SELMER GROUPS AND GENERALIZED CLASS FIELD TOWERS

AHMED MATAR

ABSTRACT. This paper proves a control theorem for the p-primary Selmer group of an abelian variety with respect to extensions of the form: maximal pro-p extension of a number field unramified outside a finite set of primes R which does not include any primes dividing p in which another finite set of primes S split completely. When the Galois group of the extension is not p-adic analytic, the control theorem gives information about p-ranks of Selmer and Tate-Shafarevich groups of the abelian variety. The paper also discusses what can be said in regards to a control theorem when the set R contains all the primes of the number field dividing p.

1. INTRODUCTION

Let K be a number field and p a prime number. Suppose K_∞/K is a $\mathbb{Z}_p$-extension of K i.e. a Galois extension K_∞/K with $\Gamma = \mathrm{Gal}(K_\infty/K)$ isomorphic to $\mathbb{Z}_p$. Then we may write, $K_\infty = \cup_n K_n$ with $[K_{i+1} : K_i] = p$.

Now suppose A is an abelian variety defined over K. For any algebraic extension L/K let $\mathrm{Sel}_p(A/L)$ denote the p-primary subgroup of the Selmer group $\mathrm{Sel}(A/L)$. A classical theorem of Mazur [20] (Mazur's 'Control Theorem') proves the following:

Theorem (Mazur)**.** *Assume p is a prime, K is a number field and A is an abelian variety defined over K with good ordinary reduction at all the primes of K above p. Assume that $K_\infty = \cup_n K_n$ is a $\mathbb{Z}_p$-extension of K. Then the natural maps (induced by restriction):*

$$\mathrm{Sel}_p(A/K_n) \longrightarrow \mathrm{Sel}_p(A/K_\infty)^{\mathrm{Gal}(K_\infty/K_n)}$$

have finite kernels and cokernels and their orders are bounded as n varies.

This theorem has been generalized in various ways by Greenberg [9], where he considers certain p-adic Lie extensions of a number field. The purpose of this paper is to prove an analog of these results in certain extensions conjectured not to be p-adic analytic: namely infinite extensions of the form $K^{(p)}_{R,S}/K$ where K is a number field, R and S are finite sets of primes of K with R *not containing any primes of K above p* (p some fixed prime) and $K^{(p)}_{R,S}/K$ is the maximal pro-p extension of K that is unramified outside of R in which all primes in S split completely. We allow R and S to be empty.

In case we have that $R = S = \varnothing$, the extension $K^{(p)}_{\varnothing,\varnothing}/K$ is the maximal unramified (everywhere) pro-p extension of K. This is the p-Hilbert class field tower of K. In this case the existence of infinite such extensions was shown for the first time in 1964 by Golod and Shafarevich [13]. To state their result, let $\rho(K)$ denote the p-rank of the ideal class group of K and $\nu(K) = r_1 + r_2 + \delta_K - 1$ where (r_1, r_2) is the signature of the number field K and $\delta_K = 1$ or 0 depending on whether (respectively) K contains a primitive p-th root of unity or not. They proved that if $\rho(K) \geq 2 + 2\sqrt{\nu(K) + 1}$, then the p-class field tower of K is infinite. We will later in section 2 explain a condition that more generally guarantees that $K^{(p)}_{R,S}/K$ is infinite where R and S are not necessarily empty.

Let now us mention (a special case of) the Fontaine-Mazur conjecture. With our notation above, we let $\Sigma^{R,S}_{K,p} = \mathrm{Gal}(K^{(p)}_{R,S}/K)$. In [8], Fontaine and Mazur conjectured:

Conjecture (Fontaine-Mazur)**.** *For any number field K, $\Sigma^{R,S}_{K,p}$ has no infinite p-adic analytic quotient.*

Assuming this conjecture, we get that $\Sigma^{R,S}_{K,p}$ is infinite if and only if it is not p-adic analytic (the "if" part follows from the fact that any finite group is p-adic analytic for any prime p). In some of the main results of this paper, we will make the assumption that $\Sigma^{R,S}_{K,p}$ is not p-adic analytic. As we will explain later, this assumption is equivalent to the unboundedness of the minimal number of topological generators of the open normal subgroups of $\Sigma^{R,S}_{K,p}$.

It has been shown in several cases that $\Sigma^{R,S}_{K,p}$ is not p-adic analytic. For example, Hajir [14] proved that if the "Golod-Shafarevich condition" (as above) $\rho(K) \geq 2 + 2\sqrt{\nu(K) + 1}$ is met, then the Galois group $\Sigma^{\varnothing,\varnothing}_{K,p}$ of the (infinite) p-class field tower of K is not p-adic analytic. Other cases for which $\Sigma^{R,S}_{K,p}$ is not p-adic analytic are shown in articles by Boston [2], Maire [19] and Wingberg [27].

In section 2, following Hajir, we explain a condition that guarantees that $\Sigma^{R,S}_{K,p}$ is not p-adic analytic.

Before stating the results of this paper let us define the *p-rank* of an abelian group G (possibly infinite) as:

$$r_p(G) = \dim_{\mathbb{F}_p} G[p]$$

This of course extends the usual definition of p-rank of a finite abelian group.

Now let p be a prime and K be a number field, with sets R and S of primes of K as above. We will denote the primes of K dividing p and archimedean primes of K by R_p and R_∞ respectively. Also, to simplify notation, we will denote $K^{(p)}_{R,S}$ by K_∞ and also denote $\mathrm{Gal}(K^{(p)}_{R,S}/K)$ by Σ. Finally, we will let $\mathcal{E}$ be the set of fields K' such that K'/K is a finite

extension contained in K_∞.

Suppose A is an abelian variety defined over K. For any non-archimedean prime v of K, let $c_{A,v}$ (also simply denoted c_v) be the Tamagawa number of A at v (we will recall its definition later). Also we will let B be the (finite) set of primes of K where A has bad reduction.

Let us say Condition (C) is satisfied if the following are met:

(i) $(c_v, p) = 1$ for all primes $v \in (B \cap R_p) \setminus S$ of K and for every prime $v \in B \setminus (R \cup S \cup R_p)$ we have either $(c_v, p) = 1$ or $A(K_v)[p^\infty] = \{0\}$.
(ii) $A(K_v)$ is connected for every prime $v \in R_\infty$ that ramifies in K_∞/K.
(iii) $A(K_v)[p^\infty] = \{0\}$ for all primes $v \in R \setminus (S \cup R_\infty)$.

We can now state the main result of this paper:

Theorem A. *For any $K' \in \mathcal{E}$, the natural map*

$$s_{K'} : \mathrm{Sel}_p(A/K') \longrightarrow \mathrm{Sel}_p(A/K_\infty)^{\mathrm{Gal}(K_\infty/K')}$$

has finite kernel and cokernel. Moreover we have:

(i) If $A(K)[p] = \{0\}$, then $\ker s_{K'} = \{0\}$ for any $K' \in \mathcal{E}$. If we also have that condition (C) is satisfied, then $\mathrm{coker}\, s_{K'} = \{0\}$ for any $K' \in \mathcal{E}$.
(ii) Suppose $A(K)[p] \neq \{0\}$ and Σ is not p-adic analytic. Then:
  (a) If condition (C) is satisfied, then $r_p(\ker s_{K'})$ is unbounded as K' varies through the set $\mathcal{E}$.
  (b) If $\mathrm{rank}(A(K'))$ is bounded as K' varies through $\mathcal{E}$, $Ш(A/K')[p^\infty]$ is finite for any $K' \in \mathcal{E}$ and K is totally imaginary if $p = 2$, then $r_p(\mathrm{coker}\, s_{K'})$ is unbounded as K' varies through $\mathcal{E}$.

Theorem A above has an interesting corollary giving a result about the structure of $Ш(A/K_\infty)[p^\infty]$ in a certain case.

Corollary A. *Suppose Σ is not p-adic analytic, K is totally imaginary in the case when $p = 2$, and A and A' are two abelian varieties defined over K with A isogenous to A' over K and:*

(i) $A(K)[p] \neq \{0\}$.
(ii) $A'(K)[p] = \{0\}$, $\mathrm{Sel}_p(A'/K) = \{0\}$ and condition (C) is satisfied (with respect to K and A').

Then $Ш(A'/K_\infty)[p^\infty] = 0$ and $Ш(A/K_\infty)[p^\infty]$ contains an infinite elementary abelian p-group. If the isogeny from A to A' is of degree p, then $Ш(A/K_\infty)[p^\infty]$ is itself an infinite elementary abelian p-group.

From Theorem A, we see that if Σ is not p-adic analytic and A is an abelian variety defined over K with $A(K)[p] \neq \{0\}$ and condition (C) is satisfied, then $r_p(\mathrm{Sel}_p(A/K'))$ is unbounded as K' varies through $\mathcal{E}$. The following theorem gives a stronger result:

Theorem B. *If Σ is not p-adic analytic and A is an abelian variety defined over K with $A(K)[p] \neq \{0\}$ and condition (C) is satisfied, then $r_p(Ш(A/K'))$ is unbounded as K' varies through $\mathcal{E}$.*

Theorem B can be strengthened in some cases to give a lower bound on $r_p(Ш(A/K'))$ of the form $c[K' : K] + 1$ where c is a positive constant. See the discussion following the proof of Theorem B.

2. Preliminaries

Throughout this paper, we will fix a prime p, a number field K, an abelian variety A defined over K and sets R and S of primes of K as in the introduction. We will also use the same notation introduced there: We will denote the primes of K dividing p and archimedean primes of K by R_p and R_∞ respectively and will also let B be the (finite) set of primes of K where A has bad reduction and $\mathcal{E}$ be the set of fields K' such that K'/K is a finite extension contained in $K_{R,S}^{(p)}$. Let us also denote $K_{R,S}^{(p)}$ by K_∞ and for any $K' \in \mathcal{E}$ denote $\mathrm{Gal}(K_{R,S}^{(p)}/K')$ by $\Sigma_{K'}$. We will often simply write Σ for Σ_K. Note that for any $K' \in \mathcal{E}$ we have ${K'}_{R',S'}^{(p)} = K_{R,S}^{(p)}$ where R' and S' are the extensions of the sets R and S to K'.

Also, for any number field F and any set S of primes of F, we will (as is standard) denote the ideal class group of F by $\mathrm{Cl}(F)$ and the S-ideal class group of F by $\mathrm{Cl}_S(F)$ (recall that $\mathrm{Cl}_S(F)$ is the quotient of $\mathrm{Cl}(F)$ by the subgroup generated by the classes of the prime ideals in S).

Finally, for any algebraic extension L/K and any prime $v \in L$, we will let L_v denote the union of the v-adic completions of all finite extensions of K contained in L.

For any pro-p group G, we set:

$$h_i(G) = \dim_{\mathbb{Z}/p\mathbb{Z}} H^i(G, \mathbb{Z}/p\mathbb{Z}) \quad (\text{G acts trivially}),\ i = 1, 2.$$

Then

$$h_1(G) = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathrm{Hom}_{\mathrm{cont}}(G, \mathbb{Z}/p\mathbb{Z}) = h_1(G^{ab})$$

and $h_1(G)$ is finite if and only if G is topologically finitely generated, in which case $h_1(G)$ is the minimal number of topological generators of G (also of G^{ab}). If in addition to $h_1(G)$ being finite we also have $h_2(G)$ finite, then $h_2(G)$ is the minimal number of relations for defining G as a pro-p group.

Now in the case where $K' \in \mathcal{E}$, we have that $h_1(\Sigma_{K'})$ and $h_2(\Sigma_{K'})$ are both finite. This follows from [23] Theorem 10.7.12 which in fact calculates both of these quantities. These calculations will be important in Lemma 2.3.

Another important observation is that for any $K' \in \mathcal{E}$, we have that $\Sigma_{K'}^{ab}$ is finite. In the case when $R = \varnothing$, this is easy: $\Sigma_{K'}^{ab} \cong \mathrm{Cl}_S(K')[p^\infty]$. In the general case, we can argue as follows: we have that $\Sigma_{K'}$ is finitely generated (since as we just discussed $h_1(\Sigma_{K'})$ is finite) and hence so is $\Sigma_{K'}^{ab}$ (implying $\Sigma_{K'}^{ab}$ is finitely generated over $\mathbb{Z}_p$). But K' cannot have a $\mathbb{Z}_p$-extension contained in K_∞, since in any such extension some prime above p must ramify (and $R \cap R_p = \varnothing$). So $\mathrm{rank}_{\mathbb{Z}_p}(\Sigma_{K'}^{ab}) = 0$ and therefore $\Sigma_{K'}^{ab}$ is finite.

Following Hajir [14], we will now give a condition that guarantees that Σ is not p-adic analytic. Before doing this let us state two theorems from the literature and introduce some notation. First, we have the following well-known theorem of Golod and Shafarevich in its sharpened form due to Gaschütz and Vinberg (see [24] Th. 10 or [23] Th. 3.7.9).

Theorem 2.1. *Let G be a finite p-group, then $h_2(G) > \frac{1}{4}\, h_1(G)^2$.*

From the work of Lubotzky (Prop. 1.3 of [17]) we get the following refinement of this theorem for p-adic Lie groups

Theorem 2.2. *Let G be a pro-p p-adic analytic group with both $h_1(G) \geq 2$ and $h_2(G) \geq 2$, then $h_2(G) > \frac{1}{4}\, h_1(G)^2$.*

We will now introduce some notation related to the set R. First let us note that the following primes cannot ramify in a pro-p extension and are therefore redundant in R:

(1) Complex primes
(2) Real primes if $p \neq 2$
(3) Primes $\mathfrak{p} \nmid p$ with $N(\mathfrak{p}) \not\equiv 1 \bmod p$ (see [25] IV Prop. 7)

Removing all of the above redundant primes and $R \cap S$ from R we obtain a subset $R_{\min} \subseteq R$ for which we have:

$$K^{(p)}_{R,S} = K^{(p)}_{R_{\min},S}$$

Let us define δ to be 1 if K contains a primitive p-th root of unity and 0 otherwise. Also, we let (r_1, r_2) be the signature of the number field K.

Lemma 2.3. *Σ is not p-adic analytic if:*

(i) $R = \varnothing$ and

$$r_p(\mathrm{Cl}_S(K)) \geq 2 + 2\sqrt{r_1 + r_2 + \delta + \#S \setminus R_\infty}$$

(ii) $R \neq \varnothing$ and

$$\#R_{\min} \geq 1 + r_1 + r_2 + \delta + \#S \setminus R_\infty + 2\sqrt{r_1 + r_2 + \#S \setminus R_\infty}$$

Proof. Assume by means of contradiction that Σ is p-adic analytic. If we further assume that $h_1(\Sigma) = 1$, then Σ is abelian and hence finite since as we mentioned before Σ^{ab} is finite.

Then from Theorem 2.1, we have:

$$h_2(\Sigma) > \tfrac{1}{4}\, h_1(\Sigma)^2$$

From this we deduce that:

$$h_1(\Sigma) < 2 + 2\sqrt{h_2(\Sigma) - h_1(\Sigma) + 1} \tag{1}$$

We now use the calculations of $h_1(\Sigma)$ and $h_2(\Sigma)$ in [23]. In case (i) of the lemma, we have by *loc. cit.* Th. 10.7.12 that:

$$h_2(\Sigma) - h_1(\Sigma) + 1 \leq r_1 + r_2 + \delta + \#S \setminus R_\infty$$

Combining this inequality with (1) gives:

$$h_1(\Sigma) < 2 + 2\sqrt{r_1 + r_2 + \delta + \#S \setminus R_\infty}$$

Since $R = \varnothing$, therefore $h_1(\Sigma) = r_p(\mathrm{Cl}_S(K))$, hence by the above inequality we get that:

$$r_p(\mathrm{Cl}_S(K)) < 2 + 2\sqrt{r_1 + r_2 + \delta + \#S \setminus R_\infty}$$

which contradicts (i), so $h_1(\Sigma) \geq 2$.

In case (ii) of the lemma, we have by *loc. cit.* Th. 10.7.12 that:

$$h_2(\Sigma) - h_1(\Sigma) + 1 \leq r_1 + r_2 + \delta + \#S \setminus R_\infty$$

Combining this inequality with (1) gives:

$$h_1(\Sigma) < 2 + 2\sqrt{r_1 + r_2 + \#S \setminus R_\infty}$$

Also, by *loc. cit.* Th. 10.7.12 we have that:

$$h_1(\Sigma) \geq 1 + R_{\min} - \delta - (r_1 + r_2) - \#S \setminus R_\infty$$

Therefore the two previous inequalities give:

$$1 + R_{\min} - \delta - (r_1 + r_2) - \#S \setminus R_\infty < 2 + 2\sqrt{r_1 + r_2 + \#S \setminus R_\infty}$$

This contradicts (ii). Therefore $h_1(\Sigma) \geq 2$.

We have shown that under the assumptions of the lemma, we must have $h_1(\Sigma) \geq 2$. Therefore, Σ is a pro-p p-adic Lie group with $h_1(\Sigma) \geq 2$. From Lemma 3.2 of the next section, we also get that $h_2(\Sigma) \geq 2$, so by Theorem 2.2 we have that: $h_2(\Sigma) > \frac{1}{4} h_1(\Sigma)^2$. But then by the same reasoning as above, this cannot by true. Therefore Σ is not p-adic analytic. □

We will now state an important equivalent condition to Σ not being p-adic analytic. A theorem of Lubotzky and Mann [18] states that for a finitely generated pro-p group G, the lim sup and lim inf of

$$\dim_{\mathbb{Z}/p\mathbb{Z}} H^1(H, \mathbb{Z}/p\mathbb{Z})$$

as H ranges over all normal open subgroups of G are equal (possibly infinite), and G is p-adic analytic if and only if this common value is finite.

From this we immediately deduce:

Theorem 2.4. *Σ is not p-adic analytic if and only if $h_1(\Sigma_{K'})$ is unbounded as K' varies over any set of finite Galois extensions K'/K contained in K_∞ such that the set of subgroups $\mathrm{Gal}(K_\infty/K')$ are a cofinal subset of the normal open subgroups of Σ.*

Throughout the proof of various lemmas and Theorem A we will frequently be comparing p-ranks of abelian groups in exact sequences. In regards to this we have the following easy observations:
If $0 \to G' \to G \to G'' \to 0$ is an exact sequence of p-primary abelian groups of finite p-rank then:

(i) $r_p(G') \leq r_p(G)$: This is trivial.

(ii) $r_p(G'') \leq r_p(G)$: We show an easy proof of this by considering Pontryagin duals. First suppose B is a discrete p-primary abelian group with finite p-rank, then it is not hard show that its Pontryagin dual $\widehat{B}$ is finitely generated over $\mathbb{Z}_p$ (or as it is usually said: B is cofinitely generated as a $\mathbb{Z}_p$-module). Also, one then easily observes that $r_p(B) = \mathrm{rank}_{\mathbb{Z}_p}(\widehat{B}) + r_p(\widehat{B}_{\mathrm{tors}})$. Now give G and G'' the discrete topology. Then the Pontryagin dual $\widehat{G''}$ of G'' is a subgroup of the Pontryagin dual $\widehat{G}$ of G and as G and G'' both have finite p-rank by assumption, then by what we just noted, to show that $r_p(G'') \leq r_p(G)$ it suffices to show that $\mathrm{rank}_{\mathbb{Z}_p}(\widehat{G''}) \leq \mathrm{rank}_{\mathbb{Z}_p}(\widehat{G})$ and $r_p(\widehat{G''}_{\mathrm{tors}}) \leq r_p(\widehat{G}_{\mathrm{tors}})$. But this is rather obvious as $\widehat{G''}$ is a $\mathbb{Z}_p$-submodule of $\widehat{G}$.

(iii) $r_p(G) \leq r_p(G') + r_p(G'')$: This follows by taking $\mathbb{F}_p$-dimensions along the exact sequence: $0 \to G'[p] \to G[p] \to G''[p]$

Let us now explain the basic strategy for the proof of Theorem A. First recall that for any algebraic extension L of K the p-primary subgroup of the Selmer group of A over L is defined by the exactness of:

$$0 \longrightarrow \mathrm{Sel}_p(A/L) \longrightarrow H^1(L, A[p^\infty]) \longrightarrow \prod_v H^1(L_v, A)[p^\infty]$$

where the last product runs over all primes v of L.

Now suppose L is a finite extension of K and let T be a finite set of primes of L containing all the primes dividing p, all archimedean primes and all primes where A has bad reduction. Also let $L_{_T}$ be the maximal extension of L unramified outside of T and $G_T(L) = \mathrm{Gal}(L_{_T}/L)$. Then it is well-known that $\mathrm{Sel}_p(A/L)$ may be defined by

$$0 \longrightarrow \mathrm{Sel}_p(A/L) \longrightarrow H^1(G_T(L), A[p^\infty]) \longrightarrow \prod_{v \in T} H^1(L_v, A)[p^\infty]$$

Let us now fix T to be the set:

$$T = R \cup B \cup R_p \cup R_\infty$$

We then define for any $K' \in \mathcal{E}$ $T_{K'}$ to be the set of primes of K' that lie over a prime in T.

Note that as K' is contained in $K_{_T}$ for any $K' \in \mathcal{E}$, we have $K'_{_{T'}} = K_{_T}$ where $T' = T_{K'}$ and so $G_{T'}(K') = \mathrm{Gal}(K_{_T}/K')$. To simplify notation, we will denote $G_{T'}(K')$ simply by $G_T(K')$. As for K_∞, we will define $G_T(K_\infty)$ as $G_T(K_\infty) = \mathrm{Gal}(K_{_T}/K_\infty)$.

For any $K' \in \mathcal{E}$ we consider the commutative diagram:
(2)

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_p(A/K_\infty)^{\Sigma_{K'}} & \longrightarrow & H^1(G_T(K_\infty), A[p^\infty])^{\Sigma_{K'}} & \xrightarrow{\psi_{K_\infty}} & (\varinjlim \bigoplus_{w \in T_{\widetilde{K}}} H^1(\widetilde{K}_w, A)[p^\infty])^{\Sigma_{K'}} \\ & & \uparrow{\scriptstyle s_{K'}} & & \uparrow{\scriptstyle h_{K'}} & & \uparrow{\scriptstyle g_{K'}} \\ 0 & \longrightarrow & \mathrm{Sel}_p(A/K') & \longrightarrow & H^1(G_T(K'), A[p^\infty]) & \xrightarrow{\lambda_{K'}} & \bigoplus_{v \in T_{K'}} H^1(K'_v, A)[p^\infty] \end{array}$$

where in the above diagram the rows are exact, the direct limit of the term on the top row is taken with respect to the restriction maps, $h_{K'}$ is given by restriction and $g_{K'}$ is the map into the direct limit.

Replacing the terms on the right in both rows of the above diagram with their images we get the following diagram:
(3)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}_p(A/K_\infty)^{\Sigma_{K'}} & \longrightarrow & H^1(G_T(K_\infty), A[p^\infty])^{\Sigma_{K'}} & \xrightarrow{\psi_{K_\infty}} & \mathrm{img}\, \psi_{K_\infty} & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle s_{K'}} & & \uparrow{\scriptstyle h_{K'}} & & \uparrow{\scriptstyle g'_{K'}} & & \\ 0 & \longrightarrow & \mathrm{Sel}_p(A/K') & \longrightarrow & H^1(G_T(K'), A[p^\infty]) & \xrightarrow{\lambda_{K'}} & \mathrm{img}\, \lambda_{K'} & \longrightarrow & 0 \end{array}$$

From this diagram we have the following exact sequence:
(4)

$$0 \to \ker s_{K'} \to \ker h_{K'} \to \ker g'_{K'} \to \mathrm{coker}\, s_{K'} \to \mathrm{coker}\, h_{K'} \to \mathrm{coker}\, g'_{K'} \to 0$$

Following Greenberg [9] we study the kernels and cokernels of $s_{K'}$ using the above sequence by studying the kernels and cokernels of $h_{K'}$ and $g'_{K'}$.

All of our results depend on the fact that $A(K_\infty)[p^\infty]$ is finite. This fact is predicted by the Fontaine-Mazur conjecture and follows from a result of Zarhin (Theorem 6.1 of [28]). However, one can give a fairly simple proof of this fact based on an idea of Greenberg in [9] of studying the determinant of the representation on $K(A(K_\infty)[p^\infty])$:

Theorem 2.5. *$A(K_\infty)[p^\infty]$ is finite*

Proof. Let $X = A(K_\infty)[p^\infty]$ and let $L = K(X)$. Suppose that X is infinite. Let us set $V_p = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $W_p = T_p(X) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ where $T_p(A)$ and $T_p(X)$ are the p-adic Tate modules of $A[p^\infty]$ and X respectively. As X is assumed to be infinite, we have $\dim_{\mathbb{Q}_p} W_p \geq 1$.

Let $G = \mathrm{Gal}(L/K)$ and let $\chi : G \to \mathbb{Z}_p^\times$ be the determinant of the representation of G induced from its action on W_p. Then χ factors through G^{ab} and as this is finite, we get that $\mathrm{img}(\chi)$ is finite i.e. consists of roots of unity. Now choose a prime v of K not dividing p at which A has good reduction. Then we have that $K_v(A[p^\infty])$ is contained in K_v^{nr}, the maximal unramified extension of K_v, and a well-known theorem of Weil states that the eigenvalues of Frobenius $\sigma_v \in \mathrm{Gal}(K_v^{nr}/K_v)$ on V_p are algebraic integers of complex absolute value $\sqrt{q}$ where q is the order of the residue field of K

at v. Letting $\sigma_v^{'}$ be Frobenius in the decomposition group of any prime w of L above v we see that $\chi(\sigma_v^{'})$ is not a root of unity which gives the required contradiction. □

3. Cohomology Group Calculations

In this section, we will prove various results mainly about cohomology groups used in the proof of Theorem A. First, we have the following elementary lemma:

Lemma 3.1. *Let G be a pro-p group and M a discrete p-primary G-module. Then $M = 0$ if and only if $M^G = 0$.*

Proof. For the nontrivial direction assume $m \in M$ with $m \neq 0$. Let D be the G-module generated by m. As M is a discrete p-primary G-module, we necessarily have that D is finite of p-power order. If $d \in D \setminus D^G$, then the cardinality of its orbit via the action of G is equal to the index of its stabilizer in G and hence is of order p^n for some $n \geq 1$ since G is pro-p. Then by considering the partition of D into orbits under the action of G, we see that $|D| \equiv |D^G| \pmod{p}$ and therefore since $|D| \equiv 0 \pmod{p}$, we have that $|D^G| \equiv 0 \pmod{p}$. But as D^G contains 0, we have that $|D^G| > 0$ and so $D^G \neq 0$. □

The next lemma will be crucial in proving the unboundedness of $r_p(\operatorname{coker} s_{K'})$ in part (ii) of Theorem A.

Lemma 3.2. *For any $K' \in \mathcal{E}$ and k with $k \geq 1$, we have that $H^i(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})$ is finite ($\Sigma_{K'}$ acts trivially) for $i = 1, 2$. And*

$$r_p(H^2(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})) \geq r_p(H^1(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z}))$$

Proof. As mentioned in section 2, we have that $H^i(\Sigma_{K'}, \mathbb{Z}/p\mathbb{Z})$ is finite for $i = 1, 2$, therefore by devissage both $H^1(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})$ and $H^2(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})$ are finite. Now to prove the statement about p-ranks consider the exact sequence:

$$0 \to \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{p^k} \mathbb{Q}_p/\mathbb{Z}_p \to 0$$

Taking the $\Sigma_{K'}$-cohomology of this sequence (considering all modules with trivial action), we get the following exact sequence:

$$0 \to H^1(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z}) \to H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{p^k} H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^2(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})$$

The zero on the left of this sequence follows from the fact that $\Sigma_{K'}$ acts trivially on all the groups in the first short exact sequence.

Note that all the groups occurring in the above sequence are finite abelian p-groups, for $H^1(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})$ and $H^2(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})$ are both finite as we just discussed and $H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontryagin dual of $\Sigma_{K'}^{ab}$ so is also a finite abelian p-group.

From the above sequence, we have that $H^1(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z}) = H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p)[p^k]$ and $H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p)/p^k H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p)$ is contained in $H^2(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})$. Since

$$r_p(H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p)[p^k]) = r_p(H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p)/p^k H^1(\Sigma_{K'}, \mathbb{Q}_p/\mathbb{Z}_p))$$

we therefore see that:

$$r_p(H^2(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z})) \geq r_p(H^1(\Sigma_{K'}, \mathbb{Z}/p^k\mathbb{Z}))$$

□

The next two propositions will give nice descriptions of certain cohomology groups attached to abelian varieties over local fields (both archimedean and non-archimedean) in certain cases. These propositions are the key tools in studying the kernels and cokernels of $g_{K'}$. Before stating the propositions let us define the component group and Tamagawa number of an abelian variety (at a prime):

Definition 3.3. Let A be an abelian variety defined over K, a finite extension of $\mathbb{Q}_p$ (p a prime), let $\mathcal{A}$ be the Néron model of A over the ring of integers of K and k be the residue field of K. Let $\mathcal{A}_k$ be the special fiber of $\mathcal{A}$ and $\mathcal{A}_k^0$ its connected component of the identity. The group $\Phi_A = \mathcal{A}_k/\mathcal{A}_k^0$ of connected components is a finite étale group scheme over k. This group scheme is called the *component group* of A, and the *Tamagawa number* of A is $c_A = \#\Phi_A(k)$.

Now suppose that A is an abelian variety over a number field K, then for any non-archimedean prime v of K the Tamagawa number of A at v denoted $c_{A,v}$ or simply c_v is the Tamagawa number of A_{K_v}; where K_v is the completion of K at v.

Proposition 3.4. *Let A be an abelian variety defined over K, a finite extension of $\mathbb{Q}_p$ (p some prime). If K'/K is an unramified extension, k' the residue field of K' and $G = \mathrm{Gal}(K'/K)$, then: $H^i(G, A(K')) = H^i(G, \Phi_A(k'))$ for $i \geq 1$.*

Proof. For $i = 1$ this is Proposition 4.3 of [20] and one notes that the proof carries over for $i > 1$. □

Proposition 3.5. *Let A be an abelian variety over $\mathbb{R}$ of dimension d. If $A^0(\mathbb{R})$ is the connected component of the identity of $A(\mathbb{R})$, then $H^1(\mathrm{Gal}(\mathbb{C}/\mathbb{R}), A) \cong A(\mathbb{R})/A^0(\mathbb{R}) = (\mathbb{Z}/2\mathbb{Z})^n$ where $n = \dim_{\mathbb{Z}/2\mathbb{Z}}(A(\mathbb{R})[2]) - d$.*

Proof. (sketch) Note that $A(\mathbb{R}) = (\mathbb{R}/\mathbb{Z})^d \times (\mathbb{Z}/2\mathbb{Z})^n$ for some $0 \leq n \leq d$ (this is the n in the statement of the proposition) and $A^0(\mathbb{R})$ is a connected compact abelian real Lie group of dimension d and therefore is isomorphic to $(\mathbb{R}/\mathbb{Z})^d$. The norm map $N : A(\mathbb{C}) \to A(\mathbb{R})$ is continuous and $A(\mathbb{C})$ is connected and compact, so its image is closed and connected. Moreover, as it contains $2A(\mathbb{R})$, it has finite index and therefore is open. Consequently, we must have that $NA(\mathbb{C}) = A^0(\mathbb{R})$.

Let A^t be the dual variety of A and $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. The Weil pairing $A(\mathbb{C})[2] \times A^t(\mathbb{C})[2] \to \mu_2$ is a non-degenerate G-equivariant pairing. From this we get that: $\#A(\mathbb{R})[2] = \#A^t(\mathbb{R})[2]$ and hence the integer n above is the same for both A and its dual A^t.

Finally, as shown in [21] p. 46, we have that $H^1(G, A)$ is dual to $A^t(\mathbb{C})^G/NA^t(\mathbb{C})$ and by the above this latter group is $A^t(\mathbb{R})/(A^t)^0(\mathbb{R})$, so we get that $H^1(G, A) \cong (\mathbb{Z}/2\mathbb{Z})^n = A(\mathbb{R})/A^0(\mathbb{R})$. □

The following lemma lists some well-known properties of isogenous abelian varieties:

Lemma 3.6. *Let A and A' be two abelian varieties defined over a number field K with A isogenous to A' over K. Then we have:*

(i) $\mathrm{rank}\,(A(K)) = \mathrm{rank}\,(A'(K))$.
(ii) $Ш(A/K)$ *is finite if and only if* $Ш(A'/K)$ *is finite.*
(iii) $\mathrm{Sel}(A/K)$ *is finite if and only if* $\mathrm{Sel}(A'/K)$ *is finite.*

Moreover, the statements of (ii) and (iii) remain true if one replaces the groups there by their p-primary subgroup (p any prime).

Proof. Since A and A' are isogenous over K we have morphisms (defined over K): $f : A \to A'$, $g : A' \to A$ such that $fg = n = gf$ for some integer $n \neq 0$. Since $\mathrm{rank}(A(K)) = \dim_{\mathbb{Q}}(A(K) \otimes \mathbb{Q})$ and $\mathrm{rank}(A'(K)) = \dim_{\mathbb{Q}}(A'(K) \otimes \mathbb{Q})$ and multiplication by n is an isomorphism on any $\mathbb{Q}$-vector space, (i) follows.

To see (ii), suppose that $Ш(A'/K)$ is finite. Then the isogenies f, g define maps $\bar{f} : Ш(A/K) \to Ш(A'/K)$ and $\bar{g} : Ш(A'/K) \to Ш(A/K)$ whose composites are multiplication by n. From this we get that the kernel of $\bar{f}$ is contained in $Ш(A/K)[n]$, but this group is well-known to be finite, therefore $\ker \bar{f}$ is finite and so we see that $Ш(A/K)$ is finite. As everything is symmetric, we have shown (ii).

Finally, for (iii) we can proceed as in (ii) noting that $\mathrm{Sel}(A/K)[n]$ is finite, or we can use (i) and (ii) since $\mathrm{Sel}(A/K)$ is finite if and only if $\mathrm{rank}(A(K)) = 0$ (i.e. $A(K)$ is finite) and $Ш(A/K)$ is finite. The statement about p-primary subgroups follows similarly to the above. □

We need one final proposition that will be used in proving Theorem A:

Proposition 3.7. *Let A be an abelian variety over a number field K, with A^t its dual variety. Let p be a prime, and assume K is totally imaginary if $p = 2$ and that $Ш(A/K)[p^\infty]$ is finite. Let T be a finite set of primes of K containing all the primes dividing p and all the primes where A has bad reduction. Let λ_K be the map:*

$$H^1(G_T(K), A[p^\infty]) \xrightarrow{\lambda_K} \prod_{v \in T} H^1(K_v, A)[p^\infty]$$

Then:

(i) $r_p(\mathrm{coker}\,\lambda_K) \leq \mathrm{rank}(A(K)) + r_p(A^t(K)_{tors})$
(ii) $r_p(H^2(G_T(K), A[p^\infty])) \leq \mathrm{rank}(A(K)) + r_p(A^t(K)_{tors})$

Proof. First, let us define the compact Selmer group: For any n, the classical p^n-Selmer group $\mathrm{Sel}^{(p^n)}(A/K)$ is defined by the exactness of:

$$0 \longrightarrow \mathrm{Sel}^{(p^n)}(A/K) \longrightarrow H^1(K, A[p^n]) \longrightarrow \prod_v H^1(K_v, A)$$

From this, we now define the compact p-Selmer group $\mathcal{R}_p(A/K)$ as:

$$\mathcal{R}_p(A/K) = \varprojlim_n \mathrm{Sel}^{(p^n)}(A/K)$$

where the inverse limit is taken with respect to the multiplication by p maps. Then we have the Cassels-Poitou-Tate exact sequence (see [3] and [5]):

$$0 \longrightarrow \mathrm{Sel}_p(A/K) \longrightarrow H^1(G_T(K), A[p^\infty]) \xrightarrow{\lambda_K} \prod_{v \in T} H^1(K_v, A)[p^\infty]$$

$$\xrightarrow{\theta_K} \widehat{\mathcal{R}_p(A^t/K)} \longrightarrow H^2(G_T(K), A[p^\infty]) \longrightarrow 0 \tag{5}$$

where in the above $\widehat{\mathcal{R}_p(A^t/K)}$ means the Pontryagin dual of the $\mathcal{R}_p(A^t/K)$.

We should note that if $p = 2$ and K has a real place, then the map $\widehat{\mathcal{R}_p(A^t/K)} \longrightarrow H^2(G_T(K), A[p^\infty])$ is not necessarily surjective and as the surjectivity is important for the results of this proposition, we have insisted that K be totally imaginary if $p = 2$.

Before proceeding further let us for any abelian group M denote $\varprojlim M/p^nM$ by M^* (where the inverse limit is over all n).

Now note that for any n we have an exact sequence:

$$0 \to A^t(K)/p^nA^t(K) \to \mathrm{Sel}^{(p^n)}(A^t/K) \to Ш(A^t/K)[p^n] \to 0$$

Taking inverse limits over n and noting that $Ш(A^t/K)[p^n]$ is finite for any n, we get:

$$0 \to A^t(K)^* \to \mathcal{R}_p(A^t/K) \to T_pШ(A^t/K) \to 0 \tag{6}$$

where $T_pШ(A^t/K)$ denotes the p-adic Tate module of $Ш(A^t/K)$.

Now as $Ш(A/K)[p^\infty]$ was assumed to be finite, therefore $Ш(A^t/K)[p^\infty]$ is also finite by Lemma 3.6 since A is isogenous to A^t. Then the finiteness of $Ш(A^t/K)[p^\infty]$ implies that $T_pШ(A^t/K) = 0$. So from the sequence (6) above we get that: $\mathcal{R}_p(A^t/K) = A^t(K)^*$.

Now let $r = \mathrm{rank}(A(K))$. Then again by Lemma 3.6, we have that $r = \mathrm{rank}(A^t(K))$. Writing $A^t(K) = \mathbb{Z}^r \times D$ where D is a finite abelian group, we get that $A^t(K)^* = \mathbb{Z}_p^r \times D'$ where $D' = D[p^\infty]$. Then $\mathcal{R}_p(A^t/K) = A^t(K)^* = \mathbb{Z}_p^r \times D'$ and so $\widehat{\mathcal{R}_p(A^t/K)} = (\mathbb{Q}_p/\mathbb{Z}_p)^r \times D'$, so $r_p(\widehat{\mathcal{R}_p(A^t/K)}) = \mathrm{rank}(A(K)) + r_p(A^t(K)_{\mathrm{tors}})$. Then from the Cassels-Poitou-Tate exact sequence (5) above, we must have that $r_p(\mathrm{coker}\,\lambda_K)$ and $r_p(H^2(G_T(K), A[p^\infty])$ are both less than or equal to $\mathrm{rank}(A(K)) + r_p(A^t(K)_{\mathrm{tors}})$ since one is a quotient and the other a subgroup of $\widehat{\mathcal{R}_p(A^t/K)}$. This proves the proposition. □

4. Proofs of Theorems A and B

We will now prove Theorem A:

Proof of Theorem A. We will break up the proof into three parts:
(A) Proof that $\ker s_{K'}$ and $\operatorname{coker} s_{K'}$ are finite for any $K' \in \mathcal{E}$:

From the sequence (4), to prove that $\ker s_{K'}$ and $\operatorname{coker} s_{K'}$ are finite, we only need to show that $\ker h_{K'}$, $\operatorname{coker} h_{K'}$ and $\ker g'_{K'}$ are finite and as $\ker g'_{K'}$ is contained in $\ker g_{K'}$ it suffices to show that $\ker g_{K'}$ is finite.

First note that for any $K' \in \mathcal{E}$ the standard inflation-restriction sequence gives the following exact sequence:

$$0 \longrightarrow H^1(\Sigma_{K'}, A(K_\infty)[p^\infty]) \longrightarrow H^1(G_T(K'), A[p^\infty]) \xrightarrow{h_{K'}} H^1(G_T(K_\infty), A[p^\infty])^{\Sigma_{K'}} \tag{7}$$
$$\longrightarrow H^2(\Sigma_{K'}, A(K_\infty)[p^\infty]) \longrightarrow H^2(G_T(K'), A[p^\infty])$$

Hence $\ker h_{K'} = H^1(\Sigma_{K'}, A(K_\infty)[p^\infty])$ and $\operatorname{coker} h_{K'} \subseteq H^2(\Sigma_{K'}, A(K_\infty)[p^\infty])$.

Let's now show that $H^1(\Sigma_{K'}, A(K_\infty)[p^\infty])$ and $H^2(\Sigma_{K'}, A(K_\infty)[p^\infty])$ are finite for any $K' \in \mathcal{E}$: By Theorem 2.5 $A(K_\infty)[p^\infty]$ is finite. Also, as mentioned in section 2, for any $K' \in \mathcal{E}$ we have that $H^1(\Sigma_{K'}, \mathbb{Z}/p\mathbb{Z})$ and $H^2(\Sigma_{K'}, \mathbb{Z}/p\mathbb{Z})$ are both finite. Then the finiteness of $H^1(\Sigma_{K'}, A(K_\infty)[p^\infty])$ and $H^2(\Sigma_{K'}, A(K_\infty)[p^\infty])$ follow by dessivage from the previous two statements and the fact that if G is a pro-p group, then the only simple discrete p-primary G-module is $\mathbb{Z}/p\mathbb{Z}$ (with trivial action). Hence $\ker h_{K'}$ and $\operatorname{coker} h_{K'}$ are finite for any $K' \in \mathcal{E}$.

Now let's deal with $\ker g'_{K'}$. This will be done by studying the map $g_{K'}$. To give a nice description of the kernel and cokernel of $g_{K'}$, it is useful to introduce the following notation: For any $K'' \supseteq K'$ and any prime $v \in T_{K'}$ we define $J_v(K'') = \bigoplus_{w|v} H^1(K''_w, A)[p^\infty]$ and define $J_v(K_\infty) = \varinjlim J_v(K'')$ (direct limit is taken with respect to the restriction maps). Then clearly we have $\bigoplus_{w \in T_{K''}} H^1(K''_w, A)[p^\infty] = \bigoplus_{v \in T_{K'}} J_v(K'')$ and $\varinjlim \bigoplus_{w \in T_{K''}} H^1(K''_w, A)[p^\infty] = \bigoplus_{v \in T_{K'}} J_v(K_\infty)$. Hence we may write $g_{K'} = \underset{v \in T_{K'}}{\oplus} g_{(K',v)}$.

Now for any $v \in T_{K'}$ the kernel and cokernel of $g_{(K',v)}$ are described by the inflation restriction sequence because of the following observation: From Shapiro's Lemma we get an isomorphism:

$$H^i(\Sigma_{K'}, J_v(K_\infty)) \cong H^i(\Sigma_{(K',w)}, H^1(K_{\infty,w}, A)[p^\infty]) \qquad \text{for all } i \geq 0$$

where w is some prime of K_∞ above v and $\Sigma_{(K',w)}$ its decomposition group. So in particular: $J_v(K_\infty)^{\Sigma_{K'}} \cong H^1(K_{\infty,w}, A)[p^\infty]^{\Sigma_{(K',w)}}$

We therefore have an exact sequence:

$$0 \longrightarrow H^1(\Sigma_{(K',w)}, A(K_{\infty,w})) \longrightarrow H^1(K'_v, A)[p^\infty] \xrightarrow{g_{(K',v)}} H^1(K_{\infty,w}, A)[p^\infty]^{\Sigma_{(K',w)}} \tag{8}$$
$$\longrightarrow H^2(\Sigma_{(K',w)}, A(K_{\infty,w}))$$

We should note two things about the above exact sequence: First, $H^1(\Sigma_{(K',w)}, A(K_{\infty_w}))$ and $H^2(\Sigma_{(K',w)}, A(K_{\infty_w}))$ are automatically p-primary since $\Sigma_{(K',w)}$ is pro-p. Secondly, if v is non-archimedean the last arrow is actually surjective. This follows from the fact that $H^2(K'_v, A[p^\infty]) = 0$ (which then implies by Kummer theory that $H^2(K'_v, A)[p^\infty] = 0$) and $H^2(K'_v, A[p^\infty]) = 0$ because by Tate local duality ([23] VII-7.2.6) we have that $H^2(K'_v, A[p^\infty])$ is dual $T_p(A(K'_v))$ and the latter group is zero since the p-primary subgroup of $A(K'_v)$ is finite by Mattuck's Theorem.

Now for any $v \in T_{K'}$, we choose a prime w of K_∞ above v and then let $T'_{K'}$ be the set of these w's (so $\#T_{K'} = \#T'_{K'}$). Since $g_{K'} = \underset{v \in T_{K'}}{\oplus} g_{(K',v)}$, therefore we have: $\ker g_{K'} = \bigoplus_{w \in T'_{K'}} H^1(\Sigma_{(K',w)}, A(K_{\infty,w}))$ and $\operatorname{coker} g_{K'} \subseteq \bigoplus_{w \in T'_{K'}} H^2(\Sigma_{(K',w)}, A(K_{\infty,w}))$ (if p is odd this is actually equality as explained above).

Now let's show that $\ker g_{K'}$ is finite, by showing that $\ker g_{(K',v)}$ is finite for any $v \in T_{K'}$: Let $v \in T_{K'}$ and $w \in T'_{K'}$ lying over v. Let's consider the archimedean and non-archimedean cases separately:
(a) v non-archimedean:
First, let $v \mid \tilde{v}$ for some $\tilde{v} \in R$:

Here we actually have that $H^1(K'_v, A)[p^\infty]$ is finite (and hence $\ker g_{(K',v)}$ is finite). This follows from the two following observations: First, by Tate duality for abelian varieties over local fields ([21] I-3.4): $\widehat{H^1(K'_v, A)} \cong A^t(K'_v)$. Therefore, $(H^1(\widehat{K'_v, A})[p^\infty]) \cong \varprojlim A^t(K'_v)/p^n A^t(K'_v)$. Secondly, by Mattuck's Theorem we have that $A^t(K'_v) = \mathbb{Z}_l^{d[K'_v:\mathbb{Q}_l]} \times D$ where D is a finite group, d is the dimension of A^t and l is the characteristic of the residue field of K'_v. But by our fundamental assumption on R, we have that $l \neq p$, therefore $\varprojlim A^t(K'_v)/p^n A^t(K'_v)$ is just the (finite) p-primary subgroup of $A^t(K'_v)$.
Now let us consider the case of $v \nmid \tilde{v}$ for all $\tilde{v} \in R$:

Let $k_{\infty,w}$ be the residue field of $K_{\infty,w}$. Now $K_{\infty,w}/K'_v$ is unramified, so Proposition 3.4 applies: $H^1(\Sigma_{(K',w)}, A(K_{\infty,w})) = H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w}))$ where to simplify notation we have chosen to let $\Phi_v(k_{\infty,w})$ denote $\Phi_{A_{K'_v}}(k_{\infty,w})$. Now as $\Sigma_{(K',w)}$ is pro-cyclic (since v is unramified in K_∞/K') and $\Phi_v(k_{\infty,w})$ has finite order, by using the expression of cohomology in the pro-cyclic case we see that $H^1(\Sigma_{(K',w)}, A(K_{\infty,w}))$ is of finite order. In fact, we can say more: $\#H^1(\Sigma_{(K',w)}, A(K_{\infty,w})) \leq c_v^{(p)}$ where $c_v^{(p)} = p^{ord_p c_v}$.

To show this we first note that as $\Sigma_{K'}$ is pro-p and therefore so is $\Sigma_{(K',w)}$. So $H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})) = H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})[p^\infty])$. Also, $\Sigma_{(K',w)}$ is pro-cyclic, so $\Sigma_{(K',w)}$ is a finite cyclic p-group or isomorphic to $\mathbb{Z}_p$.

If $\Sigma_{(K',w)}$ is a finite cyclic p-group (and as $\Phi_v(k_{\infty,w})[p^\infty]$ is finite), we have $\#H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})[p^\infty]) = \#H^2(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})[p^\infty])$. But by the expression of cohomology in the finite cyclic case we have that $\#H^2(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})[p^\infty]) \leq c_v^{(p)}$. This shows the result in the case when $\Sigma_{(K',w)}$ is finite cyclic.

If $\Sigma_{(K',w)}$ is isomorphic to $\mathbb{Z}_p$, let γ be a topological generator of $\Sigma_{(K',w)}$. Then (again using that $\Phi_v(k_{\infty,w})[p^\infty]$ is finite), we see that $H^0(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})[p^\infty]) = \ker(\Phi_v(k_{\infty,w})[p^\infty] \xrightarrow{\gamma-1} \Phi_v(k_{\infty,w})[p^\infty])$ has the same order as $H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})[p^\infty]) = \operatorname{coker}(\Phi_v(k_{\infty,w})[p^\infty] \xrightarrow{\gamma-1} \Phi_v(k_{\infty,w})[p^\infty])$. So when $\Sigma_{(K',w)}$ is isomorphic to $\mathbb{Z}_p$, $\#H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})[p^\infty]) = c_v^{(p)}$.

(b) v archimedean: This case only becomes relevant when $p = 2$, $K'_v = \mathbb{R}$ and $K_{\infty,w} = \mathbb{C}$ and in this case Proposition 3.5, shows that $H^1(\Sigma_{(K',w)}, A(K_{\infty,w}))$ is finite.

We have shown that $\ker g_{K'}$ is finite and so therefore $\ker g'_{K'}$ is finite . Combining this with the finiteness of $\ker h_{K'}$ and $\operatorname{coker} h_{K'}$ (shown above) and sequence (4), we see that $\ker s_{K'}$ and $\operatorname{coker} s_{K'}$ are indeed finite for any $K' \in \mathcal{E}$.

(B) Proof of part (i):

(B1) Statement about $\ker s_{K'}$:

Now let's prove part (i) of the Theorem A. Suppose $A(K)[p] = 0$. Then Lemma 3.1 shows that $A(K_\infty)[p^\infty] = 0$. Therefore since as shown above $\ker h_{K'} = H^1(\Sigma_{K'}, A(K_\infty)[p^\infty])$, we have that $\ker h_{K'} = 0$ for all $K' \in \mathcal{E}$ and so by sequence (4), we have that $\ker s_{K'} = 0$ for all $K' \in \mathcal{E}$.

(B2) Statement about $\operatorname{coker} s_{K'}$:

Now assume condition (C) is satisfied. Then by sequence (4), to show that $\operatorname{coker} s_{K'} = 0$ for all n, it suffices to show that $\ker g'_{K'} = 0$ and $\operatorname{coker} h_{K'} = 0$ for all $K' \in \mathcal{E}$. Since (as shown from the sequence (7)) $\operatorname{coker} h_{K'} \subseteq H^2(\Sigma_{K'}, A(K_\infty)[p^\infty])$, and as $A(K_\infty)[p^\infty] = 0$ (as in (B1)), we must have that $\operatorname{coker} h_{K'} = 0$. So it remains to show that $\ker g'_{K'}$ vanishes for any $K' \in \mathcal{E}$ and we will show this by showing that $\ker g_{K'}$ vanishes and as $g_{K'} = \bigoplus_{v \in T_{K'}} g_{(K',v)}$, we will show that $\ker g_{(K',v)} = 0$ for all $v \in T_{K'}$.

First if v is archimedean, we only have to consider the case when $K'_v = \mathbb{R}$ and $K_{\infty,w} = \mathbb{C}$ (and hence also $p = 2$). In this case, condition (C-ii) makes $\ker g_{(K',v)} = 0$ according to Proposition 3.5 (and the description of $\ker g_{(K',v)}$ as above).

Next, let us consider the case of non-archimedean v:

First, if $v \mid \tilde{v}$ for some $\tilde{v} \in R$:

In this case, by Mattuck's Theorem we have that $A(K'_v) = \mathbb{Z}_l^{d[K'_v:\mathbb{Q}_l]} \times D$

where D is a finite group, d is the dimension of A and l is the characteristic of the residue field of K'_v. By our fundamental assumption on R, we have that $l \neq p$, so $A(K'_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$. Similarly, we deduce the same result for any $K'' \supseteq K'$ and any v'' lying over v, so by taking the direct limit we also see that $A(K_{\infty,w}) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ for any prime w of K_∞ above v. Therefore, by Kummer theory, we get that $H^1(K'_v, A)[p^\infty] = H^1(K'_v, A[p^\infty])$ and $H^1(K_{\infty,w}, A)[p^\infty] = H^1(K_{\infty,w}, A[p^\infty])$, so we see that in this case (from the inflation-restriction sequence and sequence (8)), that $\ker g_{(K',v)} = H^1(\Sigma_{(K',w)}, A(K_{\infty,w})[p^\infty])$.

If v lies above some prime in the set S, then $\Sigma_{(K',w)} = \{0\}$ and hence $\ker g_{(K',v)} = 0$. Therefore, we can ignore these primes. Otherwise v does not lie above a prime in S. In this case condition (C-iii) together with Lemma 3.1 give that $A(K_{\infty,w})[p^\infty] = 0$, so we conclude that $\ker g_{(K',v)} = 0$.
Now consider the case of $v \nmid \tilde{v}$ for all $\tilde{v} \in R$:

As shown above in the proof of part (A) we have that $\ker g_{(K',v)} = H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w}))$ where w is some prime of K_∞ lying above v. Hence we must show that $H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})) = 0$. But as we noted above $\#H^1(\Sigma_{(K',w)}, \Phi_v(k_{\infty,w})) \leq c_v^{(p)}$. So it suffices to show that $c_v^{(p)} = 1$. Recall that $c_v^{(p)} = \#\Phi_v(k'_v)[p^\infty]$ where k'_v is the residue field of K'_v.

In regards to this let us note the following basic observation: Let $\tilde{v} \in T$ be the prime lying below v, then $\Phi_{\tilde{v}} \times_{k_{\tilde{v}}} k'_v = \Phi_v$. This follows from two facts. First, if $\mathcal{A}$ is the Néron model of $A_{K_{\tilde{v}}}$, then $\mathcal{A} \times_{R_{\tilde{v}}} R'_v$ is the Néron model of $A_{K'_v}$ (here $R_{\tilde{v}}$ and R'_v are the rings of integers of $K_{\tilde{v}}$ and K'_v respectively). This is because $K'_v/K_{\tilde{v}}$ is unramified and Néron models are stable under étale base change (see [1] 1.2 prop 2). Secondly, if V is an algebraic group over a field F and L/F is a field extension, then $\pi_0(V_L) = \pi_0(V) \times_F L$ (see [16] ch. 10 prop. 2.18) where $\pi_0(V_L)$ and $\pi_0(V)$ are the group of components of V_L and V. In our case the algebraic group is the special fiber of the Néron model.

We have that $\Phi_{\tilde{v}} \times_{k_{\tilde{v}}} k'_v = \Phi_v$, therefore $c_v^{(p)} = \#\Phi_{\tilde{v}}(k'_v)[p^\infty]$. Then to show that $c_v^{(p)} = 1$, it suffices by Lemma 3.1 to show that $c_{\tilde{v}}^{(p)} = \#\Phi_{\tilde{v}}(k_{\tilde{v}})[p^\infty] = 1$, because $k'_v/k_{\tilde{v}}$ is pro-p. If A has good reduction at $\tilde{v}$, then $c_{\tilde{v}} = 1$, so we only have to check that $c_{\tilde{v}}^{(p)} = 1$ for $\tilde{v} \in B$. If $\tilde{v} \in S$, then $\Sigma_{(K',w)} = \{0\}$ and hence $\ker g_{(K',v)} = 0$ (recall this is what we are trying to show). So we can ignore the primes $\tilde{v} \in S$. If $\tilde{v} \in (B \cap R_p) \setminus (R \cup S)$, then condition (C-i) gives that $c_{\tilde{v}}^{(p)} = 1$, so $\ker g_{(K',v)} = 0$. If $\tilde{v} \in B \setminus (R \cup R_p \cup S)$, then then condition (C-i) gives that $c_{\tilde{v}}^{(p)} = 1$ or that $A(K_{\tilde{v}})[p^\infty] = \{0\}$, so $\ker g_{(K',v)} = 0$ either by what we just mentioned about $c_{\tilde{v}}^{(p)}$ or (by Kummer theory) as in the proof when $\tilde{v} \in R$.

Combining the above we have that $\ker g_{K'} = 0$, which as we discussed gives that $\operatorname{coker} s_{K'} = 0$. This completes the proof of part (i) of Theorem A.

(C) Proof of part (ii):

Choose $K = K_0 \subset K_1 ... \subset K_n \subset ...$ to be a tower of fields each Galois over K and with $K_\infty = \cup_{i=0}^{\infty} K_i$. To prove the statement in part (ii) about the unboundedness of $r_p(\ker s_{K'})$ and $r_p(\operatorname{coker} s_{K'})$ (under the required conditions) as K' varies over the set $\mathcal{E}$, it suffices to prove that $r_p(\ker s_{K_n})$ and $r_p(\operatorname{coker} s_{K_n})$ are unbounded with n (under the same conditions).

To simplify notation, for any n, we will let Σ_n denote Σ_{K_n}, $\Sigma_{n,w}$ denote $\Sigma_{(K_n,w)}$ and will denote s_{K_n}, g_{K_n}, g'_{K_n} and h_{K_n} by s_n, g_n, g'_n and h_n respectively. Moreover, we will denote T_{K_n} by T_n and for any prime of v of K_n we will denote $g_{(K_n,v)}$ and $g'_{(K_n,v)}$ by $g_{n,v}$ and $g'_{n,v}$ respectively.

(C1) Statement about $\ker s_{K'}$:

Suppose that $A(K)[p] \neq 0$. Assume condition (C) is satisfied and Σ is not p-adic analytic, we will show that $r_p(\ker s_n)$ is unbounded as n varies. To show this, by sequence (4), it suffices to show that $r_p(\ker h_n)$ is unbounded as n varies and that $r_p(\ker g'_n)$ is bounded as n varies (and the latter can be shown if we show that $r_p(\ker g_n)$ is bounded as n varies).

First, let's show that $r_p(\ker h_n)$ is unbounded with n: Since $A(K_\infty)[p^\infty]$ is finite by Theorem 2.5, and $K_\infty = \cup_{i=0}^{\infty} K_i$, there exists an N such that $A(K_\infty)[p^\infty]$ is rational over K_N. Then for any $n \geq N$ we have Σ_n acts trivially on $A(K_\infty)[p^\infty]$. Now as $A(K)[p] \neq 0$, therefore $A(K_\infty)[p^\infty]$ contains a subgroup of order p and as Σ_n acts trivially on $A(K_\infty)[p^\infty]$, this subgroup will be isomorphic to $\mathbb{Z}/p\mathbb{Z}$ as a Σ_n-module.

Also, for any profinite group G and any abelian group B on which G acts trivially, we have that $H^1(G, B) = \operatorname{Hom}_{\text{cont}}(G, B)$. Therefore we have for any $n \geq N$ that $H^1(\Sigma_n, \mathbb{Z}/p\mathbb{Z})$ is a subgroup of $H^1(\Sigma_n, A(K_\infty)[p^\infty])$. Now as we assumed that Σ is not p-adic analytic, therefore by Theorem 2.4 we have that $r_p(H^1(\Sigma_k, \mathbb{Z}/p\mathbb{Z}))$ is unbounded as k varies and as $H^1(\Sigma_n, \mathbb{Z}/p\mathbb{Z})$ is a subgroup of $H^1(\Sigma_n, A(K_\infty)[p^\infty])$ for $n \geq N$, this shows that $r_p(H^1(\Sigma_k, A(K_\infty)[p^\infty]))$ is unbounded as k varies. But as we showed in the beginning of the proof of Theorem A, we have that $\ker h_k = H^1(\Sigma_k, A(K_\infty)[p^\infty])$, so $r_p(\ker h_k)$ is unbounded with k.

Now regarding the fact that $r_p(\ker g_n)$ is bounded with n, we in fact have that $\ker g_n = 0$ because condition (C) is satisfied (we showed this when proving part (i) above).

(C2) Statement about $\operatorname{coker} s_{K'}$:

Now assume that $\operatorname{rank}(A(K'))$ is bounded as n varies, $Ш(A/K')[p^\infty]$ is finite for any $K' \in \mathcal{E}$ and K is totally imaginary if $p = 2$. Note that the last statement forces K' to be totally imaginary if $p = 2$ for any $K' \in \mathcal{E}$. We will now show that $r_p(\operatorname{coker} s_n)$ is unbounded as n varies. By sequence (4), to show this it suffices to show that $r_p(\operatorname{coker} h_n)$ is unbounded with n and that $r_p(\operatorname{coker} g'_n)$ is bounded with n.

First, let's show that $r_p(\operatorname{coker} h_n)$ is unbounded with n: The same argument above (in part C1) gives that $A(K_\infty)[p^\infty]$ is finite (Theorem 2.5) and that there exists a N such that Σ_n acts trivially on $A(K_\infty)[p^\infty]$ for all

$n \geq N$. Now as $A(K)[p] \neq 0$, $A(K_\infty)[p^\infty]$ is a non-trivial finite abelian p-group. Then $A(K_\infty)[p^\infty]$ has a direct summand isomorphic as an abelian group to $\mathbb{Z}/p^m\mathbb{Z}$ for some $m \geq 1$. Moreover since for all $n \geq N$ we have that Σ_n acts trivially on $A(K_\infty)[p^\infty]$, then for such an n this direct summand is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$ as a Σ_n-module. Now as a cohomology commutes with direct sums we have that $H^2(\Sigma_n, \mathbb{Z}/p^m\mathbb{Z})$ is a subgroup of $H^2(\Sigma_n, A(K_\infty)[p^\infty])$ for all $n \geq N$.

By the exact sequence (7), to show that $r_p(\operatorname{coker} h_n)$ is unbounded with n, it suffices to show that $r_p(H^2(\Sigma_n, A(K_\infty)[p^\infty]))$ is unbounded with n and that $r_p(H^2(G_T(K_n), A[p^\infty]))$ is bounded with n. To show that $r_p(H^2(\Sigma_n, A(K_\infty)[p^\infty]))$ is unbounded, then it is enough to show that $r_p(H^2(\Sigma_n, \mathbb{Z}/p^m\mathbb{Z}))$ is unbounded for all $n \geq N$ (as the latter group is a subgroup of the former).

Now by Lemma 3.2 we have that for any n:

$$r_p(H^2(\Sigma_n, \mathbb{Z}/p^m\mathbb{Z})) \geq r_p(H^1(\Sigma_n, \mathbb{Z}/p^m\mathbb{Z}))$$

and since we may consider $H^1(\Sigma_n, \mathbb{Z}/p\mathbb{Z})$ as a subgroup of $H^1(\Sigma_n, \mathbb{Z}/p^m\mathbb{Z})$ for any m (by a similar argument to the one we used when showing that $r_p(\ker h_n)$ is unbounded), therefore

$$r_p(H^2(\Sigma_n, \mathbb{Z}/p^m\mathbb{Z})) \geq r_p(H^1(\Sigma_n, \mathbb{Z}/p\mathbb{Z}))$$

for all n. Hence to show that $r_p(H^2(\Sigma_k, A(K_\infty)[p^\infty]))$ is unbounded with k, it is now enough to show that $r_p(H^1(\Sigma_k, \mathbb{Z}/p\mathbb{Z}))$ is unbounded with k, but this follows Theorem 2.4 because we assumed that Σ is not p-adic analytic.

Now let's show that $r_p(H^2(G_T(K_n), A[p^\infty]))$ is bounded with n. This is an easy application of Proposition 3.7: If $\operatorname{rank}(A(K_n)) \leq M$ for all n, then since we assumed that $Ш(A/K_n)[p^\infty]$ is finite for n and assumed K (and hence K_n) to be totally imaginary if $p = 2$, Proposition 3.7 shows that for any n we have that:

$$r_p(H^2(G_T(K_n), A[p^\infty])) \leq M + r_p(A^t(K_n)_{\text{tors}}) \leq M + 2d$$

where d is the dimension of A (=the dimension of A^t). Hence $r_p(H^2(G_T(K_n), A[p^\infty]))$ is indeed bounded with n. This shows that $r_p(\operatorname{coker} h_n)$ is unbounded with n.

Now let's show that $r_p(\operatorname{coker} g'_n)$ is bounded. To prove this let's consider the following commutative diagram with exact rows:

(9)

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{img} \psi_{K_\infty} & \longrightarrow & (\varinjlim \bigoplus_{w \in T_m} H^1(K_{m,w}, A)[p^\infty])^{\Sigma_{K'}} & \longrightarrow & \operatorname{coker} \psi_{K_\infty} & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle g'_n} & & \uparrow{\scriptstyle g_n} & & \uparrow{\scriptstyle g''_n} & & \\
0 & \longrightarrow & \operatorname{img} \lambda_{K_n} & \longrightarrow & \bigoplus_{v \in T_n} H^1(K_{n,v}, A)[p^\infty] & \longrightarrow & \operatorname{coker} \lambda_{K_n} & \longrightarrow & 0
\end{array}$$

From the above commutative diagram and the ker-coker sequence, to show that $r_p(\operatorname{coker} g_n')$ is bounded with n, it suffices to show that $r_p(\ker g_n'')$ and $r_p(\operatorname{coker} g_n)$ are both bounded with n.

Let's first show that $r_p(\operatorname{coker} g_n)$ is bounded with n. It will be sufficient for us to show that $\operatorname{coker} g_n = 0$ for $n \gg 0$ (it will be true that $\operatorname{coker} g_n$ is finite for all n, but we won't need this). Recall that for any n we have $g_n = \underset{v \in T_n}{\oplus} g_{n,v}$. For every $\tilde{v} \in T$ we will show that $\operatorname{coker} g_{n,v} = 0$ for $n \gg 0$ and any $v \mid \tilde{v}$.

Now let $\tilde{v} \in T$: If $\tilde{v}$ is archimedean, it is clear that $\operatorname{coker} g_{n,v} = 0$ for any n and any $v \mid \tilde{v}$ so we don't have to worry about archimedean primes. Now suppose that $\tilde{v}$ is non-archimedean. We will consider two cases:
(a) $\tilde{v} \in R$:

First note that as in the proof of part (i) of Theorem A, for any n and any $v \mid \tilde{v}$, by Kummer theory (see also the remark after sequence (8) we have $g_{n,v}$ is the restriction map: $H^1(K_{n,v}, A[p^\infty]) \longrightarrow H^1(K_{\infty,w}, A[p^\infty])$ and $\operatorname{coker} g_{n,v} = H^2(\Sigma_{n,w}, A(K_{\infty,w})[p^\infty])$. Now by our assumption on R, we have that v does not lie above p. Also, $K_{\infty,w}/K_{\tilde{v}}$ is a pro-p extension for any w lying over $\tilde{v}$. So $K_{\infty,w}$ is contained in $K_{\tilde{v}}^{tr,p}$; the maximal pro-p tamely ramified extension of $K_{\tilde{v}}$. If $K_{\tilde{v}}^{nr,p}$ is the maximal unramified pro-p extension of $K_{\tilde{v}}$ we have $\operatorname{Gal}(K_{\tilde{v}}^{tr,p}/K_{\tilde{v}}^{nr,p}) \cong \mathbb{Z}_p$ (see [22] Corollary 9.15). Therefore $\operatorname{Gal}(K_{\tilde{v}}^{tr,p}/K_{\tilde{v}}) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p$, a pro-$p$ p-adic Lie group of dimension 2. We conclude that $\Sigma_w = \operatorname{Gal}(K_{\infty,w}/K_{\tilde{v}})$ is a pro-p p-adic Lie group of dimension ≤ 2 (note that the dimension of this group is of course independent of the prime w above $\tilde{v}$). We have three cases:
(a-1) Σ_w is finite (i.e. has dimension 0): Since $K_{\infty,w}$ is the union of the w-adic completions of the K_n's and $K_{\infty,w}/K_{\tilde{v}}$ is finite, it is easy to conclude for large enough n that $\Sigma_{n,w}$ will be trivial so $\operatorname{coker} g_{n,v} = 0$ for $n \gg 0$ and $v \mid \tilde{v}$.
(a-2) Σ_w has dimension 1: In this case Σ_w has an open normal subgroup isomorphic to $\mathbb{Z}_p$ (see [7] for this and other basic facts about p-adic Lie groups). From this it is easy to conclude that for large enough n, $\Sigma_{n,w}$ will always be isomorphic to $\mathbb{Z}_p$ and so for $n \gg 0$ and $v \mid \tilde{v}$ we have $\operatorname{coker} g_{n,v} = 0$ because $\mathbb{Z}_p$ has cohomological dimension 1.
(a-3) Σ_w has dimension 2: In this case we must have $K_{\infty,w} = K_{\tilde{v}}^{tr,p}$, so the absolute Galois group of $K_{\infty,w}$ has profinite order relatively prime to p. Therefore, $H^1(K_{\infty,w}, A[p^\infty]) = 0$ and so $\operatorname{coker} g_{n,v} = 0$ for any n and $v \mid \tilde{v}$.
(b) $\tilde{v} \notin R$:

Recall that for any n and any $v \mid \tilde{v}$, we have $\operatorname{coker} g_{n,v} = H^2(\Sigma_{n,w}, A(K_{\infty,w}))$. Also, by basically the same arguments when we used when we considered $\ker g_{n,v}$, we have that $H^2(\Sigma_{n,w}, A(K_{\infty,w})) = H^2(\Sigma_{n,w}, \Phi_v(k_{\infty,w}))$ (using Proposition 3.4 with $i = 2$). Now as discussed before Σ_w is either a finite cyclic p-group or isomorphic to $\mathbb{Z}_p$. If Σ_w is finite, then $\Sigma_{n,w}$ will be trivial for sufficiently large n and so $\operatorname{coker} g_{n,v}$ will also be trivial. If $\Sigma_w \cong \mathbb{Z}_p$, then $\Sigma_{n,w}$ will also be isomorphic to $\mathbb{Z}_p$ for any n

and therefore $\operatorname{coker} g_{n,v} = 0$ because $\mathbb{Z}_p$ has cohomological dimension 1 and $\Phi_v(k_{\infty,w})$ is a finite group.

We have therefore shown that $\operatorname{coker} g_n = 0$ for $n \gg 0$. As for $r_p(\ker g_n'')$, if we have that $\operatorname{rank}(A(K')) \leq M$, then by Proposition 3.7, we get that $r_p(\operatorname{coker} \lambda_K) \leq M + 2d$ where d is the dimension of A. So $r_p(\ker g_n'')$ is bounded since $\ker g_n''$ is contained $\operatorname{coker} \lambda_K$.

We have now shown that $r_p(\operatorname{coker} g_n')$ is bounded with n, thus finally completing the proof that $r_p(\operatorname{coker} s_{K'})$ is unbounded (under the required assumptions). □

Proof of Corollary A. For any $K' \in \mathcal{E}$ consider the maps:

$$s_{K'} : \operatorname{Sel}_p(A/K') \longrightarrow \operatorname{Sel}_p(A/K_\infty)^{\operatorname{Gal}(K_\infty/K')}$$

$$s'_{K'} : \operatorname{Sel}_p(A'/K') \longrightarrow \operatorname{Sel}_p(A'/K_\infty)^{\operatorname{Gal}(K_\infty/K')}$$

Under the assumptions of the corollary, we get by Theorem A that $s'_{K'}$ is an isomorphism for all $K' \in \mathcal{E}$. In particular as s'_K is surjective and $\operatorname{Sel}_p(A'/K) = 0$, we get that $\operatorname{Sel}_p(A'/K_\infty)^{\operatorname{Gal}(K_\infty/K)} = 0$ and hence by Lemma 3.1, we get that $\operatorname{Sel}_p(A'/K_\infty) = 0$ which implies that $Ш(A'/K_\infty)[p^\infty] = 0$.

Now as $s'_{K'}$ is injective for all $K' \in \mathcal{E}$ and $\operatorname{Sel}_p(A'/K_\infty) = 0$, we get that $\operatorname{Sel}_p(A'/K') = 0$ for any $K' \in \mathcal{E}$. Therefore as A and A' are isogenous over K (and hence over K'), we have that by Lemma 3.6, that $\operatorname{Sel}_p(A/K')$ is finite for all $K' \in \mathcal{E}$. So $\operatorname{rank}(A(K'))$ is bounded (by zero) for all $K' \in \mathcal{E}$ and $Ш(A/K')[p^\infty]$ is finite for all $K' \in \mathcal{E}$. Therefore by Theorem A, we get that $r_p(\operatorname{coker} s_{K'})$ is unbounded as K' varies over the set $\mathcal{E}$ and hence as $\operatorname{coker} s_{K'}$ is a quotient of $\operatorname{Sel}_p(A/K_\infty)^{\operatorname{Gal}(K_\infty/K')}$, we conclude that $r_p(\operatorname{Sel}_p(A/K_\infty))$ is infinite.

But now because $\operatorname{Sel}_p(A/K')$ is finite for all $K' \in \mathcal{E}$, we must have the $A(K') \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ for all $K' \in \mathcal{E}$. Therefore $A(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p = \varinjlim A(K') \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$ and so by the exact sequence:

$$0 \longrightarrow A(K_\infty) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \operatorname{Sel}_p(A/K_\infty) \longrightarrow Ш(A/K_\infty)[p^\infty] \longrightarrow 0$$

we get that $\operatorname{Sel}_p(A/K_\infty) \cong Ш(A/K_\infty)[p^\infty]$ so $r_p(Ш(A/K_\infty)[p^\infty])$ is infinite i.e. $Ш(A/K_\infty)[p^\infty]$ contains an infinite elementary abelian p-group.

If the isogeny between A and A' is of degree p, then as in Lemma 3.6, we have maps $\bar{f} : Ш(A/K)[p^\infty] \to Ш(A'/K)[p^\infty]$ and $\bar{g} : Ш(A'/K)[p^\infty] \to Ш(A/K)[p^\infty]$ whose composites are multiplication by p, but as $Ш(A'/K_\infty)[p^\infty] = 0$, we therefore get that p annihilates $Ш(A/K_\infty)[p^\infty]$ and so $Ш(A/K_\infty)[p^\infty] = Ш(A/K_\infty)[p]$. So in this case $Ш(A/K_\infty)[p^\infty]$ is itself an infinite elementary abelian p-group. □

Proof of Theorem B. Choose $K = K_0 \subset K_1 ... \subset K_n \subset ...$ to be a tower of fields each Galois over K and with $K_\infty = \cup_{i=0}^{\infty} K_i$. We will prove that $r_p(Ш(A/K_n))$ is unbounded with n. Let us denote T_{K_n} by T_n and Σ_{K_n} by

Σ_n. Also for any n, let K'_n be the fixed field of the commutator subgroup of Σ_n. Now consider the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Sel}_p(A/K_n) & \longrightarrow & H^1(G_T(K_n), A[p^\infty]) & \longrightarrow & \prod_{v\in T_n} H^1(K_{n,v}, A)[p^\infty] \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & W_n & \longrightarrow & H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty]) & \longrightarrow & \prod_{v\in T_n} H^1(\Delta_v, A(K'_n))[p^\infty] \end{array}$$

In the above diagram W_n is just the kernel of the lower map, the left two vertical maps are inflation maps and Δ_v (for $v \in T_n$) is the decomposition group in Σ_n^{ab} of a prime of K'_n above v chosen to make the diagram commute (note that the top right map is induced by inflation followed by restrictions to decomposition groups at chosen primes of $\overline{\mathbb{Q}}$ above each $v \in T_n$).

Since condition (C) is satisfied, then by a similar argument to the one used in the proof of Theorem A (part B2) we see that $H^1(\Delta_v, A(K'_n))[p^\infty]$ is trivial for any $v \in T_n$. Therefore the bottom right hand map is trivial. So $H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty])$ coincides with the kernel W_n proving that the image of the inflation map $H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty]) \hookrightarrow H^1(G_T(K_n), A[p^\infty])$ is contained in $\mathrm{Sel}_p(A/K_n)$.

Now consider the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Sel}_p(A/K_n) & \longrightarrow & Ш(A/K_n) \\ \downarrow & & \downarrow \\ H^1(G_T(K_n), A[p^\infty]) & \longrightarrow & H^1(K_n, A) \\ \uparrow & & \uparrow \\ H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty]) & \longrightarrow & H^1(\Sigma_n^{ab}, A(K'_n)) \end{array}$$

In this diagram, the top two vertical maps are just natural inclusion and the lower two vertical maps are inflation. Now as Σ_n^{ab} is finite, we have that $K'_n/\mathbb{Q}$ is a finite extension and so by the Mordell-Weil Theorem $A(K'_n)$ is finitely generated. Therefore, $A(K'_n)[p^\infty]$ is a direct summand of $A(K'_n)$. This implies that the lower horizontal map in the diagram is an injection. From this, the commutativity of the diagram and the fact that the image of the lower left hand vertical arrow is contained in $\mathrm{Sel}_p(A/K_n)$ (which we deduced above), we see that $H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty])$ injects (via the appropriate map) into $Ш(A/K_n)$. So to show that $r_p(Ш(A/K_n))$ is unbounded with n it suffices to show that $r_p(H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty]))$ is unbounded with n.

To show that $r_p(H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty]))$ is unbounded with n, we first note that by Theorem 2.5 we have that $A(K_\infty)[p^\infty]$ is finite. Therefore there exists an N such that $A(K_\infty)[p^\infty]$ is rational over K_N. So for any $n \geq N$ we have that Σ_n^{ab} acts trivially on $A(K'_n)[p^\infty]$ and so $H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty]) = \mathrm{Hom}(\Sigma_n^{ab}, A(K'_n)[p^\infty])$. Moreover, as we assumed that $A(K)[p] \neq \{0\}$, therefore $A(K'_n)[p^\infty] = A(K_\infty)[p^\infty]$ is a non-trivial finite abelian p-group.

From these facts we see for any $n \geq N$ that we have:

$$r_p(H^1(\Sigma_n^{ab}, A(K'_n)[p^\infty])) = r_p(\mathrm{Hom}(\Sigma_n^{ab}, A(K'_n)[p^\infty])) \geq r_p(\Sigma_n^{ab})$$

Therefore, to prove the theorem we only have to show that $r_p(\Sigma_n^{ab})$ is unbounded with n. But as Σ was assumed not to be p-adic analytic, this follows from Theorem 2.4 since $h_1(\Sigma_n) = h_1(\Sigma_n^{ab}) = r_p(\Sigma_n^{ab})$. □

Remark. It would be interesting to strengthen Theorem B to show that $r_p(Ш(A/K'))$ is bounded below by a linear function in $[K' : K]$ i.e. a bound of the form $c[K' : K] + d$ where c and d are constants with c positive. If such a lower bound exists, then using the method of proof of Theorem B one should show that $h_1(\Sigma_{K'}) \geq c[K' : K] + d$. Also, the method of proof of Theorem B suggests that if such a lower bound exists, then it would only be valid for all K' such that $K' \supseteq K(A(K_\infty)[p^\infty])$.

If G is not a p-adic analytic group, and H is a closed subgroup of G, then a lower bound on $h_1(H)$ of the form $c[G : H] + d$ is known for free pro-p groups (see [23] Corollary 3.9.6). However, this does not apply to the groups we are considering here, since for any number field K, Σ_K has finite abelianization and hence is not free pro-p. As to how $h_1(H)$ changes as $[G : H]$ grows is unknown in general for non-p-adic analytic groups. For a discussion on this see section 3 of Hajir's article [14].

Despite this fact that we do not know in general how $h_1(H)$ changes as $[G : H]$ grows, Hajir *loc. cit.* has shown for any positive c how to construct number fields K with an infinite p-class field tower such that if K_n is the n-th p-class field, then $h_1(K_n) \geq c[K_n : K] + 1$.

Let us give an example with $p = 2$ and $c = 1$ using Hajir's method: the field $K = \mathbb{Q}(\sqrt{5 \cdot 13 \cdot 29 \cdot 37 \cdot 41 \cdot 53 \cdot 73 \cdot 89}, \sqrt{-3})$ has an infinite 2-class field tower with $h_1(K_n) \geq [K_n : K] + 1$ for all n (this is a slight modification of the example at the end of Hajir's paper).

Now consider the elliptic curve $A : y^2 + xy + y = x^3 - x^2 - x$ of conductor 17. This is the curve 17A4 in Cremona's tables [6]. For this elliptic curve, we have that $c_p = 1$ for all primes p. As $[K : \mathbb{Q}] = 4$, this implies by Lemma 3.1 that $(c_v, 2) = 1$ for all primes v of K. Therefore, condition (C) is satisfied (with $p = 2$ and $R = S = \varnothing$) for the field K and the elliptic curve A. We also have that $A(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$. So by the discussion above we have that $r_2(Ш(A/K_n)) \geq [K_n : K] + 1$ for all $K_n \supseteq K(A(K_\infty)[2^\infty])$.

However, one can show that $A(K_\infty)[2^\infty] = A(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$. To show this, assume the contrary i.e. that $F/\mathbb{Q}$ where $F = \mathbb{Q}(A(K_\infty)[2^\infty])$ is a non-trivial extension. Then some rational prime ramifies in $F/\mathbb{Q}$ (there are no non-trivial extensions of $\mathbb{Q}$ with discriminant 1). Since A has bad reduction only at the prime 17, it follows from the Criterion of Néron-Ogg-Shafarevich that the only primes that can ramify in $F/\mathbb{Q}$ are the primes 2 and 17. But ramification at these primes cannot occur in $K_\infty/\mathbb{Q}$ since the discriminant of K is prime to both 2 and 17 and K_∞/K is unramified at all primes. This shows that $A(K_\infty)[2^\infty] = A(\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$. From this it follows that: $r_2(Ш(A/K_n)) \geq [K_n : K] + 1$ for all n.

5. Further Considerations

The purpose of this section is to discuss what can be said regarding the control theorem (Theorem A) if we let the set R there contain all the primes of K above p. When $R_p \subseteq R$, many of the arguments used in the proof of Theorem A fail. For example, it is possible for $A(K_\infty)[p^\infty]$ to be infinite in this case. For if the set R contains $R_p \cup B \cup R_\infty$, $S = \varnothing$ and $A[p]$ is rational over K, then $K(A[p^\infty])$ is contained in K_∞ (the fact that $A[p]$ is rational over K ensures that $K(A[p^\infty])/K$ is pro-p). Note that in this case it is easy to prove that $\mathrm{Sel}_p(A/K_\infty)$ is trivial (see the discussion regarding $\ker s_{K'}$ for an argument) and hence there is nothing to say in regards to a control theorem.

In fact we will show that if $R_p \subseteq R$ and, as in Mazur's Control Theorem, A has good ordinary reduction at all primes of K dividing p, then the control theorem can fail in the sense that $\ker s_{K'}$ can be infinite and $\operatorname{coker} s_{K'}$ can be infinite of unbounded $\mathbb{Z}_p$-corank as K' varies over $\mathcal{E}$ (see the discussion after Prop 2.5 of [10] regarding what can happen in the supersingular case).

We will assume throughout this section, unless explicitly stated, that *the set S is empty* and let $K_\infty = K^{(p)}_{R,\varnothing}$ where R is a finite set of primes of K containing R_p.

$\ker s_{K'}$ *can be infinite*: This is easy. Suppose $A[p]$ is rational over K and $R = R_p \cup B \cup R_\infty$, then it is not hard to show that $\mathrm{Sel}_p(A/K_\infty)$ is trivial. This is because by a direct limit argument as in diagram (2) we have that $\mathrm{Sel}_p(A/K_\infty)$ is contained $H^1(G_R(K_\infty), A[p^\infty])$ where as before we have $G_R(K_\infty) = \mathrm{Gal}(K_R/K_\infty)$ with K_R the maximal extension of K unramified outside of R. Since $A[p]$ is rational over K, then $K(A[p^\infty])/K$ is pro-p and hence $K(A[p^\infty])$ is contained in K_∞. So $G_R(K_\infty)$ acts trivially on $A[p^\infty]$, we have that

$$H^1(G_R(K_\infty), A[p^\infty]) = \mathrm{Hom}_{\mathrm{cont}}(G_R(K_\infty), A[p^\infty])$$

and this is zero since $A[p^\infty]$ is p-primary and $G_R(K_\infty)$ has no non-trivial pro-p quotient. Therefore, $\mathrm{Sel}_p(A/K_\infty)$ is trivial and so $\ker s_{K'} = \mathrm{Sel}_p(A/K')$ can be infinite if $\mathrm{rank}(A(K'))$ is positive. Note that it is still possible for $\ker s_{K'}$ to be infinite even if the set B is not contained in R. This can be achieved by $A = A_1 \times_K A_2$ be the product of two abelian varieties A_1 and A_2 defined over K having bad reduction at primes in the sets B_1 and B_2 respectively with B_1 not contained in B_2. One then lets R be the set $R_p \cup B_2 \cup R_\infty$. If $A_2[p]$ is rational over K, then $\ker s_{K'}$ contains a copy of $\mathrm{Sel}_p(A_2/K')$ and so can be infinite if $\mathrm{rank}(A_2(K'))$ is positive.

$\operatorname{coker} s_{K'}$ *can be infinite of unbounded $\mathbb{Z}_p$-corank*: This is a more interesting situation than $\ker s_{K'}$. As we mentioned earlier, we will show this when A (as in Mazur's Control Theorem) has good ordinary reduction at

all primes of K above p. Before proving the main result here, we will make a few observations.

Assume that A has good ordinary reduction at all primes of K above p and R_p is contained in R. Then if w is a prime of K_∞ above p, $K_{\infty,w}$ will be deeply ramified in the sense of [4] (this is because K^{cyc}, the cyclotomic $\mathbb{Z}_p$-extension of K, is contained in K_∞). From this we have an exact sequence (see *loc. cit.* and [9])

$$0 \to \tilde{A}_v(k'_v)[p^\infty] \to \ker g_{(K',v)} \to H^1(\Sigma_{(K',w)}, \tilde{A}_v(k_{\infty,w})[p^\infty]) \to 0 \tag{10}$$

where in the above $\tilde{A}_v$ is the reduction modulo v of the Néron model of A over the ring of integers of K'_v, and k'_v and $k_{\infty,w}$ are the residue fields of K'_v and $K_{\infty,w}$ respectively.

Now to show that $\operatorname{coker} s_{K'}$ is infinite, it will be important to show that $\ker g_{(K',v)}$ is infinite. As $\tilde{A}_v(k'_v)[p^\infty]$ is finite we see from the above exact sequence that the finiteness of $\ker g_{(K',v)}$ is equivalent to the finiteness of $H^1(\Sigma_{(K',w)}, \tilde{A}_v(k_{\infty,w})[p^\infty])$. There is an interesting case for which this latter group is infinite. It is based on the following theorem of of Kuz'min [15], which we quote from [23] X§8. Let us first introduce the following notation for a number field K:
$G_{R,p} = \Sigma_{K,p}^{R,\varnothing}$ (using the notation in the introduction) where R is *any* finite set of primes of K.
$G_{v,p}$ the decomposition group of $G_{R,p}$ at a chosen prime above v.
$\mathcal{G}_{v,p} = \operatorname{Gal}(K_v(p)/K_v)$ where v is a prime of K, K_v the completion and $K_v(p)$ the maximal pro-p extension of K_v.
Let us also denote the group of p-th roots of unity (in $\overline{\mathbb{Q}}$) by μ_p.

Theorem (Kuz'min)**.** *Let K be a totally imaginary number field with $\mu_p \subseteq K$ and let $R \supseteq R_p$ be a finite set of primes of K. Suppose that for a prime $v \in R$ the group $G_{v,p}$ is not open in $G_{R,p}$ (i.e. has infinite index). Then the canonical map:*

$$\mathcal{G}_{v,p} \longrightarrow G_{v,p}$$

is an isomorphism, i.e. every p-extension of the local field K_v is realized by a p-extension of the global field K which is unramified outside R.

We will now explain how $H^1(\Sigma_{(K',w)}, \tilde{A}_v(k_{\infty,w})[p^\infty])$ can in fact be infinite. For simplicity we will work with K below rather than any $K' \in \mathcal{E}$, but the observations are easily seen to hold for any $K' \in \mathcal{E}$. Suppose $K_\infty = K_{R,\varnothing}^{(p)}$ where R is a finite set of primes of K containing R_p and K is totally imaginary containing μ_p as in the above theorem.

Let us also suppose that for our prime $v \in R_p$ we have that $G_{v,p}$ is not open in $G_{R,p}$ (we will explain later how this can occur). Then by the above theorem we have $\Sigma_{(K,w)} = \mathcal{G}_{v,p}$. So we are dealing with the group $H^1(\mathcal{G}_{v,p}, \tilde{A}_v(k_{\infty,w})[p^\infty])$. Let us further suppose that $\tilde{A}_v(k_{\infty,w})[p^\infty]$ is infinite (which is of course possible) and denote $\tilde{A}_v(k_{\infty,w})[p^\infty]$ by M. We now claim the following:

CLAIM: $\operatorname{corank}_{\mathbb{Z}_p}(H^1(\mathcal{G}_{v,p}, M)) = [K_v : \mathbb{Q}_p] \operatorname{corank}_{\mathbb{Z}_p}(M)$, where for any discrete p-primary abelian group D, $\operatorname{corank}_{\mathbb{Z}_p}(D)$ means the $\mathbb{Z}_p$-rank of the Pontryagin dual of D in case it is finitely generated over $\mathbb{Z}_p$.

Note that by sequence (10), the above claim will imply that $\ker g_{(K,v)}$ has $\mathbb{Z}_p$-corank $[K_v : \mathbb{Q}_p] \operatorname{corank}_{\mathbb{Z}_p}(M)$. To show why the claim is true, we first note that $H^1(\mathcal{G}_{v,p}, M)$ is isomorphic to $H^1(K_v, M)$ via the inflation map. To show this we only need to show that
$H^1(\operatorname{Gal}(\overline{K}_v/K_v(p)), M) = 0$. But as $\operatorname{Gal}(\overline{K}_v/K_v(p))$ acts trivially on M, we have that

$$H^1(\operatorname{Gal}(\overline{K}_v/K_v(p)), M) = \operatorname{Hom}_{\text{cont}}(\operatorname{Gal}(\overline{K}_v/K_v(p)), M)$$

and this is zero since M is p-primary and $\operatorname{Gal}(\overline{K}_v/K_v(p))$ has no non-trivial pro-p quotient.

So now we just have to show that the $\mathbb{Z}_p$-corank of $H^1(K_v, M)$ is as stated above. For this we will need the following:

Lemma (Local Corank Lemma)**.** *Let K_v be a finite extension of $\mathbb{Q}_p$ and D a discrete $\operatorname{Gal}(\overline{K}_v/K_v)$-module with $D \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ for some $r \geq 1$. Let $D' = \operatorname{Hom}(D, \mu_{p^\infty})$. Then $H^1(K_v, D)$ is $\mathbb{Z}_p$-cofinitely generated and $\operatorname{corank}_{\mathbb{Z}_p}(H^1(K_v, D))$ is equal to*

$$r[K_v : \mathbb{Q}_p] + \operatorname{corank}_{\mathbb{Z}_p}(H^0(K_v, D)) + \operatorname{rank}_{\mathbb{Z}_p}(H^0(K_v, D'))$$

Regarding the above lemma the fact that $H^1(K_v, D)$ is $\mathbb{Z}_p$-cofinitely generated (i.e. its Pontryagin dual is finitely generated over $\mathbb{Z}_p$) can be deduced form the fact that $H^1(K_v, D[p])$ is finite. As for the statement about coranks the idea is to write $D = \cup_n D[p^n]$ and then to apply Tate's local Euler characteristic formula ([23] Th. 7.3.1) to $D[p^n]$. Also, one uses Tate local duality *loc. cit.* Th. 7.2.6 to show that $H^2(K_v, D)$ is dual to $H^0(K_v, D')$. For details on the proof of the above lemma see [11] §3.

Let us now go back to our group $H^1(K_v, M)$. Now since M_{div} is a $\operatorname{Gal}(\overline{K}_v/K_v)$ submodule of M and $H^i(K_v, M/M_{\text{div}})$ is finite for any $i = 0, 1, 2$, therefore we may assume M is divisible to prove our required claim. So under this assumption our claim will follow from the above Corank Lemma if we can show that $\operatorname{corank}_{\mathbb{Z}_p}(H^0(K_v, M))$ and $\operatorname{rank}_{\mathbb{Z}_p}(H^0(K_v, M'))$ are both zero.

This is clear for the group $H^0(K_v, M)$ because this is just $\tilde{A}_v(k_v)[p^\infty]$ which is finite so its corank is zero. As for $H^0(K_v, M')$, this group is in fact trivial because the inertia subgroup acts trivially on M but non-trivially on μ_{p^∞} and also since any nontrivial homomorphism $\varphi \in \operatorname{Hom}(M, \mu_{p^\infty})$ is necessarily surjective. Hence we have finally shown our claim.

Before stating the main result, along with the observations we just made we need the following theorem of Zerbes [29]:

Theorem (Zerbes)**.** *Let K be a number field, p an odd prime and L/K a Galois extension containing the cyclotomic $\mathbb{Z}_p$-extension of K. Suppose A*

is an elliptic curve defined over K. If $A[p^\infty]$ is not rational over L, then $A(L)[p^\infty]$ is finite.

We can now state the main theorem here:

Theorem 5.1. *Let p be an odd prime and K a number field containing μ_p. Assume that A is an elliptic curve defined over K satisfying: (i) A has good ordinary reduction at all primes of K above p, (ii) A does not have good reduction everywhere (i.e. B is nonempty), and (iii) $\tilde{A}_v(k_v)[p] \neq \{0\}$ for all primes v of K lying above p (k_v is the residue field at v). Let R be a finite set of primes of K containing R_p but not containing B, with the additional restriction: if $R' = R \setminus R_p$, then*

$$\#R'_{\min} \geq 2 + \tfrac{1}{2}[K:\mathbb{Q}] + \#R_p + 2\sqrt{\tfrac{1}{2}[K:\mathbb{Q}] + \#R_p}$$

With all the above assumptions we have the following result: for any $K' \in \mathcal{E}$ if $Ш(A/K')[p^\infty]$ is finite and $\operatorname{rank}(A(K')) < [K':\mathbb{Q}]$, then $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{coker} s_{K'}) \geq [K':\mathbb{Q}] - \operatorname{rank}(A(K'))$. Also if for some $K' \in \mathcal{E}$ we have $Ш(A/K')[p^\infty]$ is finite and $\operatorname{rank}(A(K')) = 0$, then $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{coker} s_{\tilde{K}})$ is unbounded as $\tilde{K}$ varies over $\mathcal{E}$.

Proof. Let us first show that $A(K_\infty)[p^\infty]$ is finite. To show this it will suffice by Zerbes's Theorem to show that $A[p^\infty]$ is not rational over K_∞: since $B \cap R_p = \varnothing$, by the Criterion of Néron-Ogg-Shafarevich, we have that every prime in B ramifies in $K(A[p^\infty])/K$. But B is not contained in R, so $A[p^\infty]$ is not rational over K_∞. Hence $A(K_\infty)[p^\infty]$ is finite.

Now it is simple to show that $H^1(\Sigma_{K'}, A(K_\infty)[p^\infty])$ and $H^2(\Sigma_{K'}, A(K_\infty)[p^\infty])$ are finite. This by a similar argument to the one used in Theorem A: [23] Th. 10.7.12 shows that $H^1(\Sigma_{K'}, \mathbb{Z}/p\mathbb{Z})$ and $H^2(\Sigma_{K'}, \mathbb{Z}/p\mathbb{Z})$ are both finite. This together with the observation (above) that $A(K_\infty)[p^\infty]$ is finite and the fact that if G is a pro-p group, then the only simple discrete p-primary G-module is $\mathbb{Z}/p\mathbb{Z}$ (with trivial action) immediately gives the finiteness of $H^1(\Sigma_{K'}, A(K_\infty)[p^\infty])$ and $H^2(\Sigma_{K'}, A(K_\infty)[p^\infty])$. Also, as we noted in the proof of Theorem A, this implies that $\ker h_{K'}$ and $\operatorname{coker} h_{K'}$ are both finite.

Therefore by the exact sequence (4), we have that $\operatorname{corank}_{\mathbb{Z}_p}(\operatorname{coker} s_{K'}) = \operatorname{corank}_{\mathbb{Z}_p}(\ker g'_{K'})$. We will now determine $\operatorname{corank}_{\mathbb{Z}_p}(\ker g_{K'})$. Let $K_\infty^S = K^{(p)}_{R',R_p}$ i.e. the maximal pro-p extension of K unramified outside R' in which R_p splits completely. Clearly K_∞^S is contained in K_∞.

Moreover, the assumption on the cardinality of $R'_{\min}$ implies by Lemma 2.3 that the extension K_∞^S/K is infinite. Therefore, since R_p splits completely in K_∞^S/K, we see that the decomposition group of Σ_K at any prime of K_∞ lying above p must have infinite index in Σ_K.

Let v be any prime of K above p and w any prime K_∞ above v. Then by what we have shown, it follows from Kuz'min's Theorem, that the extension $K_{\infty,w}/K_v$ coincides with the maximal pro-p extension of K_v. Also,

our assumption (iii) on the elliptic curve A in the statement of the theorem implies that $k_v(\tilde{A}_v[p^\infty])/k_v$ is pro-p (where $\tilde{A}_v$ is the reduction modulo v of the Néron model of A over the ring of integers of K_v). So since in particular $K_{\infty,w}/K_v$ contains the maximal unramified pro-p extension of K_v, we therefore see that $\tilde{A}_v(k_{\infty,w})[p^\infty] = \tilde{A}_v[p^\infty]$ and so $\mathrm{corank}_{\mathbb{Z}_p}(\tilde{A}_v(k_{\infty,w})[p^\infty]) = 1$.

Now let $K' \in \mathcal{E}$ and v a prime of K' above p and w a prime of K_∞ above v. Then as we have shown that the decomposition group of w in Σ_K is not open, it therefore follows from the Claim (proceeding this theorem) and the discussion surrounding it that: $\mathrm{corank}_{\mathbb{Z}_p}(\ker g_{(K',v)}) = [K'_v : \mathbb{Q}_p]\,\mathrm{corank}_{\mathbb{Z}_p}(\tilde{A}_v(k_{\infty,w})[p^\infty])$. But as we showed above we have $\mathrm{corank}_{\mathbb{Z}_p}(\tilde{A}_v(k_{\infty,w})[p^\infty]) = 1$, therefore $\mathrm{corank}_{\mathbb{Z}_p}(\ker g_{(K',v)}) = [K'_v : \mathbb{Q}_p]$.

Now $g_{K'}$ is a direct sum of $g_{(K',v)}$ over a finite number of primes v which include all the primes of K' dividing p. As we showed in the proof of Theorem A, for any prime v of K' not dividing p, we have that $\ker g_{(K',v)}$ is finite. Therefore only primes above p contribute to the $\mathbb{Z}_p$-corank of $\ker g_{K'}$. Adding up these coranks which we calculated above gives that $\mathrm{corank}_{\mathbb{Z}_p}(\ker g_{K'}) = [K' : \mathbb{Q}]$.

Suppose now that $Ш(A/K')[p^\infty]$ is finite. Then the proof of Proposition 3.7 (using the Cassels-Poitou-Tate exact sequence) shows that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\,\lambda_{K'}) \leq \mathrm{rank}(A(K'))$. Therefore if $\mathrm{rank}(A(K')) < [K' : \mathbb{Q}]$, then by diagram (9) in the proof of Theorem A and its associated $\ker - \mathrm{coker}$ sequence, we see from our observations that $\mathrm{corank}_{\mathbb{Z}_p}(\ker g'_{K'}) \geq [K' : \mathbb{Q}] - \mathrm{rank}(A(K'))$. But as we showed in the beginning of this proof, we have $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\, s_{K'}) = \mathrm{corank}_{\mathbb{Z}_p}(\ker g'_{K'})$. Therefore $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\, s_{K'}) \geq [K' : \mathbb{Q}] - \mathrm{rank}(A(K'))$.

Now let's prove the final statement of the theorem. Suppose that $K' \in \mathcal{E}$, $Ш(A/K')[p^\infty]$ is finite and $\mathrm{rank}(A(K')) = 0$ i.e. $\mathrm{Sel}_p(A/K')$ is finite. Note that the K'^{cyc}, the cyclotomic $\mathbb{Z}_p$-extension of K', is contained in K_∞ (because R_p is contained in R). So to show that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\, s_{\tilde{K}})$ is unbounded as $\tilde{K}$ varies over $\mathcal{E}$, by our observations above, it suffices to show that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\,\lambda_{K'_n})$ is bounded with n, where K'_n are the fields associated to the $\mathbb{Z}_p$-extension K'^{cyc}/K'.

This follows from Mazur's Control Theorem: the proof of Corollary 4.9 to Mazur's Control Theorem in [12], shows that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_p(A/K'_n))$ is bounded when $\mathrm{Sel}_p(A/K')$ is finite. So we only have to show that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\,\lambda_{K'_n}) \leq \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_p(A/K'_n))$ for any n. This follows from the proof of Proposition 3.7 (using the Cassels-Poitou-Tate exact sequence), and the fact that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_p(A/K'_n)) = \mathrm{rank}_{\mathbb{Z}_p}(\mathcal{R}_p(A, K'_n))$ (note that elliptic curves are self-dual i.e. $A^t = A$). □

Let us now give an example related to the above theorem. Consider the elliptic curve A: $y^2 + y = x^3 - x^2$ defined over $\mathbb{Q}$ of conductor 11 with good ordinary reduction at 5. This is the modular curve $X_1(11)$. Note that $\tilde{A}_5(\mathbb{F}_5) = \mathbb{Z}/5\mathbb{Z}$. To give an example of the theorem for this elliptic curve,

we will take $p = 5$, $K = \mathbb{Q}(\mu_5)$. Then A has bad reduction at the four primes $\mathfrak{P}_{11,1}, \mathfrak{P}_{11,2}, \mathfrak{P}_{11,3}, \mathfrak{P}_{11,4}$ of K dividing 11. For the set R, we will take:

$$R = \{\mathfrak{P}_5, \mathfrak{P}_{31,1}, \mathfrak{P}_{31,2}, \mathfrak{P}_{31,3}, \mathfrak{P}_{31,4}, \mathfrak{P}_{41,1}, \mathfrak{P}_{41,2}, \mathfrak{P}_{41,3}, \mathfrak{P}_{41,4}, \mathfrak{P}_{61,1}\}$$

where $\mathfrak{P}_5$ is the unique prime above 5 and the ones following it are the four primes above 31, the four primes above 41 and $\mathfrak{P}_{61,1}$ is any prime of K above 61. This set R satisfies the required property in the statement of the theorem.

In [5], it is shown that $\mathrm{Sel}_p(A/K) = \{0\}$. From this, the above theorem gives that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\, s_K) = [K : \mathbb{Q}] = 4$ (the statement of the theorem gives that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\, s_K) \geq [K : \mathbb{Q}]$, but the proof shows that we also have $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\, s_K) \leq [K : \mathbb{Q}]$). The theorem also gives that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{coker}\, s_{K'})$ is unbounded as K' varies through the set $\mathcal{E}$. Since $\mathrm{coker}\, s_{K'}$ is a quotient of $\mathrm{Sel}_p(A/K_\infty)^{\mathrm{Gal}(K_\infty/K')}$ which in turn is a subgroup of $\mathrm{Sel}_p(A/K_\infty)$, we therefore see that:

$$\dim_{\mathbb{Q}_p}(\widehat{\mathrm{Sel}_p(A/K_\infty)} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \infty$$

where $\widehat{\mathrm{Sel}_p(A/K_\infty)}$ is the Pontryagin dual of $\mathrm{Sel}_p(A/K_\infty)$.

Acknowledgements I would like to thank Nancy Childress for her interest in my work and helpful discussions. I would also like to thank Romyar Sharifi for helpful comments.

References

[1] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete **21**, Springer Verlag (1990).

[2] N. Boston, *Some cases of the Fontaine-Mazur conjecture*, J. Number Theory **42** (1992), 285-291.

[3] J. Cassels, *Arithmetic on curves of genus 1. VII. The dual exact sequence*, J. Reine Angew. Math. **216** (1964), 150-158.

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

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

[6] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[7] J. Dixon, M. du Sautoy, A. Mann, and D. Segal, *Analytic Pro-p Groups*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, Cambridge, 1999.

[8] J.-M. Fontaine, B. Mazur, *Geometric Galois representations* in: Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong 1993), Internat. Press, Cambridge, MA (1995), 41-78.

[9] R. Greenberg, *Galois theory for the Selmer group of an abelian variety*, Compos. Math. **136** (2003), 255-297.

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

[11] R. Greenberg, *Iwasawa theory for p-adic representations*, Advanced Studies in Pure Mathematics **17**, Algebraic Number Theory-in honour of K. Iwasawa 97-137, 1989.

[12] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves*, IAS/Park City Math. Ser. 9, Amer. Math Soc. Providence, 2001, pp. 407-464.
[13] E.S. Golod, I.R. Shafarevich, *On the class field tower*. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. **28** 1964 261-272. English translation in: I.R. Shafarevich, Collected mathematical papers. Springer-Verlag, Berlin, 1989.
[14] F. Hajir, *On the growth of p-class groups in p-class field towers*, Journal of Algebra **188** (1997), 256-271.
[15] L.V. Kuz'min, *Local extensions associated with l-extensions with restricted ramification*, Izv. Akad. Nauk SSSR **39** (1975), no. 4. English translation in Math. USSR Izv. 9 (1975), 693-726.
[16] Q. Liu, *Algebraic Geometry and Arithmetic Curves*. Oxford Graduate Texts in Mathematics **6**. Oxford University Press 2002.
[17] A. Lubotzky, *Group presentation, p-adic analytic groups and lattices in* $SL_2(\mathbb{C})$, Ann. Math. **118** (1983), 115-130.
[18] A. Lubotzky, A. Mann, *Powerful p-groups II*, J. Alg. **105** (1987), 506-515.
[19] C. Maire, *Some new evidence for the Fontaine-Mazur conjecture*, Math. Res. Lett. **14** (4) (2007) 673-680.
[20] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math **18** (1972), 183-266.
[21] J.S. Milne, *Arithmetic Duality Theorems*, second ed., BookSurge, LLC, Charleston, SC, 2006.
[22] J. Neukirch, *Algebraic Number Theory*, Springer Grundlehren **322**, 1999.
[23] J. Neukirch, A. Schmidt, K. Wingberg, *Cohomology of Number Fields*, second edition, Grundlehren der Mathematischen Wissenschaften **323**, Springer, 2008, xvi+825.
[24] P. Roquette, *On class field towers*, in Algebraic Number Theory (J. Cassels and A. Fröhlich, Eds.), Academic Press, New York, 1980.
[25] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, 1979.
[26] J.S. Wilson, *Profinite Groups*, Oxford University Press, Oxford, UK, 1998.
[27] K. Wingberg, *On the Fontaine-Mazur conjecture for CM-fields*, Compositio Math. **131** (2002), no. 3, 341-354.
[28] Y. Zarhin, *Torsion of Abelian varieties, Weil classes and cyclotomic extensions*, Math. Proc. Cambridge Philos. Soc. **126** (1999), no. 1, 1-15.
[29] S. Zerbes, *Generalised Euler characterisitcs of Selmer groups*, Proc. London. Math. Soc. **3**, 98, 2009, no.3, 775-796.

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

E-mail address: amatar@uob.edu.bh