mathrm{K}_\infty/\mathrm{K}$ and $\mathrm{K}(\mathrm{E}_{p^k})/\mathrm{K}$ are disjoint for all $k \in \mathbb{N}$.

Proof
We first prove that $\mathrm{K}_\infty/\mathrm{K}$ and $\mathrm{K}(\mathrm{E}_p)/\mathrm{K}$ are disjoint. If they were not, then $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_p)/\mathrm{K})$ would have a normal subgroup of order p, and this would also be a normal subgroup of $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_p)/\mathrm{K}(\mu_p))$, which is either of order prime to p or isomorphic to $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Since $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ is simple, we conclude that $\mathrm{K}_\infty/\mathrm{K}$ and $\mathrm{K}(\mathrm{E}_p)/\mathrm{K}$ have a trivial intersection.

We now use induction. Assuming that $\mathrm{K}_\infty/\mathrm{K}$ and $\mathrm{K}(\mathrm{E}_{p^k})/\mathrm{K}$ are disjoint, we show that $\mathrm{K}_\infty/\mathrm{K}$ and $\mathrm{K}(\mathrm{E}_{p^{k+1}})/\mathrm{K}$ are disjoint. Since $\mathrm{K}_\infty/\mathrm{K}$ and $\mathrm{K}(\mathrm{E}_p)/\mathrm{K}$ are disjoint, $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_p)/\mathrm{K})$ acts trivially on $\mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K})$. On the other hand,

$K(E_{p^{k+1}})/K(E_{p^k}, \mu_{p^{k+1}}) \subseteq \mathtt{Ad}_\rho$, where $\mathtt{Ad}_\rho$ denotes the adjoint representation of $\rho : \mathrm{Gal}(K(E_p)/K) \to GL_2(\mathbb{Z}/p\mathbb{Z})$. In addition, we know that K_∞/K and $K(E_{p^k}, \mu_{p^\infty})/K$ are disjoint. It then follows that K_∞/K and $K(E_{p^{k+1}})/K$ are also disjoint. □

PROPOSITION 2.5.4
We have $H^1(\mathscr{G}_{n,k}, E_{p^k}) = 0$ *for all* $n, k \in \mathbb{N}$.

Proof
Since, by Proposition 1.3.1, we have $H^1(\mathscr{G}_{0,k}, E_{p^k}) = 0$ for all $k \in \mathbb{N}$, Lemma 2.5.3 implies that $H^1(\mathscr{G}_{n,k}, E_{p^k}) = 0$. □

COROLLARY 2.5.5
The restriction map

$$H^1(K_n, E_{p^k}) \longrightarrow \mathrm{Hom}_{\mathscr{G}_{n,k}}\big(\mathrm{Gal}(\overline{L}_{n,k}/L_{n,k}), E_{p^k}\big)$$

is injective.

Proof
This follows immediately from diagram (48) and Proposition 2.5.4. □

We set $L'_n = L_{n,m_n} = K_n(E_{p^{m_n}})$, and Lemma 2.5.3 implies that

$$\mathscr{G}_n = \mathrm{Gal}\big(K(E_{p^{m_n}})/K\big) \simeq \mathrm{Gal}(L'_n/K_n) = \mathscr{G}_{n,m_n}.$$

Corollary 2.5.5 gives us the $\mathscr{G}_n$-pairing

$$H^1(K_n, E_{p^{m_n}}) \times \mathrm{Gal}(\overline{L'_n}/L'_n) \longrightarrow E_{p^{m_n}}. \tag{49}$$

Let M'_n be the fixed field of the subgroup of $\mathrm{Gal}(\overline{L'_n}/L'_n)$ which pairs to zero with the finite subgroup $H^1_{\mathrm{Sel}}(K_n, E_{p^{m_n}})$ of $H^1(K_n, E_{p^{m_n}})$. We then have the nondegenerate $\mathscr{G}_n$-pairing

$$H^1_{\mathrm{Sel}}(K_n, E_{p^{m_n}}) \times \mathrm{Gal}(M'_n/L'_n) \longrightarrow E_{p^{m_n}}. \tag{50}$$

PROPOSITION 2.5.6
If $s \in H^1_{\mathrm{Sel}}(K_n, E_{p^{m_n}})$, $\rho \in \mathrm{Gal}(M'_n/L'_n)$, *and* λ_n *is a prime of* K_n *such that* $\mathrm{Frob}_{\lambda_n}(M'_n/K_n) = \{g\rho g^{-1} : g \in \mathscr{G}_n\}$, *then the following are equivalent:*
(1) $[s, \sigma] = 0$ *for some* $\sigma \in \mathrm{Frob}_{\lambda_n}(M'_n/K_n)$*;*
(2) $[s, \mathrm{Frob}_{\lambda_n}] = 0$*; and*
(3) $s_{\lambda_n} = 0$ *in* $H^1(K_{\lambda_n}, E_{p^{m_n}})$.

Proof

We have (1) $\Leftrightarrow$ (2) because the pairing (50) is $\mathcal{G}_n$-invariant and s is fixed by $\mathcal{G}_n$.

Now, we show that (2) $\Leftrightarrow$ (3). Since s is in the Selmer group, s_{λ_n} lies in the image of $\mathrm{E}(\mathrm{K}_n(\lambda_n))/p^{m_n}\mathrm{E}(\mathrm{K}_{\lambda_n})$, say, $s_{\lambda_n} = \mathrm{im}(\mathrm{P}_{\lambda_n})$. Then $[s,\sigma] = (\mathrm{P}_{\lambda_n}/p^{m_n})^{\sigma-1}$. It follows that $[s,\sigma] = 0$ if and only if $\mathrm{P}_{\lambda_n} \in p^{m_n}\mathrm{E}(\mathrm{L}'_n(\tilde{\lambda}_n))$, where $\tilde{\lambda}_n$ is the prime of L'_n above λ_n associated to σ. Therefore, (2) is equivalent to $\mathrm{P}_{\lambda_n} \in p^{m_n}\mathrm{E}(\mathrm{L}'_n(\tilde{\lambda}_n))$ for all $\tilde{\lambda}_n$ above λ_n. □

We can now prove the following result, with ℓ_n and h_n as chosen after Proposition 2.5.2.

PROPOSITION 2.5.7

The R_n*-modules* $\mathrm{res}_{\ell_n}(\mathrm{R}_n\alpha_n)$ *and* $[\mathrm{R}_n\alpha_n](h_n)$ *are isomorphic for every* $n \geq n_0$.

Proof

We have defined the map $\psi_n = \psi|_{\mathrm{R}_n\alpha_n}$, $\psi_n : \mathrm{R}_n\alpha_n \to [\mathrm{R}_n\alpha_n](h_n)$. Let $s \in \ker\psi_n$, which is equivalent to saying that $s(gh_ng^{-1}) = 0$ for all $g \in G_n$. Since $s \in \mathrm{R}_n\alpha_n \subset \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, Proposition 2.5.6 implies that $s(gh_ng^{-1}) = 0$ is equivalent to $s_{\lambda_n} = 0$, where λ_n is the prime of K_n above ℓ_n associated to gh_ng^{-1}. It then follows that $s \in \ker\psi_n$ if and only if $s \in \ker \mathrm{res}_{\ell_n}$. This allows us to see that

$$\mathrm{res}_{\ell_n}(\mathrm{R}_n\alpha_n) \simeq \mathrm{R}_n\alpha_n/\ker\mathrm{res}_{\ell_n} \simeq \mathrm{R}_n\alpha_n/\ker\psi_n \simeq [\mathrm{R}_n\alpha_n](h_n)$$

and concludes the proof of the proposition. □

Let us consider $c_n(\ell_m) \in \mathrm{H}^1(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ for all $m \geq n$. Starting with $n = n_0$, we perform the following steps:

(1) since the sizes of the modules $\mathrm{R}_n c_n(\ell_m)$ are bounded by the size of R_n, we can find an infinite set $\mathrm{N}_n \subseteq \mathbb{N}$ so that

$$\mathrm{R}_n c_n(\ell_m) \text{ are isomorphic } \mathrm{R}_n^\tau\text{-modules for all } m \in \mathrm{N}_n;$$

(2) consider $\mathrm{R}_{n+1}c_{n+1}(\ell_m)$ for all $n+1 \leq m \in \mathrm{N}_n$. Since the sizes of these modules are bounded by the size of R_{n+1}, we can find an infinite set $\mathrm{N}_{n+1} \subseteq \mathrm{N}_n$ so that

$$\mathrm{R}_{n+1}c_{n+1}(\ell_m) \text{ are isomorphic } \mathrm{R}_{n+1}^\tau\text{-modules for all } m \in \mathrm{N}_{n+1}.$$

We then pick a sequence $\{k''_n \mid n \in \mathbb{N}\}$ so that $k''_n \in \mathrm{N}_n$. Property (4) in §2.5.1 of these cohomology classes implies that

$$\mathrm{R}_n c_n(\ell_{k''_n}) \simeq \mathrm{R}_n c_n(\ell_{k''_{n+1}}) \subseteq \mathrm{R}_{n+1}c_{n+1}(\ell_{k''_{n+1}})$$

and gives rise to an injective map $\mathrm{R}_n c_n(\ell_{k''_n}) \hookrightarrow \mathrm{R}_{n+1}c_{n+1}(\ell_{k''_{n+1}})$.

In the same way as above, we now choose a subsequence $\{k_n \mid n \in \mathbb{N}\}$ of $\{k''_n \mid n \in \mathbb{N}\}$ so that $\{\mathrm{R}_n d_n(\ell_{k_n}) \mid n \geq n_0\}$ as well as $\{\mathrm{R}_n c_n(\ell_{k_n}) \mid n \geq n_0\}$ are compatible as R_n^τ-modules as $n \to \infty$ in the following sense:

$$\mathrm{R}_n d_n(\ell_{k_n}) \simeq \mathrm{R}_n d_n(\ell_{k_{n+1}}) \subseteq \mathrm{R}_{n+1} d_{n+1}(\ell_{k_{n+1}}),$$

and

$$\mathrm{R}_n c_n(\ell_{k_n}) \simeq \mathrm{R}_n c_n(\ell_{k_{n+1}}) \subseteq \mathrm{R}_{n+1} c_{n+1}(\ell_{k_{n+1}}).$$

We can now construct the Λ-modules $\varinjlim \mathrm{R}_n c_n(\ell_{k_n})$ and $\varinjlim \mathrm{R}_n d_n(\ell_{k_n})$. We stress that these are created using noncanonical injections whose existence is guaranteed by the pigeon-hole principle above.

Using §2.5.1(3) and Proposition 2.5.7, we see that

$$\mathrm{res}_{\ell_{k_n}}\big(\mathrm{R}_n d_n(\ell_{k_n})\big) \simeq \mathrm{res}_{\ell_{k_n}}(\mathrm{R}_n \alpha_n) \simeq [\mathrm{R}_n \alpha_n](h_{k_n}).$$

Since $[\mathrm{R}_n \alpha_n](h_{k_n}) \simeq [\mathrm{R}_n \alpha_n](h_n)$ and $\varinjlim [\mathrm{R}_n \alpha_n](h_n)$ has nontrivial corank, it follows that $\varinjlim \mathrm{R}_n d_n(\ell_{k_n})$ and, consequently, also $\varinjlim \mathrm{R}_n c_n(\ell_{k_n})$ are not cotorsion Λ-modules.

2.5.3

We now choose other primes for which we need to construct two distinct modules of ramified classes. In order to accomplish this, we need to use $\mathrm{im}\,\phi \subseteq \varinjlim \mathrm{R}_n \alpha_n$ and $\varinjlim \mathrm{R}_n c_n(\ell_{k_n})$. Since $\widehat{\varinjlim \mathrm{R}_n c_n(\ell_{k_n})}$ is not a torsion Λ-module, there exists a nonzero map

$$\phi' : \hat{\Lambda} \to \varinjlim_n \mathrm{R}_n c_n(\ell_{k_n}),$$

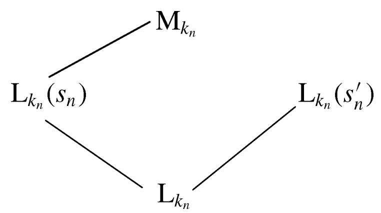
and just as in the case of ϕ, we can assume that $(\phi')^\tau = \pm\phi'$.

Observe that $[\mathrm{im}\,\phi]^\Gamma \subset [\varinjlim \mathrm{R}_n \alpha_n]^\Gamma$ and $[\mathrm{im}\,\phi']^\Gamma \subset [\varinjlim \mathrm{R}_n c_n(\ell_{k_n})]^\Gamma$ each contain a unique copy of $\mathbb{Q}_p/\mathbb{Z}_p$. This implies that $([\mathrm{im}\,\phi]^\Gamma)^{\mathrm{div}} \cap \mathrm{R}_n \alpha_n$ contains an element s_n, and $([\mathrm{im}\,\phi']^\Gamma)^{\mathrm{div}} \cap \mathrm{R}_n c_n(\ell_{k_n})$ contains an element s'_n such that the orders of s_n and s'_n go to infinity as n grows. Furthermore, since $\phi^\tau = \pm\phi$ and $(\phi')^\tau = \pm\phi'$, we know that $[\mathrm{im}\,\phi]^\Gamma$ and $[\mathrm{im}\,\phi']^\Gamma$ are fixed by τ. Consequently, the elements s_n and s'_n are eigenvectors of τ.

We are now ready to start the process of choosing the set Q_{k_n}. There are two cases that we need to consider, depending on how complex conjugation acts on s_n and s'_n.

Case 1. Assume that s_n and s'_n lie in different eigenspaces of the complex conjugation τ.

Consider the field extensions



where for any $s \in H^1_{\mathrm{Sel}}(K, E_{p^{m_{k_n}}})$, the extension $L_{k_n}(s)$ denotes the splitting field of s over L_{k_n}.

Since the groups generated by s_n and s'_n intersect trivially, the extensions $L_{k_n}(s_n)$ and $L_{k_n}(s'_n)$ are disjoint over L_{k_n}. Let us start by fixing $h'_{k_n} \in \mathrm{Gal}(L_{k_n}(s'_n)/L_{k_n})^+$ so that $s'_n(h'_{k_n})$ has the same order as s'_n, where $\mathrm{Gal}(L_{k_n}(s'_n)/L_{k_n})^+$ denotes the $+1$-eigenspace of $\mathrm{Gal}(L_{k_n}(s'_n)/L_{k_n})$ for the action of the complex conjugation τ. The next step is to pick $h_{k_n,i} \in \mathrm{Gal}(M_{k_n}/L_{k_n})^+$ so that the order of $s_n(h_{k_n,i})$ is equal to the order of s_n and $\langle h_{k_n}, h_{k_n,i} \mid 2 \le i \le t\rangle = \mathrm{Gal}(M_{k_n}/L_{k_n})^+$.

Let us extend τ to a complex conjugation in $\mathrm{Gal}(M_{k_n}(s'_n)/\mathbb{Q})$. We are now able to choose the elements of Q_{k_n} for this case. Let $\ell_{k_n}(i) \in \mathbb{Q}$ be so that

$$\tau h'_{k_n,i} \in \mathrm{Frob}_{\ell_{k_n}(i)}(M_{k_n}/\mathbb{Q}) \qquad \text{and} \qquad \tau h''_{k_n} \in \mathrm{Frob}_{\ell_{k_n}(i)}\big(L_{k_n}(s'_n)/\mathbb{Q}\big),$$

where $(\tau h'_{k_n,i})^2 = h_{k_n,i}$ and $(\tau h''_{k_n})^2 = h'_{k_n}$. (As in the choices made at the end of §1.4, we choose $h'_{k_n,i}$ and h''_{k_n} to fix L_{k_n}, thus ensuring their compatibility.) Finally, we define

$$Q_{k_n} = \big\{\ell_{k_n}(1) = \ell_{k_n}, \ell_{k_n}(i) \,\big|\, i = 2, \ldots, t\big\}.$$

Case 2. Assume that s_n and s'_n lie in the same eigenspace of the complex conjugation τ.

In this case, we need to consider the invariants of the module $\mathrm{im}\,\phi/\langle s_n \mid n \in \mathbb{N}\rangle$. Choose $e_n \in (\mathrm{im}\,\phi \cap R_n\alpha_n) - [R_n\alpha_n]^{G_n}$ so that the image of $\varinjlim\langle e_n, s_n\rangle$ in $(\mathrm{im}\,\phi)/\langle s_n \mid n \in \mathbb{N}\rangle$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a $\hat{\Lambda}$-module. This is possible because $\widehat{\mathrm{im}\,\phi} \simeq \Lambda$.

Since $(\mathrm{im}\,\phi)/\langle s_n \mid n \in \mathbb{N}\rangle$ is fixed by complex conjugation τ, it follows that the invariants are eigenvectors of τ. In particular, the image of e_n in $(\mathrm{im}\,\phi)/\langle s_n \mid n \in \mathbb{N}\rangle$ is an eigenvector for the action of τ. We now see that the eigenvalues corresponding to e_n and s_n are different. Let $\tau e_n = \epsilon e_n + x s_n$ and $\tau s_n = \epsilon' s_n$, where $\epsilon, \epsilon' \in \{\pm 1\}$ and $x \in \mathbb{Z}/p^{m_n}\mathbb{Z}$. Then we have

$$e_n = \epsilon\tau e_n + x\tau s_n = e_n + \epsilon x s_n + \epsilon' x s_n = e_n + (\epsilon + \epsilon')x s_n,$$

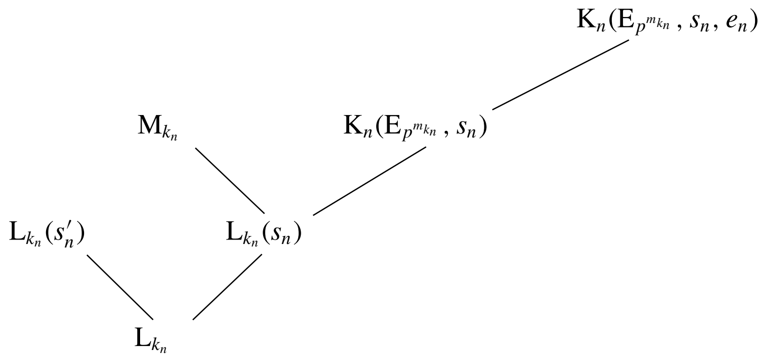
and it follows that $\epsilon = -\epsilon'$ if $x s_n \neq 0$. So, we still need to consider the case where $\tau e_n = \epsilon e_n$. We now use the fact that $(g-1)e_n = y s_n \neq 0$, where $y \in \mathbb{Z}/p^{m_n}\mathbb{Z}$ and

$G_n = \langle g \rangle$. Observe that

$$\tau(g-1)e_n = (g^{-1}-1)\epsilon e_n = -\epsilon g^{-1}[(g-1)e_n] = -\epsilon g^{-1} y s_n = -\epsilon y s_n.$$

Since, on the other hand, $\tau(g-1)e_n = y\tau s_n = \epsilon' y s_n$, we have $\epsilon' = -\epsilon$.

Let us now consider the extensions



We now analyze the extensions $\mathrm{L}_{k_n}(s'_n)/\mathrm{L}_{k_n}$ and $\mathrm{L}_{k_n}(s_n)/\mathrm{L}_{k_n}$. We know that $c_n(\ell)$ becomes trivial when restricted to $\mathrm{K}_n[\ell]$, and $\mathrm{K}_n[\ell]/\mathrm{K}_n$ is totally ramified at the primes of K_n dividing ℓ. It follows that the elements of $\mathrm{res}_\ell(\mathrm{R}_n c_n(\ell))$ are also totally ramified at primes dividing ℓ.

If, for infinitely many n, there exists s''_n, a nontrivial p-power multiple of s'_n which is unramified at ℓ_{k_n}, then we simply restrict to this subsequence of ℓ_{k_n}. In this subcase, $\mathrm{res}_{\ell_{k_n}} s''_n = 0$, which implies that $\mathrm{L}_{k_n}(s''_n)$ and $\mathrm{L}_{k_n}(s_n)$ are disjoint over L_{k_n}. By choosing s''_n to be the minimal p-power multiple of s'_n with this property, we ensure that $\mathrm{L}_{k_n}(s'_n)/\mathrm{L}_{k_n}(s''_n)$ is disjoint from $\mathrm{M}_{k_n}/\mathrm{L}_{k_n}(s''_n)$. It then follows that $\mathrm{L}_{k_n}(s'_n)/\mathrm{L}_{k_n}$ and $\mathrm{L}_{k_n}(s_n)/\mathrm{L}_{k_n}$ are disjoint, independently of whether s'_n is ramified or not.

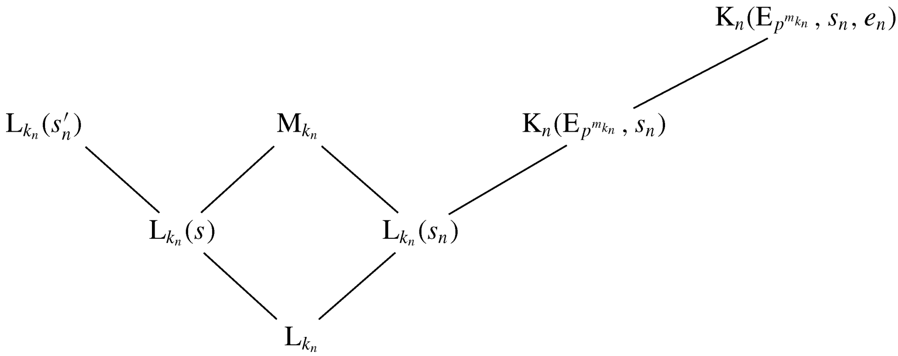
Since $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_p)$ is finite, there exists an $s \in \mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_p)$ such that $s \in \langle s''_n \rangle$ for infinitely many n. By restricting to this subsequence of ℓ_{k_n}, we can assume that $s \in \bigcap_{n \in \mathbb{N}} \langle s''_n \rangle$. If the cohomology classes s'_n are totally ramified at ℓ_{k_n} for almost all n, we set $s = 0$.

The next step in understanding the above tower of extensions is to show that $\mathrm{M}_{k_n}/\mathrm{L}_{k_n}(s_n)$ and $\mathrm{K}_n(\mathrm{E}_{p^{m_{k_n}}}, s_n)/\mathrm{L}_{k_n}(s_n)$ are disjoint. This follows by considering the action of $\mathrm{Gal}(\mathrm{L}_{k_n}/\mathrm{K})$ on $\mathrm{Gal}(\mathrm{M}_{k_n}/\mathrm{L}_{k_n}(s_n))$ and on $\mathrm{Gal}(\mathrm{K}_n(\mathrm{E}_{p^{m_{k_n}}}, s_n)/\mathrm{L}_{k_n}(s_n))$. (The action of $\mathrm{Gal}(\mathrm{L}_{k_n}(s_n)/\mathrm{K})$ on $\mathrm{Gal}(\mathrm{M}_{k_n}/\mathrm{L}_{k_n}(s_n))$ and $\mathrm{Gal}(\mathrm{K}_n(\mathrm{E}_{p^{m_{k_n}}}, s_n)/\mathrm{L}_{k_n}(s_n))$ factors through $\mathrm{Gal}(\mathrm{L}_{k_n}/\mathrm{K})$.) On the one hand, since $\mathrm{L}_{k_n}/\mathrm{K}$ and K_n/K are disjoint, $\mathrm{Gal}(\mathrm{L}_{k_n}/\mathrm{K})$ acts trivially on $\mathrm{Gal}(\mathrm{K}_n(\mathrm{E}_{p^{m_{k_n}}}, s_n)/\mathrm{L}_{k_n}(s_n))$. On the other hand,

$$\mathrm{Gal}\big(\mathrm{M}_{k_n}/\mathrm{L}_{k_n}(s_n)\big)/p\,\mathrm{Gal}\big(\mathrm{M}_{k_n}/\mathrm{L}_{k_n}(s_n)\big) \simeq \mathrm{E}_{p^{\delta_1}} \oplus \cdots \oplus \mathrm{E}_{p^{\delta_{2t-1}}}, \quad \text{where } \delta_i \in \{0, 1\},$$

as a $\mathrm{Gal}(\mathrm{L}_{k_n}/\mathrm{K})$-module.

We have the tower



Let us fix $h_{k_n}^{\circ} \in \mathrm{Gal}(K_n(E_{p^{m_{k_n}}}, s_n, e_n)/K_n(E_{p^{m_{k_n}}}, s_n))^+$.

We can now pick $h_{k_n,i} \in \mathrm{Gal}(M_{k_n}/L_{k_n}(s_n))^+$ $(i \geq 2)$ so that

$$\mathrm{Gal}(M_{k_n}/L_{k_n})^+ = \langle h_{k_n,i} \mid 1 \leq i \leq t \rangle, \quad \text{where } h_{k_n,1} = h_{k_n},$$

and if $s \neq 0$, we require that $s(h_{k_n,i}) \neq 0$ for all $i \geq 2$. (Recall that h_{k_n} was chosen after Proposition 2.5.2.) If $s = 0$, then $L_{k_n}(s_n')$ and M_{k_n} are disjoint over L_{k_n}. In this case, we fix $h_{k_n}^* \in \mathrm{Gal}(L_{k_n}(s_n')/L_{k_n})^+$ so that $s_n'(h_{k_n}^*)$ has the same order as s_n' for all $i \geq 2$.

Let us extend τ to a complex conjugation in $\mathrm{Gal}(M_{k_n}K_n(E_{p^{m_{k_n}}}, s_n)/\mathbb{Q})$. We now choose $\ell_{k_n}(i) \in \mathbb{Q}$ so that

$$\tau h_{k_n,i}' \in \mathrm{Frob}_{\ell_{k_n}(i)}(M_{k_n}/\mathbb{Q}), \quad \text{where } (\tau h_{k_n,i}')^2 = h_{k_n,i},$$

and

$$\tau h_{k_n}'' \in \mathrm{Frob}_{\ell_{k_n}(i)}\big(K_n(E_{p^{m_{k_n}}}, s_n, e_n)/\mathbb{Q}\big), \quad \text{where } (\tau h_{k_n}'')^2 = h_{k_n}^{\circ}.$$

(As in the choices made at the end of §1.4, we choose $h_{k_n,i}'$ and h_{k_n}'' to fix the fields $L_{k_n}(s_n)$ and $K_n(E_{p^{m_{k_n}}}, s_n)$, resp., thus ensuring their compatibility.)

If $s = 0$, we must also require that

$$\tau h_{k_n}''' \in \mathrm{Frob}_{\ell_{k_n}(i)}\big(L_{k_n}(s_n')/\mathbb{Q}\big), \quad \text{where } (\tau h_{k_n}''')^2 = h_{k_n}^*.$$

Finally, we set $Q_{k_n} = \{\ell_{k_n}(1) = \ell_{k_n}, \ell_{k_n}(i) \mid i = 2, \ldots, t\}$.

2.5.4

In this section, we analyze the cohomology classes that we can construct using the primes in Q_{k_n}. For each n, we consider

$$\mathrm{res}_{\ell_{k_{n'}}(i)}\big[R_n d_n\big(\ell_{k_{n'}}(i)\big) + R_n d_n\big(\ell_{k_{n'}}(1)\ell_{k_{n'}}(i)\big)\big]$$

for all n' such that $n' \geq n \geq n_0$. Since

$$\#\big(\mathrm{res}_{\ell_{k_{n'}}(i)}\big[\mathrm{R}_n d_n(\ell_{k_{n'}}(i)) + \mathrm{R}_n d_n(\ell_{k_{n'}}(1)\ell_{k_{n'}}(i))\big]\big) \leq \#(\mathrm{R}_n \oplus \mathrm{R}_n) = p^{2m_n p^n}.$$

It follows that for each n, we have an infinite set of modules of order bounded by $p^{2m_n p^n}$. By the pigeon-hole principle, we can find a subsequence k_n' such that there exist R_n-module isomorphisms

$$\begin{aligned}&\mathrm{res}_{\ell_{k_n'}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k_n'}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k_n'}(1)\ell_{k_n'}(i)\big)\big]\\ &\quad\simeq \mathrm{res}_{\ell_{k_m'}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k_m'}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k_m'}(1)\ell_{k_m'}(i)\big)\big]\end{aligned}$$

for all $m > n$.

We can then consider the formal direct limit

$$\varinjlim_n \mathrm{res}_{\ell_{k_n'}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k_n'}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k_n'}(1)\ell_{k_n'}(i)\big)\big]$$

for each $i \geq 2$. Notice that the transitional maps are injective by construction.

PROPOSITION 2.5.8
The Λ-module

$$\varinjlim_n \mathrm{res}_{\ell_{k_n'}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k_n'}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k_n'}(1)\ell_{k_n'}(i)\big)\big]$$

has corank 2 for each $i \geq 2$.

Proof
The fact that

$$\mathrm{res}_{\ell_{k_n'}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k_n'}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k_n'}(1)\ell_{k_n'}(i)\big)\big] \subseteq \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k_n'}(i)), \mathrm{E}\big)_{p^{m_n}} \simeq {\mathrm{R}_n}^2$$

implies that

$$\mathrm{res}_{\ell_{k_n'}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k_n'}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k_n'}(1)\ell_{k_n'}(i)\big)\big][T, p] \subseteq (\mathbb{Z}/p\mathbb{Z})^2,$$

and consequently, the corank of the above direct limit is at most 2. If the corank were 1, then there would exist $f \in \Lambda$ such that the invariants of

$$f\big(\mathrm{res}_{\ell_{k_n'}(i)}\big[\mathrm{R}_n d_n(\ell_{k_n'}(i)) + \mathrm{R}_n d_n(\ell_{k_n'}(1)\ell_{k_n'}(i))\big]\big)$$

are cyclic up to a finite group of order bounded independently of n.

We know that there exist τ-antiequivariant R_n-module isomorphisms

$$\mathrm{res}_{\ell_{k'_n}(i)}\, \mathrm{R}_n d_n\big(\ell_{k'_n}(i)\big) \simeq \mathrm{res}_{\ell_{k'_n}(i)} \mathrm{R}_n \alpha_n$$

and

$$\mathrm{res}_{\ell_{k'_n}(i)}\, \mathrm{R}_n d_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big) \simeq \mathrm{res}_{\ell_{k'_n}(i)}\, \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\big).$$

Under the above isomorphisms, let $s'_{\ell_{k'_n}(i)} \in \mathrm{R}_n d_n(\ell_{k'_n}(1)\ell_{k'_n}(i))$ correspond to $\mathrm{res}_{\ell_{k'_n}(i)}\, s'_n$, and let $s_{\ell_{k'_n}(i)} \in \mathrm{R}_n d_n(\ell_{k'_n}(i))$ correspond to $\mathrm{res}_{\ell_{k'_n}(i)}\, s_n$ if s'_n and s_n lie in distinct eigenspaces of τ and to $\mathrm{res}_{\ell_{k'_n}(i)}\, e_n$ otherwise. It follows that

$$\mathrm{res}_{\ell_{k'_n}(i)} \langle s_{\ell_{k'_n}(i)}, s'_{\ell_{k'_n}(i)} \rangle \subseteq \big(\mathrm{res}_{\ell_{k'_n}(i)}\, \mathrm{R}_n d_n(\ell_{k'_n}(1)\ell_{k'_n}(i))\big)^{G_n} + \big(\mathrm{res}_{\ell_{k'_n}(i)}\, \mathrm{R}_n d_n(\ell_{k'_n}(i))\big)^{G_n}$$

is not cyclic, and the orders of its generators are not bounded as n goes to ∞.

Since $\mathrm{im}\,\phi \subseteq \varinjlim \mathrm{R}_n \alpha_n$ and $\mathrm{im}\,\phi' \subseteq \varinjlim \mathrm{R}_n c_n(\ell_{k'_n}(1))$ have corank 1, $f\ \mathrm{im}\,\phi$ and $f\ \mathrm{im}\,\phi'$ have the same property. This implies that

$$\big((f\ \mathrm{im}\,\phi)^{\Gamma}\big)^{\mathrm{div}} \simeq \big((\mathrm{im}\,\phi)^{\Gamma}\big)^{\mathrm{div}} \simeq \mathbb{Q}_p/\mathbb{Z}_p,$$
$$\big((f\ \mathrm{im}\,\phi')^{\Gamma}\big)^{\mathrm{div}} \simeq \big((\mathrm{im}\,\phi')^{\Gamma}\big)^{\mathrm{div}} \simeq \mathbb{Q}_p/\mathbb{Z}_p.$$

It then follows that there exist sequences $k_{f,n}, k'_{f,n} \in \mathbb{N}$ such that

$$\mathrm{res}_{\ell_{k'_n}(i)} \langle p^{k_{f,n}} s_{\ell_{k'_n}(i)}, p^{k'_{f,n}} s'_{\ell_{k'_n}(i)} \rangle \subseteq f\Big(\mathrm{res}_{\ell_{k'_n}(i)}\big[\mathrm{R}_n d_n(\ell_{k'_n}(i)) + \mathrm{R}_n d_n(\ell_{k'_n}(1)\ell_{k'_n}(i))\big]\Big),$$

and the order of $p^{k_{f,n}} s_{\ell_{k'_n}(i)}$, as well as that of $p^{k'_{f,n}} s'_{\ell_{k'_n}(i)}$, is not bounded as n grows. Hence, the corank of $\varinjlim \mathrm{res}_{\ell_{k'_n}(i)}[\mathrm{R}_n d_n(\ell_{k'_n}(i)) + \mathrm{R}_n d_n(\ell_{k'_n}(1)\ell_{k'_n}(i))]$ is at least 2. □

We now consider

$$\mathrm{R}_n c_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n c_n\big(\ell_m(1)\ell_m(i)\big) \subseteq \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_m}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}),$$

where $i \geq 2$ and $m \in \{k'_i \mid i \geq n\}$. Since $\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_m}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) = p^{2m_n t p^n}$ with $t = \#\mathrm{Q}_m$, for each $n \in \mathbb{N}$ we have an infinite set of modules of bounded order. So, by restricting to a subsequence of $\{k'_n\}_{n\in\mathbb{N}}$, we can assume that there exist R_n-module isomorphisms

$$\mathrm{R}_n c_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big) \simeq \mathrm{R}_n c_n\big(\ell_{k'_m}(i)\big) + \mathrm{R}_n c_n\big(\ell_{k'_m}(1)\ell_{k'_m}(i)\big)$$

for all $m > n$, and we can consider the formal direct limit

$$\varinjlim_n \mathrm{R}_n c_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big).$$

Our next aim is to understand the unramified submodule of $\mathrm{R}_n c_n(\ell_{k'_n}(i)) + \mathrm{R}_n c_n(\ell_{k'_n}(1)\ell_{k'_n}(i))$.

PROPOSITION 2.5.9
There exists an $f \in \Lambda$ which annihilates the kernel of the map

$$\mathrm{R}_n c_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big) \to \mathrm{res}_{\ell_{k'_n}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big)\big] \tag{51}$$

for all $n \in \mathbb{N}$ and $i \geq 2$.

Proof
Let $\mathrm{J}_n(i) \subseteq \mathrm{I}_n(i)$ be two Λ-submodules of Λ^2 so that

$$\mathrm{R}_n c_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big) \simeq \Lambda^2/\mathrm{J}_n(i)$$

and

$$\mathrm{res}_{\ell_{k'_n}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big)\big] \simeq \Lambda^2/\mathrm{I}_n(i).$$

It follows that the kernel of the map (51) is isomorphic to $\mathrm{I}_n(i)/\mathrm{J}_n(i)$. Observe that

$$p^{m_{n+1}-m_n}\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n}\, c_{n+1} = h_{c_n} c_n \qquad \text{and} \qquad p^{m_{n+1}-m_n}\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n}\, d_{n+1} = h_{c_n} d_n$$

for almost all $n \in \mathbb{N}$ and some invertible element $h_{c_n} \in \Lambda$, where

$$c_n \in \big\{c_n\big(\ell_{k'_n}(i)\big), c_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big)\big\}, \qquad d_n \in \big\{d_n\big(\ell_{k'_n}(i)\big), d_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big)\big\},$$

and d_n is the image of c_n in $\mathrm{H}^1(\mathrm{K}_n, \mathrm{E})_{p^{m_n}}$. It follows that $1 \mapsto p^{m_{n+1}-m_n} \sum_{i=0}^{i=p-1} g^{p^n i}$ induces the injections

$$\Lambda^2/\mathrm{J}_n(i) \hookrightarrow \Lambda^2/\mathrm{J}_{n+1}(i) \qquad \text{and} \qquad \Lambda^2/\mathrm{I}_n(i) \hookrightarrow \Lambda^2/\mathrm{I}_{n+1}(i).$$

We can now consider $\varinjlim \Lambda^2/\mathrm{J}_n(i)$ and $\varinjlim \Lambda^2/\mathrm{I}_n(i)$. The identity map on Λ induces the surjective map

$$\varinjlim_n \Lambda^2/\mathrm{J}_n(i) \to \varinjlim_n \Lambda^2/\mathrm{I}_n(i).$$

By Proposition 2.5.8, we know that $\widehat{\varinjlim \Lambda^2/\mathrm{I}_n}(i)$ has rank 2 over Λ, which implies that $\widehat{\varinjlim \Lambda^2/\mathrm{J}_n}(i)$ has rank at least 2. Since the Λ-corank of $\varinjlim \Lambda^2/\mathrm{J}_n(i)$ cannot be higher than 2, we deduce that $\varinjlim \mathrm{I}_n(i)/\mathrm{J}_n(i)$ is a cotorsion Λ-module. It then follows that there exists $f_i \in \Lambda$, which annihilates $\mathrm{I}_n(i)/\mathrm{J}_n(i)$ for all n, and we set $f = \prod_{i \geq 2} f_i$. □

We now denote by H_n the module generated by all the classes that we have constructed in $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k'_n}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$,

$$\begin{aligned}\mathrm{H}_n &= \mathrm{R}_n\alpha_n + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\big) + \mathrm{R}_n c_n\big(\ell_{k'_n}(2)\big) + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\ell_{k'_n}(2)\big)\\ &\quad + \cdots + \mathrm{R}_n c_n\big(\ell_{k'_n}(t)\big) + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\ell_{k'_n}(t)\big).\end{aligned}$$

We can assume that the modules H_n are compatible by restricting to a subsequence, and we consider their direct limit

$$\mathrm{H} = \varinjlim_n \mathrm{H}_n.$$

PROPOSITION 2.5.10
The Λ*-module* H *has corank* $2t$*.*

Proof
Let us consider the map

$$\phi_n : \mathrm{H}_n \to \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(2)), \mathrm{E}_{p^{m_n}}\big) \oplus \prod_{i\ge 3} \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}\big)_{p^{m_n}}.$$

We know that

$$\mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}_{p^{m_n}}\big) = \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}_{p^{m_n}}\big)^{\mathrm{unr}} \oplus \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}\big)_{p^{m_n}}$$

and

$$\mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}\big)_{p^{m_n}} \simeq \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}_{p^{m_n}}\big)^{\mathrm{unr}} \simeq \big(\Lambda/(p^{m_n}, (T+1)^{p^n} - 1)\big)^2,$$

where $\mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}_{p^{m_n}}\big)^{\mathrm{unr}}$ denotes the unramified submodule of $\mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}_{p^{m_n}}\big)$. Observe that

$$\phi_n(\mathrm{H}_n) \cap \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}\big)_{p^{m_n}} = \mathrm{res}_{\ell_{k'_n}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big)\big]$$

for each $i \ge 2$. Furthermore, by Proposition 2.5.9, we know that there exists an $f \in \Lambda$ such that

$$f\big(\phi_n(\mathrm{H}_n) \cap \mathrm{H}^1(\mathrm{K}_n(\ell_{k'_n}(2)), \mathrm{E}_{p^{m_n}})^{\mathrm{unr}}\big) = f\,\mathrm{res}_{\ell_{k'_n}(2)}\big[\mathrm{R}_n\alpha_n + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\big)\big].$$

Notice that the image of $\mathrm{R}_n\alpha_n + \mathrm{R}_n c_n(\ell_{k'_n}(1))$ in $\prod_{i\ge 2} \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}\big)_{p^{m_n}}$ is zero. We can now look at the image of $\mathrm{R}_n\alpha_n + \mathrm{R}_n c_n(\ell_{k'_n}(1))$ in $\mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(2)), \mathrm{E}_{p^{m_n}}\big)^{\mathrm{unr}}$. By restricting to a subsequence of $\{k'_n \mid n \in \mathbb{N}\}$, we can assume that the modules $\mathrm{res}_{\ell_{k'_n}(2)}[\mathrm{R}_n\alpha_n + \mathrm{R}_n c_n(\ell_{k'_n}(1))]$ are formally compatible as n grows and can see that their direct limit has corank 2, just as we did in Proposition 2.5.8.

As in Proposition 2.5.9, for each $i \geq 2$, we have $I_n(i) \subseteq \Lambda^2$ such that

$$\Lambda^2/I_n(i) \simeq \mathrm{res}_{\ell_{k'_n}(i)}\big[\mathrm{R}_n d_n\big(\ell_{k'_n}(i)\big) + \mathrm{R}_n d_n\big(\ell_{k'_n}(1)\ell_{k'_n}(i)\big)\big] \subseteq \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(i)), \mathrm{E}\big)_{p^{m_n}}.$$

We also let $I_n(1) \subseteq \Lambda^2$ be such that

$$\Lambda^2/I_n(1) \simeq \mathrm{res}_{\ell_{k'_n}(2)}\big[\mathrm{R}_n \alpha_n + \mathrm{R}_n c_n\big(\ell_{k'_n}(1)\big)\big] \subseteq \mathrm{H}^1\big(\mathrm{K}_n(\ell_{k'_n}(2)), \mathrm{E}_{p^{m_n}}\big)^{\mathrm{unr}}.$$

We know that $\varinjlim \Lambda^2/I_n(i)$ has Λ-corank 2 for each $i \geq 1$ (by Proposition 2.5.8 for $i \geq 2$ and the above remarks for $i = 1$) and

$$\varinjlim_n f\phi_n(\mathrm{H}_n) \simeq f\Big(\bigoplus_{1\leq i\leq t} \varinjlim_n \Lambda^2/I_n(i)\Big),$$

where $t = \#\mathrm{Q}_{k'_n}$. We can then conclude that $\varinjlim f\phi_n(\mathrm{H}_n)$ has Λ-corank $2t$. Hence, the corank of H is at least $2t$.

By Proposition 2.5.9, we know that

$$\ker\big(\mathrm{R}_n c_n(\ell_{k'_n}(i)) + \mathrm{R}_n c_n(\ell_{k'_n}(1)\ell_{k'_n}(i)) \to \mathrm{res}_{\ell_{k'_n}(i)}\big[\mathrm{R}_n d_n(\ell_{k'_n}(i)) + \mathrm{R}_n d_n(\ell_{k'_n}(1)\ell_{k'_n}(i))\big]\big)$$

is annihilated by f for every $i \geq 2$. Similarly, we can show that there exists an $f_0 \in \Lambda$ which annihilates

$$\ker\big(\mathrm{R}_n \alpha_n + \mathrm{R}_n c_n(\ell_{k'_n}(1)) \to \mathrm{H}^1(\mathrm{K}_n(\ell_{k'_n}(2)), \mathrm{E}_{p^{m_n}})^{\mathrm{unr}}\big).$$

It follows that ff_0 annihilates the kernel of ϕ_n for all n, which implies that the corank of H cannot be greater than $2t$. This concludes the proof of the proposition. □

Since $\mathrm{H} = \varinjlim \mathrm{H}_n$ has corank $2t$, we know that H^Γ contains a subgroup isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{2t}$. This implies that for each $r \in \mathbb{N}$, there exists n_r such that

$$\begin{aligned}(\mathbb{Z}/p^r\mathbb{Z})^{2t} &\subseteq \mathrm{H}[g-1, p^r] \subseteq \mathrm{H}_{n_r}[g-1, p^r] \\ &\subseteq \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k'_{n_r}}}}(\mathrm{K}_{n_r}, \mathrm{E}_{p^{m_{n_r}}})[g-1, p^r] \simeq \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k'_{n_r}}}}(\mathrm{K}, \mathrm{E}_{p^r}),\end{aligned}$$

where $\Gamma = \mathrm{Gal}(\mathrm{K}_\infty/\mathrm{K}) = \langle g \rangle$.

By Proposition 2.2.4, we have

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k'_{n_r}}}}(\mathrm{K}, \mathrm{E}_{p^r}) \simeq (\mathbb{Z}/p^r\mathbb{Z})^{2t}.$$

Hence, for each $r \in \mathbb{N}$, there exists n_r such that

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k'_{n_r}}}}(\mathrm{K}, \mathrm{E}_{p^r}) \simeq \mathrm{H}_{n_r}[g-1, p^r]$$

under the restriction map.

Since Kolyvagin's cohomology classes come from points defined over abelian extensions of K, the same is true for $H^1_{\mathrm{Sel}}(K, E_{p^r})$ for every $r \in \mathbb{N}$, and this allows us to conclude as follows.

THEOREM 2.5.11
All elements of $Ш(E/K)_{p^\infty}$ *split over solvable extensions of* $\mathbb{Q}$ *if* p *is a prime of good ordinary reduction.*

Remark 2.5.12
The above theorem has only been proven when E has good ordinary nonanomalous reduction at p, but in §2.5.5, we show that it also holds when $\widetilde{E}(K_{\wp})_p \neq 0$.

2.5.5
The only new element in the case when p has good ordinary anomalous reduction lies in the behavior of the Heegner points. More precisely, 2.5.1(4) may not hold.

We have assumed that p is inert in $K/\mathbb{Q}$ in this case. Perrin-Riou [Pe, §3.3, Lemma 2] has shown that

$$a_p y_{rp^{n+1}} = y_{rp^n} + \mathrm{tr}_{K[rp^{n+2}]/K[rp^{n+1}]}\, y_{rp^{n+2}},$$
$$a_p y_r = \mathrm{tr}_{K[rp]/K[r]}\, y_{rp}$$

for any $n,\ r \in \mathbb{N}$ such that r is prime to p.

We know that since p is inert in $K/\mathbb{Q}$, the Galois group of $K[rp^\infty]/K[rp]$ is isomorphic to $\mathbb{Z}_p$, and $\mathrm{Gal}(K[rp]/K[r])$ has order $p+1$. It then follows that $k(n) = n + 1 - k_0$ for $n \geq k_0$ and $k(n) = 0$ for $n < k_0$, where $\alpha_n = \mathrm{tr}_{K[rp^{k(n)}]/K_n}\, y_{p^{k(n)}}$ and p^{k_0} is the order of the Galois group of the intersection of the maximal $\mathbb{Z}_p$-extension of K with the Hilbert class field of K, over K. For $r = 1$, we have

$$\mathrm{tr}_{K_{k_0+1}/K_{k_0}}\, \alpha_{k_0+1} = \big(a_p - a_p^{-1}(p+1)\big)\alpha_{k_0},$$
$$\mathrm{tr}_{K_{n+2}/K_{n+1}}\, \alpha_{n+2} = a_p \alpha_{n+1} - \alpha_n \quad \text{for } n \geq k_0,$$

and consequently,

$$\mathrm{tr}_{K_{k_0+1}/K_{k_0}}(\alpha_{k_0+1} - \alpha_{k_0}) = \big(a_p - a_p^{-1}(p+1) - p\big)\alpha_{k_0},$$

$$\mathrm{tr}_{K_{n+2}/K_{n+1}}(\alpha_{n+2} - \alpha_{k_0}) = a_p(\alpha_{n+1} - \alpha_{k_0}) - (\alpha_n - \alpha_{k_0}) + (a_p - 1 - p)\alpha_{k_0} \quad \text{for } n \geq k_0.$$

Since $a_p \in \{1, 1-p\}$, it follows that

$$\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n}(\alpha_{n+1} - \alpha_{k_0}) = f_n(T)(\alpha_n - \alpha_{k_0}),$$

where $f_n(T) \in \Lambda$ is invertible for all $n \geq k_0 + 1$. This implies that $\mathrm{R}_n(\alpha_n - \alpha_{k_0}) \subseteq \mathrm{R}_{n+1}(\alpha_{n+1} - \alpha_{k_0})$. In the same way, one can see that $\mathrm{R}_n(c_n(r) - c_{k_0}(r)) \subseteq \mathrm{R}_{n+1}(c_{n+1}(r) - c_{k_0}(r))$.

By replacing α_n and $c_n(r)$ by $\alpha_n - \alpha_{k_0}$ and $c_n(r) - c_{k_0}(r)$, respectively, in the arguments of §2.5.2 – 2.5.4, we construct $2t$ independent copies of $\mathbb{Q}_p/\mathbb{Z}_p$ in $\mathscr{M}_a^\Gamma$.

Observe that

(1) $\mathscr{M}_a^\Gamma[p^k] = \mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_{k_n}}}(\mathrm{K}, \mathrm{E}_{p^k})$ for any $k \leq n$,

(2) $p^{n_0}\mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_{k_n}}}(\mathrm{K}, \mathrm{E}_{p^k}) = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k_n}}}(\mathrm{K}, \mathrm{E}_{p^{k-n_0}})$

(see Proposition 2.3.5 and §2.2.2).

For every $k \in \mathbb{N}$, we can find n such that the classes that we have constructed generate $p^{n_0}\mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_{k_n}}}(\mathrm{K}, \mathrm{E}_{p^k})$. It follows that we have constructed the whole group $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}, \mathrm{E}_{p^\infty})$. It is then clear that Theorem 2.5.11 holds for primes p of good ordinary anomalous reduction.

2.6. *The supersingular case*

We now consider the case when E has good supersingular reduction at p. In this case, we need to choose the field K so that

(a) all primes dividing N split in $\mathrm{K}/\mathbb{Q}$; and

(b) p splits completely in the intersection of K_∞ with the Hilbert class field of K.

These two conditions are needed to ensure that $\mathrm{K}_{\wp_n}$ is a totally ramified extension of $\mathbb{Q}_p$ which is assumed when we use a result of Iovita and Pollack [IP, §2.6.3]. We now see that it is possible to find an imaginary quadratic field K that satisfies the above conditions.

For every prime ℓ that divides N and not $p-1$, we choose, if possible, $m_\ell \in \mathbb{N}$ prime to $\mathrm{N}p(p-1)$ so that ℓ divides $p^{m_\ell} - 1$. If such a positive integer does not exist, we set $m_\ell = 1$. Then, set $m' = \prod_{\ell \mid \mathrm{N}, \ell \nmid p-1} m_\ell$. Notice that if ℓ is a rational prime dividing $\gcd(N, p-1)$ and $m \in \mathbb{Z}$ is prime to $p(p-1)$, then ℓ^r divides $p^m - 1$ if and only if ℓ^r divides $p-1$ because ℓ divides $\sum_{k=0}^{m-1} p^k$ if and only if $\ell \mid m$.

Now, for every prime ℓ dividing N, we set r_ℓ to be the highest power of ℓ which divides $p^{m'}+1$ or $p^{m'}-1$ and $r = \max\{r_\ell : \ell \mid \mathrm{N}\}$. If $p^{m'} > \mathrm{N}^{2(2r+3)}$, then we let $m = m'$. Otherwise, we choose m_0 prime to $\mathrm{N}p(p-1)$ so that $p^{m'm_0} > \mathrm{N}^{2(2r+3)}$ and set $m = m'm_0$. It follows that ℓ^{r+1} does not divide $p^m + 1$ or $p^m - 1$ for any $\ell \mid \mathrm{N}$.

Let $a = (p^m - 1)/2$, $x = (p^m + 1)/2$ and $z \equiv x \pmod{\mathrm{N}^{2r+3}}$, where $0 < z < \mathrm{N}^{2r+3}$. Since $p^m > \mathrm{N}^{2(2r+3)} > z^2$, there exists a squarefree positive integer d such that $p^m - z^2 = dy^2$ for some $y \in \mathbb{Z}$.

Consider $K = \mathbb{Q}(\sqrt{-d})$. Since $p^m = z^2 + dy^2$, where m is odd and prime to p, it follows that p splits completely in the intersection of K_∞ with the Hilbert class field of K. We now show that N splits in $K/\mathbb{Q}$. Since $p^m = x^2 - a^2$, it follows that $dy^2 \equiv -a^2 \pmod{N^{2r+3}}$. Our choice of r implies that $\gcd(N^r, a) = \gcd(N^{2r+3}, a)$, and we set $a = a_1 a_2$, where $a_1 = \gcd(N^r, a)$ and $\gcd(a_2, N) = 1$. Consequently, $y = a_1 y_2$ for some $y_2 \in \mathbb{Z}$ such that $\gcd(y_2, N) = 1$. It follows that $-dy_2^2 \equiv a_2^2$ (mod $(N^r/a_1)^2 N^3$), and hence, $-d$ is a square modulo N^3, which implies that every prime dividing N splits in $K/\mathbb{Q}$.

2.6.1

In this case, we study the group $H^1_{\mathrm{Sel}_p}(K, E_{p^k})$ for any $k \in \mathbb{N}$ such that $p^{k-1} H^1_{\mathrm{Sel}_p}(K, E_{p^\infty})$ is divisible. We assume this restriction on k for the rest of §2.6. Recall that Sel_p imposes no local condition at primes of K dividing p, while Sel^p requires that the cohomology classes be trivial at $\wp \mid p$.

As in §2.2.1, we fix $s_1, \ldots, s_r \in H^1_{\mathrm{Sel}^p}(K, E_{p^{2k}})$ such that

$$\langle s_1, \ldots, s_r \rangle = H^1_{\mathrm{Sel}^p}(K, E_{p^\infty})^{\mathrm{div}}_{p^{2k}}.$$

It follows that each s_i has order p^{2k}.

Let Q be a set of rational primes such that:

(i) $q \in Q$ is inert in $K/\mathbb{Q}$;

(ii) $q \notin \Sigma$;

(iii) $E(K_q)_{p^\infty} = E(\overline{K_q})_{p^k}$; and

(iv) $H^1_{\mathrm{Sel}^p}(K, E_{p^k}) \hookrightarrow \prod_{q \in Q} H^1(K_q^{\mathrm{unr}}/K_q, E_{p^k})$.

We set $\Sigma' = \Sigma \cup \{\lambda_i \mid 1 \le i \le r\}$, where $\{\lambda_i \mid 1 \le i \le r\}$ is a set of primes of K not in $\Sigma \cup Q$ such that:

(a) $E(K_\lambda)_{p^\infty} = E(\overline{K_\lambda})_{p^{2k}}$ for all $\lambda \in \{\lambda_i \mid 1 \le i \le r\}$; and

(b) the local cohomology class $(s_i)_{\lambda_j}$ has order p^{2k} if $i = j$ and is trivial if $i \neq j$.

We can then consider the group $H^1{}_L(K_{\Sigma' \cup Q}/K, E_{p^{2k}})$. Observe that

$$H^1{}_{L^*}(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \subset H^1_{\mathrm{Sel}^p}(K, E_{p^{2k}}).$$

This implies that Proposition 2.2.2 applies, and we have

$$0 \longrightarrow H^1(K_{\Sigma'}/K, E_{p^{2k}}) \longrightarrow H^1(K_{\Sigma' \cup Q}/K, E_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^{2t} \longrightarrow 0,$$

where t denotes the cardinality of the set Q.

PROPOSITION 2.6.1

The following sequence is exact:

$$0 \longrightarrow H^1_{\mathrm{Sel}_p}(K, E_{p^{2k}}) \longrightarrow H^1_{\mathrm{Sel}_{Q \cup p}}(K, E_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^{2t-r} \longrightarrow 0.$$

Proof
Set $W = \prod_{\lambda\in\Sigma'\setminus\{p\}} H^1(K_\lambda, E_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k})$. We apply the snake lemma to the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(K_{\Sigma'}/K, E_{p^{2k}}) & \longrightarrow & H^1(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) & \longrightarrow & (\mathbb{Z}/p^k\mathbb{Z})^{2t} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_2} & & \downarrow & & \\
0 & \longrightarrow & W & \longrightarrow & W & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

and we get

$$\begin{array}{ccccccc}
0 & \longrightarrow & H^1_{\mathrm{Sel}_p}(K_{\Sigma'}/K, E_{p^{2k}}) & \longrightarrow & H^1_{\mathrm{Sel}_{Q\cup p}}(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) & \longrightarrow & (\mathbb{Z}/p^k\mathbb{Z})^{2t} \\
 & & & & & & \downarrow \\
 & & 0 & \longleftarrow & \operatorname{coker}\phi_2 & \xleftarrow{\gamma_0} & \operatorname{coker}\phi_1
\end{array}$$

Seeing the maps ϕ_1 and ϕ_2 as part of the corresponding exact sequences of Cassels, Poitou, and Tate, we have

$$\begin{array}{ccccc}
H^1(K_{\Sigma'}/K, E_{p^{2k}}) & \xrightarrow{\phi_1} & \prod_{\lambda\in\Sigma'\setminus\{p\}} H^1(K_\lambda, E_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_1} & \widehat{H^1_{(\mathrm{Sel}_p)^*}(K, E_{p^{2k}})} \\
\downarrow & & \downarrow & & \downarrow \\
H^1(K_{\Sigma'\cup Q}/K, E_{p^{2k}}) & \xrightarrow{\phi_2} & \prod_{\lambda\in\Sigma'\setminus\{p\}} H^1(K_\lambda, E_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_2} & \widehat{H^1_{(\mathrm{Sel}_{Q\cup p})^*}(K, E_{p^{2k}})}
\end{array}$$

Since $\mathrm{Sel} = \mathrm{Sel}^*$, it follows that

$$H^1_{(\mathrm{Sel}_p)^*}(K, E_{p^{2k}}) = H^1_{\mathrm{Sel}^p}(K, E_{p^{2k}}) \qquad \text{and} \qquad H^1_{(\mathrm{Sel}_{Q\cup p})^*}(K, E_{p^{2k}}) = H^1_{\mathrm{Sel}^{Q\cup p}}(K, E_{p^{2k}}).$$

We show that $H^1_{\mathrm{Sel}^{Q\cup p}}(K, E_{p^{2k}}) = H^1_{\mathrm{Sel}^p}(K, E_{p^k})$. As we saw in the proof of Proposition 2.2.3, properties (iii) and (iv) of the elements of Q imply that

$$H^1_{\mathrm{Sel}^p}(K, E_{p^k}) \subseteq H^1_{\mathrm{Sel}^{Q\cup p}}(K, E_{p^{2k}}) \subseteq H^1_{\mathrm{Sel}}(K, E_{p^k}).$$

Since $E_{p^k}(K_\wp) = 0$, we have $H^1(K_\wp, E_{p^k}) \hookrightarrow H^1(K_\wp, E_{p^{2k}})$, and consequently, $H^1_{\mathrm{Sel}^{Q\cup p}}(K, E_{p^{2k}}) \subseteq H^1_{\mathrm{Sel}^p}(K, E_{p^k})$. It then follows that

$$H^1_{\mathrm{Sel}^{Q\cup p}}(K, E_{p^{2k}}) = H^1_{\mathrm{Sel}^p}(K, E_{p^k}),$$

and the right-hand square of the above diagram may be viewed as

$$\begin{array}{ccc}
\prod_{\lambda\in\Sigma'\setminus\{p\}} H^1(K_\lambda, E_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_1} & \widehat{H^1_{\mathrm{Sel}^p}(K, E_{p^{2k}})} \\
\downarrow & & \downarrow \\
\prod_{\lambda\in\Sigma'\setminus\{p\}} H^1(K_\lambda, E_{p^{2k}})/\mathrm{Sel}_\lambda(p^{2k}) & \xrightarrow{\psi_2} & \widehat{H^1_{\mathrm{Sel}^p}(K, E_{p^k})}
\end{array}$$

We have now reduced the problem to an exact copy of the one in Proposition 2.2.3, except that the Selmer condition has been replaced by Sel^p. Therefore, we deduce that $\ker \gamma_0 \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$, which implies that

$$0 \longrightarrow \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \longrightarrow (\mathbb{Z}/p^k\mathbb{Z})^{2t-r} \longrightarrow 0. \qquad \square$$

PROPOSITION 2.6.2
The group $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^k})$ *is isomorphic to* $(\mathbb{Z}/p^k\mathbb{Z})^{2(t+1)}$, *where* t *denotes the cardinality of the set* Q.

Proof
Let us consider the map

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^{2k}}) \oplus \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}}). \tag{52}$$

We know that

$$\mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}}) \simeq \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}) \oplus \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}})$$

for all $q \in \mathrm{Q}$.

We have seen in the proof of Proposition 2.6.1 that the kernel of the map in (52) is $\mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^k})$. In order to understand its image, we analyze the images of the maps

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q, \mathrm{E}_{p^{2k}})/\mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}), \tag{53}$$

$$\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{q\in\mathrm{Q}} \mathrm{H}^1(\mathrm{K}_q^{\mathrm{unr}}/\mathrm{K}_q, \mathrm{E}_{p^{2k}}), \tag{54}$$

$$\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to \prod_{\wp | p} \mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^{2k}}). \tag{55}$$

By Proposition 2.6.1, the image of the map (53) is isomorphic to $(\mathbb{Z}/p^k\mathbb{Z})^{2t-r}$. We have assumed that $p^k\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$, and we know that the kernel of the map (54) is $\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^k})$. It follows that the image of the map (54) is isomorphic to $(\mathbb{Z}/p^k\mathbb{Z})^r$. Let us now consider the image of the map (55). By using the fact that $(\mathrm{Sel}_p)^* = (\mathrm{Sel}^p)$ and (15) as in the proof of Theorem 1.1.7, we have

$$\#\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^{2m}})/\#\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^{2m}}) = p^{4m} \quad \text{for all } m \in \mathbb{N}.$$

We know that

$$\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \simeq (\mathbb{Z}/p^{2k}\mathbb{Z})^r \times \mathbb{Z}/p^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{m_{2t-r}}\mathbb{Z}, \tag{56}$$

where $m_i \leq k-1$, and the m_i's are independent of k as $k \to \infty$. It follows that

$$\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \simeq (\mathbb{Z}/p^{2k}\mathbb{Z})^{r+2} \times \mathbb{Z}/p^{m_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{m_{2t-r}}\mathbb{Z}. \tag{57}$$

This implies that the image of the map (55) is isomorphic to $(\mathbb{Z}/p^{2k}\mathbb{Z})^2$. Finally, using

$$\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \ker(55) \subseteq \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^{2k}}) = \ker(53) \subseteq \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}}),$$

we see that the image of (52) contains a subgroup isomorphic to $(\mathbb{Z}/p^{2k}\mathbb{Z})^2 \oplus (\mathbb{Z}/p^k\mathbb{Z})^{2t}$. By comparing the sizes of the groups appearing below, we claim that there is an exact sequence

$$0 \to \mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^k}) \to \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \to (\mathbb{Z}/p^{2k}\mathbb{Z})^2 \oplus (\mathbb{Z}/p^k\mathbb{Z})^{2t} \to 0.$$

Here, we use Proposition 2.6.1 to compute the quotient of the orders of $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ and $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^{2k}})$, and then (56) and (57) to relate $\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^{2k}})$ with $\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}, \mathrm{E}_{p^k})$.

Using the properties of the elements of Q and the fact that $\mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^k}) = 0$, we deduce that $\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^k}) = p^{2k(t+1)}$. It then follows that

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^{2k}}) \simeq (\mathbb{Z}/p^{2k}\mathbb{Z})^{r+2} \times \mathbb{Z}/p^{m_1+k}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{m_{2t-r}+k}\mathbb{Z}.$$

Hence, we conclude that

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}\cup p}}(\mathrm{K}, \mathrm{E}_{p^k}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^{2(t+1)}. \qquad \square$$

2.6.2

Let us choose $n_0 \in \mathbb{N}$ so that it satisfies §2.3.1(2), and $p^{n_0-1}\mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_{p^\infty})$ is p-divisible.

Consider $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n\cup p}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ for all $n \geq n_0$, where Q_n and m_n are defined in §2.3.1, except that instead of property (4), we only require

$$\mathrm{H}^1_{\mathrm{Sel}^p}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}}) \hookrightarrow \prod_{q\in \mathrm{Q}_n} \mathrm{H}^1\big(\mathrm{K}_n(q)^{\mathrm{unr}}/\mathrm{K}_n(q), \mathrm{E}_{p^{m_n}}\big).$$

PROPOSITION 2.6.3

We have $\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n\cup p}}(\mathrm{K}_m, \mathrm{E}_{p^k}) = \#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2(t+1)}$ *for all* $m \leq n$ *and* $k \leq m_n$.

Proof

The proof of this proposition is the same as that of Proposition 2.3.1, except for a few minor differences that we describe. We know that

$$\mathrm{H}^1_{(\mathrm{Sel}_{\mathrm{Q}_n\cup p})^*}(\mathrm{K}_m, \mathrm{E}_{p^k}) = \mathrm{H}^1_{\mathrm{Sel}^{\mathrm{Q}_n\cup p}}(\mathrm{K}_m, \mathrm{E}_{p^k}) = 0.$$

Consequently, the properties of the elements of Q_n allow us to deduce that

$$\#\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n \cup p}}(\mathrm{K}_m, \mathrm{E}_{p^k}) = p^{2kp^m} \prod_{q \in \mathrm{Q}_n} \#\mathrm{E}\big(\mathrm{K}_m(q)\big)_{p^k} = \#(\mathbb{Z}/p^k\mathbb{Z}[G_m])^{2t+2}. \qquad \square$$

As in Proposition 2.3.2, one can verify that the set Q_n satisfies the properties that we required for Proposition 2.6.2, and therefore, we have

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n \cup p}}(\mathrm{K}, \mathrm{E}_{p^{m_n}}) \simeq (\mathbb{Z}/p^{m_n}\mathbb{Z})^{2t+2} \quad \text{for all } n \geq n_0.$$

In addition, one can easily prove, as we have done in Proposition 2.3.3, that

$$\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n \cup p}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m} = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n \cup p}}(\mathrm{K}_m, \mathrm{E}_{p^{m_n}}) \quad \text{for all } m \leq n.$$

We now consider the R_n^τ-modules $\mathrm{X}(k, n) = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_k \cup p}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ for all $n \leq k$ and inductively choose a sequence $\mathrm{X}_n = \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k_n} \cup p}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$ of compatible R_n^τ-module structures. Let us define the $\mathbb{Z}_p[[\Gamma]]$-module

$$\mathscr{M}_s := \varinjlim_n \mathrm{X}_n.$$

THEOREM 2.6.4
The Λ-module $\widehat{\mathscr{M}_s}$ is isomorphic to Λ^{2t+2}.

Proof
The proof of this theorem is identical to that of Theorem 2.3.4, if one replaces $2t$ by $2t + 2$. $\square$

2.6.3
Since the issue of choosing the sets Q_n with the required properties is the same as in the ordinary case, which was studied in §2.4.1, we now prove that the Heegner points $\alpha_n \in \mathrm{E}(\mathrm{K}_n)$ give rise to two independent copies of $\hat{\Lambda}$ in the module $\mathscr{M}_s$.

Since we are assuming that $p \geq 5$, we know that $a_p = 0$. Perrin-Riou [Pe, §3.3, Lemma 2] has shown that

$$a_p y_{rp^{n+1}} = y_{rp^n} + \mathrm{tr}_{\mathrm{K}[rp^{n+2}]/\mathrm{K}[rp^{n+1}]} y_{rp^{n+2}}$$

for $n \geq 0$ and any $r \in \mathbb{N}$ prime to p. It then follows that

$$y_{rp^n} = -\mathrm{tr}_{\mathrm{K}[rp^{n+2}]/\mathrm{K}[rp^{n+1}]} y_{rp^{n+2}},$$

which in turn implies that

$$\alpha_n = -\mathrm{tr}_{\mathrm{K}_{n+2}/\mathrm{K}_{n+1}} \alpha_{n+2} \qquad \text{and} \qquad c_n(r) = -\mathrm{tr}_{\mathrm{K}_{n+2}/\mathrm{K}_{n+1}} c_{n+2}(r)$$

for $n \geq k_0 + 1$ (where $\mathrm{K}[1] \cap \mathrm{K}_\infty = \mathrm{K}_{k_0}$) and r a squarefree product of primes ℓ such that $\mathrm{Frob}_\ell(\mathrm{K}(\mathrm{E}_{p^{m_{n+2}}})/\mathbb{Q}) = \tau$.

We can then define $\varinjlim \mathrm{R}_{2n}\alpha_{2n}$ and $\varinjlim \mathrm{R}_{2n+1}\alpha_{2n+1}$. As in Theorem 2.5.1, one can see that these Λ-modules are not cotorsion. We now need to distinguish the above two modules from one another.

LEMMA 2.6.5
The submodule of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ *generated by* $\varinjlim \mathrm{R}_{2n}\alpha_{2n}$ *and* $\varinjlim \mathrm{R}_{2n+1}\alpha_{2n+1}$ *has corank at least* 2.

Proof
Let us consider the exact sequence

$$0 \longrightarrow \mathrm{E}^1(\mathrm{K}_{\wp_n}) \longrightarrow \mathrm{E}(\mathrm{K}_{\wp_n}) \longrightarrow \widetilde{\mathrm{E}}(k_{\wp_n}) \longrightarrow 0.$$

Following Kobayashi [K], we now define the following submodules of $\mathrm{E}^1(\mathrm{K}_{\wp_n})$:

$$\mathrm{E}^{1+}(\mathrm{K}_{\wp_n}) := \left\{x \in \mathrm{E}^1(\mathrm{K}_{\wp_n}) \,\middle|\, \mathrm{tr}_{\mathrm{K}_{\wp_n}/\mathrm{K}_{\wp_m}}(x) \in \mathrm{E}^1(\mathrm{K}_{\wp_{m-1}}) \text{ for all } 1 \leq m \leq n,\ m \text{ odd}\right\},$$

$$\mathrm{E}^{1-}(\mathrm{K}_{\wp_n}) := \left\{x \in \mathrm{E}^1(\mathrm{K}_{\wp_n}) \,\middle|\, \mathrm{tr}_{\mathrm{K}_{\wp_n}/\mathrm{K}_{\wp_m}}(x) \in \mathrm{E}^1(\mathrm{K}_{\wp_{m-1}}) \text{ for all } 1 \leq m \leq n,\ m \text{ even}\right\}.$$

Since $\mathrm{K}_{\wp_n}/\mathbb{Q}_p$ is totally ramified at p and $\widetilde{\mathrm{E}}(k_{\wp_n})_p = 0$, it follows that $\widetilde{\mathrm{E}}(k_{\wp_n}) = \widetilde{\mathrm{E}}(\mathbb{Q}_p)$ and that there exists $m_\circ \in \mathbb{N}$ prime to p and independent of n such that $m_\circ \mathrm{E}(\mathrm{K}_{\wp_n}) \subseteq \mathrm{E}^1(\mathrm{K}_{\wp_n})$. Hence, the fact that $\alpha_n = -\mathrm{tr}_{\mathrm{K}_{n+2}/\mathrm{K}_{n+1}}\alpha_{n+2}$ for all $n \geq k_0 + 1$ implies that

$$m_\circ \mathrm{Res}_{\wp_{2n+1}}(\mathbb{Z}[G_{2n}]\alpha_{2n}) \in \mathrm{E}^{1+}(\mathrm{K}_{\wp_{2n+1}}), \qquad m_\circ \mathrm{Res}_{\wp_{2n+1}}(\mathbb{Z}[G_{2n+1}]\alpha_{2n+1}) \in \mathrm{E}^{1-}(\mathrm{K}_{\wp_{2n+1}})$$

and

$$\mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n}\alpha_{2n}) \subseteq \mathrm{E}^{1+}(\mathrm{K}_{\wp_{2n+1}})/p^{m_{2n}}, \qquad \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n+1}\alpha_{2n+1}) \subseteq \mathrm{E}^{1-}(\mathrm{K}_{\wp_{2n+1}})/p^{m_{2n+1}}.$$

We analyze the intersection of $\mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n}\alpha_{2n})$ and $\mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n+1}\alpha_{2n+1})$. Let

$$P^+ \in \mathrm{Res}_{\wp_{2n+1}}(\mathbb{Z}[G_{2n}]\alpha_{2n}) \qquad \text{and} \qquad P^- \in \mathrm{Res}_{\wp_{2n+1}}(\mathbb{Z}[G_{2n+1}]\alpha_{2n+1})$$

so that $P^+ \equiv P^- \pmod{p^{m_{2n+1}}}$. This is equivalent to saying that there exists $Q \in \mathrm{E}(\mathrm{K}_{\wp_{2n+1}})$ such that $P^+ - P^- = p^{m_{2n+1}}Q$. Iovita and Pollack [IP] have shown that

$$0 \to \mathrm{E}^1(\mathrm{K}_\wp) \to \mathrm{E}^{1+}(\mathrm{K}_{\wp_n}) \oplus \mathrm{E}^{1-}(\mathrm{K}_{\wp_n}) \to \mathrm{E}^1(\mathrm{K}_{\wp_n}) \to 0$$

for all $n \in \mathbb{N}$, which implies that $m_\circ Q = Q^+ + Q^-$, where $Q^+ \in \mathrm{E}^{1+}(\mathrm{K}_{\wp_{2n+1}})$ and $Q^- \in \mathrm{E}^{1-}(\mathrm{K}_{\wp_{2n+1}})$. Consequently, we have

$$m_\circ P^+ - p^{m_{2n+1}} Q^+ = m_\circ P^- + p^{m_{2n+1}} Q^- \in \mathrm{E}^1(\mathrm{K}_\wp).$$

Since $m_\circ$ is prime to p, it follows that

$$\mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n}\alpha_{2n}) \cap \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n+1}\alpha_{2n+1}) \subseteq \mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^{m_{2n+1}}}). \tag{58}$$

We now consider the submodules

$$\varinjlim_n \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n}\alpha_{2n}), \qquad \varinjlim_n \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n+1}\alpha_{2n+1}) \subseteq \varinjlim_n \mathrm{H}^1(\mathrm{K}_{\wp_{2n+1}}, \mathrm{E}_{p^{m_{2n+1}}}).$$

By (58), we know that

$$\varinjlim_n \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n}\alpha_{2n}) \cap \varinjlim_n \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n+1}\alpha_{2n+1}) \subseteq \mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^\infty}).$$

When p is a prime of supersingular reduction, the representation of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on $\mathrm{E}(\overline{\mathbb{Q}_p})_p$ is known to be absolutely irreducible with image of order $2(p^2-1)$. Since $\mathrm{Gal}(\mathrm{K}_{\wp_n}/\mathbb{Q}_p) \simeq \mathbb{Z}/p^n\mathbb{Z}$, we have

$$\mathrm{E}(\mathrm{K}_{\wp_n})_{p^\infty} = \mathrm{E}(\mathbb{Q}_p)_{p^\infty} = 0.$$

In view of the above result, the argument used in Theorem 2.5.1 can easily be adapted to prove that the coranks of $\varinjlim \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n}\alpha_{2n})$ and $\varinjlim \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n+1}\alpha_{2n+1})$ are not zero. Moreover, we know that the intersection of $\varinjlim \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n}\alpha_{2n})$ and $\varinjlim \mathrm{Res}_{\wp_{2n+1}}(\mathrm{R}_{2n+1}\alpha_{2n+1})$ lies in $\mathrm{H}^1(\mathrm{K}_\wp, \mathrm{E}_{p^\infty})$, and therefore, it is cotorsion. Thus the submodule of $\mathrm{H}^1_{\mathrm{Sel}}(\mathrm{K}_\infty, \mathrm{E}_{p^\infty})$ generated by $\varinjlim \mathrm{R}_{2n}\alpha_{2n}$ and $\varinjlim \mathrm{R}_{2n+1}\alpha_{2n+1}$ has corank at least 2. □

2.6.4

We now choose the primes that we need in order to construct the ramified cohomology classes. Since $\varinjlim \mathrm{R}_{2n}\alpha_{2n}$ and $\varinjlim \mathrm{R}_{2n+1}\alpha_{2n+1}$ have nontrivial coranks, we have the nonzero maps

$$\phi^+ : \hat{\Lambda} \to \varinjlim_n \mathrm{R}_{2n}\alpha_{2n},$$

$$\phi^- : \hat{\Lambda} \to \varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n+1}.$$

The fact that $\phi + \phi^\tau$ and $\phi - \phi^\tau$ cannot be simultaneouly zero for $\phi = \phi^+$ or $\phi = \phi^-$ allows us to assume that $(\phi)^\tau = \pm\phi$ for $\phi = \phi^\pm$. We fix $s_n^+ \in \mathrm{R}_{2n}\alpha_{2n}$ and

$s_n^- \in \mathrm{R}_{2n+1}\alpha_{2n+1}$ so that

$$\langle s_n^+\rangle = \big((\mathrm{im}\,\phi^+)^\Gamma\big)^{\mathrm{div}} \cap (\mathrm{R}_{2n}\alpha_{2n})^{G_{2n}}, \qquad \langle s_n^-\rangle = \big((\mathrm{im}\,\phi^-)^\Gamma\big)^{\mathrm{div}} \cap (\mathrm{R}_{2n+1}\alpha_{2n+1})^{G_{2n+1}}$$

and

$$\varinjlim_n (\mathbb{Z}/p^{m_{2n}}\mathbb{Z})s_n^+ \in [\varinjlim_n \mathrm{R}_{2n}\alpha_{2n}]^\Gamma, \qquad \varinjlim_n (\mathbb{Z}/p^{m_{2n+1}}\mathbb{Z})s_n^- \in [\varinjlim_n \mathrm{R}_{2n+1}\alpha_{2n+1}]^\Gamma.$$

It follows that $s_n^\pm \in \mathrm{H}^1_{\mathrm{Sel_p}}(\mathrm{K}, \mathrm{E}_{p^\infty})$ are eigenvectors of τ and

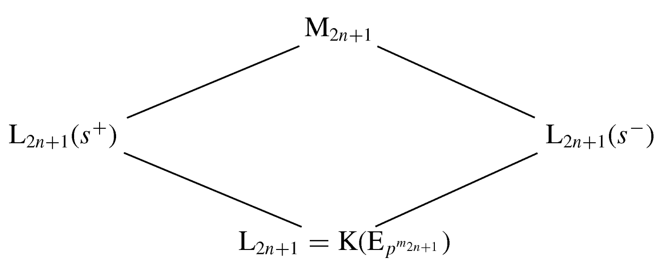
$$\varinjlim_n (\mathbb{Z}/p^{m_{2n}}\mathbb{Z})s_n^+ \simeq \varinjlim_n (\mathbb{Z}/p^{m_{2n+1}}\mathbb{Z})s_n^- \simeq \mathbb{Q}_p/\mathbb{Z}_p.$$

Let $s^\pm \in \mathrm{H}^1_{\mathrm{Sel_p}}(\mathrm{K}, \mathrm{E}_p)$ be such that

$$\varinjlim_n (\mathbb{Z}/p^{m_{2n}}\mathbb{Z})s_n^+ \cap \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_p) = \langle s^+\rangle,$$
$$\varinjlim_n (\mathbb{Z}/p^{m_{2n+1}}\mathbb{Z})s_n^- \cap \mathrm{H}^1_{\mathrm{Sel}_p}(\mathrm{K}, \mathrm{E}_p) = \langle s^-\rangle.$$

We then have three cases to consider.

Case 1: s^+ and s^- lie in different eigenspaces of the complex conjugation τ. Consider the field extensions



where M_{2n+1} denotes the fixed field of $\mathrm{Gal}(\overline{\mathrm{L}}_{2n+1}/\mathrm{L}_{2n+1})$ which pairs to zero with the finite subgroup $\mathrm{H}^1_{\mathrm{Sel_p}}(\mathrm{K}, \mathrm{E}_{p^{m_{2n+1}}})$ of $\mathrm{H}^1(\mathrm{K}, \mathrm{E}_{p^{m_{2n+1}}})$.

We choose $h_{2n+1,i} \in \mathrm{Gal}(\mathrm{M}_{2n+1}/\mathrm{L}_{2n+1})^+$ so that

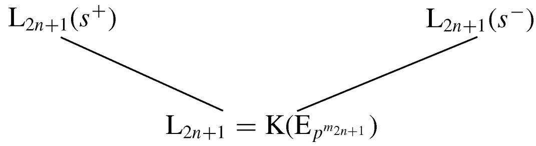
$$s^+(h_{2n+1,i}) \neq 0, \qquad s^-(h_{2n+1,i}) \neq 0,$$

and

$$\langle h_{2n+1,i} \mid i = 1, \ldots, t\rangle = \mathrm{Gal}(\mathrm{M}_{2n+1}/\mathrm{L}_{2n+1})^+.$$

We now fix primes $\ell_{2n+1}(i) \in \mathbb{Q}$ so that $\tau h'_{2n+1,i} \in \mathrm{Frob}_{\ell_{2n+1}(i)}(\mathrm{M}_{2n+1}/\mathbb{Q})$, where $h_{2n+1,i} = (\tau h'_{2n+1,i})^2$. Then we set $\mathrm{Q}_{2n+1} = \{\ell_{2n+1}(i) \mid i = 1, \ldots, t\}$.

Case 2: $\langle s^+\rangle \cap \langle s^-\rangle = 0$. We can assume that $s^{\pm}$ are eigenvectors of τ lying in the same eigenspace because if $s_n^{\pm}$ were in different eigenspaces, then we would go back to the case 1. We now show that the field extensions



are disjoint. If these two extensions are not disjoint, we must have

$$\mathrm{Gal}\big(L_{2n+1}(s^+)/L_{2n+1}\big) = \mathrm{Gal}\big(L_{2n+1}(s^-)/L_{2n+1}\big).$$

In this case, we let $h \in \mathrm{Gal}(L_{2n+1}(s^{\pm})/L_{2n+1})$ generate $\mathrm{Gal}(L_{2n+1}(s^{\pm})/L_{2n+1})^+$, the 1-eigenspace for the action of τ. Since s^+ and s^- lie in the same eigenspace of τ, we can see that $s^+(h) = xs^-(h)$ for some $(x \in \mathbb{Z}/p\mathbb{Z})^*$. It then follows that

$$(s^+ - xs^-)\big(\mathrm{Gal}(L_{2n+1}(s^{\pm})/L_{2n+1})^+\big) = 0.$$

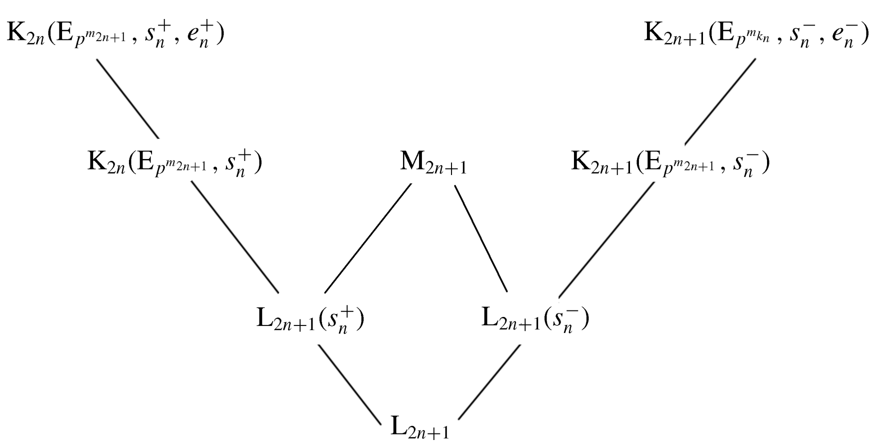
This implies that $s^+ - xs^- = 0$ and contradicts our assumption that $\langle s^+\rangle \cap \langle s^-\rangle = 0$.

The fact that $L_{2n+1}(s^+)$ and $L_{2n+1}(s^-)$ are disjoint over L_{2n+1} implies that the extensions $L_{2n+1}(s_n^+)/L_{2n+1}$ and $L_{2n+1}(s_n^-)/L_{2n+1}$ are also disjoint. As in case 2 of §2.5.3, we choose

(a) $e_n^+ \in (\mathrm{im}\,\phi^+ \cap R_{2n}\alpha_{2n}) - [R_{2n}\alpha_{2n}]^{G_{2n}}$ so that the image of $\varinjlim \langle e_n^+, s_n^+\rangle$ in $(\mathrm{im}\,\phi^+)/\langle s_n^+ \mid n \in \mathbb{N}\rangle$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a Λ-module; and

(b) $e_n^- \in (\mathrm{im}\,\phi^- \cap R_{2n+1}\alpha_{2n+1}) - [R_{2n+1}\alpha_{2n+1}]^{G_{2n+1}}$ so that the image of $\varinjlim \langle e_n^-, s_n^-\rangle$ in $(\mathrm{im}\,\phi^-)/\langle s_n^- \mid n \in \mathbb{N}\rangle$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a Λ-module.

We then consider the tower of field extensions



We know that $K_{2n}(E_{p^{m_{2n+1}}}, s_n^+, e_n^+)$ (resp., $K_{2n+1}(E_{p^{m_{2n+1}}}, s_n^-, e_n^-)$) and M_{2n+1} are disjoint over $L_{2n+1}(s_n^+)$ (resp., $L_{2n+1}(s_n^-)$). Let us fix nonzero elements

$$h_n^{\circ+} \in \mathrm{Gal}\big(K_{2n}(E_{p^{m_{2n+1}}}, s_n^+, e_n^+)/K_{2n}(E_{p^{m_{2n+1}}}, s_n^+)\big)^+$$

and

$$h_n^{\circ-} \in \mathrm{Gal}\big(K_{2n+1}(E_{p^{m_{2n+1}}}, s_n^-, e_n^-)/K_{2n+1}(E_{p^{m_{2n+1}}}, s_n^-)\big)^+.$$

We can now pick $h_{n,i} \in \mathrm{Gal}(M_{2n+1}/L_{2n+1}(s_n^+))^+$ $(1 \le i \le t-1)$ so that

$$\mathrm{Gal}\big(M_{2n+1}/L_{2n+1}(s_n^+)\big)^+ = \langle h_{n,i} \mid 1 \le i \le t-1\rangle$$

and

$$s^-(h_{n,i}) \neq 0 \quad \text{for all } i \le t-1,$$

and $h_{n,t} \in \mathrm{Gal}(M_{2n+1}/L_{2n+1}(s_n^-))^+$ so that $s^+(h_{n,t}) \neq 0$.

We choose primes $\ell_{2n+1}(i) \in \mathbb{Q}$ so that

$$\tau h'_{n,i} \in \mathrm{Frob}_{\ell_{2n+1}(i)}(M_{2n+1}/\mathbb{Q}), \quad \text{where } (\tau h'_{n,i})^2 = h_{n,i},$$
$$\tau h_n^{*+} \in \mathrm{Frob}_{\ell_{2n+1}(i)}\big(K_{2n}(E_{p^{m_{2n+1}}}, s_n^+, e_n^+)/\mathbb{Q}\big), \quad \text{where } (\tau h_n^{*+})^2 = h_n^{\circ+} \text{ for all } i \le t-1,$$
$$\tau h_n^{*-} \in \mathrm{Frob}_{\ell_{2n+1}(t)}\big(K_{2n+1}(E_{p^{m_{2n+1}}}, s_n^-, e_n^-)/\mathbb{Q}\big), \quad \text{where } (\tau h_n^{*-})^2 = h_n^{\circ-}.$$

This ensures that the invariants of the restriction at $\ell_{2n+1}(i)$ of $\operatorname{im}\phi^+ \cap R_{2n}\alpha_{2n}$ and of $\operatorname{im}\phi^- \cap R_{2n+1}\alpha_{2n+1}$ lie in distinct eigenspaces of τ. Finally, we set $Q_{2n+1} = \{\ell_{2n+1}(i) \mid i = 1, \dots, t\}$.

Case 3: $\langle s^+\rangle \cap \langle s^-\rangle \neq 0$. In this case, we have $\langle s^+\rangle = \langle s^-\rangle$. Since the module

$$R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1} \subseteq H^1_{\mathrm{Sel}}(K_{2n+1}, E_{p^{m_{2n+1}}})$$

is fixed by the complex conjugation τ and the Λ-corank of

$$\varinjlim_n (R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1})$$

is at least 2 by Lemma 2.6.5, one can check that there exists a map

$$\psi : \hat{\Lambda}^2 \longrightarrow \varinjlim_n (R_{2n}\alpha_{2n} + R_{2n+1}\alpha_{2n+1})$$

such that $\operatorname{im}\psi$ has Λ-corank 2 and $\tau(\operatorname{im}\psi) = \operatorname{im}\psi$. It follows that $(\operatorname{im}\psi)^\Gamma \subseteq H^1_{\mathrm{Sel_p}}(K, E_{p^\infty})$ contains a finite-index subgroup generated by two disjoint copies of $\mathbb{Q}_p/\mathbb{Z}_p$ which we denote by $\varinjlim (\mathbb{Z}/p^{m_{2n+1}}\mathbb{Z})s'_n$ and $\varinjlim (\mathbb{Z}/p^{m_{2n+1}}\mathbb{Z})s''_n$. Moreover, as $\tau(\operatorname{im}\psi) = \operatorname{im}\psi$, we can assume that s'_n and s''_n are eigenvectors of τ.

Let s' (resp., s'') be a generator of the intersection of $\varinjlim (\mathbb{Z}/p^{m_{2n+1}}\mathbb{Z})s'_n$ (resp., $\varinjlim (\mathbb{Z}/p^{m_{2n+1}}\mathbb{Z})s''_n$) with $\mathrm{H}^1_{\mathrm{Sel_p}}(\mathrm{K}, \mathrm{E}_p)$. We can assume that $\langle s^+\rangle \neq \langle s'\rangle$. There exists a map

$$\phi' : \hat{\Lambda} \longrightarrow \varinjlim_n (\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1})$$

such that $(\phi')^\tau = \pm\phi'$ and $\varinjlim \langle s'_n\rangle \subseteq (\mathrm{im}\,\phi')^\Gamma$. If s^+ and s' lie in distinct eigenspaces of τ, we choose Q_{k_n} using the method of case 1 with s' instead of s^-. Otherwise, we pick

$$e'_n \in \big((\mathrm{im}\,\phi') \cap (\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1})\big) - (\mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1})^\Gamma$$

so that the image of $\varinjlim \langle e'_n, s'_n\rangle$ in $(\mathrm{im}\,\phi')/\langle s'_n \mid n \in \mathbb{N}\rangle$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a Λ-module. We can then replace s^-_n and e^-_n with s'_n and e'_n, respectively, and proceed just as we did in case 2.

Finally, for every $i \in \{1, \dots, t\}$, we consider the modules

$$\mathrm{R}_{2n}c_{2n}\big(\ell_{2m+1}(i)\big),\ \mathrm{R}_{2n+1}c_{2n+1}\big(\ell_{2m+1}(i)\big) \subseteq \mathrm{H}^1(\mathrm{K}_{2n+1}, \mathrm{E}_{p^{m_{2n+1}}}) \quad \text{for all } m \geq n.$$

Just as we did in §2.5.4, we choose a sequence of k_n so that

$$\begin{aligned}&\mathrm{Res}_{\ell_{k_{2n+1}}(i)}\big[\mathrm{R}_{2n}c_{2n}\big(\ell_{k_{2n+1}}(i)\big) + \mathrm{R}_{2n+1}c_{2n+1}\big(\ell_{k_{2n+1}}(i)\big)\big]\\ &\quad\simeq \mathrm{Res}_{\ell_{k_{2m+1}}(i)}\big[\mathrm{R}_{2n}c_{2n}\big(\ell_{k_{2m+1}}(i)\big) + \mathrm{R}_{2n+1}c_{2n+1}\big(\ell_{k_{2m+1}}(i)\big)\big]\end{aligned}$$

for all $m > n$, and we consider the direct limits

$$\varinjlim_n \mathrm{Res}_{\ell_{k_{2n+1}}(i)}\big[\mathrm{R}_{2n}c_{2n}\big(\ell_{k_{2n+1}}(i)\big) + \mathrm{R}_{2n+1}c_{2n+1}\big(\ell_{k_{2n+1}}(i)\big)\big]$$

for each $i \in \{1, \dots, t\}$. By our choice of the primes Q_{k_n}, as in Proposition 2.5.8, we can show that each of the above Λ-modules has corank 2.

Let us now consider $\mathrm{H}_n \subseteq \mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_{k'_n}\cup\{p\}}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$, defined as

$$\begin{aligned}\mathrm{H}_n &= \mathrm{R}_{2n}\alpha_{2n} + \mathrm{R}_{2n+1}\alpha_{2n+1} + \mathrm{R}_{2n}c_{2n}\big(\ell_{k_{2n+1}}(1)\big) + \mathrm{R}_{2n+1}c_{2n+1}\big(\ell_{k_{2n+1}}(1)\big)\\ &\quad + \cdots + \mathrm{R}_{2n}c_{2n}\big(\ell_{k_{2n+1}}(i)\big) + \mathrm{R}_{2n+1}c_{2n+1}\big(\ell_{k_{2n+1}}(i)\big).\end{aligned}$$

By restricting to a subsequence of $\{k_n \mid n \in \mathbb{N}\}$, we can assume that the H_n are compatible as n grows. We consider their direct limit

$$\mathrm{H} = \varinjlim_n \mathrm{H}_n.$$

In the same manner as in the ordinary case (Proposition 2.5.10), H can be shown to have Λ-corank $2t+2$ by analyzing the image of the map

$$\phi_n : \mathrm{H}_n \to \mathrm{H}^1\big(\mathrm{K}_{2n+1}(\ell_{k_{2n+1}}(1)), \mathrm{E}_{p^{m_{2n+1}}}\big) \oplus \prod_{i\geq 2} \mathrm{H}^1\big(\mathrm{K}_{2n+1}(\ell_{k_{2n+1}}(i)), \mathrm{E}\big)_{p^{m_{2n+1}}}.$$

This implies that the invariants of H contain $2t+2$ copies of $\mathbb{Q}_p/\mathbb{Z}_p$, and consequently, we have the following.

THEOREM 2.6.6
The elements of $\text{Ш}(\mathrm{E}/\mathrm{K})_{p^\infty}$ *split over solvable extensions of* $\mathbb{Q}$ *for all primes* p *of good reduction.*

2.7. The multiplicative case
The situation in the case when E has multiplicative reduction at p is nearly identical to the one in which p is a prime of good ordinary reduction. One of the important differences is the definition of the Heegner points. Let Np denote the conductor of E. We assume that the primes dividing N split and that $\mathrm{N} = \mathcal{N}\overline{\mathcal{N}}$. Let $\langle 1, \omega\rangle = \mathcal{O}_\mathrm{K}$, where $\mathcal{O}_\mathrm{K}$ denotes the ring of integers of K. The Heegner point of conductor rp^n for $r \in \mathbb{N}$ such that $\gcd(p, r) = 1$, $x_{rp^n} = (\mathbb{C}/(rp^n\omega, 1), \ker \mathcal{N}, \langle rp^{n-1}\omega\rangle) \in \mathrm{X}_0(\mathrm{N}p)$ is defined over the ring class field K_{rp^n}. Let y_{rp^n} denote the image of x_{rp^n} under $\pi : \mathrm{X}_0(\mathrm{N}p) \to \mathrm{E}$.

LEMMA 2.7.1
We have $\mathrm{U}_p y_{rp^n} = \mathrm{tr}_{\mathrm{K}_{rp^{n+1}}/\mathrm{K}_{rp^n}}\, y_{rp^{n+1}}$.

Proof
One can check that this formula holds on $\mathrm{J}_0(\mathrm{N}p) = \mathrm{Jac}\,\mathrm{X}_0(\mathrm{N}p)$ by using the standard definition of the correspondence U_p

$$\mathrm{U}_p(\mathrm{E}, \mathrm{G}_\mathrm{N}, \mathrm{G}_p) = \sum (\mathrm{E}/\mathrm{G}'_p, \overline{\mathrm{G}_\mathrm{N}}, \overline{\mathrm{G}_p}),$$

where G'_p runs through the p-subgroups of E distinct from G_p, and $\overline{\mathrm{G}_\mathrm{N}}$ (resp., $\overline{\mathrm{G}_p}$) denote the images of G_N (resp., G_p) in $\overline{\mathrm{E}} = \mathrm{E}/\mathrm{G}'_p$. □

Let $\mathrm{K}_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mathrm{K}_{p^n}$, $\mathrm{K}_\infty = \mathrm{K}_{p^\infty}^{\mathrm{Gal}(\mathrm{K}_{p^\infty}/\mathrm{K})^{\mathrm{tors}}}$, and let

$$\alpha_n = \mathrm{tr}_{\mathrm{K}_{p^\infty}/\mathrm{K}_\infty}\, y_{p^n} \in \mathrm{E}(\mathrm{K}_\infty).$$

Cornut [C] has shown that infinitely many of the points $\{\alpha_n \mid n \in \mathbb{N}\}$ are non-torsion. Denote by K_n the subextension of K_∞ so that $\mathrm{Gal}(\mathrm{K}_n/\mathrm{K}) \simeq \mathbb{Z}/p^n\mathbb{Z}$. By

Lemma 2.7.1, we know that

$$\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n}\,\alpha_{n+1} = \mathrm{U}_p\alpha_n.$$

Since E has multiplicative reduction at p, we know that $U_p\alpha_n = \pm\alpha_n$, and hence, $\mathrm{tr}_{\mathrm{K}_{n+1}/\mathrm{K}_n}\,\alpha_{n+1} = \pm\alpha_n$. Consequently, the fact that α_{n_0} is nontorsion for some $n_0 \in \mathbb{N}$ implies that α_n is nontorsion for all $n \geq n_0$, and there exists some $k \in \mathbb{N}$ such that if $n \geq k$, then α_n and α_{n+1} are not defined over the same layer of K_∞. This is enough to prove that $\widehat{\varinjlim \mathrm{R}_n\alpha_n}$ is of nontrivial Λ-corank, as we did in Theorem 2.5.1.

The only other step of the proof when the reduction of E at p plays a role is in comparing $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{G_n/G_m}$ with $\mathrm{H}^1_{\mathrm{Sel}_{\mathrm{Q}_n}}(\mathrm{K}_m, \mathrm{E}_{p^{m_n}})$ for $m \leq n$. In order to do this, we need to relax the Selmer condition at primes above p as we did in the case when p is a prime of good ordinary anomalous reduction (see §2.3.2). We can then consider $\mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})$. The only conditions needed for the proof of

$$\mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_n}}(\mathrm{K}_n, \mathrm{E}_{p^{m_n}})^{\mathrm{Gal}(\mathrm{K}_n/\mathrm{K}_k)} = \mathrm{H}^1_{\mathrm{Sel}'_{\mathrm{Q}_n}}(\mathrm{K}_k, \mathrm{E}_{p^{m_n}})$$

for all $k \leq n$ are

(i) $\mathrm{E}^1(\mathrm{K}_{\wp_m})_{p^\infty} = 0$ for all $m \in \mathbb{N}$; and

(ii) $\mathrm{E}(\mathrm{K}_{\wp_m})_{p^\infty} = \mathrm{E}(\mathrm{K}_{\wp_{k_0}})_{p^\infty}$ for some $k_0 \in \mathbb{N}$.

When E has split multiplicative reduction at p, we choose $\mathrm{K}/\mathbb{Q}$ so that p does not split. This implies that our $\mathbb{Z}_p$-extension K_∞ is disjoint from the cyclotomic one. Hence, $\mathrm{E}^1(\mathrm{K}_{\wp_m})_{p^\infty} = 0$, and this in turn implies that $\mathrm{E}(\mathrm{K}_{\wp_m})_{p^\infty} = \mathrm{E}(\mathrm{K}_{\wp})_{p^\infty}$.

In the case when E has nonsplit multiplicative reduction at p, we choose an imaginary quadratic extension K so that E has split multiplicative reduction at the prime above p. Then, by the argument for the split case, we see that conditions (i) and (ii) hold.

2.8. Conclusion

We have proved that for every rational prime p, where E does not have additive reduction, the elements of $\text{Ш}(\mathrm{E}/\mathbb{Q})_{p^\infty}$ come from points defined over solvable extensions of $\mathbb{Q}$. Hence, we can conclude the following.

THEOREM 2.8.1

If E *is semistable, then each element of* $\text{Ш}(\mathrm{E}/\mathbb{Q})$ *splits over some solvable extension of* $\mathbb{Q}$.

Remark 2.8.2

When E has additive reduction at some rational prime p, the group $\text{Ш}(\mathrm{E}/\mathbb{Q})_p$ may be nontrivial. In this case, we have not been able to prove directly the same result as in the semistable case. We believe that a more natural approach is to base change to a solvable totally real field, where the curve has semistable reduction, and to apply our approach with the totally real field as base field. We hope to discuss this in a subsequent paper.

References

[B] M. I. BAŠMAKOV, *Cohomology of Abelian varieties over a number field* (in Russian), Uspehi Mat. Nauk **27**, no. 6 (1972), 25 – 66; English translation in Russian Math. Surveys **27** (1972), 25 – 70. MR 0399110

[BD] M. BERTOLINI and H. DARMON, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, J. Reine Angew. Math. **412** (1990), 63 – 74. MR 1079001

[BCDT] C. BREUIL, B. CONRAD, F. DIAMOND, and R. TAYLOR, *On the modularity of elliptic curves over* $\mathbb{Q}$*: Wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843 – 939. MR 1839918

[BFH] D. BUMP, S. FRIEDBERG, and J. HOFFSTEIN, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Invent. Math. **102** (1990), 543 – 618. MR 1074487

[C] C. CORNUT, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), 495 – 523. MR 1908058

[D] H. DARMON, *Integration on* $\mathcal{H}_p \times \mathcal{H}$ *and arithmetic applications*, Ann. of Math. (2) **154** (2001), 589 – 639. MR 1884617

[G] R. GREENBERG, "Introduction to Iwasawa theory for elliptic curves" in *Arithmetic Algebraic Geometry (Park City, Utah, 1999)*, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, 2001, 407 – 464. MR 1860044

[Gr] B. H. GROSS, "Kolyvagin's work on modular elliptic curves" in *L-Functions and Arithmetic (Durham, U.K., 1989)*, London Math. Soc. Lecture Note Ser. **153**, Cambridge Univ. Press, Cambridge, 1991, 235 – 256. MR 1110395

[GZ] B. H. GROSS and D. B. ZAGIER, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225 – 320. MR 0833192

[IP] A. IOVITA and R. POLLACK, *Iwasawa theory of elliptic curves at supersingular primes over* $\mathbb{Z}_p$*-extensions of number fields*, J. Reine Angew. Math. **598** (2006), 71 – 103. MR 2270567

[K] S. KOBAYASHI, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), 1 – 36. MR 1965358

[Ko1] V. A. KOLYVAGIN, "Euler systems" in *The Grothendieck Festschrift, Vol. II*, Progr. Math. **87**, Birkhäuser, Boston, 1990, 435 – 483. MR 1106906

[Ko2] ———, *On the structure of Selmer groups*, Math. Ann. **291** (1991), 253 – 259. MR 1129365

[Ko3] ———, "On the structure of Shafarevich-Tate groups" in *Algebraic Geometry (Chicago, 1989)*, Lecture Notes in Math. **1479**, Springer, Berlin, 1991, 94 – 121. MR 1181210

[MR] B. MAZUR and K. RUBIN, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799. MR 2031496

[M] W. G. MCCALLUM, “Kolyvagin’s work on Shafarevich-Tate groups” in *L-Functions and Arithmetic (Durham, U.K., 1989)*, London Math. Soc. Lecture Note Ser. **153**, Cambridge Univ. Press, Cambridge, 1991, 295 – 316. MR 1110398

[Mi] J. S. MILNE, *Arithmetic Duality Theorems*, Perspect. Math. **1**, Academic Press, Boston, 1986. MR 0881804

[MM] M. R. MURTY and V. K. MURTY, *Mean values of derivatives of modular L-series*, Ann. of Math. (2) **133** (1991), 447 – 475. MR 1109350

[P] A. PÁL, *Solvable points on projective algebraic curves*, Canad. J. Math. **56** (2004), 612 – 637. MR 2057289

[Pe] B. PERRIN-RIOU, *Fonctions L p-adiques, théorie d’Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), 399 – 456. MR 0928018

[R] K. RUBIN, “The work of Kolyvagin on the arithmetic of elliptic curves” in *Arithmetic of Complex Manifolds (Erlangen, West Germany, 1988)*, Lecture Notes in Math. **1399**, Springer, Berlin, 1989, 128 – 136. MR 1034261

[S1] J.-P. SERRE, “Facteur locaux des fonctions zêta des variétés algébriques (définitions et conjectures)” in *Séminaire Delange-Pisot-Poitou, 11e année: 1969/70: Théorie des numbers, fasc. 2: Exposés 16 á 24*, Secrétariat Mathématique, Paris, 1970, no. 19. MR 0401396

[S2] ———, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259 – 331. MR 0387283

[T] R. TAYLOR, *Galois representations*, Ann. Fac. Sci. Toulouse Math. (6) **13** (2004), 73 – 119. MR 2060030

[TW] R. TAYLOR and A. WILES, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), 553 – 572. MR 1333036

[V] V. VATSAL, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), 219 – 261. MR 1953292

[W] J.-L. WALDSPURGER, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. (9) **60** (1981), 375 – 484. MR 0646366

[Wi] A. WILES, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math. (2) **141** (1995), 443 – 551. MR 1333035

Çiperiani
Department of Mathematics, Columbia University, New York, New York 10027, USA;
mirela@math.columbia.edu

Wiles
Department of Mathematics, Princeton University, Princeton, New Jersey 08544, USA;
wiles@math.princeton.edu