Asian J. Math.
Vol. 24, No. 3, pp. 437–456, June 2020

ON THE Λ-COTORSION SUBGROUP OF THE SELMER GROUP[*]

AHMED MATAR[†]

Abstract. Let E be an elliptic curve defined over a number field K with supersingular reduction at all primes of K above p. If K_∞/K is a $\mathbb{Z}_p$-extension such that $E(K_\infty)[p^\infty]$ is finite and $H^2(G_S(K_\infty), E[p^\infty]) = 0$, then we prove that the Λ-torsion subgroup of the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty)$ is pseudo-isomorphic to the Pontryagin dual of the fine Selmer group of E over K_∞. This is the Galois-cohomological analog of a flat-cohomological result of Wingberg.

Key words. elliptic curve, Selmer group, Iwasawa theory.

Mathematics Subject Classification. 11R23, 11G05, 12G05.

1. Introduction. If A is a Hausdorff, abelian locally-compact topological group we denote its Pontryagin dual by A^*. Let Γ be a pro-p group isomorphic to $\mathbb{Z}_p$ and let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the completed group ring. If A is a finitely generated Λ-module, we let $T_\Lambda(A)$ denote its Λ-torsion submodule. Also we let $\dot{A}$ be the Λ-module A with the inverse Λ-action: $\gamma \cdot a = \gamma^{-1}a$ for $a \in A, \gamma \in \Gamma$. We denote $T_\Lambda(\dot{A})$ by $\dot{T}_\Lambda(A)$.

We now define the p^∞-Selmer group and the fine p^∞-Selmer group. Assume that p is a prime, F a number field and E is an elliptic curve defined over F. Let S be a finite set of primes of F containing all the primes dividing p, all the primes where E has bad reduction and all the archimedean primes. We let F_S be the maximal extension of F unramified outside S. Suppose now that L is a field with $F \subseteq L \subseteq F_S$. We let $G_S(L) = \mathrm{Gal}(F_S/L)$ and S_L be the set of primes of L above those in S. We define the p^∞-Selmer group of E/L as

$$0 \longrightarrow \mathrm{Sel}_{p^\infty}(E/L) \longrightarrow H^1(G_S(L), E[p^\infty]) \longrightarrow \prod_{v\in S_L} H^1(L_v, E)[p^\infty].$$

Also we define the fine p^∞-Selmer group of E/L as

$$0 \longrightarrow R_{p^\infty}(E/L) \longrightarrow H^1(G_S(L), E[p^\infty]) \longrightarrow \prod_{v\in S_L} H^1(L_v, E[p^\infty]).$$

The goal of this paper is to prove the following result

Theorem 1.1. *Let K be a number field, E an elliptic curve defined over K and p a rational prime such that E has good supersingular reduction at all primes of K above p. Let K_∞/K be a $\mathbb{Z}_p$-extension such that every prime of K above p ramifies and such that: (i) $E(K_\infty)[p^\infty]$ is finite (ii) $H^2(G_S(K_\infty), E[p^\infty]) = 0$. Then there exists a pseudo-isomorphism*

$$\dot{T}_\Lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*) \sim R_{p^\infty}(E/K_\infty)^*.$$

Concerning the conditions in the theorem, condition (i) is a mild one (see proposition 1.2 below) whereas condition (ii) implies that $R_{p^\infty}(E/K_\infty)^*$ is Λ-torsion (see theorem 2.2).

[*] Received November 19, 2018; accepted for publication July 30, 2019.

[†] Department of Mathematics, University of Bahrain, P.O. Box 32038, Sukhair, Bahrain (amatar@uob.edu.bh).

The theorem shows a nice relationship between the structures of the Selmer and fine Selmer group that is not at all clear exists from the definitions of these groups. The Selmer group in the supersingular case is difficult to deal with mainly due to the lack of a control theorem. The above theorem, we hope, will help us understand the structure of the Selmer group by proving results about the fine Selmer group which is more approachable.

Let p be a fixed odd prime. If K is a number field, we let K^{cyc} be the cyclotomic $\mathbb{Z}_p$-extension of K and if K is an imaginary quadratic field, we let K^{anti} be the anticyclotomic $\mathbb{Z}_p$-extension of K. Coates and Sujatha ([5] conjecture A) and the author ([14] conjecture B) have conjectured when $K_\infty = K^{cyc}$ (respectively $K_\infty = K^{anti}$) that $R_{p^\infty}(E/K_\infty)^*$ is a finitely generated $\mathbb{Z}_p$-module. This is equivalent to $R_{p^\infty}(E/K_\infty)^*$ being a Λ-torsion module with μ-invariant zero. Taking into account theorem 2.2, the above theorem then predicts that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^*$ has μ-invariant zero when E has supersingular reduction at primes of K above p.

Using the results of Wuthrich [27], one can in some cases prove results on the structure of $R_{p^\infty}(E/K_\infty)^*$ and hence by the above theorem (if it's conditions are met) give results on $T_\Lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. To illustrate this, consider the curve $E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$. This curve has supersingular reduction at $p = 29$. Let $\mathbb{Q}^{cyc}$ be the cyclotomic $\mathbb{Z}_{29}$-extension of $\mathbb{Q}$. Wuthrich ([27] prop. 9.3) has shown that $R_{p^\infty}(E/\mathbb{Q}^{cyc})$ is finite. This together with theorem 2.2 guarantees that condition (ii) of theorem 1.1 is satisfied. Also by proposition 1.2 condition (i) is satisfied since for example E does not have CM. It follows from theorem 1.1 that $T_\Lambda(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}^{cyc})^*)$ is finite.

We give one more example. Let $K = \mathbb{Q}(\sqrt{-7})$ and K_∞/K the anticyclotomic $\mathbb{Z}_{29}$-extension of K. By using Wuthrich's work, the author has shown ([14] sec 4) that $R_{p^\infty}(E/K_\infty)^*$ is Λ-torsion with $\mu = 0$. Hence by theorem 1.1 $\mathrm{Sel}_{p^\infty}(E/K_\infty)^*$ has $\mu = 0$.

Wingberg ([24] corollary 2.5) has proven a similar result to theorem 1.1 stated in terms of flat cohomology rather than Galois cohomology. Although it may appear that the above theorem follows from Wingberg's result, the author has found difficulties in attempting such a deduction in the case when a prime v of K where E has bad reduction splits completely in K_∞/K. The following argument illustrates the potential obstacles. Let E and K be as in the theorem and let $\mathcal{E}$ be the Néron model of E over $\mathcal{O}_K$.

To attempt to deduce the above theorem from Wingberg's result, one would hope to show that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^*$ and $H^1(\mathcal{O}_\infty, \mathcal{E}[p^\infty])^*$ are pseudo-isomorphic (where $\mathcal{O}_\infty$ is the ring of integers of K_∞). In hope of showing the existence of such a pseudo-isomorphism, one may use the results of Česnavičius's paper [3] as they are relevant. Assuming that no prime v of K where E has bad reduction splits completely in K_∞/K, the proof of [3] prop. 5.4 together with [3] prop. 2.5 show that the difference between the groups $\mathrm{Sel}_{p^\infty}(E/K_n)$ and $H^1(\mathcal{O}_{K_n}, \mathcal{E}[p^\infty])$ is finite and bounded with n. This proves that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^*$ and $H^1(\mathcal{O}_\infty, \mathcal{E}[p^\infty])^*$ are pseudo-isomorphic in this case. However in the case when a prime v of K where E has bad reduction splits completely in K_∞/K, this argument can fail and hence it is unclear that a pseudo-isomorphism exists in this case.

Also in order to invoke Wingberg's theorem, one needs the Λ-module $H^2(\mathcal{O}_\infty, \mathcal{E}[p^\infty])^*$ to be torsion. If no prime v of K where E has bad reduction splits completely in K_∞/K, then assuming $H^2(G_S(K_\infty), E[p^\infty]) = 0$ one can deduce the fact that $H^2(\mathcal{O}_\infty, \mathcal{E}[p^\infty])^*$ is Λ-torsion from [9] prop. 3, prop. 2.3 below, [21] sec3 corollary 5 and Česnavičius's results referred to above. However such a deduction can fail when a prime v of K where E has bad reduction splits completely in K_∞/K.

The above arguments illustrate the difficulties in attempting to deduce theorem 1.1 from Wingberg's result. Everything is done in this paper with Galois cohomology. Our method of proof generally follows Wingberg's with major differences being that all exact sequences arising from the spectral sequences of Schneider [20] are replaced with sequences arising from the snake lemma together with the Kummer sequence. The other difference is that the Artin-Mazur duality of flat cohomology groups is replaced with the Poitou-Tate duality of Galois cohomology groups.

The following proposition shows that condition (i) in theorem 1.1 is a mild one. As the proposition shows, all elliptic curves without complex multiplication satisfy condition (i) in the theorem. For elliptic curves with complex multiplication a slightly weaker version of theorem 1.1 is given in [1].

Proposition 1.2. *With the setup and conditions in theorem 1.1, we have that $E(K_\infty)[p^\infty]$ is finite in the following cases:*

(1) *E does not have complex multiplication;*

(2) *K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension of K;*

(3) *p is odd and splits in $K/\mathbb{Q}$.*

Proof. (i) Suppose that E does not have complex multiplication. By a theorem of Serre [22] this implies that $\mathrm{Gal}(K(E[p^\infty])/K)$ is an open subgroup of $GL_2(\mathbb{Z}_p)$. Suppose that $E(K_\infty)[p^\infty]$ is infinite. Then either $E(K_\infty)[p^\infty]$ has $\mathbb{Z}_p$-corank one or $E[p^\infty]$ is rational over K_∞. In the first case $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ has a one-dimensional $\mathrm{Gal}(\bar{K}/K)$-invariant subspace. This clearly contradicts Serre's theorem. In the second case $K(E[p^\infty])/K$ is a subextension of K_∞/K and hence must be an abelian extension. This also contradicts Serre's theorem.
(ii) Follows from Ribet's theorem [19]
(iii) Suppose thet p is odd and splits in $K/\mathbb{Q}$. Choose a prime v of K above p. Since E has supersingular reduction at v, we have $E(K_v)[p^\infty] = E(\mathbb{Q}_p)[p^\infty] = \hat{E}(p\mathbb{Z}_p)[p^\infty]$ where $\hat{E}$ is the formal group of $E/\mathbb{Q}_p$. By [23] ch. 4 th. 6.1 $\hat{E}(p\mathbb{Z}_p)$ has no p-torsion if p is odd so $E(K_v)[p^\infty] = \{0\}$. Therefore $E(K_\infty)[p^\infty]^\Gamma = E(K)[p^\infty] = \{0\}$ which implies that $E(K_\infty)[p^\infty] = \{0\}$. □

2. Proof of Theorem. Theorem 1.1 will be proven in this section. The proof will be broken up into a number of propositions. We keep all the definitions and notation from the introduction and furthermore denote Γ^{p^n} by Γ_n.

Let A be a finitely generated Λ-module. We let $T_\Lambda(A)$ and $T_\mu(A)$ be the Λ-torsion submodule and $\mathbb{Z}_p$-torsion submodule of A respectively. Then define $T_\lambda(A) := T_\Lambda(A)/T_\mu(A)$. As in the introduction, we use the notation $\dot{T}_-(A) = T_-(\dot{A})$. We have the following lemma of Wingberg ([24] lemma 1.1)

Lemma 2.1. *Let A be a finitely generated Λ-module. Then we have pseudo-isomorphisms*

(i) $\varprojlim_{n,m} (A^*/p^m)^{\Gamma_n} \sim \dot{T}_\mu(A)$

(ii) $\varprojlim_{n,m} (A^*[p^m])_{\Gamma_n} \sim \dot{T}_\lambda(A)$

(iii) $\varprojlim_{n,m} (A^*/p^m)_{\Gamma_n} \sim 0$

where the inverse limits are taken with respect to multiplication-by-p resp. canonical surjection and the norm map resp. canonical surjection.

Now let F be a number field, S a finite set of primes of F and B a finite G_S-module whose order is only divisible by rational primes lying below primes in S. Define $B' := \mathrm{Hom}(B, \mu)$ where μ is the group of all roots of unity in $\mathbb{C}$. We let F_S be the maximal extension of F unramified outside S. Suppose now that L is a number field with $F \subseteq L \subseteq F_S$. We let $G_S(L) = \mathrm{Gal}(F_S/L)$ and S_L be the set of primes of L above those in S. Then we have the following perfect Poitou-Tate duality pairing ([17] theorem 8.6.7)

$$Ш^1(G_S(L), B') \times Ш^2(G_S(L), B) \to \mathbb{Q}/\mathbb{Z} \tag{1}$$

where $Ш^i(G_S(L), M)$ (M is any G_S-module) is defined to be the kernel of the restriction map $H^i(G_S(L), M) \to \prod_{v\in S_L} H^i(L_v, M)$. If L_∞/F is an infinite extension contained in F_S we define $Ш^i(G_S(L_\infty), M) = \varinjlim Ш^i(G_S(L'), M)$ where the direct limit is taken over all intermediate finite extensions L'/L contained in L_∞ with respect to the restriction maps.

Now if E is an elliptic curve defined over F, p a rational prime and S a finite set of primes of F containing all primes dividing p, then for any $n \geq 0$ the Weil pairing together with the above pairing give a perfect pairing

$$\langle\ ,\ \rangle : Ш^1(G_S(L), E[p^n]) \times Ш^2(G_S(L), E[p^n]) \to \mathbb{Q}_p/\mathbb{Z}_p. \tag{2}$$

Now let L' be a finite extension of L contained in F_S. The definition of this pairing (see [17] theorem 8.6.7) shows that it is induced by the cup product. Therefore for $a \in Ш^1(G_S(L'), E[p^n])$ and $b \in Ш^2(G_S(L), E[p^n])$ we have $\langle \mathrm{cor}\, a, b\rangle = \langle a, \mathrm{res}\, b\rangle$ where $\mathrm{cor} : Ш^1(G_S(L'), E[p^n]) \to Ш^1(G_S(L), E[p^n])$ is the corestriction map and $\mathrm{res} : Ш^2(G_S(L), E[p^n]) \to Ш^2(G_S(L'), E[p^n])$ is the restriction map.

The following theorem is well-known (see for example [18] prop. 1.3.2). Using the above pairing and a control theorem, we will present another proof of this theorem

Theorem 2.2. *Let K be a number field, p a rational prime, K_∞/K a $\mathbb{Z}_p$-extension and E an elliptic curve defined over K. Let S be a finite set of primes of K containing all the primes dividing p, all the primes where E has bad reduction and all the archimedean primes. Then $R_{p^\infty}(E/K_\infty)^*$ is Λ-torsion if and only if $Ш^2(G_S(K_\infty), E[p^\infty])^*$ is Λ-torsion. If p is odd, this statement is equivalent to $H^2(G_S(K_\infty), E[p^\infty]) = 0$.*

Proof. Suppose that p is odd. According to [9] prop. 4, $H^2(G_S(K_\infty), E[p^\infty])$ is a cofree Λ-module. We will now show that $Ш^2(G_S(K_\infty), E[p^\infty]) = H^2(G_S(K_\infty), E[p^\infty])$. This together with the result just mentioned will show that the second statement of the theorem will follow from the first. Let w be a prime of K_∞ above a prime v is S. We will show that $H^2(K_{\infty,w}, E[p^\infty]) = 0$. This is true for archimedean primes w since p is odd.

Now assume that w is nonarchimedean. We consider two cases. First we consider the case where v splits completely in K_∞/K. In this case we have $H^2(K_{\infty,w}, E[p^\infty]) = H^2(K_v, E[p^\infty])$. By Tate local duality this group is dual to $T_p(E(K_v)[p^\infty])$ (the p-adic Tate module of $E(K_v)[p^\infty]$) and hence $H^2(K_{\infty,w}, E[p^\infty]) = 0$ since $E(K_v)[p^\infty]$ is finite. Now consider the case where v does not split completely in K_∞/K. In this case, the extension $K_{\infty,w}/K_v$ is an infinite pro-p extension. Hence by [17] theorem 7.1.8(i) $cd_p(K_{\infty,w}) \leq 1$. So $H^2(K_{\infty,w}, E[p^\infty]) = 0$ in this case also. This proves that $Ш^2(G_s(K_\infty), E[p^\infty]) = H^2(G_S(K_\infty), E[p^\infty])$ as desired.

Now we prove the first statement. By the restriction-corestriction property of the pairing (2), the Pontryagin dual of $Ш^2(G_S(K_\infty), E[p^\infty])$ can be identified with

$\varprojlim_{n,m} Ш^1(G_S(K_n), E[p^m])$ where K_n is the fixed field of Γ_n and the inverse limit is taken over m with regards to multiplication-by-p and over n with regards to corestriction. Therefore we see that to prove the first statement, we must show that $\mathrm{rank}_\Lambda(\varprojlim_{n,m} Ш^1(G_S(K_n), E[p^m])) = \mathrm{rank}_\Lambda(R_{p^\infty}(E/K_\infty)^*)$.

Consider the group $\varprojlim_{n,m} Ш^1(G_S(K_\infty), E[p^\infty])[p^m]^{\Gamma_n} = \varprojlim_{n,m} R_{p^\infty}(E/K_\infty)[p^m]^{\Gamma_n}$ where the inverse limit is taken over m with regards to multiplication-by-p and over n with regards to the norm map. According to [17] prop. 5.5.10(i) this group is a free Λ-module with rank equal to the the Λ-corank of $R_{p^\infty}(E/K_\infty)$. Therefore it will suffice to show that

$$\begin{aligned}\mathrm{rank}_\Lambda(\varprojlim_{n,m} Ш^1(G_S(K_n), E[p^m])) &= \mathrm{rank}_\Lambda(\varprojlim_{n,m} Ш^1(G_S(K_\infty), E[p^m])^{\Gamma_n}) && (3)\\ &= \mathrm{rank}_\Lambda(\varprojlim_{n,m} Ш^1(G_S(K_\infty), E[p^\infty])[p^m]^{\Gamma_n}). && (4)\end{aligned}$$

We first show the equality (4). For any $m \geq 0$ the snake lemma gives a long exact sequence which we split into two short exact sequences below

$$0 \to \mathcal{M}_{p^m}(E/K_\infty) \to Ш^1(G_S(K_\infty), E[p^m]) \to \mathcal{D}_{p^m}(E/K_\infty) \to 0 \qquad (5)$$

$$0 \to \mathcal{D}_{p^m}(E/K_\infty) \to Ш^1(G_S(K_\infty), E[p^\infty])[p^m] \to \mathcal{C}_{p^m}(E/K_\infty) \qquad (6)$$

where $\mathcal{M}_{p^m}(E/K_\infty) = E(K_\infty)[p^\infty]/p^m \cap Ш^1(G_S(K_\infty), E[p^m]), \mathcal{D}_{p^m}(E/K_\infty) = \mathrm{img}(Ш^1(G_S(K_\infty), E[p^m]) \to Ш^1(G_S(K_\infty), E[p^\infty])[p^m])$ and $\mathcal{C}_{p^m}(E/K_\infty) = \mathrm{coker}(E(K_\infty)[p^\infty]/p^m \to \bigoplus_{w \in S_\infty} E(K_{\infty,w})[p^\infty]/p^m)$. S_∞ being the primes of K_∞ above those in S.

For any $n \geq 0$, the sequence (5) induces another sequence

$$0 \to \mathcal{M}_{p^m}(E/K_\infty)^{\Gamma_n} \to Ш^1(G_S(K_\infty), E[p^m])^{\Gamma_n} \to \mathcal{D}_{p^m}(E/K_\infty)^{\Gamma_n} \to \mathcal{M}_{p^m}(E/K_\infty)_{\Gamma_n}.$$

We claim that all the groups in this exact sequence are finite. Since $E(K_\infty)[p^\infty]/p^m$ is finite, therefore the first and last terms of the sequence are finite. So we only have to show that the third term is finite. This will follow if we show that $Ш^1(G_S(K_\infty), E[p^\infty])[p^m]^{\Gamma_n}$ is finite. The finiteness of this group is easily seen by taking Pontryagin duals and noting that $Ш^1(G_S(K_\infty), E[p^\infty])^*$ is a finitely generated Λ-module ($Ш^1(G_S(K_\infty), E[p^\infty]) \subseteq \mathrm{Sel}_{p^\infty}(E/K_\infty)$ and $\mathrm{Sel}_{p^\infty}(E/K_\infty)^*$ is a finitely generated Λ-module by [12] theorem 4.5). Therefore we have seen that all the groups in the above exact sequence are finite and so by taking inverse limits the sequence remains exact

$$\begin{aligned}0 \to \varprojlim_{n,m} \mathcal{M}_{p^m}(E/K_\infty)^{\Gamma_n} &\to \varprojlim_{n,m} Ш^1(G_S(K_\infty, E[p^m])^{\Gamma_n}\\ &\to \varprojlim_{n,m} \mathcal{D}_{p^m}(E/K_\infty)^{\Gamma_n} \to \varprojlim_{n,m} \mathcal{M}_{p^m}(E/K_\infty)_{\Gamma_n}.\end{aligned}$$

The groups $E(K_\infty)[p^\infty]/p^m$ are finite of bounded order as m varies whence the groups $\mathcal{M}_{p^m}(E/K_\infty)^{\Gamma_n}$ and $\mathcal{M}_{p^m}(E/K_\infty)_{\Gamma_n}$ are finite of bounded order as n and m vary. It follows that the first and last inverse limits in the above sequence are finite.

Therefore the map

$$\varprojlim_{n,m} \text{Ш}^1(G_S(K_\infty), E[p^m])^{\Gamma_n} \to \varprojlim_{n,m} \mathcal{D}_{p^m}(E/K_\infty)^{\Gamma_n}$$

has finite kernel and cokernel which shows that

$$\operatorname{rank}_\Lambda(\varprojlim_{n,m} \text{Ш}^1(G_S(K_\infty), E[p^m])^{\Gamma_n}) = \operatorname{rank}_\Lambda(\varprojlim_{n,m} \mathcal{D}_{p^m}(E/K_\infty)^{\Gamma_n}).$$

From this and the sequence (6), we see that in order to show the equality (4) we only have to show that $\varprojlim_{n,m} \mathcal{C}_{p^m}(E/K_\infty)^{\Gamma_n}$ is Λ-torsion. That the group $\varprojlim_{n,m} \mathcal{C}_{p^m}(E/K_\infty)^{\Gamma_n}$ is Λ-torsion follows from the facts that $\varprojlim_{n,m}(\bigoplus_{w\in S_\infty} E(K_{\infty,w})[p^\infty]/p^m)^{\Gamma_n}$ and $\varprojlim_{n,m}(E(K_\infty)[p^\infty]/p^m)_{\Gamma_n}$ are Λ-torsion from lemma 2.1. Therefore we have established the equality (4).

We now prove the equality (3) by means of a control theorem. We denote $\varprojlim_{n,m} \text{Ш}^1(G_S(K_n), E[p^m])$ by $X_{p^\infty}(E/K_\infty)$ and $\varprojlim_{n,m} \text{Ш}^1(G_S(K_\infty), E[p^m])^{\Gamma_n}$ by $Y_{p^\infty}(E/K_\infty)$. In order to prove the equality (3), it suffices to show that the map $\Xi : X_{p^\infty}(E/K_\infty) \to Y_{p^\infty}(E/K_\infty)$ induced by restriction has Λ-torsion kernel and cokernel. We do this by means of a control theorem. Consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \text{Ш}^1(G_S(K_\infty), E[p^m])^{\Gamma_n} \arrow[r] & H^1(G_S(K_\infty), E[p^m])^{\Gamma_n} \arrow[r, "\psi_{\infty,m}"] & \bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E[p^m])^{\Gamma_n} \\
0 \arrow[r] & \text{Ш}^1(G_S(K_n), E[p^m]) \arrow[r] \arrow[u, "s_{n,m}"'] & H^1(G_S(K_n), E[p^m]) \arrow[r, "\psi_{n,m}"] \arrow[u, "h_{n,m}"'] & \bigoplus_{v\in S_n} H^1(K_{n,v}, E[p^m]) \arrow[u, "g_{n,m}"']
\end{tikzcd} \tag{7}$$

In the commutative diagram above the sets S_n and S_∞ are the sets of primes above S in K_n and K_∞ respectively and the vertical maps are restriction. Taking inverse limits over n and m in the above, we get another commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & Y_{p^\infty}(E/K_\infty) \arrow[r] & \varprojlim_{n,m} H^1(G_S(K_\infty), E[p^m])^{\Gamma_n} \arrow[r, "\Phi"] & \varprojlim_{n,m} \bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E[p^m])^{\Gamma_n} \\
0 \arrow[r] & X_{p^\infty}(E/K_\infty) \arrow[r] \arrow[u, "\Xi"'] & \varprojlim_{n,m} H^1(G_S(K_n), E[p^m]) \arrow[r, "\Psi"] \arrow[u, "\Xi'"'] & \varprojlim_{n,m} \bigoplus_{v\in S_n} H^1(K_{n,v}, E[p^m]) \arrow[u, "\Xi''"']
\end{tikzcd} \tag{8}$$

From the snake lemma, we see that in order to show that $\operatorname{coker}\Xi$ is Λ-torsion, we only have to show that both $\ker\Xi''$ and $\operatorname{coker}\Xi'$ are Λ-torsion. Since $cd_p(\Gamma) = 1$, therefore it follows that $\operatorname{coker}\Xi' = 0$. Now we deal with $\ker\Xi''$. Primes in S that split completely in K_∞/K do not contribute anything to $\ker\Xi''$ so we may assume that S has no such primes.

Now choose an M such that $\#S_M = \#S_\infty$ and let $m = \#S_M$. For every $n \geq M$ we label the primes in S_n as $v_1, v_2, ..., v_m$ and the primes of S_∞ as $w_1, w_2, ..., w_m$. We choose a labelling such that if $k \geq j \geq M$ then $w_i \in S_\infty$ lies above $v_i \in S_k$ lies above $v_i \in S_j$. With this labelling we have

$$\ker\Xi'' = \bigoplus_{i=1}^{m} \varprojlim_{m} \varprojlim_{n\geq M} H^1(\operatorname{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p^m])$$

where the inverse limit is taken over n with respect to the corestriction maps and over m with respect to multiplication-by-p.

For any $n \geq M$ and any i we have $\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}) = \Gamma_n$, therefore if g is a topological generator of Γ we have $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p^m]) = E(K_{\infty,w_i})[p^m]/(g^{p^n} - 1)E(K_{\infty,w_i})[p^m]$. For sufficiently large n we have $E(K_{\infty,w_i})[p^m] = E(K_{n,v_i})[p^m]$, so $(g^{p^n} - 1)E(K_{\infty,w_i})[p^m] = \{0\}$ i.e. $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p^m]) = E(K_{\infty,w_i})[p^m]$. For such sufficiently large $n' \geq n \geq M$ one can check that the corestriction map from $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n',v_i}), E(K_{\infty,w_i})[p^m])$ to $H^1(\mathrm{Gal}(K_{\infty,w_i}/K_{n,v_i}), E(K_{\infty,w_i})[p^m])$ is the identity map on $E(K_{\infty,w_i})[p^m]$. This shows that $\ker \Xi'' = \bigoplus_{i=1}^m T_p(E(K_{\infty,w_i}))$ (where $T_p(E(K_{\infty,w_i}))$ means the Tate module of $E(K_{\infty,w_i})$). It follows that $\ker \Xi''$ is Λ-torsion as desired. A similar proof shows that $\ker \Xi'$ is Λ-torsion, whence $\ker \Xi$ is Λ-torsion. This completes the proof of the equality (3) thereby finally finishing the proof of the theorem. □

Throughout the rest of the section let K be a number field, E an elliptic curve defined over K and p a rational prime such that E has good supersingular reduction at all primes of K above p. Let K_∞/K be a $\mathbb{Z}_p$-extension such that every prime of K above p ramifies. We will assume that (i) $E(K_\infty)[p^\infty]$ is finite and (ii) $H^2(G_S(K_\infty), E[p^\infty]) = \{0\}$. Finally we let S_n and S_∞ be the set of primes of K_n and K_∞ above the primes in S, respectively.

The first key result is

Proposition 2.3. *For any prime w of K_∞ above p we have $H^1(K_{\infty,w}, E)[p^\infty] = 0$.*

Proof. Let v be the prime of S below w. Since by assumption v ramifies in K_∞/K therefore the extension $K_{\infty,w}/K_v$ is deeply ramified in the sense of [4]. Therefore the result follows as explained in [8] pg. 70. □

Now we need

Proposition 2.4. *The map $H^1(G_S(K_\infty), E[p^\infty]) \xrightarrow{\psi_\infty} \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty]$ is surjective.*

Proof. To understand $\operatorname{coker} \psi_\infty$ we use the Cassels-Poitou-Tate exact sequence [6]. First for any n and m we define $\mathrm{Sel}_{p^m}(E/K_n)$ as

$$0 \longrightarrow \mathrm{Sel}_{p^m}(E/K_n) \longrightarrow H^1(G_S(K_n), E[p^m]) \longrightarrow \prod_{v \in S_n} H^1(K_{n,v}, E)[p^m].$$

Then for any $n \geq 0$ the Cassels-Poitou-Tate exact sequence is

$$H^1(G_S(K_n), E[p^\infty]) \xrightarrow{\psi_n} \bigoplus_{v \in S_n} H^1(K_{n,v}, E)[p^\infty] \to \mathfrak{S}(E/K_n)^* \to H^2(G_S(K_n), E[p^\infty])$$

where $\mathfrak{C}(E/K_n) = \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n) \subseteq H^1(G_S(K_n), T_p(E))$ (inverse limit with respect to multiplication-by-p).

Taking the direct limit of the above sequence with respect to restriction over n we get

$$H^1(G_S(K_\infty), E[p^\infty]) \xrightarrow{\psi_\infty} \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty] \to \mathfrak{S}(E/K_\infty)^* \to H^2(G_S(K_\infty), E[p^\infty])$$

where $\mathfrak{S}(E/K_\infty) = \varprojlim_{n,m} \mathrm{Sel}_{p^m}(E/K_n) \subseteq \varprojlim_{n} H^1(G_S(K_n), T_p(E))$ (inverse limit over n with regards to corestriction and over m with regards to multiplication-by-p).

By assumption, we have $H^2(G_S(K_\infty), E[p^\infty]) = \{0\}$ and so we see from the above sequence that $\operatorname{coker}\psi_\infty$ is isomorphic to $\mathfrak{S}(E/K_\infty)^*$. We will show that $\operatorname{coker}\psi_\infty = 0$ by showing that the Pontryagin dual of $\operatorname{coker}\psi_\infty$ is Λ-torsion while $\mathfrak{S}(E/K_\infty)$ is Λ-torsion-free.

First we show that $\operatorname{coker}\psi_\infty$ is Λ-cotorsion. We will also prove that it is cofinitely generated over Λ since we will need this fact later. We do this by actually showing that $J := \bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E)[p^\infty]$ is cofinitely generated cotorsion over Λ. Note that by proposition 2.3 we may (and will) assume that S_∞ contains no primes above p. We will also assume that S_∞ contains no complex archimedean primes since they contribute nothing to the group J. Write $S_\infty = T \cup T'$ where T is the set of all the primes of K_∞ above those primes of S that do not split completely in K_∞/K and T' is its complement containing all primes of S_∞ that lie above a prime of K that splits completely in K_∞/K. Let $J_T := \bigoplus_{w\in T} H^1(K_{\infty,w}, E)[p^\infty]$ and $J_{T'} := \bigoplus_{w\in T'} H^1(K_{\infty,w}, E)[p^\infty]$ so that $J = J_T \times J_{T'}$. For any $w \in T$ by [9] prop. 2 $H^1(K_{\infty,w}, E[p^\infty])$ is a cofinitely generated $\mathbb{Z}_p$-module and hence the same is true for $H^1(K_{\infty,w}, E)[p^\infty]$ as this group is a quotient of $H^1(K_{\infty,w}, E[p^\infty])$. Therefore J_T is a cofinitely generated $\mathbb{Z}_p$-module.

Now we deal with $J_{T'}$. Let S' be the set of primes of K that split completely in K_∞/K. For any such prime $v \in S'$ we let $J_v := \bigoplus_{w|v} H^1(K_{\infty,w}, E)[p^\infty]$ where the sum runs over all primes of K_∞ above v. Clearly $J_{T'} = \bigoplus_{v\in S'} J_v$. By Shapiro's lemma, for any $v \in S'$, we have $J_v^\Gamma = H^1(K_v, E)[p^\infty]$. If v is archimedean, then $H^1(K_v, E)$ is finite (see [10] prop. 1.3). If v is non-archimedean, then by Tate duality for abelian varieties over local fields ([16] I-3.4): $H^1(K_v, E)^* \cong E(K_v)$ so $H^1(K_v, E)[p^\infty]^* \cong \varprojlim E(K_v)/p^m$.

By Mattuck's theorem $E(K_v) = \mathbb{Z}_l^{[K_v:\mathbb{Q}_l]} \times T$ where $l \neq p$ is the characteristic of the residue field of K_v and T is a finite group. It follows that $\varprojlim E(K_v)/p^m$ is the finite p-primary subgroup of $E(K_v)$. So $H^1(K_v, E)$ is finite in the non-archimedean case also. This proves that $J_v^\Gamma = H^1(K_v, E)[p^\infty]$ is finite which shows that $J_{T'}$ is cofinitely generated over Λ. Also for any $w \in T'$ we have $H^1(K_{\infty,w}, E)[p^\infty] = H^1(K_v, E)[p^\infty]$ where v is the prime of K below w and by what we just showed this is a finite group. All together this shows that $J_{T'}$ is a cofinitely generated Λ-module that is annihilated by some power of p.

Thus we have shown that $J = A \times B$ (decomposition as cofinitely generated Λ-modules) where A is a cofinitely generated $\mathbb{Z}_p$-module and B is a torsion $\mathbb{Z}_p$-module that is annihilated by some power of p. This shows that J^* is a finitely generated Λ-torsion module and hence the same is true of $\operatorname{coker}\psi_\infty$.

Now we prove that $\mathfrak{S}(E/K_\infty)$ is Λ-torsion-free. First consider the groups $Y' := \varprojlim_{n,m} \mathrm{Sel}_{p^m}(E/K_\infty)^{\Gamma_n}$ and the group $Y := \varprojlim_{n,m} \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]^{\Gamma_n}$. We claim that Y' injects into Y. To see this, note that the natural map from $\mathrm{Sel}_{p^m}(E/K_\infty)$ to $\mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]$ has kernel $E(K_\infty)[p^\infty]/p^m$. This map induces a map from Y' to Y with kernel $Z := \varprojlim_{n,m} (E(K_\infty)[p^\infty]/p^m)^{\Gamma_n}$. Since the groups $E(K_\infty)[p^\infty]/p^m$ are finite and bounded as m varies therefore $Z = 0$ (for large enough n Γ_n acts trivially on $E(K_\infty)[p^\infty]/p^m$ and hence the norm maps in the inverse limit eventually become multiplication-by-p). So we see that in fact Y' injects into Y. By [17] prop 5.5.10 Y is a free Λ-module. This implies that Y' is Λ-torsion-free. Now consider the commutative diagram with vertical maps induced by restriction

$$\begin{tikzcd}
Y' \arrow[r, hook] & \varprojlim_{n,m} H^1(G_S(K_\infty), E[p^m])^{\Gamma_n} \\
\mathfrak{S}(E/K_\infty) \arrow[u, "\Xi"] \arrow[r, hook] & \varprojlim_{n,m} H^1(G_S(K_n), E[p^m]). \arrow[u, "\Xi'"']
\end{tikzcd}$$

Since Y' is Λ-torsion-free, therefore to show that $\mathfrak{S}(E/K_\infty)$ is Λ-torsion-free, it will suffice to show that the map Ξ is an injection. From the commutative diagram this will be shown once we show that Ξ' is an injection. We have

$$\ker \Xi' = \varprojlim_{n} \varprojlim_{m} H^1(\Gamma_n, E(K_\infty)[p^m]).$$

Since by assumption $E(K_\infty)[p^\infty]$ is finite, it follows that for any $n \geq 0$ that $\varprojlim_{m} H^1(\Gamma_n, E(K_\infty)[p^m]) = 0$ and hence $\ker \Xi' = 0$. This completes the proof. □

The next 2 lemmas are the most important ingredients in our proof

Lemma 2.5. *We have a pseudo-isomorphism*

$$\varprojlim_{n,m} \text{Ш}^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \sim \dot{T}_\mu(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*).$$

Proof. The exact Kummer sequences

$$0 \to E[p^m] \to E \xrightarrow{p^m} E \to 0 \tag{9}$$

and

$$0 \to E[p^m] \to E[p^\infty] \xrightarrow{p^m} E[p^\infty] \to 0 \tag{10}$$

yield a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & p^m \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty] \arrow[r] & \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty] \arrow[r] & \bigoplus_{w \in S_\infty} H^2(K_{\infty,w}, E[p^m]) & \\
0 \arrow[r] & p^m H^1(G_S(K_\infty), E[p^\infty]) \arrow[r] \arrow[u, "\psi"] & H^1(G_S(K_\infty), E[p^\infty]) \arrow[r] \arrow[u, "\psi'"] & H^2(G_S(K_\infty), E[p^m]) \arrow[r] \arrow[u, "\psi''"] & 0
\end{tikzcd}$$

(11)

where the 0 at the right of the lower sequence is because $H^2(G_S(K_\infty), E[p^\infty]) = 0$. Since $\ker \psi' = \mathrm{Sel}_{p^\infty}(E/K_\infty)$, $\ker \psi'' = \text{Ш}^2(G_S(K_\infty), E[p^m])$ and ψ is surjective by proposition 2.4, therefore by the snake lemma we get the following exact sequence

$$0 \to \ker \psi \to \mathrm{Sel}_{p^\infty}(E/K_\infty) \to \text{Ш}^2(G_S(K_\infty), E[p^m]) \to 0. \tag{12}$$

Now consider the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^m] \arrow[r] & \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty] \arrow[r, "p^m"] & p^m \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty] & \\
 & H^1(G_S(K_\infty), E[p^m]) \arrow[r] \arrow[u, "\phi_m"] & H^1(G_S(K_\infty), E[p^\infty]) \arrow[r, "p^m"] \arrow[u, "\psi'"] & p^m H^1(G_S(K_\infty), E[p^\infty]) \arrow[r] \arrow[u, "\psi"] & 0
\end{tikzcd}$$

(13)

Since $\ker\psi' = \mathrm{Sel}_{p^\infty}(E/K_\infty)$ and ψ' is surjective by proposition 2.4, therefore by the snake lemma we get an exact sequence

$$0 \to p^m\mathrm{Sel}_{p^\infty}(E/K_\infty) \to \ker\psi \to \operatorname{coker}\phi_m \to 0. \tag{14}$$

This sequence in turn gives the following exact sequence

$$0 \to \operatorname{coker}\phi_m \to \mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m \to \mathrm{Sel}_{p^\infty}(E/K_\infty)/\ker\psi \to 0. \tag{15}$$

From the sequences (12) and (15) we get the following exact sequence

$$0 \to \operatorname{coker}\phi_m \to \mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m \to Ш^2(G_S(K_\infty), E[p^m]) \to 0. \tag{16}$$

For any $n \geq 0$ this sequence induces another exact sequence

$$\begin{aligned} 0 &\to (\operatorname{coker}\phi_m)^{\Gamma_n} \to (\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{\Gamma_n} \to Ш^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \\ &\to (\operatorname{coker}\phi_m)_{\Gamma_n}. \end{aligned} \tag{17}$$

We claim that each of the terms in this exact sequence is finite. Clearly it will suffice to prove that the second term and fourth term are finite. Since $\mathrm{Sel}_{p^\infty}(E/K_\infty)^*$ is a finitely generated Λ-module (see [12] theorem 4.5), the finiteness of the second term is easily seen by taking Pontryagin duals. Also in the proof of proposition 2.4 we have shown that $J := \bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E)[p^\infty]$ is a cofinitely generated Λ-module and hence by considering Pontryagin duals $J[p^m]_{\Gamma_n}$ is finite. Since $J[p^m]_{\Gamma_n}$ surjects onto $(\operatorname{coker}\phi_m)_{\Gamma_n}$, it follows that the fourth term is finite. Therefore we have seen that all the terms in the sequence (17) are finite so by taking inverse limits the sequence remains exact

$$\begin{aligned} 0 &\to \varprojlim_{n,m}(\operatorname{coker}\phi_m)^{\Gamma_n} \to \varprojlim_{n,m}(\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{\Gamma_n} \to \varprojlim_{n,m} Ш^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \\ &\xrightarrow{\theta} \varprojlim_{n,m}(\operatorname{coker}\phi_m)_{\Gamma_n}. \end{aligned} \tag{18}$$

By lemma 2.1(i) the second term in the above sequence is pseudo-isomorphic to $\dot{T}_\mu(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. Therefore to prove the lemma it will suffice to show that the first term and $\operatorname{img}\theta$ in the above sequence are both finite.

First we deal with $\operatorname{img}\theta$. Consider the group $J := \bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E)[p^\infty]$. By lemma 2.1(ii) $\varprojlim_{n,m}(J[p^m])_{\Gamma_n} \sim \dot{T}_\lambda(J^*)$. Hence $\varprojlim_{n,m}(J[p^m])_{\Gamma_n}$ is a finitely generated $\mathbb{Z}_p$-module. Now $\varprojlim_{n,m}(J[p^m])_{\Gamma_n}$ surjects onto $\varprojlim_{n,m}(\operatorname{coker}\phi_m)_{\Gamma_n}$ and so it follows that $\varprojlim_{n,m}(\operatorname{coker}\phi_m)_{\Gamma_n}$ is also a finitely generated $\mathbb{Z}_p$-module.

We now prove that the group $\varprojlim_{n,m} Ш^2(G_S(K_\infty), E[p^m])^{\Gamma_n}$ is a torsion $\mathbb{Z}_p$-module. Taking into account the fact that $H^2(G_S(K_\infty), E[p^\infty]) = 0$, the Kummer sequence (10) gives an isomorphism $H^1(G_S(K_\infty), E[p^\infty])/p^m \cong H^2(G_S(K_\infty), E[p^m])$. Combining the injection $Ш^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \hookrightarrow H^2(G_S(K_\infty), E[p^m])$ with this isomorphism we get an injection

$$\varprojlim_{n,m} Ш^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \hookrightarrow \varprojlim_{n,m}(H^1(G_S(K_\infty), E[p^\infty])/p^m)^{\Gamma_n}. \tag{19}$$

Lemma 2.1 shows that $\varprojlim_{n,m}(H^1(G_S(K_\infty),E[p^\infty])/p^m)^{\Gamma_n}$ is a $\mathbb{Z}_p$-torsion module and hence from the injection above the same is true for $\varprojlim_{n,m} Ш^2(G_S(K_\infty),E[p^m])^{\Gamma_n}$. Therefore $\operatorname{img}\theta$ is a $\mathbb{Z}_p$-torsion module. It is also a finitely generated $\mathbb{Z}_p$-module since $\varprojlim_{n,m}(\operatorname{coker}\phi_m)_{\Gamma_n}$ is finitely generated over $\mathbb{Z}_p$ as shown above. This implies that $\operatorname{img}\theta$ is finite as claimed.

We now deal with $\varprojlim_{n,m}(\operatorname{coker}\phi_m)^{\Gamma_n}$. We will actually show this group is trivial. Let $J := \bigoplus_{w\in S_\infty} H^1(K_{\infty,w},E)[p^\infty]$. In the proof of proposition 2.4 we have shown that $J = A\times B$ where A is a cofinitely generated $\mathbb{Z}_p$-module and B is a torsion $\mathbb{Z}_p$-module that is annihilated by p^t for some t. For any $m \geq 0, \operatorname{coker}\phi_m$ is the quotient of $J[p^m] = A[p^m]\times B[p^m]$. Let $\alpha = (\alpha_{n,m}) \in \varprojlim_{n,m}(\operatorname{coker}\phi_m)^{\Gamma_n}$. Note that the transition map on the first index is the norm map and on the second index it is multiplication-by-p. For each $(n,m)\in\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{\geq 1}$ choose $a_{n,m}\in A[p^m]$ and $b_{n,m}\in B[p^m]$ such that $\alpha_{n,m}$ is represented by $(a_{n,m},b_{n,m})$

Now let $(n,m)\in\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{\geq 1}$. We will show that $\alpha_{n,m} = 0$. Recall that p^t annihilates B. Consider $(a_{n,m'},b_{n,m'})$ where $m' = m+t$. We claim that $(a_{n,m'},b_{n,m'}) \equiv (0,b')$ for some $b'\in B[p^{m'}]$ (the congruence is modulo $\operatorname{img}\phi_{m'}$). To see this, note that since A is cofinitely generated over $\mathbb{Z}_p$, therefore $A[p^{m'}]$ is finite and hence is fixed by $\Gamma_{n'}$ for some $n'\geq n$. Since for any $n'' > n'$ we have $\operatorname{Tr}_{K_{n''}/K_{n'}}(\alpha_{n'',m'}) = \alpha_{n',m'}$ and $\Gamma_{n'}$ acts trivially on $A[p^{m'}]$, therefore by considering large enough $n'' > n'$ we easily see that $(a_{n',m'},b_{n',m'}) \equiv (0,b'')$ for some $b''\in B[p^{m'}]$ and hence $(a_{n,m'},b_{n,m'}) \equiv (0,b')$ for some $b'\in B[p^{m'}]$ as claimed.

Now we have that $p^t\alpha_{n,m'} = \alpha_{n,m}$. Since $(a_{n,m'},b_{n,m'}) \equiv (0,b')$ and p^t annihilates B, therefore we see that $(a_{n,m},b_{n,m}) \equiv (0,0)$ i.e. $\alpha_{n,m} = 0$. This proves that $\alpha = 0$ thus showing that $\varprojlim_{n,m}(\operatorname{coker}\phi_m)^{\Gamma_n}$ is trivial. This completes the proof of the lemma. □

We now define $K_{n,m}$ to be the kernel of the map (induced by restriction) $H^1(G_S(K_\infty),E[p^m])_{\Gamma_n} \to \big(\bigoplus_{w\in S_\infty} H^1(K_{\infty,w},E[p^m])\big)_{\Gamma_n}$

Lemma 2.6. *We have a pseudo-isomorphism*

$$\varprojlim_{n,m} K_{n,m} \sim \dot{T}_\lambda(\operatorname{Sel}_{p^\infty}(E/K_\infty)^*).$$

Proof. The exact Kummer sequences

$$0\to E[p^m]\to E\xrightarrow{p^m} E\to 0 \tag{20}$$

and

$$0\to E[p^m]\to E[p^\infty]\xrightarrow{p^m} E[p^\infty]\to 0 \tag{21}$$

yield a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \bigoplus_{w\in S_\infty} E(K_{\infty,w})/p^m \arrow[r] & \bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E[p^m]) \arrow[r] & \bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E)[p^m] \arrow[r] & 0 \\
0 \arrow[r] & E(K_\infty)[p^\infty]/p^m \arrow[r] \arrow[u, "\phi_m"] & H^1(G_S(K_\infty), E[p^m]) \arrow[r] \arrow[u, "\psi_m"] & H^1(G_S(K_\infty), E[p^\infty])[p^m] \arrow[r] \arrow[u, "\psi'_m"] & 0
\end{tikzcd} \tag{22}$$

Taking Γ_n-coinvariants we get

$$\begin{tikzcd}
0 \arrow[r] & B_{n,m} \arrow[r] & \big(\bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E[p^m])\big)_{\Gamma_n} \arrow[r] & \big(\bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E)[p^m]\big)_{\Gamma_n} \arrow[r] & 0 \\
0 \arrow[r] & A_{n,m} \arrow[r] \arrow[u, "\phi_{n,m}"] & H^1(G_S(K_\infty), E[p^m])_{\Gamma_n} \arrow[r] \arrow[u, "\psi_{n,m}"] & H^1(G_S(K_\infty), E[p^\infty])[p^m]_{\Gamma_n} \arrow[r] \arrow[u, "\psi'_{n,m}"] & 0
\end{tikzcd} \tag{23}$$

where $A_{n,m}$ is the image of the map

$$(E(K_\infty)[p^\infty]/p^m)_{\Gamma_n} \to H^1(G_S(K_\infty), E[p^m])_{\Gamma_n}$$

and $B_{n,m}$ is the image of the map

$$\Big(\bigoplus_{w\in S_\infty} E(K_{\infty,w})/p^m\Big)_{\Gamma_n} \to \Big(\bigoplus_{w\in S_\infty} H^1(K_{\infty,w}, E[p^m])\Big)_{\Gamma_n}.$$

Applying the snake lemma to the diagram (23) we get an exact sequence

$$0 \to \ker\phi_{n,m} \to K_{n,m} \to \ker\psi'_{n,m} \to \operatorname{coker}\phi_{n,m}. \tag{24}$$

We claim that each of the terms in this exact sequence is finite. To simplify arguments, we prove this fact subject to the condition that $n \geq N$ where $N \geq 0$ is an integer such that K_∞/K_N is totally ramified at all primes of K_N above p and such that every prime of K_N above a prime in S that does not split completely in K_∞/K_N is inert in this extension. Clearly it will suffice to prove that the first, third and fourth terms are finite. In what follows all inverse limits with indices involving n will be taken over $n \geq N$

Since $E(K_\infty)[p^\infty]/p^m$ is finite, therefore $\ker\phi_{n,m}$ is finite. Moreover, the order of $E(K_\infty)[p^\infty]/p^m$ is bounded as m varies. Hence the order of $(E(K_\infty)[p^\infty]/p^m)_{\Gamma_n}$ is bounded as n and m vary. This in turn shows that the order of $\ker\phi_{n,m}$ is bounded as n and m vary. It follows that $\varprojlim_{n,m}\ker\phi_{n,m}$ is finite. This last fact will be needed later.

Now we show that $\operatorname{coker}\phi_{n,m}$ is finite by showing that $D(n,m) := \big(\bigoplus_{w\in S_\infty} E(K_{\infty,w})/p^m\big)_{\Gamma_n}$ is finite. We will also show that $\varprojlim_{n,m}\operatorname{coker}\phi_{n,m}$ is finite as we will need this later. We write $S_\infty = S_p \cup S_{\text{split}} \cup S_{\text{nsplit}}$ where S_p is the set of primes of S_∞ above p and S_{split} is the set of primes in S_∞ above those in S that split completely in K_∞/K. First we show that $D_p(n,m) := \big(\bigoplus_{w\in S_p} E(K_{\infty,w})/p^m\big)_{\Gamma_n}$ is finite. Let $w \in S_p$. Note that by the condition on n, Γ_n acts on $E(K_{\infty,w})/p^m$. We let $\text{Tor}(E(K_{\infty,w})$ be the $\mathbb{Z}$-torsion subgroup of $E(K_{\infty,w})$ and $E(K_{\infty,w})_{\text{Tor}} := E(K_{\infty,w})/\text{Tor}(E(K_{\infty,w}))$. We have an exact sequence

$$((\text{Tor}(E(K_{\infty,w})))/p^m)_{\Gamma_n} \to (E(K_{\infty,w})/p^m)_{\Gamma_n} \to (E(K_{\infty,w})_{\text{Tor}}/p^m)_{\Gamma_n} \to 0. \tag{25}$$

Note that the Pontryagin dual of $E(K_{\infty,w})[p^\infty]$ is a finitely generated $\mathbb{Z}_p[[\Gamma_N]]$-module. Since $\mathrm{Tor}(E(K_{\infty,w}))/p^m = E(K_{\infty,w})[p^\infty]/p^m$, therefore by considering Pontryagin duals it follows that $((\mathrm{Tor}(E(K_{\infty,w})))/p^m)_{\Gamma_n}$ is finite. Also from lemma 2.1 it follows that $\varprojlim_{n,m}((\mathrm{Tor}(E(K_{\infty,w})))/p^m)_{\Gamma_n}$ is finite.

Now we turn to the group $(E(K_{\infty,w})_{\mathrm{Tor}}/p^m)_{\Gamma_n}$. Since $E(K_{\infty,w})_{\mathrm{Tor}}$ is torsion-free, therefore it follows that $(E(K_{\infty,w})_{\mathrm{Tor}} \otimes \mathbb{Q}_p/\mathbb{Z}_p)[p^m] = E(K_{\infty,w})_{\mathrm{Tor}}/p^m$. Also note that $E(K_{\infty,w})_{\mathrm{Tor}} \otimes \mathbb{Q}_p/\mathbb{Z}_p = E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$. These 2 facts show that

$$((E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)[p^m])_{\Gamma_n} = (E(K_{\infty,w})_{\mathrm{Tor}}/p^m)_{\Gamma_n}. \tag{26}$$

Wingberg ([25] theorem 2.2) has shown that $(E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p)^*$ is pseudo-isomorphic to a finitely generated free $\mathbb{Z}_p[[\Gamma_N]]$-module. This together with the equality (26) show that $(E(K_{\infty,w})_{\mathrm{Tor}}/p^m)_{\Gamma_n}$ is finite. Using lemma 2.1 we also see that $\varprojlim_{n,m}(E(K_{\infty,w})_{\mathrm{Tor}}/p^m)_{\Gamma_n}$ is finite. From the facts above and the exact sequence (25) it follows that $(E(K_{\infty,w})/p^n)_{\Gamma_n}$ is finite and that $\varprojlim_{n,m}(E(K_{\infty,w})/p^m)_{\Gamma_n}$ is finite. Thus we have shown that for any $n \geq N, m \geq 1$ that $D_p(n,m)$ is finite and $\varprojlim_{n,m} D_p(n,m)$ is also finite.

Now we turn to the group $D_{\mathrm{nsplit}}(n,m) := \big(\bigoplus_{w \in S_{\mathrm{nsplit}}} E(K_{\infty,w})/p^m\big)_{\Gamma_n}$. Let $w \in S_{\mathrm{nsplit}}$. We claim that $E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. To see this, it will suffice to show for any $t \geq 0$ that $E(K_{t,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. By Mattuck's theorem $E(K_{t,w}) = \mathbb{Z}_l^{[K_{t,w}:\mathbb{Q}_l]} \times T$ where $l \neq p$ is the characteristic of the residue field of $K_{t,w}$ and T is a finite group. It follows from this that $E(K_{t,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ and hence $E(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ as claimed. Then just as in the case of $D_p(n,m)$, we also have $D_{\mathrm{nsplit}}(n,m)$ is finite and $\varprojlim_{n,m} D_{\mathrm{nsplit}}(n,m)$ is also finite.

Finally we turn to the group $D_{\mathrm{split}}(n,m) := \big(\bigoplus_{w \in S_{\mathrm{split}}} E(K_{\infty,w})/p^m\big)_{\Gamma_n}$. Let $v \in S$ be a prime that splits completely in K_∞/K and define $C_v := \bigoplus_{w|v} E(K_{\infty,w})/p^m$ where the sum runs over all primes of K_∞ lying over v. We claim that $H^1(\Gamma_n, C_v) = (C_v)_{\Gamma_n} = 0$. To simplify matters, we prove this for $n = 0$ (for arbitrary n the proof is similar). The group C_v is a direct limit of induced Γ-modules and hence by Shapiro's lemma it follows that $H^1(\Gamma, C_v) = H^1(\{1\}, E(K_v)/p^m) = 0$. Thus we see that $D_{\mathrm{split}}(n,m) = 0$.

All in all, we see from the above for any $n \geq N, m \geq 1$ that $D(n,m)$ is finite and that $\varprojlim_{n,m} D(n,m)$ is also finite. It follows that $\operatorname{coker} \phi_{n,m}$ is finite and that $\varprojlim_{n,m} \operatorname{coker} \phi_{n,m}$ is also finite.

Finally we prove that $\ker \psi'_{n,m}$ is finite. Since $\ker \psi'_{n,m} \subseteq H^1(G_S(K_\infty), E[p^\infty])[p^m]_{\Gamma_n}$ we easily see that by taking Pontryagin duals that it suffices to prove that $H^1(G_S(K_\infty), E[p^\infty])^*$ is a finitely generated Λ-module. To show this last fact we have to show that $H^1(G_S(K_\infty), E[p^\infty])^\Gamma$ is cofinitely generated over $\mathbb{Z}_p$. Since $cd_p(\Gamma) = 1$, therefore we have a surjection $H^1(G_S(K), E[p^\infty]) \twoheadrightarrow H^1(G_S(K_\infty), E[p^\infty])^\Gamma$ so it suffices to prove that $H^1(G_S(K), E[p^\infty])$ is cofinitely generated over $\mathbb{Z}_p$ i.e. we must show that $H^1(G_S(K), E[p^\infty])[p]$ is finite. But $H^1(G_S(K), E[p])$ is finite (see [17] theorem

8.3.20) and this group surjects onto $H^1(G_S(K), E[p^\infty])[p]$ so it indeed follows that $H^1(G_S(K), E[p^\infty])$ is cofinitely generated over $\mathbb{Z}_p$. This proves that $\ker \psi'_{n,m}$ is finite.

We have now shown that each of the terms in the exact sequence (24) are finite and so by taking inverse limits the sequence remains exact

$$0 \to \varprojlim_{n,m} \ker \phi_{n,m} \to \varprojlim_{n,m} K_{n,m} \to \varprojlim_{n,m} \ker \psi'_{n,m} \to \varprojlim_{n,m} \operatorname{coker} \phi_{n,m}. \tag{27}$$

We have shown above that $\varprojlim_{n,m} \ker \phi_{n,m}$ and $\varprojlim_{n,m} \operatorname{coker} \phi_{n,m}$ are both finite so from the exact sequence (27) we get a pseudo-isomorphism $\varprojlim_{n,m} K_{n,m} \sim \varprojlim_{n,m} \ker \psi'_{n,m}$. Therefore to prove the lemma we only have to show that $\varprojlim_{n,m} \ker \psi'_{n,m}$ is pseudo-isomorphic to $\dot{T}_\lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. To show this, first consider the exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/K_\infty) \to H^1(G_S(K_\infty), E[p^\infty]) \xrightarrow{\psi'} \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E) \to 0. \tag{28}$$

The surjectivity of ψ' is due to proposition 2.4. This exact sequence induces another sequence

$$\begin{aligned} 0 \to \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m] \to H^1(G_S(K_\infty), E[p^\infty])[p^m] \xrightarrow{\psi'_m} \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^m] \\ \xrightarrow{\psi''_m} \mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m. \end{aligned} \tag{29}$$

We break this sequence into 2 exact sequences

$$0 \to \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m] \to H^1(G_S(K_\infty), E[p^\infty])[p^m] \xrightarrow{\phi_m} \operatorname{img} \psi'_m \to 0, \tag{30}$$

$$0 \to \operatorname{img} \psi'_m \xrightarrow{\theta_m} \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^m] \to \operatorname{img} \psi''_m \to 0. \tag{31}$$

Taking Γ_n-coinvaraints of both these sequences we get

$$\begin{aligned} (\operatorname{img} \psi'_m)^{\Gamma_n} \to \mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]_{\Gamma_n} \to H^1(G_S(K_\infty), E[p^\infty])[p^m]_{\Gamma_n} \\ \xrightarrow{\phi_{n,m}} (\operatorname{img} \psi'_m)_{\Gamma_n} \to 0, \end{aligned} \tag{32}$$

$$(\operatorname{img} \psi''_m)^{\Gamma_n} \to (\operatorname{img} \psi'_m)_{\Gamma_n} \xrightarrow{\theta_{n,m}} \Big(\bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^m]\Big)_{\Gamma_n}. \tag{33}$$

We claim the each of the terms in the sequences (32) and (33) is finite. First we deal with (32): Let $J := \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty]$. Then $(\operatorname{img} \psi'_m)^{\Gamma_n} \subseteq J[p^m]^{\Gamma_n}$. In the proof of proposition 2.4 we proved that J is a cofinitely generated Λ-module. It follows from this that $J[p^m]^{\Gamma_n}$ is finite and hence $(\operatorname{img} \psi'_m)^{\Gamma_n}$ is also finite. We showed above that $H^1(G_S(K_\infty), E[p^\infty])$ is a cofinitely generated Λ-module. It follows that $H^1(G_S(K_\infty), E[p^\infty])[p^m]_{\Gamma_n}$ is finite. This proves that all the terms in the sequence (32) are finite.

Now we deal with the sequence (33). We know that $\mathrm{Sel}_{p^\infty}(E/K_\infty)^*$ is a finitely generated Λ-module (see [12] theorem 4.5) so it follows that $(\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{\Gamma_n}$ is finite. Since $(\operatorname{img}\psi''_m)^{\Gamma_n} \subseteq (\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{\Gamma_n}$, it follows that $(\operatorname{img}\psi''_m)^{\Gamma_n}$ is also finite. Also since J is a cofinitely generated Λ-module, it follows that $J[p^m]_{\Gamma_n} = \big(\bigoplus_{w\in S_\infty} H^1(K_{\infty,w},E)[p^m]\big)_{\Gamma_n}$ is finite. Therefore all the terms in the sequence (33) are finite.

As all the terms in the sequence (32) and (33) are finite, therefore by taking inverse limits the sequences remain exact

$$\begin{aligned}\varprojlim_{n,m}(\operatorname{img}\psi'_m)^{\Gamma_n} \to \varprojlim_{n,m}\mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]_{\Gamma_n} \to \varprojlim_{n,m} H^1(G_S(K_\infty),E[p^\infty])[p^m]_{\Gamma_n}\\ \xrightarrow{\Phi} \varprojlim_{n,m}(\operatorname{img}\psi'_m)_{\Gamma_n} \to 0,\end{aligned} \tag{34}$$

$$\varprojlim_{n,m}(\operatorname{img}\psi''_m)^{\Gamma_n} \to \varprojlim_{n,m}(\operatorname{img}\psi'_m)_{\Gamma_n} \xrightarrow{\Theta} \varprojlim_{n,m}\Big(\bigoplus_{w\in S_\infty} H^1(K_{\infty,w},E)[p^m]\Big)_{\Gamma_n}. \tag{35}$$

We have an exact sequence

$$0 \to \ker(\Phi) \to \ker(\Theta\circ\Phi) \xrightarrow{\Phi} \ker(\Theta). \tag{36}$$

Note that $\ker(\Theta\circ\Phi) = \varprojlim_{n,m}\ker\psi'_{n,m}$. Therefore from the exact sequence, we see that to prove the lemma, we only have to show that $\ker\Phi$ is pseudo-isomorphic to $\dot{T}_\lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$ and that $\Phi(\ker(\Theta\circ\Phi))$ is finite.

First we deal with $\ker\Phi$. From lemma 2.1 $\varprojlim_{n,m}\mathrm{Sel}_{p^\infty}(E/K_\infty)[p^m]_{\Gamma_n}$ is pseudo-isomorphic to $\dot{T}_\lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. Therefore from the exact sequence (34), to show the existence of a pseudo-isomorphism $\ker\Phi \sim \dot{T}_\lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$, we see that it will suffice to show that $\varprojlim_{n,m}(\operatorname{img}\psi'_m)^{\Gamma_n} = 0$. Let $J := \bigoplus_{w\in S_\infty} H^1(K_{\infty,w},E)[p^\infty]$. Then $\varprojlim_{n,m}(\operatorname{img}\psi'_m)^{\Gamma_n} \subseteq \varprojlim_{n,m} J[p^m]^{\Gamma_n}$. According to [17] prop. 5.5.10 $\varprojlim_{n,m} J[p^m]^{\Gamma_n}$ is a free Λ-module with the same rank as J^*. In the proof of proposition 2.4 we showed that J^* is a torsion Λ-module. Therefore it follows that $\varprojlim_{n,m} J[p^m]^{\Gamma_n} = 0$ and hence also $\varprojlim_{n,m}(\operatorname{img}\psi'_m)^{\Gamma_n} = 0$. This proves that $\ker\Phi$ is pseudo-isomorphic to $\dot{T}_\lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$.

Now we show that $\Phi(\ker(\Theta\circ\Phi))$ is finite. First we show that this group is finitely generated over $\mathbb{Z}_p$. Recall that we showed above that $\ker(\Theta\circ\Phi) = \varprojlim_{n,m}\ker\psi'_{n,m}$ is pseudo-isomorphic to $\varprojlim_{n,m} K_{n,m}$. We have $\varprojlim_{n,m} K_{n,m} \subseteq \varprojlim_{n,m} H^1(G_S(K_\infty),E[p^m])_{\Gamma_n}$. Therefore to show that $\Phi(\ker(\Theta\circ\Phi))$ is finitely generated over $\mathbb{Z}_p$, it will suffice to show that $\varprojlim_{n,m} H^1(G_S(K_\infty),E[p^m])_{\Gamma_n}$ is finitely generated over $\mathbb{Z}_p$. Consider the bottom row of the commutative diagram (23)

$$(E(K_\infty)[p^\infty]/p^m)_{\Gamma_n} \to H^1(G_S(K_\infty),E[p^m])_{\Gamma_n} \to H^1(G_S(K_\infty),E[p^\infty])[p^m]_{\Gamma_n} \to 0.$$

We showed above that all the terms in the above exact sequence are finite. Therefore by taking inverse limits the sequence remains exact

$$\begin{aligned}\varprojlim_{n,m}(E(K_\infty)[p^\infty]/p^m)_{\Gamma_n} \to &\varprojlim_{n,m} H^1(G_S(K_\infty), E[p^m])_{\Gamma_n} \\ &\to \varprojlim_{n,m} H^1(G_S(K_\infty), E[p^\infty])[p^m]_{\Gamma_n} \to 0.\end{aligned}$$

Applying lemma 2.1 to the first and last terms of the above sequence, it follows that $\varprojlim_{n,m} H^1(G_S(K_\infty), E[p^m])_{\Gamma_n}$ is in fact finitely generated over $\mathbb{Z}_p$ as desired.

Now we show that $\Phi(\ker(\Theta \circ \Phi))$ is a $\mathbb{Z}_p$-torsion module. From the exact sequence (36), this will follow if we can prove that $\ker \Theta$ is a torsion $\mathbb{Z}_p$-module. From the exact sequence (35), this will follow once we show that $\varprojlim_{n,m}(\operatorname{img} \psi''_m)^{\Gamma_n}$ has this property. But $\varprojlim_{n,m}(\operatorname{img} \psi''_m)^{\Gamma_n} \subseteq (\mathrm{Sel}_{p^\infty}(E/K_\infty)/p^m)^{\Gamma_n}$ and so the desired result follows from lemma 2.1.

Thus we have shown that $\Phi(\ker(\Theta \circ \Phi))$ is a finitely generated torsion $\mathbb{Z}_p$-module. It follows that this group is finite. This completes the proof of the lemma. □

Assume that we have a first quadrant spectral sequence $E_r^{st} \Rightarrow E^{s+t}$ such that $E_2^{s,t} = 0$ for all $s > 1$ and all t, then we have an exact sequence (see [17] lemma 2.1.3 and [2] prop. XV-5.7)

$$0 \to E_2^{1,1} \to E^2 \to E_2^{0,2} \to 0.$$

Now let $n, m \geq 0$. Since $cd_p(\Gamma_n) = 1$, therefore we can apply the above result to the Hochschild-Serre spectral sequence $H^s(\Gamma_n, H^t(G_S(K_\infty), E[p^m])) \Rightarrow H^{s+t}(G_S(K_n), E[p^m])$ (where K_n is the fixed field of Γ_n) to get an exact sequence

$$\begin{aligned}0 \to H^1(G_S(K_\infty), E[p^m])_{\Gamma_n} &\xrightarrow{f_{n,m}} H^2(G_S(K_n), E[p^m]) \\ &\xrightarrow{g_{n,m}} H^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \to 0 \qquad (37)\end{aligned}$$

Lemma 2.7. *For $n' > n$ we have a commutative diagram*

$$\begin{tikzcd} H^1(G_S(K_\infty), E[p^m])_{\Gamma_{n'}} \arrow[r, "f_{n',m}"] \arrow[d, "\mathrm{can}"'] & H^2(G_S(K_{n'}), E[p^m]) \arrow[r, "g_{n',m}"] \arrow[d, "\mathrm{cor}"'] & H^2(G_S(K_\infty), E[p^m])^{\Gamma_{n'}} \arrow[d, "\mathrm{norm}"'] \\ H^1(G_S(K_\infty), E[p^m])_{\Gamma_n} \arrow[r, "f_{n,m}"] & H^2(G_S(K_n), E[p^m]) \arrow[r, "g_{n,m}"] & H^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \end{tikzcd}$$

where the maps can, cor and norm are the canonical projection, corestriction and norm, respectively. Also for $m' > m$ we have a commutative diagram

$$\begin{tikzcd} H^1(G_S(K_\infty), E[p^{m'}])_{\Gamma_n} \arrow[r, "f_{n,m'}"] \arrow[d, "p^{m'-m}"'] & H^2(G_S(K_n), E[p^{m'}]) \arrow[r, "g_{n,m'}"] \arrow[d, "p^{m'-m}"'] & H^2(G_S(K_\infty), E[p^{m'}])^{\Gamma_n} \arrow[d, "p^{m'-m}"'] \\ H^1(G_S(K_\infty), E[p^m])_{\Gamma_n} \arrow[r, "f_{n,m}"] & H^2(G_S(K_n), E[p^m]) \arrow[r, "g_{n,m}"] & H^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \end{tikzcd}$$

where the vertical maps are induced by multiplication by $p^{m'-m}$

Proof. From the formula for the corestriction map ([26] prop. 2.5.2) it is easy to show that the corestriction map $\mathrm{cor} : H^1(\Gamma_{n'}, H^1(G_S(K_\infty), E[p^m])) \to H^1(\Gamma_n, H^1(G_S(K_\infty), E[p^m]))$ corresponds to the canonical projection $\mathrm{can} : H^1(G_S(K_\infty), E[p^m])_{\Gamma_{n'}} \to H^1(G_S(K_\infty), E[p^m])_{\Gamma_n}$. Also we know that the corestriction map $\mathrm{cor} : H^2(G_S(K_\infty), E[p^m])^{\Gamma_{n'}} \to H^2(G_S(K_\infty), E[p^m])^{\Gamma_n}$ is equal to the norm map. Therefore we see that to show that the first diagram commutes, it suffices to show the commutativity of the following diagram

$$\begin{tikzcd}
H^1(\Gamma_{n'}, H^1(G_S(K_\infty), E[p^m])) \arrow[r, "f_{n',m}"] \arrow[d, "\mathrm{cor}"'] & H^2(G_S(K_{n'}), E[p^m]) \arrow[r, "g_{n',m}"] \arrow[d, "\mathrm{cor}"'] & H^2(G_S(K_\infty), E[p^m])^{\Gamma_{n'}} \arrow[d, "\mathrm{cor}"'] \\
H^1(\Gamma_n, H^1(G_S(K_\infty), E[p^m])) \arrow[r, "f_{n,m}"] & H^2(G_S(K_n), E[p^m]) \arrow[r, "g_{n,m}"] & H^2(G_S(K_\infty), E[p^m])^{\Gamma_n}
\end{tikzcd} \tag{38}$$

As in the proof of [17] theorem 2.4.1, the data $(G_S(K_{n'}), \Gamma_{n'}, E[p^m])$ determines a double complex $D(G_S(K_{n'}), \Gamma_{n'}, E[p^m])$. Similarly, we have a double complex $D(G_S(K_n), \Gamma_n, E[p^m])$. By taking the column-wise filtrations of the total complexes of these double complexes we obtain 2 Hochschild-Serre spectral sequences $SS(G_S(K_{n'}), \Gamma_{n'}, E[p^m])$ and $SS(G_S(K_n), \Gamma_n, E[p^m])$ (see [15] theorem 2.15 and [17] theorem 2.4.1). The obvious corestriction map on cochains induces a morphism of double complex $\mathrm{cor} : D(G_S(K_{n'}), \Gamma_{n'}, E[p^m]) \to D(G_S(K_n, \Gamma_n, E[p^m])$ which, in turn, induces a morphism of spectral sequences $\mathrm{cor} : SS(G_S(K_{n'}), \Gamma_{n'}, E[p^m]) \to SS(G_S(K_n, \Gamma_n, E[p^m])$ and their corresponding limit terms.

One checks using the definitions of $f_{n,m}$ and $g_{n,m}$ (see [2] prop. XV-5.7) that these morphisms commute with the induced maps on the terms in the diagram (38) and that these induced maps are actually corestriction. This proves that the diagram (38) commutes and hence the first diagram in the statement of the lemma commutes.

To show that the second diagram in the statement of the lemma commutes one argues similar fashion using the map $p^{m'-m} : D(G_S(K_n), \Gamma_n, E[p^{m'}]) \to D(G_S(K_n), \Gamma_n, E[p^m])$ which is induced by multiplication by $p^{m'-m}$

Alternatively, to show that the 2 diagrams commute, one can use the explicit descriptions of $f_{n,m}$ and $g_{n,m}$: the map $g_{n,m}$ is the restriction map (see [13] prop. XI-10.2) whereas the map $f_{n,m}^{-1} : \operatorname{img} f_{n,m} \to H^1(G_S(K_\infty), E[p^m])_{\Gamma_n}$ is described in [7] (see also [11] theorem 2). □

Now let v be a prime of K_n, w a prime of K_∞ above v and $\Gamma_{n,w}$ the decomposition group of w in K_∞/K. We have a Hochschild-Serre spectral sequence $H^s(\Gamma_{n,w}, H^t(K_{\infty,w}, E[p^m])) \Rightarrow H^{s+t}(K_{n,v}, E[p^m])$. We certainly have $cd_p(\Gamma_{n,w}) = 1$ so as in the the global case we get an exact sequence

$$\begin{aligned} 0 \to H^1(K_{\infty,w}, E[p^m])_{\Gamma_{n,w}} &\xrightarrow{f_{w,n,m}} H^2(K_{n,v}, E[p^m]) \\ &\xrightarrow{g_{w,n,m}} H^2(K_{\infty,w}, E[p^m])^{\Gamma_{n,w}} \to 0 \end{aligned} \tag{39}$$

By Shapiro's lemma $H^1(K_{\infty,w}, E[p^m])_{\Gamma_{n,w}} = (\bigoplus_{w|v} H^1(K_{\infty,w}, E[p^m]))_{\Gamma_n}$ and $H^2(K_{\infty,w}, E[p^m])^{\Gamma_{n,w}} = (\bigoplus_{w|v} H^2(K_{\infty,w}, E[p^m]))^{\Gamma_n}$ where the direct sum runs over all primes of w dividing v. Taking direct sums, we get a diagram

$$\begin{tikzcd}
0 \arrow[r] & (\bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E[p^m]))_{\Gamma_n} \arrow[r, "f'_{n,m}"] & \bigoplus_{v \in S_n} H^2(K_{n,v}, E[p^m]) \arrow[r, "g'_{n,m}"] & (\bigoplus_{w \in S_\infty} H^2(K_{\infty,w}, E[p^m]))^{\Gamma_n} \arrow[r] & 0 \\
0 \arrow[r] & H^1(G_S(K_\infty), E[p^m])_{\Gamma_n} \arrow[r, "f_{n,m}"] \arrow[u, "\psi_{n,m}"] & H^2(G_S(K_n), E[p^m]) \arrow[r, "g_{n,m}"] \arrow[u, "\psi'_{n,m}"] & H^2(G_S(K_\infty), E[p^m])^{\Gamma_n} \arrow[r] \arrow[u, "\psi''_{n,m}"] & 0
\end{tikzcd}$$

The vertical maps in the diagram are induced by restriction. This diagram commutes. To see this, one argues as in the proof of lemma 2.7 taking the restriction map of the appropriate double complexes. Applying the snake lemma we get an exact sequence

$$0 \to \ker \psi_{n,m} \to \ker \psi'_{n,m} \to \ker \psi''_{n,m} \to \operatorname{coker} \psi_{n,m}. \tag{40}$$

Lemma 2.7 and its local analog allow us to take inverse limits of this exact sequence. By [17] theorem 8.3.20 $H^2(G_S(K_n), E[p^m])$ is finite and therefore $\ker \psi'_{n,m}$ is also finite. Therefore by taking inverse limits the sequence remains exact

$$0 \to \varprojlim_{n,m} \ker \psi_{n,m} \to \varprojlim_{n,m} \ker \psi'_{n,m} \to \varprojlim_{n,m} \ker \psi''_{n,m} \xrightarrow{\theta} \varprojlim_{n,m} \operatorname{coker} \psi_{n,m}. \tag{41}$$

By lemma 2.6 $\varprojlim_{n,m} \ker \psi_{n,m} \sim \dot{T}_\lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. Also note that $\varprojlim_{n,m} \ker \psi''_{n,m} = \varprojlim_{n,m} Ш^2(G_S(K_\infty), E[p^m])^{\Gamma_n}$ so by lemma 2.5 we have $\varprojlim_{n,m} \ker \psi''_{n,m} \sim \dot{T}_\mu(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. We claim that $\operatorname{img} \theta$ is finite. Since $\varprojlim_{n,m} \ker \psi''_{n,m} \sim \dot{T}_\mu(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$ therefore $\operatorname{img} \theta$ is a $\mathbb{Z}_p$-torsion module. Define $J := \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E)[p^\infty]$. Then we have an exact sequence

$$0 \to \bigoplus_{w \in S_\infty} E(K_{\infty,w})/p^m \to \bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E[p^m]) \to J[p^m] \to 0.$$

This, in turn, induces another exact sequence

$$(\bigoplus_{w \in S_\infty} E(K_{\infty,w})/p^m)_{\Gamma_n} \to (\bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E[p^m]))_{\Gamma_n} \to J[p^m]_{\Gamma_n} \to 0. \tag{42}$$

In the proof of proposition 2.4 we showed that J^* is a finitely generated torsion Λ-module. Hence it follows that $J[p^m]_{\Gamma_n}$ is finite. Also in lemma 2.6 we showed that $(\bigoplus_{w \in S_\infty} E(K_{\infty,w})/p^m)_{\Gamma_n}$ is finite. Therefore it follows from the exact sequence (42) that $(\bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E[p^m]))_{\Gamma_n}$ is finite and hence $\operatorname{coker} \psi_{n,m}$ is finite.

It follows that $\varprojlim_{n,m} \operatorname{coker} \psi_{n,m} = \operatorname{coker} \psi$ where $\psi := \varprojlim_{n,m} \psi_{n,m}$

Since the groups in the exact sequence (42) are finite, therefore by taking inverse limits the sequence remains exact

$$\varprojlim_{n,m} (\bigoplus_{w \in S_\infty} E(K_{\infty,w})/p^m)_{\Gamma_n} \to \varprojlim_{n,m} (\bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E[p^m]))_{\Gamma_n} \xrightarrow{\varphi} \varprojlim_{n,m} J[p^m]_{\Gamma_n} \to 0. \tag{43}$$

Now for any pair of maps of abelain groups $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ it is easy to prove from the snake lemma that we have an exact sequence

$$\begin{aligned} 0 \to \ker(\alpha) \to \ker(\beta \circ \alpha) \to \ker(\beta) \\ \to \operatorname{coker}(\alpha) \to \operatorname{coker}(\beta \circ \alpha) \to \operatorname{coker}(\beta) \to 0. \end{aligned}$$

Applying this to the maps

$$\varprojlim_{n,m} H^1(G_S(K_\infty), E[p^m])_{\Gamma_n} \xrightarrow{\psi} \varprojlim_{n,m} (\bigoplus_{w \in S_\infty} H^1(K_{\infty,w}, E[p^m]))_{\Gamma_n} \xrightarrow{\varphi} \varprojlim_{n,m} J[p^m]_{\Gamma_n}$$

and taking the sequence (43) into account we get an exact sequence

$$\varprojlim_{n,m}(\bigoplus_{w\in S_\infty} E(K_{\infty,w})/p^m)_{\Gamma_n} \to \operatorname{coker}(\psi) \to \operatorname{coker}(\varphi\circ\psi) \to 0.$$

Since J^* is a finitely generated Λ-module, it follows from lemma 2.1 that $\varprojlim_{n,m} J[p^m]_{\Gamma_n}$ is a finitely generated $\mathbb{Z}_p$-module and so the same is true for $\operatorname{coker}(\varphi\circ\psi)$. Also in the proof of lemma 2.6 we showed that $\varprojlim_{n,m}(\bigoplus_{w\in S_\infty} E(K_{\infty,w})/p^m)_{\Gamma_n}$ is finite. Therefore from the above exact sequence $\varprojlim_{n,m} \operatorname{coker}\psi_{n,m} = \operatorname{coker}\psi$ is a finitely generated $\mathbb{Z}_p$-module. It follows that $\operatorname{img}\theta$ is finite since as we showed above it is a torsion $\mathbb{Z}_p$-module. It follows from this, the exact sequence (41) and the observations noted after this sequence that we have an exact sequence

$$0 \to A \to \varprojlim_{n,m} \ker\psi'_{n,m} \to B \to 0$$

where $A \sim \dot{T}_\lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$ and $B \sim \dot{T}_\mu(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. So we get $\varprojlim_{n,m} \ker\psi'_{n,m} \sim \dot{T}_\Lambda(\mathrm{Sel}_{p^\infty}(E/K_\infty)^*)$. On the other hand $\varprojlim_{n,m} \ker\psi'_{n,m} = \varprojlim_{n,m} Ш^2(G_S(K_n), E[p^m])$ which by the pairing (2) defined in the beginning of this section may be identified with the Pontryagin dual of $R_{p^\infty}(E/K_\infty)$. This completes the proof of theorem 1.1.

Acknowledgments. The author would like to thank Kęstutis Česnavičius for many helpful correspondences about some of the arguments in the introduction. The author would also like to thank Robert Pollack for his helpful comments about this paper.

REFERENCES

[1] P. Billot, *Quelques aspects de la descente sur une courbe elliptique dans le cas de reduction supersinguliere*, Compos. Math., 58 (1986), pp. 341–369.

[2] E. Cartan and S. Eilenberg, *Homological Algebra*, Princeton Math Ser. 19, Princeton 1956.

[3] K. Česnavičius, *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc., 31:1 (2016), pp. 31–61.

[4] J. Coates and R. Greenberg, *Kummer Theory for Abelian Varieties over Local Fields*, Invent. Math., 124 (1996), pp. 129–174.

[5] J. Coates and R. Sujatha, *Fine Selmer groups of elliptic curves over p-adic Lie extensions*, Math. Ann., 331 (2005), pp. 809–839.

[6] J. Coates and R. Sujatha, *Galois Cohomology of Elliptic Curves*, Tata Inst. Fund. Res. Lecture Notes, Narosa Publishing House, 2000.

[7] K. Dekimpe, M. Hartl and S. Wauters, *A seven-term exact sequence for the cohomology of a group extension*, J. Algebra, 369 (2012), pp. 70–95.

[8] R. Greenberg, *Iwasawa theory for elliptic curves*, Lecture Notes in Math. 1716, Springer, New York 1999, pp. 51–144.

[9] R. Greenberg, *Iwasawa theory for p-adic representations*, in Algebraic number theory, pp. 97–137, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.

[10] B. Gross and J. Harris, *Real algebraic curves*, Ann. Sci. École. Norm. Sup., 14:4 (1981), pp. 157–182.

[11] J. Huebschmann, *Exact sequences in the cohomology of a group extension*, J. Algebra, 444 (2015), pp. 297–312.

[12] Y. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys, 26:6 (1971), pp. 7–78.

[13] S. Maclane, *Homology*, Springer 1967.

[14] A. Matar, *Fine Selmer Groups, Heegner points and Anticyclotomic $\mathbb{Z}_p$-extensions*, International Journal of Number Theory, 14:5 (2018), pp. 1279–1304.

[15] J. McCleary, *A user's guide to spectral sequences*, second edition, Cambridge Studies in Advanced Mathematics, 58, Cambridge University Press, Cambridge, 2001.

[16] J. S. Milne, *Arithmetic Duality Theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.

[17] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, second edition, Grundlehren der Mathematischen Wissenschaften, 323, Springer, 2008, xvi+825.

[18] B. Perrin-Riou, *Fonctions L p-adiques des représentations p-adiques, Astérisque*, 229 (1995), 198 pp.

[19] K. Ribet, *Torsion points of Abelian varieties in cyclotomic extensions*, appendix to N. Katz and S. Lang, Finiteness theorems in geometric classfield theory, Enseign. Math., 27 (1981), pp. 285–319.

[20] P. Schneider, *Iwasawa L-functions of varieties over algebraic number fields. A first approach*, Invent. Math., 71 (1983), pp. 251–293.

[21] P. Schnider, *p-adic height pairings II*, Invent. Math., 79 (1985), pp. 329–374.

[22] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math., 15:4 (1972), pp. 259–331

[23] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math., 106, Springer-Verlag (1986).

[24] K. Wingberg, *Duality theorems for abelian varieties over $\mathbb{Z}_p$-extensions*, in Algebraic number theory, pp. 471–492, Adv. Stud. Pure Math., 17, Academic Press, Boston, MA, 1989.

[25] K. Wingberg, *On the rational points of abelian varieties over $\mathbb{Z}_p$-extensions of number fields*, Math. Ann., 279 (1987), pp. 9–24.

[26] E. Weiss, *Cohomology of groups*, Academic Press 1969.

[27] C. Wuthrich, *Iwasawa theory of the fine Selmer group*, J. Algebraic Geom., 16:1 (2007), pp. 83–108.