Galois Theory for the Selmer Group of an Abelian Variety

Ralph Greenberg*

Introduction

Let A be an abelian variety defined over a number field F. Let K denote the cyclotomic $\mathbb{Z}_p$-extension of F, where p is any prime. Thus the Galois group $G(K/F)$ is isomorphic to $\mathbb{Z}_p$, the additive group of p-adic integers. For any algebraic extension F' of F, we let $\mathrm{Sel}_A(F')_p$ denote the p-primary subgroup of the Selmer group $\mathrm{Sel}_A(F')$ for A over F'. The purpose of this article is to consider some generalizations of the following classical theorem of Mazur.

Theorem. *Assume that A has good, ordinary reduction at all primes of F lying over p. Let F' be a finite extension of F contained in K. Then the natural map*

$$\mathrm{Sel}_A(F')_p \to \mathrm{Sel}_A(K)_p^{G(K/F')}$$

has finite kernel and cokernel. The orders of the kernels and cokernels are bounded as F' varies.

This is Mazur's "Control Theorem", which he proves for any $\mathbb{Z}_p$-extension K/F satisfying certain mild conditions. Actually the theorem is true for the full Selmer group since one can show easily that, for any prime $q \neq p$, the q-primary subgroups of Selmer groups behave very well Galois theoretically. That is, the maps $\mathrm{Sel}_A(F')_q \to \mathrm{Sel}_A(K)_q^{G(K/F')}$ are isomorphisms.

We will consider Galois extensions K/F such that $G(K/F)$ is a p-adic Lie group. For any field F' such that $F \subseteq F' \subseteq K$, we let $s_{K/F'}$ denote the natural restriction homomorphism

$$s_{K/F'} : \mathrm{Sel}_A(F')_p \to \mathrm{Sel}_A(K)_p^{G(K/F')}.$$

*Supported partially by a National Science Foundation grant.

For our main theorems we will need to assume that K/F is "Σ-ramified" for some finite set Σ of primes of F. That is, every prime v of F not in Σ is unramified in K/F. We will make this assumption throughout the article. Let $\mathfrak{p}$ be a prime of F lying over p. Let $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ denote the decomposition and inertia subgroups of $G(K/F)$ for some prime of K lying over $\mathfrak{p}$. Both $D_{\mathfrak{p}}$ and $I_{\mathfrak{p}}$ are closed subgroups of $G(K/F)$ and hence are also p-adic Lie groups. Let $\mathfrak{d}_{\mathfrak{p}}$ and $\mathfrak{i}_{\mathfrak{p}}$ denote their Lie algebras. They are subalgebras of the Lie algebra $\mathfrak{g}$ of $G(K/F)$.

Definition. *We say that K/F is admissible if, in addition to being a Σ-ramified p-adic Lie extension, we have $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ for all $\mathfrak{p}$ lying over p.*

Here, for any Lie algebra $\mathfrak{l}$, we let $\mathfrak{l}'$ denote the derived Lie subalgebra of $\mathfrak{l}$. (That is, $\mathfrak{l}'$ is the $\mathbb{Q}_p$-subspace spanned by $[x, y]$, $x, y \in \mathfrak{l}$, which is an ideal of $\mathfrak{l}$.) Now $\mathfrak{i}'_{\mathfrak{p}}$ is actually an ideal of $\mathfrak{d}_{\mathfrak{p}}$. The equality $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ is equivalent to saying that the Lie algebra $\mathfrak{d}_{\mathfrak{p}}/\mathfrak{i}'_{\mathfrak{p}}$ is abelian. In attempting to prove the finiteness of the cokernel of $s_{K/F'}$, this condition arises quite naturally as a hypothesis. Examples where it is satisfied are rather abundant. Any $\mathbb{Z}_p$-extension K/F is admissible. More generally, if the Lie algebra $\mathfrak{g}$ is abelian (i.e., if $G(K/F)$ contains a subgroup of finite index isomorphic to $\mathbb{Z}_p^d$ for some d), then K/F is admissible. The condition $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ for $\mathfrak{p}|p$ is obviously satisfied since $\mathfrak{d}_{\mathfrak{p}}$ is abelian and so $\mathfrak{d}'_{\mathfrak{p}} = 0$. Another class of examples are those where the inertia subgroup $I_{\mathfrak{p}}$ has finite index in $G(K/F)$ for all $\mathfrak{p}|p$. Then $\mathfrak{d}_{\mathfrak{p}} = \mathfrak{i}_{\mathfrak{p}} = \mathfrak{g}$ and so again $\mathfrak{d}'_{\mathfrak{p}} = \mathfrak{i}'_{\mathfrak{p}}$ obviously holds. An important class of examples, which we discuss below, are those where $G(K/F)$ admits a faithful, finite-dimensional p-adic representation which is of Hodge-Tate type at the primes $\mathfrak{p}$ of F above p.

In our first theorem, we assume that the p-primary subgroup $A(K)_p$ of $A(K)$ is finite.

Theorem 1. *Assume that A has potentially ordinary reduction at all primes of F lying over p. Assume that K/F is admissible and that $A(K)_p$ is finite. Then, for every finite extension F' of F contained in K, the kernel and cokernel of $s_{K/F'}$ are finite.*

Note that the hypotheses in the above theorem are preserved when K/F is replaced by K/F' for any finite extension F' of F contained in K. Thus, it would be enough to prove just that $\ker(s_{K/F})$ and $\mathrm{coker}(s_{K/F})$ are both finite. The same remark applies to theorems 2 and 3 below. Nevertheless, we will usually present the proofs allowing F' to vary in order to see how the order and structure of the kernel and cokernel behave. Under the hypotheses of theorem 1, the kernel of $s_{K/F'}$ is relatively easy to bound. In fact, it would suffice to just assume that K/F is a p-adic Lie extension and that $A(K)_p$ is finite to conclude that $\ker(s_{K/F'})$ is of bounded order as F' varies. For this one needs no hypothesis on the reduction of A. (See proposition 1.1.) However, as will become clear later, one cannot expect $\mathrm{coker}(s_{K/F'})$ to have bounded order as F' varies unless one imposes rather stringent hypotheses.

It is not difficult to prove that if the Lie algebra $\mathfrak{g}$ of $G(K/F)$ is semisimple (i.e., a direct product of simple, nonabelian Lie algebras), then $A(K)_p$ is necessarily finite. (See proposition

1.2 for this and some other sufficient conditions for the finiteness of $A(K)_p$.) It seems that for the p-adic Lie extensions K/F which arise in various natural ways in number theory, the corresponding Lie algebra $\mathfrak{g}$ is often reductive (i.e., a direct product of a semisimple Lie algebra and an abelian one). In this case, it is certainly possible for $A(K)_p$ to be infinite. Nevertheless, one can use theorem 1 to prove the following result.

Theorem 2. *Assume that A has potentially ordinary reduction at all primes of F lying over p. Assume that K/F is admissible and that $\mathfrak{g}$ is reductive. Then* $\ker(s_{K/F'})$ *and* $\mathrm{coker}(s_{K/F'})$ *are finite for every finite extension F' of F contained in K.*

Suppose that $\rho : G_F \to GL_n(\mathbb{Q}_p)$ is a continuous, finite-dimensional $\mathbb{Q}_p$-representation of the absolute Galois group $G_F = G(\overline{\mathbb{Q}}/F)$. If we let $K = \overline{\mathbb{Q}}^{\ker(\rho)}$, then ρ induces an isomorphism of $G(K/F)$ to the compact subgroup $\mathrm{im}(\rho)$ of $GL_n(\mathbb{Q}_p)$. Such a subgroup must be a p-adic Lie group of dimension $d \leq n^2$. We suppose also that ρ is unramified outside a finite set Σ of primes of F and so K/F is Σ-ramified. If ρ is a completely reducible representation of G_F, then the Lie algebra of $\mathrm{im}(\rho)$ (which is isomorphic to $\mathfrak{g}$) must be reductive. For every prime $\mathfrak{p}$ of F lying over p, we can restrict ρ to a decomposition subgroup obtaining the representation $\rho|_{G_{F_\mathfrak{p}}}$ of the local Galois group $G_{F_\mathfrak{p}} = G(\overline{\mathbb{Q}}_p/F_\mathfrak{p})$. We will prove later (proposition 2.7) that if $\rho|_{G_{F_\mathfrak{p}}}$ is a Hodge-Tate representation, then the equality $\mathfrak{d}'_\mathfrak{p} = \mathfrak{i}'_\mathfrak{p}$ does hold. As a consequence we obtain the following result, which perhaps is the most interesting theorem of this article.

Theorem 3. *Assume that ρ is completely reducible and that $\rho|_{G_{F_\mathfrak{p}}}$ is Hodge-Tate for all primes $\mathfrak{p}$ of F lying above p. Assume that the abelian variety A has potentially ordinary reduction at the primes of F lying over p. Then, for every finite extension F' of F contained in K, the kernel and cokernel of $s_{K/F'}$ are finite.*

The hypothesis in theorem 3 are often known to be true for p-adic representations ρ that arise naturally in number theory. For example, suppose that B is an arbitrary abelian variety defined over F and let $V_p(B) = T_p(B) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p(B)$ denotes the Tate module for B. Then the representation $\rho : G_F \to \mathrm{Aut}_{\mathbb{Q}_p}(V_p(B))$ giving the natural action of G_F on $V_p(B)$ is unramified outside the set Σ of primes of F lying above p or where B has bad reduction. Faltings has proven that ρ is completely reducible. It is also known that $\rho|_{G_{F_\mathfrak{p}}}$ is Hodge-Tate for the primes $\mathfrak{p}$ of F above p. (A result of Tate when B has good reduction at $\mathfrak{p}$, extended by Raynaud to the general case.) In this example, $K = F(B[p^\infty])$.

As another example, let $F = \mathbb{Q}$ and let ρ_f be the π-adic representation of $G_\mathbb{Q}$ associated to a cusp form of level N. Here π is a prime of the field E generated by the coefficients in the q-expansion for f. The representation ρ_f is of dimension 2 over the completion E_π. Then ρ_f is known to be irreducible. (See Thm 2.3 in [R].) That suffices to imply that the Lie algebra $\mathfrak{g}$ is reductive. Faltings has proven that $\rho_f|_{G_{\mathbb{Q}_p}}$ is Hodge-Tate. This means that the $\mathbb{Q}_p$-representation ρ of dimension $2[E_\pi : \mathbb{Q}_p]$ defined by ρ_f is Hodge-Tate. Since $\ker(\rho) = \ker(\rho_f)$, theorem 3 can be applied to $K/\mathbb{Q}$, where $K = \overline{\mathbb{Q}}^{\ker(\rho_f)}$.

Faltings has also proven that the $\mathbb{Q}_p$-representations giving the action of $G_{F_\mathfrak{p}}$ on the p-adic étale cohomology of a nonsingular, projective algebraic variety X defined over $F_\mathfrak{p}$ is Hodge-Tate. If X is defined over the number field F, then it is also expected that the corresponding $\mathbb{Q}_p$-representations of G_F are completely reducible.

In this article, we will single out the case $K = F(A[p^\infty])$. As mentioned above, theorem 3 applies to this case (since we can take $B = A$ in the discussion following that theorem). Thus, as a corollary, we have

Theorem 4. *Assume that A is an abelian variety defined over F with potentially ordinary reduction at all primes of F over p. Let $K = F(A[p^\infty])$. Then, for every finite extension F' of F contained in K, $\ker(s_{K/F'})$ and $\mathrm{coker}(s_{K/F'})$ are finite.*

This theorem is equivalent to a result proved by M. Harris. (See the "effectivity theorem" of [H]. The statement there seems rather different, but can be shown to be equivalent to Theorem 4.) Although this theorem is a consequence of theorem 3, it seems worthwhile to treat it separately and as directly as possible. In the case where $\dim(A) = 1$, we will prove that $\ker(s_{K/F_n})$ is actually of bounded order, where $F_n = F(A[p^\infty])$. This may seem somewhat surprising because $A(K)_p = A[p^\infty]$ is infinite. A similar result may possibly be true for abelian varieties of arbitrary dimension.

Under various sets of assumptions about A and K/F, one can show that $\mathrm{coker}(s_{K/F'})$ is nontrivial for all F' or that this group grows in some way. Such results would obviously give information about the structure of $\mathrm{Sel}_A(K)_p^{G(K/F')}$ and hence of $\mathrm{Sel}_A(K)_p$ itself. Here are two sample theorems of that kind. In both theorems, we assume that K/F is a p-adic Lie extension which is Σ-ramified for some finite set Σ of primes of F. We assume that the abelian variety A has good, ordinary reduction at a prime $\mathfrak{p}$ of F lying over p, but make no assumption about the reduction of A at other primes of F. Let $f_\mathfrak{p}$ denote the residue field for $\mathfrak{p}$ and $\widetilde{A}_\mathfrak{p}$ denote the reduction of A modulo $\mathfrak{p}$. The group of points $\widetilde{A}_\mathfrak{p}(f_\mathfrak{p})$ is of course finite. Let A^t denote the dual abelian variety.

Theorem 5. *Assume that $\widetilde{A}_\mathfrak{p}(f_\mathfrak{p})_p \neq 0$. Assume also that $\mathfrak{p}$ is infinitely ramified in K/F and that $A(K)_p = A^t(K)_p = 0$. Then $\mathrm{Sel}_A(K)_p$ is infinite.*

Theorem 6. *Assume that $\widetilde{A}_\mathfrak{p}(f_\mathfrak{p})_p \neq 0$. Assume also that there are infinitely many primes of K lying above $\mathfrak{p}$, that the residue field k_η for any such prime η is infinite, and that $\mathfrak{p}$ is infinitely ramified in K/F. Then $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ is isomorphic to an infinite (but countable) direct sum of copies of $\mathbb{Q}_p/\mathbb{Z}_p$.*

The hypothesis that $\widetilde{A}_{\mathfrak{p}}(f_{\mathfrak{p}})_p \neq 0$ plays an important role in [M]. Following Mazur, one calls $\mathfrak{p}$ an anomalous prime for A if A has good ordinary reduction at $\mathfrak{p}$ and $\widetilde{A}_{\mathfrak{p}}(f_{\mathfrak{p}})_p \neq 0$. For a given A/F, it seems likely that infinitely many such primes should exist. The hypothesis that $\mathfrak{p}$ is infinitely ramified in K/F simply means that $\mathfrak{i}_{\mathfrak{p}} \neq 0$. Infinitely many primes lying above $\mathfrak{p}$ exist if $\mathfrak{d}_{\mathfrak{p}} \neq \mathfrak{g}$ and the residue field for such primes is infinite if $\mathfrak{i}_{\mathfrak{p}} \neq \mathfrak{d}_{\mathfrak{p}}$. It is also worth remarking that if $G(K/F)$ is pro-p, then $A(F)_p = A^t(F)_p = 0$ easily implies that $A(K)_p = A^t(K)_p = 0$. In particular, if K/F is the cyclotomic $\mathbb{Z}_p$-extension and if $\dim(A) = 1$ (so that $A = A^t$), then just assuming that $A(F)_p = 0$ and that some prime $\mathfrak{p}|p$ is anomalous for A would imply that $\mathrm{Sel}_A(K)_p$ is infinite. (This is proposition 8.5 in [M] when $F = \mathbb{Q}$. See also proposition 5.3 in [G1].) If $\mathrm{Sel}_A(K)_p$ is infinite, then either $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}} \neq 0$ or $\mathrm{Sel}_A(K)[p]$ is infinite. Both cases can occur. Also, if $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ is infinite, then either $A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p)$ is infinite or $(Ш_A(K)_p)_{\mathrm{div}}$ is infinite. Again, both cases can occur.

To illustrate theorem 6, consider again the case of an elliptic curve A/F. Assume that A does not have complex multiplication and that A has potentially ordinary reduction at a prime $\mathfrak{p}$ of F lying over p. Let $K = F(A[p^\infty])$. If one replaces F by $F' = F(A[p])$ (or by $F' = F(A[4])$ if $p = 2$), then all the hypotheses in theorem 6 are satisfied. A now has good, ordinary reduction at any prime $\mathfrak{p}'$ of F' above $\mathfrak{p}$, we have $\widetilde{A}_{\mathfrak{p}'}(f_{\mathfrak{p}'})_p \neq 0$, and the Lie algebras $\mathfrak{g}$, $\mathfrak{d}_{\mathfrak{p}'}$, and $\mathfrak{i}_{\mathfrak{p}'}$ are distinct because they have dimensions 4, 3, and 2, respectively. Hence $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ is an infinite direct sum of copies of $\mathbb{Q}_p/\mathbb{Z}_p$. A proof of essentially the same result is given in [CH2].

This article should be regarded as a sequel to [CG]. In that paper one finds a rather simple description of the local conditions occurring in the definition of the Selmer group. This description makes it easy to study Galois theory for the Selmer group, especially in the case where A has potentially ordinary reduction.

Our proofs will be based on a certain exact sequence which we now explain. Let A be an arbitrary abelian variety defined over F. Let L be any algebraic extension of F. For any prime v of F, let F_v denote the v-adic completion of F. If η is any prime of L lying over v, we let L_η denote the union of the η-adic completions of all finite extensions of F contained in L (so that L_η is an algebraic extension of F_v). We denote by κ_η the corresponding Kummer homomorphism

$$\kappa_\eta : A(L_\eta) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(L_\eta, A[p^\infty]).$$

For each η, we let $\mathcal{H}_A(L_\eta) = H^1(L_\eta, A[p^\infty])/\mathrm{im}(\kappa_\eta)$. Then the p-Selmer group for A over L is defined by

$$\mathrm{Sel}_A(L)_p = \ker\Big(H^1(L, A[p^\infty]) \to \prod_\eta \mathcal{H}_A(L_\eta)\Big),$$

where the map is induced by restricting cocycles to decomposition groups. Here η runs over all primes of L, including the archimedean primes (important only for $p = 2$). We will let $\mathcal{P}_A(L) = \prod_{\eta} \mathcal{H}_A(L_\eta)$ for brevity. Also we put

$$\mathcal{G}_A(L) = \operatorname{im}\big(H^1(L, A[p^\infty]) \to \mathcal{P}_A(L)\big).$$

Now suppose that K/F is a Galois extension and F' is an intermediate field. We then obtain the following commutative diagram with exact rows.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_A(F')_p \arrow[r] \arrow[d, "s_{K/F'}"] & H^1(F', A[p^\infty]) \arrow[r] \arrow[d, "h_{K/F'}"] & \mathcal{G}_A(F') \arrow[r] \arrow[d, "g_{K/F'}"] & 0 \\
0 \arrow[r] & \mathrm{Sel}_A(K)_p^{G(K/F')} \arrow[r] & H^1(K, A[p^\infty])^{G(K/F')} \arrow[r] & \mathcal{G}_A(K)^{G(K/F')} &
\end{tikzcd}$$

The snake lemma then gives the exact sequence

$$(1) \qquad 0 \to \ker(s_{K/F'}) \to \ker(h_{K/F'}) \to \ker(g_{K/F'}) \to \operatorname{coker}(s_{K/F'}) \to \operatorname{coker}(h_{K/F'}).$$

As mentioned above, this exact sequence will be the basis of our proofs. In the literature it has often been used in a similar way, especially in the case of $\mathbb{Z}_p$-extensions. (See [CM], [P] for example.) We also use certain basic results about compact p-adic Lie groups, recalled in section 0. In the subsequent sections we will study (1) $\ker(h_{K/F'})$ and $\operatorname{coker}(h_{K/F'})$, and (2) $\ker(g_{K/F'})$. This will of course give information about the kernel and cokernel of $s_{K/F'}$, which is the subject of section 3. In each section we first consider the two important special cases where $G(K/F) \cong \mathbb{Z}_p$ and where $K = F(A[p^\infty])$.

0 Cohomology of compact p-adic Lie groups.

We will collect here several useful results. Let G be a compact p-adic Lie group of dimension d. In the following lemma we regard $\mathbb{Z}/p\mathbb{Z}$ as a trivial G-module.

Lemma 0.1. *(i) Let $\mathcal{V}$ be a closed subgroup of G. Then $H^1(\mathcal{V}, \mathbb{Z}/p\mathbb{Z})$ is finite. Its order is bounded. There exists an open subgroup $\mathcal{U}$ of G such that $|H^1(\mathcal{V}, \mathbb{Z}/p\mathbb{Z})| \leq p^d$ for all closed subgroups $\mathcal{V}$ of $\mathcal{U}$.*

(ii) Let $\mathcal{V}$ be a closed subgroup of G. Then $H^2(\mathcal{V}, \mathbb{Z}/p\mathbb{Z})$ is finite. Its order is bounded.

Proof. We will use the notation and results of [DSMS]. Let P be a Sylow pro-p subgroup of G. Then P is an open subgroup and the restriction map $H^n(G, \mathbb{Z}/p\mathbb{Z}) \to H^n(P, \mathbb{Z}/p\mathbb{Z})$ is injective, for any $n \geq 1$. It suffices to prove lemma 0.1 for open subgroups $\mathcal{V}$ of P. P is a pro-p p-adic analytic group, and so P has finite rank in the sense of [DSMS]. This means that $d(\mathcal{V}) = \dim_{\mathbb{Z}/p\mathbb{Z}}(H^1(\mathcal{V}, \mathbb{Z}/p\mathbb{Z}))$, which is the cardinality of a minimal topological generating set for $\mathcal{V}$, is finite and bounded as $\mathcal{V}$ varies over closed subgroups of P. Also P contains an open subgroup $\mathcal{U}$, which is uniformly powerful (Thm. 9.34 of [DSMS].) Thus, if $\mathcal{V}$ is any closed subgroup of $\mathcal{U}$, then $d(\mathcal{V}) \leq d(\mathcal{U}) = \dim(\mathcal{U}) = d$. (Thms. 9.36, 9.38, proposition 4.4 of [DSMS].) These results prove (i).

As for (ii), $t(\mathcal{V}) = \dim(H^2(\mathcal{V}, \mathbb{Z}/p\mathbb{Z}))$ is the number of relations for a minimal topological generating set for $\mathcal{V}$, which is finite. (Thm. 4.25). For a uniformly powerful subgroup $\mathcal{U}$, we have $t(\mathcal{U}) = d(d-1)/2$. (Thm. 4.26.) Using this, one can give an explicit upper bound for $t(\mathcal{V})$ valid for all closed subgroups of G. (See exercise 9, p. 83 of [DSMS].) ■

Remark. We will apply this lemma to the subgroups $\mathcal{V} = G(K/F')$ of the p-adic Lie group $G = G(K/F)$. These subgroups are open (and hence closed) if $[F' : F] < \infty$. In fact, $G(K/F)$ has a base of open subgroups $\mathcal{V}$ such that $H^1(\mathcal{V}, \mathbb{Z}/p\mathbb{Z})$ has order p^d and $H^2(\mathcal{V}, \mathbb{Z}/p\mathbb{Z})$ has order $p^{d(d-1)/2}$, where $d = \dim(G)$.

Now let V be a finite dimensional $\mathbb{Q}_p$-vector space on which G acts continuously. Let T be a G-invariant $\mathbb{Z}_p$-lattice in V. Let $M = V/T$. Then $M[p] \cong (\mathbb{Z}/p\mathbb{Z})^{\dim(V)}$. Let $i = 1$ or 2. By a simple devissage argument, it follows from lemma 0.1 that $H^i(\mathcal{V}, M[p])$ is finite and of bounded order as $\mathcal{V}$ varies over all closed subgroups of G. But $H^i(\mathcal{V}, M)[p]$ is a homomorphic image of $H^i(\mathcal{V}, M[p])$, and therefore also has bounded order. It follows that the p-primary group $H^i(\mathcal{V}, M)$ is cofinitely generated as a $\mathbb{Z}_p$-module. It also follows that the $\mathbb{Z}_p$-corank of $H^i(\mathcal{V}, M)$ is bounded as $\mathcal{V}$ varies over all closed subgroups of G. Here is a more precise result for open subgroups.

Lemma 0.2. *Let $\mathfrak{g}$ be the Lie algebra of G. Let $i = 1$ or 2. For every open subgroup $\mathcal{V}$ of G, we have*

$$\mathrm{corank}_{\mathbb{Z}_p}(H^i(\mathcal{V}, M)) \leq \dim_{\mathbb{Q}_p}(H^i(\mathfrak{g}, V).$$

There exists an open subgroup $\mathcal{U}$ of G such that equality holds for all open subgroups $\mathcal{V}$ of $\mathcal{U}$.

Proof. We have $\mathrm{corank}_{\mathbb{Z}_p}(H^i(\mathcal{V}, M)) = \dim_{\mathbb{Q}_p}(H^i(\mathcal{V}, V))$. If $\mathcal{V}_1$, $\mathcal{V}_2$ are any two open subgroups of G with $\mathcal{V}_2 \subseteq \mathcal{V}_1$, then the restriction map $H^i(\mathcal{V}_1, V) \to H^i(\mathcal{V}_2, V)$ is injective. There exists an open subgroup $\mathcal{U}$ of G such that $H^i(\mathcal{V}, V) = H^i(\mathfrak{g}, V)$ for all open subgroups $\mathcal{V}$ of $\mathcal{U}$. Lemma 0.2 follows from these remarks. ■

Remark. As a consequence, if $H^i(\mathfrak{g}, V) = 0$, then $H^i(\mathcal{V}, M)$ is finite for all open subgroups $\mathcal{V}$ of G. This is true if $\mathfrak{g}$ is a semisimple Lie algebra.

1 The kernel and cokernel of $h_{K/F'}$.

By the inflation-restriction exact sequence we have

$$\ker(h_{K/F'}) \cong H^1(K/F', A(K)_p).$$

As a group, $A(K)_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^t \times$(a finite group), where $0 \le t \le 2g$, $g = \dim(A)$. Note that $\ker(s_{K/F'}) = \ker(h_{K/F'}) \cap \mathrm{Sel}_A(F')_p$. This is often smaller than $\ker(h_{K/F'})$, but we will postpone the discussion of this issue. The inflation-restriction sequence also gives

$$\mathrm{coker}(h_{K/F'}) \cong \ker(H^2(K/F', A(K)_p) \to H^2(F', A[p^\infty])).$$

But $H^2(F', A[p^\infty]) \cong \bigoplus_{v'} H^2(F'_{v'}, A[p^\infty])$, where v' varies over the real primes of F'. (This follows from corollary 6.24 in [Mi]. Thus, $H^2(F', A[p^\infty]) = 0$ if p is odd and is a finite elementary 2-group if $p = 2$. We will simply use the upper bound

$$|\mathrm{coker}(h_{K/F'})| \le |H^2(K/F', A(K)_p|$$

which is an equality if p is odd or if F' is totally complex.

I. *K/F is a $\mathbb{Z}_p$-extension.*

Assume that σ_0 is a topological generator of $G(K/F) \cong \mathbb{Z}_p$. The finite extensions F' of F contained in K form a tower $F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots$, where F_n/F is cyclic of degree p^n and $G(K/F_n)$ is generated topologically by $\sigma_0^{p^n}$. We have

$$H^1(K/F_n, A(K)_p) \cong A(K)_p/(\sigma_0^{p^n} - 1)A(K)_p.$$

We consider $\sigma_0^{p^n} - 1$ as an endomorphism of the abelian group $A(K)_p$. Its kernel is the finite group $A(F_n)_p$. This implies that the restriction of $\sigma_0^{p^n} - 1$ to the maximal divisible subgroup $(A(K)_p)_{\mathrm{div}}$ is surjective. Hence it follows that

$$(A(K)_p)_{\mathrm{div}} \subseteq (\sigma_0^{p^n} - 1)A(K)_p \subseteq A(K)_p$$

for all n, and therefore $H^1(K/F_n, A(K)_p)$ is finite. Its order is bounded above by the index $[A(K)_p : (A(K)_p)_{\mathrm{div}}]$ with equality for $n \gg 0$. Thus $|\ker(h_{K/F'})|$ is finite and bounded as F' varies.

Since $\mathrm{Gal}(K/F') \cong \mathbb{Z}_p$ is a free pro-p group and so has p-cohomological dimension 1, it follows that $H^2(K/F', A(K)_p) = 0$. Therefore $\mathrm{coker}(h_{K/F'}) = 0$ for all F'.

II. $K = F(A[p^\infty])$.

A theorem of Serre (Corollaire of Theoreme 2, [Se]), implies that $H^n(G(K/F'), A[p^\infty])$ is finite for any $n \geq 0$ and any finite extension F' of F contained in K. In particular, $\ker(h_{K/F'})$ is finite. But its order turns out to be unbounded. More precisely, we have the following result: Let $F_n = F(A[p^n])$ for $n \geq 1$. Then

$$\ker(h_{K/F_n}) \cong (\mathbb{Z}/p^n\mathbb{Z})^{2g(m-1)} \tag{2}$$

for $n \gg 0$. Here $m = m_A$ denotes the dimension of the p-adic Lie group $G(K/F)$. One can show easily that $m > 1$ and hence indeed $|\ker(h_{K/F'})|$ is unbounded as F' varies.

To justify (2), consider the subgroup $\mathcal{Z}$ of $G(K/F)$ defined as follows. Let $\sigma \in G(K/F)$. Then, $\sigma \in \mathcal{Z} \Leftrightarrow \sigma$ acts on $T_p(A)$ as multiplication by a scalar $\delta(\sigma) \in 1 + 2p\mathbb{Z}_p$. According to a result of Bashmakov, δ defines an isomorphism of $\mathcal{Z}$ to an open subgroup of $1 + 2p\mathbb{Z}_p$, i.e., $\mathcal{Z} \cong \mathbb{Z}_p$. Let $M = K^{\mathcal{Z}}$. For $n \geq 1$, let $M_n = F_n M = M(A[p^n])$. We assume hereon that n is sufficiently large. Then $1 + p^n\mathbb{Z}_p \subseteq \delta(\mathcal{Z})$. We have $G(K/M_n) = \mathcal{Z}_n$, where $\mathcal{Z}_n = \delta^{-1}(1 + p^n\mathbb{Z}_p)$. We also have $A(M_n)_p = A(F_n)_p = A[p^n]$. Now since $\mathcal{Z}_n$ is topologically cyclic and $A(M_n)_p$ is finite, one sees easily that $H^1(\mathcal{Z}_n, A[p^\infty]) = 0$ and hence the inflation-restriction sequence gives an isomorphism

$$H^1(M_n/F_n, A[p^n]) \xrightarrow{\sim} H^1(K/F_n, A[p^\infty]).$$

Therefore, $\ker(h_{K/F_n}) = \mathrm{Hom}(G(M_n/F_n), A[p^n])$. Note that $G(M_n/F_n) \cong G(M/M \cap F_n) = H_n$, say. This is an open subgroup of the p-adic Lie group $G(M/F)$, which has dimension $m-1$. Using Lemma 0.1, one sees that H_n can be generated topologically by $m-1$ elements. Also, $[F_{n+1} : F_n] = p^m$, $[M_{n+1} : M_n] = p$ from which it follows that $[H_n : H_{n+1}] = p^{m-1}$. Now $G(F_{2n}/F_n)$ is abelian and of exponent p^n. It follows that H_n/H_{2n} is abelian, of exponent p^n, and of order $p^{n(m-1)}$. The above remarks imply that $H_n/H_{2n} \cong (\mathbb{Z}/p^n\mathbb{Z})^{m-1}$ and that $H_{2n} = (H_n, H_n)H_n^{p^n}$, which justifies (2).

Serre's theorem referred to earlier states that $H^2(K/F', A[p^\infty])$, and hence $\mathrm{coker}(h_{K/F'})$, are finite. Alternatively, one can prove the finiteness as follows. Define M as above. For any F', let $M' = F'M$. Then $K/M' \cong \mathbb{Z}_p$ and so $H^2(K/M', A[p^\infty]) = 0$. Since $H^1(K/M', A[p^\infty]) = 0$ also, we obtain an isomorphism

$$H^2(M'/F', A(M')_p) \xrightarrow{\sim} H^2(K/F', A[p^\infty]).$$

Now $A(M')_p$ is finite. If $\mathcal{V}$ is the Sylow pro-p subgroup of the p-adic Lie group $G(M'/F')$, then $H^2(\mathcal{V}, \mathbb{Z}/p\mathbb{Z})$ is finite. The finiteness of $H^2(\mathcal{V}, A(M')_p)$ and hence of $\mathrm{coker}(h_{K/F'})$ follows by devissage. Lemma 0.1 (ii) asserts that $\dim_{\mathbb{Z}/p\mathbb{Z}}(H^2(\mathcal{V}, \mathbb{Z}/p\mathbb{Z}) < C$, for some C. Then an upper bound for $|\mathrm{coker}(h_{K/F'})|$ would be $|A(M')_p|^C$. But note that $|A(M')_p|$ is unbounded as F' varies.

III. *Arbitrary K/F.*

Here is one general result valid for any abelian variety defined over F.

Proposition 1.1. *Let K/F be a Galois extension such that $G(K/F)$ is a p-adic Lie group. Assume that $A(K)_p$ is finite. Then $\ker(h_{K/F'})$ and $\mathrm{coker}(h_{K/F'})$ are finite and have bounded order as F' varies over all extensions of F contained in K.*

Proof. $A(K)_p$ is a finite $G(K/F)$-module. It is enough to bound the order of $H^i(\mathcal{V}, A(K)_p)$ for all open pro-p subgroups $\mathcal{V}$ of $G(K/F)$, where $i = 1$ or 2. But $A(K)_p$ has a $\mathcal{V}$-composition series with corresponding quotients isomorphic to $\mathbb{Z}/p\mathbb{Z}$. Thus, by devissage, one can bound the order of $H^i(\mathcal{V}, A(K)_p)$ by $|A(K)_p|^{d_i(\mathcal{V})}$, where $d_i(\mathcal{V}) = \dim_{\mathbb{Z}/p\mathbb{Z}}(H^i(\mathcal{V}, \mathbb{Z}/p\mathbb{Z})$. By Lemma 0.1, $d_i(\mathcal{V})$ is bounded. ∎

There are various hypotheses which imply that $A(K)_p$ is finite, some of which are included in the following result. A number of other results can be found in articles of Zarhin. (See [Z1], [Z2], and some of the references there.) We assume only that A is an abelian variety defined over F and that $G(K/F)$ is a p-adic Lie group.

Proposition 1.2. *$A(K)_p$ is finite if any of the following conditions are satisfied.*

(i) There exists a nonarchimedean prime η of K not lying over p such that the corresponding residue field k_η is finite.

(ii) The Lie algebra $\mathfrak{g}$ is solvable, A has potentially ordinary reduction at all primes of F lying above p, and the residue field k_η is finite for all primes η of K lying above p.

(iii) The Lie algebra $\mathfrak{g}$ is semisimple.

Proof of (i). Suppose that v is the prime of F lying below η and that $v|l$, $l \neq p$. The stated condition is actually equivalent to asserting that K_η is a finite extension of F_v. For $G(K_\eta/F_v)$ is a p-adic Lie group of dimension ≤ 2. If it has positive dimension, then K_η must contain the cyclotomic $\mathbb{Z}_p$-extension of F_v (which is the only $\mathbb{Z}_p$-extension of F_v and is unramified). Then the residue field k_η would be infinite. Since K_η is a finite extension of F_v, it is now obvious that $A(K_\eta)_{\mathrm{tors}}$ is finite, and hence so is $A(K)_{\mathrm{tors}}$ and, in particular, $A(K)_p$.

Proof of (ii). Replacing F and K by finite extensions, we can assume that A has good, ordinary reduction at all primes v of F lying above p. The other conditions still hold. Assume that $A(K)_p$ is infinite. Let $W_p = H^0(K, V_p(A))$. That is, $W_p = T_p(A(K)_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p(A(K)_p)$ denotes the Tate module of $A(K)_p$. Then $\dim(W_p) \geq 1$ and we can consider the representation

$$\rho : G(K/F) \to \mathrm{Aut}(W_p)$$

induced from the action of $G(K/F)$ on $A(K)_p$. Since $\widetilde{A}_v(k_\eta)$ is finite, it follows that

$$W_p \subset \ker(V_p(A) \to V_p(\widetilde{A}_v)).$$

Let A^t denote the dual abelian variety for A. Then A^t also has good reduction in v and the action of G_{F_v} on $V_p(\widetilde{A_v^t})$ is unramified. Since we are assuming that A has ordinary reduction at v, the Weil pairing $V_p(A) \times V_p(A^t) \to \mathbb{Q}_p(1)$ induces an isomorphism

$$\ker(V_p(A) \to V_p(\widetilde{A}_v)) \cong \mathrm{Hom}(V_p(\widetilde{A_v^t}), \mathbb{Q}_p(1))$$

as representation spaces for G_{F_v}. Let $\chi : G_F \to \mathbb{Z}_p^\times$ denote the cyclotomic character and let $\sigma = \rho \otimes \chi^{-1}$, which gives the action of G_F on $\mathrm{Hom}(\mathbb{Q}_p(1), W_p)$. Then σ is a finite dimensional representation of G_F and its restriction $\sigma|_{G_{F_v}}$ gives the action of G_{F_v} on some nonzero subspace of $\mathrm{Hom}(V_p(\widetilde{A_v^t}), \mathbb{Q}_p)$ and hence is unramified and has infinite image. It follows that $L = \overline{F}^{\ker(\sigma)}$ is an infinite p-adic Lie extension of F which is unramified at all primes of F lying over p. It is unlikely that such an extension L/F can exist. That would follow from a conjecture of Fontaine and Mazur. But if $\mathfrak{g}$ is solvable, then the nonexistence of L/F is easy to show. Then the Lie algebra of $G(L/F)$ is also solvable. Replacing F by a finite extension, if necessary, we can assume that $G(L/F)/G(L/F)'$ is infinite and hence L must contain a $\mathbb{Z}_p$-extension F_∞ of F. But the only primes of F which can ramify in F_∞/F are those lying over p, and at least one such prime must ramify. This proves that $A(K)_p$ must be finite.

Proof of (iii). All that we need is that the Lie subalgebra $\mathfrak{g}'$ is equal to $\mathfrak{g}$. If $\delta : G(K/F) \to \mathbb{Z}_p^\times$ denotes the determinant of the representation ρ of $G(K/F)$ giving the action on W_p, then it follows that δ is a character of finite order. Hence $\delta|_{G(K_\eta/F_v)}$ also has finite order, where v is any prime of F and η is a prime of K lying above v. Choose v to be a prime not lying over p where A has good reduction. Then the natural action of G_{F_v} on $V_p(A)$, and hence on W_p, is unramified. The eigenvalues of the Frobenius automorphism φ_v in $G(F_v^{\mathrm{unr}}/F_v)$ on $V_p(A)$ are algebraic numbers which have absolute value $\sqrt{|f_v|}$ at all archimedean primes (of $\overline{\mathbb{Q}}$). Here f_v is the residue field for v. Assume that $A(K)_p$ is infinite. Then $\dim(W_p) \geq 1$ and the above discussion shows that $\delta|_{G_{F_v}}$ must have infinite order and hence so does δ. This is not possible and hence $A(K)_p$ must be finite. ∎

As a step towards proving theorems 2 and 3, we now consider the case where $\mathfrak{g}$ is reductive. As mentioned in the introduction, such K/F arise naturally.

Proposition 1.3. *Assume that the Lie algebra $\mathfrak{g}$ of $G(K/F)$ is reductive. Then* $\ker(h_{K/F'})$ *and* $\mathrm{coker}(h_{K/F'})$ *are finite.*

Proof. Let $\mathfrak{n}$ denote the radical of $\mathfrak{g}$. The proof of this proposition will be based just on the hypothesis that $\mathfrak{n}$ is abelian, which is true by definition if $\mathfrak{g}$ is reductive. Let $n = \dim_{\mathbb{Q}_p}(\mathfrak{n})$. It follows that $G(K/F)$ contains an open subgroup G and a normal subgroup N of G such that $N \cong \mathbb{Z}_p^n$ and the Lie algebra $\mathfrak{g}/\mathfrak{n}$ of G/N is semisimple. To simplify notation, we replace F by the finite extension K^G and so have $G = G(K/F)$. Let $L = K^N$. If F' is any finite extension of F, let $L' = F'L$ and let $N' = G(K/L')$, which is also isomorphic to $\mathbb{Z}_p^n$. The Lie algebra of $G(L'/F')$ is still $\mathfrak{g}/\mathfrak{n}$ and hence proposition 1.2 implies that $A(L')_p$ is finite. That is, for every subgroup $\mathcal{N}$ of N of finite index, we have that $H^0(\mathcal{N}, A(K)_p)$ is finite. This last property is all that we need. We will show that $H^1(G, A(K)_p)$ and $H^2(G, A(K)_p)$ are both finite. This implies that $\ker(h_{K/F})$ and $\mathrm{coker}(h_{K/F})$ are finite. Proposition 1.3 then follows since F can be replaced by any finite extension F'. (It simplifies the notation to just consider the case K/F.)

As before, we let $W_p = T_p(A(K)_p) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, where $T_p(A(K)_p)$ denotes the Tate module for $A(K)_p$. The inflation-restriction sequence gives an exact sequence

$$H^1(G/N, W_p^N) \to H^1(G, W_p) \to H^1(N, W_p).$$

Since $W_p^N = 0$, the first term is trivial. To show that the last term is trivial, we show that N contains a subgroup Z isomorphic to $\mathbb{Z}_p$ with the property that $W_p^Z = 0$. Using the inflation-restriction sequence again, it will then follow that $H^1(N, W_p)$ is isomorphic to a subspace of $H^1(Z, W_p) = W_p/(z-1)W_p$, where z is a topological generator for Z. But $W_p^Z = 0$ implies that $H^1(Z, W_p) = 0$. Hence $H^1(N, W_p) = 0$ and therefore $H^1(G, W_p)$ is indeed trivial. The fact that $H^1(N, W_p) = 0$ gives another exact sequence

$$H^2(G/N, W_p^N) \to H^2(G, W_p) \to H^2(N, W_p).$$

Just as above, the first term is trivial and the last term is isomorphic to a subspace of $H^2(Z, W_p)$, which is trivial because Z has p-cohomological dimension 1.

To prove the existence of such a subgroup Z, consider W_p as a representation space for N. Since N is abelian, all of its irreducible representations over $\overline{\mathbb{Q}}_p$ are 1-dimensional. Thus the composition factors in the representation space $W_p \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p$ are 1-dimensional and the action of N on them is given by homomorphisms $\chi_i : N \to \overline{\mathbb{Q}}_p^{\times}$ for $1 \le i \le \dim_{\mathbb{Q}_p}(W_p)$. Since $H^0(\mathcal{N}, W_p) = 0$ for every subgroup $\mathcal{N}$ of finite index in N, it is clear that $\chi_i|_{\mathcal{N}}$ is nontrivial for each i. (Otherwise, the elements of $\mathcal{N}$ would have 1 as a common eigenvalue and a common eigenvector would exist since $\mathcal{N}$ is abelian.) Thus, each χ_i has infinite order. Hence $\mathrm{rank}_{\mathbb{Z}_p}(\ker(\chi_i)) < n$. One must just choose $Z \cong \mathbb{Z}_p$ so that $Z \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is not contained in any of the proper subspaces $\ker(\chi_i) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of $N \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, which is certainly possible. ■

We also include a proof of the following simple result.

Proposition 1.4. *Let K/F be any Galois extension such that $G(K/F)$ is a p-adic Lie group. Then* $\ker(h_{K/F'})[p]$ *and* $\mathrm{coker}(h_{K/F'})[p]$ *have bounded order as F' varies. The $\mathbb{Z}_p$-corank of* $\ker(h_{K/F'})$ *and* $\mathrm{coker}(h_{K/F'})$ *are also bounded as F' varies.*

Proof. Let $B = (A(K)_p)_{\mathrm{div}}$ and $C = A(K)_p/(A(K)_p)_{\mathrm{div}}$. Let $i = 1$ or 2. Since C is finite, the proof of proposition 1.1 shows that $H^i(K/F', C)$ has bounded order. Also, $B[p]$ is finite and so $H^i(K/F', B[p])$ has bounded order. Since B is divisible, one has a surjective map from $H^i(K/F', B[p])$ to $H^i(K/F', B)[p]$, which therefore also has bounded order. It follows easily that $|H^i(K/F', A(K)_p)[p]|$ is bounded as F' varies, which gives the first assertion in proposition 1.4. The second assertion follows from this. Or one could use lemma 0.2 to get the upper bound $\dim_{\mathbb{Q}_p}(H^1(\mathfrak{g}, W_p))$ on the $\mathbb{Z}_p$-corank of $\ker(h_{K/F'})$ and the upper bound $\dim_{\mathbb{Q}_p}(H^2(\mathfrak{g}, W_p))$ for the $\mathbb{Z}_p$-corank of $\mathrm{coker}(h_{K/F'})$, where $\mathfrak{g}$ is the Lie algebra of $G(K/F)$ and $W_p = (\varprojlim B[p^n]) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. ∎

Remark. The finiteness of $\ker(h_{K/F'})$ for all F' is equivalent to the vanishing of $H^1(\mathfrak{g}, W_p)$. The finiteness of $\mathrm{coker}(h_{K/F'})$ for all F' is equivalent to the vanishing of $H^2(\mathfrak{g}, W_p)$.

It is possible for $\ker(h_{K/F'})$ to have positive $\mathbb{Z}_p$-corank. For example, let A be any abelian variety defined over a number field F. Let F_Σ be the maximal extension of F unramified outside Σ, where Σ is the set of primes of F lying over p or ∞ or where A has bad reduction. Then $H^1(F_\Sigma/F,\ A[p^\infty])$ is a cofinitely generated $\mathbb{Z}_p$-module and so $H^1(F_\Sigma/F, A[p^\infty])_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^a$, where $[F:\mathbb{Q}]g \le a < \infty$. This follows from the fact that the Euler-Poincaré characteristic of the $G(F_\Sigma/F)$-module $A[p^\infty]$ is $-[F:\mathbb{Q}]g$. Let $L = F(A[p^\infty])$. Let $\mathcal{H}_F$ be any subgroup of $H^1(F_\Sigma/F, A[p^\infty])$ isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. Then $\mathcal{H}_L = h_{L/F}(\mathcal{H}_F)$ is a subgroup of $\mathrm{Hom}_{G(L/F)}(G(L^{\mathrm{ab}}/L), A[p^\infty])$ which is also isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$, since $\ker(h_{L/F})$ is finite by Serre's theorem. It is clear that $\mathcal{H}_L$ determines a unique extension K/L such that $\mathcal{H}_L \subseteq \mathrm{Hom}(G(K/L), A[p^\infty])$ and K is minimal. It is not hard to see that K/F is Galois and that $G(K/L) \cong \mathbb{Z}_p^b$ for some b ($\le 2g$). Therefore $G(K/F)$ is a p-adic Lie group. Also, K/F is Σ-ramified. It is clear that $\mathcal{H}_F \subseteq \ker(h_{K/F})$, which therefore has $\mathbb{Z}_p$-corank ≥ 1.

More generally, one could take $\mathcal{H}_F$ to be any subgroup of $H^1(F_\Sigma/F, A[p^\infty])$. One obtains just as above a p-adic Lie extension K/F such that $K \subset F_\Sigma$ and $\mathcal{H}_F \subset \ker(h_{K/F})$. A similar construction works locally. Let v be a prime of F. Suppose that D_v is any G_{F_v}-module of finite $\mathbb{Z}_p$-corank. Then $H^1(F_v, D_v)$ also has finite $\mathbb{Z}_p$-corank. Let $\mathcal{H}_{F_v}$ be any subgroup of $H^1(F_v, D_v)$. Then one can construct a p-adic Lie extension K of F_v such that $\mathcal{H}_{F_v}$ is contained in the kernel of the restriction map $H^1(F_v, D_v) \to H^1(K, D_v)$.

2 The kernel of $g_{K/F'}$.

We will study the kernel of the natural restriction map on each factor of $\mathcal{P}_A(F')$. This will give information about the kernel of the natural map $r_{K/F'} : \mathcal{P}_A(F') \to \mathcal{P}_A(K)$. We have $\ker(g_{K/F'}) = \mathcal{G}_A(F') \cap \ker(r_{K/F'})$ and hence we will obtain information about $\ker(g_{K/F'})$. If v' is any prime of F', let v denote the prime of F such that $v'|v$ and let η denote any prime of K lying over v'. We let $r_{v'}$ denote the restriction map

$$r_{v'} : \mathcal{H}_A(F'_{v'}) \to \mathcal{H}_A(K_\eta).$$

The kernel of $r_{v'}$ doesn't depend on the choice of η. This section will have five parts **A**–**E**. We consider separately the cases **A**: $v \nmid p$ or ∞, **B**: $v|\infty$, and **C**: $v|p$. We then bring these cases together in part **D**, where we study $\ker(r_{K/F'})$. Finally, we will say what we can about $\ker(g_{K/F'})$ in part **E**. In parts **A**–**D**, we discuss the cases I, II, and III as in section 1.

(A) $v \nmid p$, v nonarchimedean.

In this case, proposition 4.1 of [CG] states that the image of $\kappa_{v'}$ and of κ_η are zero. Thus the map $r_{v'}$ is simply the restriction map $H^1(F_{v'}, A[p^\infty]) \to H^1(K_\eta, A[p^\infty])$ and so

$$\ker(r_{v'}) \cong H^1(K_\eta/F_{v'}, A(K_\eta)_p).$$

Now results of Tate imply easily that $H^1(F_{v'}, A[p^\infty])$ is finite and so obviously $\ker(r_{v'})$ is also finite. The question therefore is whether the order of $\ker(r_{v'})$ is bounded or unbounded as F' varies and as v' varies over primes of F' lying over v.

I. *K/F is a $\mathbb{Z}_p$-extension.*

In this case it is well-known that v is unramified in K/F. We will prove the following general result which will be useful for other p-adic Lie extensions too.

Proposition 2.1. *Assume that $v \nmid p$ and that K_η/F_v is unramified. Then there is a constant $c_v^{(p)}$ (which depends only on A, F_v, and p) such that $|\ker(r_{v'})| \le c_v^{(p)}$. If A has good reduction at v, then* $\ker(r_{v'}) = 0$.

Proof. We first give the bound $c_v^{(p)}$. Let I_v denote the inertia subgroup of $G_{F_v} = \mathrm{Gal}(\overline{F}_v/F_v)$, where $\overline{F_v}$ denotes an algebraic closure of F_v. Let $F_v^{\mathrm{unr}} = \overline{F}_v^{I_v}$, the maximal unramified extension of F_v. Then we let

$$c_v^{(p)} = [A(F_v^{\mathrm{unr}})_p : (A(F_v^{\mathrm{unr}})_p)_{\mathrm{div}}].$$

Now $|\ker(r_{v'})|$ is bounded by the order of $\ker(H^1(F'_{v'}, A[p^\infty]) \to H^1(F_v^{\mathrm{unr}}, A[p^\infty])$. This is given by

$$H^1(F_v^{\mathrm{unr}}/F'_{v'}, A(F_v^{\mathrm{unr}})_p) \cong A(F_v^{\mathrm{unr}})_p/(\sigma'-1)A(F_v^{\mathrm{unr}})_p.$$

Here σ' denotes a topological generator of $G(F_v^{\mathrm{unr}}/F'_{v'})$. The kernel of $\sigma'-1$ acting on $A(F_v^{\mathrm{unr}})_p$ is $A(F'_{v'})_p$, which is finite, and so the cokernel of $\sigma'-1$ is also finite. It follows that

$$(A(F_v^{\mathrm{unr}})_p)_{\mathrm{div}} \subseteq (\sigma'-1)A(F_v^{\mathrm{unr}})_p \subseteq A(F_v^{\mathrm{unr}})_p.$$

Thus indeed $|\ker(r_{v'})| \leq c_v^{(p)}$. For the final part of proposition 2.1, note that if A has good reduction at v, then the action of I_v on $A[p^\infty]$ is trivial. Hence $A(F_v^{\mathrm{unr}})_p = A[p^\infty]$ is divisible and so $c_v^{(p)} = 1$. ■

Remark. The bound c_v can often be improved. If K_η/F_v is an infinite extension, then the pro-p Sylow subgroup of $G(K_\eta/F_v)$ is isomorphic to $\mathbb{Z}_p$. The above argument would show that

$$|\ker(r_{v'})| \leq [A(K_\eta)_p : (A(K_\eta)_p)_{\mathrm{div}}].$$

This bound is sharp since $G(K_\eta/F_v)$ acts on $A(K_\eta)_p/\left(A(K_\eta)_p\right)_{\mathrm{div}}$ through a finite quotient group. Hence $(\sigma'-1)A(K_\eta)_p = \left(A(K_\eta)_p\right)_{\mathrm{div}}$ if $F'_{v'}$ is sufficiently large. Then this inequality becomes an equality. As a special case, if K/F is a $\mathbb{Z}_p$-extension and $A(F_v)_p = 0$, then one sees easily that $A(K_\eta)_p = 0$ too, and so $\ker(r_{v'}) = 0$. On the other hand, it can happen that v splits completely in K/F (i.e., $K_\eta = F_v$). In that case, it is obvious that $\ker(r_{v'}) = 0$.

The invariant $c_v^{(p)}$ of an abelian variety A/F_v has the following interpretation. Let $\widetilde{A}_v$ denote the reduction modulo v of the Neron model for A over the ring of integers in F_v. Then $\widetilde{A}_v$ is an abelian algebraic group defined over the residue field f_v. Let $l = \mathrm{char}(f_v)$. For any finite extension of F_v, the kernel of the reduction map is a pro-l group. Since $l \neq p$, it follows easily that $A(F_v^{\mathrm{unr}})_p \cong \widetilde{A}_v(\overline{f}_v)_p$, where $\overline{f}_v$ is an algebraic closure of f_v. Let $\widetilde{B}_v$ denote the connected component of the identity in $\widetilde{A}_v$. Then $\widetilde{B}_v(\overline{f}_v)$ is divisible and has finite index in $\widetilde{A}_v(\overline{f}_v)$. Therefore, $(\widetilde{A}_v(\overline{f}_v)_p)_{\mathrm{div}} = \widetilde{B}_v(\overline{f}_v)_p$ and, since $\widetilde{A}_v(\overline{f}_v)$ is a torsion group, it follows that $c_v^{(p)}$ is just the order of the Sylow p-subgroup of the group $\mathcal{C}_v = \widetilde{A}_v(\overline{f}_v)/\widetilde{B}_v(\overline{f}_v)$ of connected components for $\widetilde{A}_v$.

If K_η/F_v is an infinite, unramified, p-adic Lie extension, then K_η is just a finite extension of the unramified $\mathbb{Z}_p$-extension of F_v. Letting k_η denote the residue field for η, the group $\widetilde{B}_v(k_\eta)_p$ is still divisible. (This follows easily from the fact that $G(\overline{f}_v/k_\eta)$ has profinite order not divisible by p.) We therefore have $(\widetilde{A}_v(k_\eta)_p)_{\mathrm{div}} = \widetilde{B}_v(k_\eta)_p$. One can then see that

$A(K_\eta)_p/(A(K_\eta)_p)_{\text{div}} \cong \mathcal{C}_v^{G_{K_\eta}}$ and that $\ker(r_{v'})$ is isomorphic to $\mathcal{C}_v^{G_{K_\eta}}/(\sigma'-1)\mathcal{C}_v^{G_{K_\eta}}$, where σ' is a topological generator for $G(K_\eta/F'_{v'})$. As a consequence, $\ker(r_{v'})$ has the same order as $\mathcal{C}_v^{G_{F'_{v'}}}$.

II. $K = F(A[p^\infty])$.

Since $v \nmid p$, the criterion of Serre-Tate states that v is ramified in K_η/F_v if and only if A has bad reduction at v. Thus, if A has good reduction at v, then proposition 2.1 implies that $\ker(r_{v'}) = 0$. If A has bad reduction at v, we consider two cases.

(i) *A has potentially good reduction at v.*

Equivalently, the inertia group I_v acts on $A[p^\infty]$ through a finite quotient group Δ. In fact, $\Delta = \Delta(F_v, A)$ is independent of p. Also, A achieves good reduction over $F_v(A[m])$ for any $m \geq 3$ such that $v \nmid m$. (See section 2 of [ST].) It is rare for p to divide the order of Δ. (For the case where $g = \dim(A) = 1$, this could happen only for $p = 2$ or 3. For $g \geq 1$, the set of primes which can divide $|\Delta|$ is finite and depends only on g.) If $p \nmid |\Delta|$, then proposition 3.1 implies that $\ker(r_{v'}) = 0$.

On the other hand, if p does divide $|\Delta|$, one can remark that there is a bound on $|\ker(r_{v'})|$ which depends only on g. Let L be a fixed finite Galois extension of F_v over which A achieves good reduction. (One can choose L to depend only on g and not on A.) It suffices to bound the order of $H^1(LK_\eta/F'_{v'}, A[p^\infty])$. But, by proposition 2.1, this is $H^1(LF'_{v'}/F'_{v'}, A(LF'_{v'})_p)$ and its order is bounded by that of $H^1(P', A(LF'_{v'})_p)$, where P' is a p-Sylow subgroup of $G(LF'_{v'}/F'_{v'})$. P' has bounded order (dividing $[L{:}F_v]$). It is an easy exercise (by devissage) to bound the order of $H^1(P', B)$, where B is any finite p-primary P'-module, in terms of $|P'|$ and $|B[p]|$, which justifies our remark.

(ii) *A doesn't have potentially good reduction at v.*

Thus the image of I_v in $\mathrm{Aut}_{\mathbb{Z}_p}(T_p(A))$ is infinite. Assume $v|l$, where l is a rational prime (and $l \neq p$). Since $\mathrm{Aut}_{\mathbb{Z}_p}(T_p(A))$ contains a pro-p subgroup of finite index, the same is true for the image of I_v and one can see easily by local class field theory that K_η contains the field $F_v(\mu_{p^\infty}, \sqrt[p^\infty]{l})$. This implies that G_{K_η} has profinite order prime to p. Thus $H^1(K_\eta, A[p^\infty]) = 0$. As a consequence, $\ker(r_{v'})$ is as large as it could be:

$$\ker(r_{v'}) = H^1(F'_{v'}, A[p^\infty]).$$

This group is finite and isomorphic to $H^2(F'_{v'}, T_p(A))$. To see this we use the exact sequence $0 \to T_p(A) \to V_p(A) \to A[p^\infty] \to 0$ together with the fact that $H^i(F'_{v'}, V_p(A)) = 0$ for $i = 1, 2$. By using Tate's local duality theorem, one sees that $H^2(F'_{v'}, T_p(A))$ is dual to $H^0(F'_{v'}, A^t[p^\infty]) = A^t(F'_{v'})_p$, where A^t is the dual abelian variety. Thus $\ker(r_{v'})$ and $A^t(F'_{v'})_p$

have the same order. But since A and A^t are isogenous over F_v, we have $K_\eta = F_v(A^t[p^\infty])$. Thus, it is clear that $|\ker(r_{v'})|$ will be unbounded in this case. One can be somewhat more precise about the structure of $\ker(r_{v'})$ if one takes $F' = F_n = F(A[p^\infty])$ and if $v' = v_n$ is some prime of F_n lying above v. Then it is not hard to show that $\ker(r_{v_n}) \sim (\mathbb{Z}/p^n\mathbb{Z})^{2g}$ as $n \to \infty$. Here the notation $A_n \sim B_n$ as $n \to \infty$, where A_n, B_n are two sequences of groups, means that there are homomorphisms $f_n : A_n \to B_n$ whose kernels and cokernels are finite and of bounded order as $n \to \infty$.

III. *Arbitrary K/F.*

The Galois group $G(K_\eta/F_v)$ is a p-adic Lie group. Local class field theory implies that $\dim(G(K_\eta/F_v)) \leq 2$. If $G(K_\eta/F_v)$ is finite, there is little to say. The order of $\ker(r_{v'})$ is trivially bounded. (This can occur. For example, it is possible for a prime v of F to split completely in K/F, in which case $\ker(r_{v'}) = 0$.) If $\dim(G(K_\eta/F_v)) = 1$, then the Lie algebra of $G(K_\eta/F_v)$ is abelian. Let $K_\eta^u = K_\eta \cap F_v^{\mathrm{unr}}$. One must have $[K_\eta{:}K_\eta^u] < \infty$. Then, by using proposition 2.1, it is easy to verify that $|\ker(r_{v'})|$ is bounded.

Finally, if $\dim(G(K_\eta/F_v)) = 2$, it follows that G_{K_η} has profinite order relatively prime to p and hence $H^1(K_\eta, A[p^\infty]) = 0$. In this case, we have, as in II(ii),

$$\ker(r_{v'}) = H^1(F'_{v'}, A[p^\infty]),$$

which is isomorphic to $A^t(F'_{v'})\widehat{\ }_p$. This will be of bounded order if and only if $A^t(K_\eta)_p$ is finite. Note that $A^t(K_\eta)_p$ is finite if and only if $A(K_\eta)_p$ is finite. If we assume that A has good reduction at v', then the kernel of the reduction map $A(F'_{v'}) \to \widetilde{A}_{v'}(f_{v'})$ is a pro-l group, where $f_{v'}$ denotes the residue field for v' and l denotes its characteristic. Since the reduction map is surjective, it follows that $A(F'_{v'})_p \cong \widetilde{A}_{v'}(f_{v'})_p$. Also, A^t will have good reduction at v' and $A^t(F'_{v'})_p \cong \widetilde{A^t}_{v'}(f_{v'})_p$ will have the same order as $\widetilde{A}_{v'}(f_{v'})_p$. Thus, if A has good reduction at η, then $\ker(r_{v'})$ will have bounded order if and only if $\widetilde{A}(k_\eta)_p$ is finite, where k_η denotes the residue field of η. We also remark that, since K/F is a Galois extension, both $G(K_\eta/F_v)$ and $A(K_\eta)_p$ are independent of the choice of η lying over a fixed prime v of F.

(B) v archimedean.

We need only worry about the case when $p = 2$, $F'_{v'} = \mathbb{R}$, and $K_\eta = \mathbb{C}$. This does not occur when K/F is a $\mathbb{Z}_p$-extension, since archimedean primes of F will split completely in K/F. If $K = F(A[2^\infty])$, then $K_\eta = \mathbb{C}$ for all archimedean primes of K. If one restricts attention to fields F' which are totally complex (e.g. those containing $F(A[4])$), then again $\ker(r_{v'}) = 0$. Let K/F be arbitrary. Assume now that $F'_{v'} = \mathbb{R}$, $K_\eta = \mathbb{C}$. We again have $\mathrm{Im}(\kappa_{v'}) = 0$,

$\mathrm{Im}(\kappa_\eta) = 0$. Thus

$$\ker(r_{v'}) \cong H^1(\mathbb{C}/\mathbb{R}, A[2^\infty])$$

where one considers A as an abelian variety/$\mathbb{R}$ by the identification $F_v = \mathbb{R}$, (and v is the prime of F lying below v'). Let σ be the nontrivial element of $G(\mathbb{C}/\mathbb{R})$. Then we have $\ker(r_{v'}) \cong \ker(1+\sigma)/\mathrm{im}(1-\sigma)$, when $1+\sigma$, $1-\sigma$ are regarded as endomorphisms of $A[2^\infty]$. One verifies easily that

$$\ker(r_{v'}) \cong (\mathbb{Z}/2\mathbb{Z})^{e_v}$$

where $e_v = \dim_{\mathbb{Z}/2\mathbb{Z}}(A(\mathbb{R})[2]) - g$. This of course can be positive.

(C) $v|p$.

Before we discuss the special cases I and II, we must recall some of the results of [CG] and make some general observations. Let L be any algebraic extension of F_v. Let

$$\kappa_L : A(L) \otimes (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(L, A[p^\infty])$$

denote the Kummer homomorphism for A over L. Then κ_L is injective. If L is a finite extension of F_v, then as explained in [CG] (see page 150), we have

$$\mathrm{im}(\kappa_L) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{g[L:\mathbb{Q}_p]}, \qquad H^1(L, A[p^\infty])_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2g[L:\mathbb{Q}_p]} \tag{3}$$

as groups. On the other hand, a certain canonical G_{F_v}-invariant subgroup C of $A[p^\infty]$ is defined in [CG], p. 150–151, which can be characterized in the following way: $D = A[p^\infty]/C$ is the maximal G_{F_v}-quotient of $A[p^\infty]$ on which some subgroup of finite index in the inertia group I_v acts trivially. (That is, D is "almost" unramified.) This subgroup C is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^h$ as a group, where h is the height of the formal group $\mathcal{F}$ for a Neron model for A over the integers in a finite extension of F_v where A achieves semistable reduction. In fact, $C = \mathcal{F}(\overline{\mathfrak{m}})[p^\infty]$. (Later we may use the notation C_v for C and D_v for D.) We then define

$$\lambda_L : H^1(L, C) \to H^1(L, A[p^\infty]).$$

According to (4.9) of [CG], we have

$$\mathrm{im}(\kappa_L) \subseteq \mathrm{im}(\lambda_L)$$

for all L. Proposition 4.3 of [CG] states that equality holds if L is deeply ramified (e.g., if L/F_v is a p-adic Lie extension which is infinitely ramified).

Assume that the inertia subgroup of $G(K_\eta/F_v)$ is infinite. Then K_η is deeply ramified. For any L, let $\mathcal{H}_A(L) = H^1(L, A[p^\infty])/\mathrm{im}(\kappa_L)$ as before. Note that $\mathcal{H}_A(K_\eta) = H^1(K_\eta, A[p^\infty])/\mathrm{im}(\lambda_{K_\eta})$. Hence we can factor the map $r_{v'}$ as indicated by the following commutative diagram (where we let $\lambda_{v'} = \lambda_{F'_{v'}}$ for brevity):

$$\begin{tikzcd} \mathcal{H}_A(F'_{v'}) \arrow[r, "a_{v'}"] \arrow[dr, "r_{v'}"] & H^1(F'_{v'}, A[p^\infty])/\mathrm{im}(\lambda_{v'}) \arrow[d, "b_{v'}"] \\ & \mathcal{H}_A(K_\eta) \end{tikzcd} \tag{4}$$

We have $\ker(a_{v'}) \subseteq \ker(r_{v'})$ and

$$\ker(a_{v'}) \cong \mathrm{im}(\lambda_{v'})/\mathrm{im}(\kappa_{v'}), \qquad \ker(r_{v'})/\ker(a_{v'}) \cong \ker(b_{v'}),$$

the last isomorphism because $a_{v'}$ is surjective. Thus we can study $\ker(r_{v'})$ by studying $\mathrm{im}(\lambda_{v'})/\mathrm{im}(\kappa_{v'})$ and $\ker(b_{v'})$. $\mathrm{Ker}(b_{v'})$ can be studied by the following commutative diagram

$$\begin{tikzcd} H^1(F'_{v'}, C) \arrow[r, "\lambda_{v'}"] \arrow[d] & H^1(F'_{v'}, A[p^\infty]) \arrow[r, "\pi_{v'}"] \arrow[d] & H^1(F'_{v'}, D) \arrow[d, "d_{v'}"] \\ H^1(K_\eta, C) \arrow[r, "\lambda_\eta"] & H^1(K_\eta, A[p^\infty]) \arrow[r, "\pi_\eta"] & H^1(K_\eta, D). \end{tikzcd} \tag{5}$$

Thus obviously $\ker(b_{v'})$ is isomorphic to a subgroup of $\ker(d_{v'})$. In many cases, the map $\pi_{v'}$ is surjective and hence we would have $\ker(b_{v'}) \cong \ker(d_{v'})$. (This is true for example if A has potentially good reduction at v since then one sees easily that $H^2(F'_{v'}, C) = 0$.)

Assume that A has potentially ordinary reduction at v. Then, by proposition 4.5 of [CG], we have $\mathrm{im}(\kappa_{v'}) = \mathrm{im}(\lambda_{v'})_{\mathrm{div}}$. (This is not hard to show. It involves simply showing that $\mathrm{im}(\kappa_{v'}) \subseteq \mathrm{im}(\lambda_{v'})$ and that these groups have the same $\mathbb{Z}_p$-corank.) Using this, we can prove the following result. Here $C^t \subseteq A^t[p^\infty]$ and $D^t = A^t[p^\infty]/C^t$ are the G_{F_v}-modules associated to A^t which are defined analogously to C and D.

Proposition 2.2. *Assume that A has potentially ordinary reduction at v and that the inertia subgroup of $G(K_\eta/F_v)$ is infinite. Then $\ker(a_{v'})$ is finite and*

$$|\ker(a_{v'})| \le |H^0(F'_{v'}, D^t)|.$$

If A has good, ordinary reduction over $F'_{v'}$ then one has equality. In this case,

$$|\ker(a_{v'})| = |\widetilde{A}_{v'}(f'_{v'})_p|,$$

where $f'_{v'} = \mathcal{O}_{F'_{v'}}/\mathfrak{m}_{F'_{v'}}$ is the residue field for v' and $\widetilde{A}_{v'}$ is the reduction of A at v'.

Proof. We have $\ker(a_{v'}) \cong \mathrm{im}(\lambda_{v'})/\mathrm{im}(\lambda_{v'})_{\mathrm{div}}$. This is a homomorphic image of the group $H^1(F'_{v'}, C)/H^1(F'_{v'}, C)_{\mathrm{div}}$. Therefore

$$|\ker(a_{v'})| \leq |H^1(F'_{v'}, C)/H^1(F'_{v'}, C)_{\mathrm{div}}|.$$

Now $H^2(F'_{v'}, C) = 0$ and so, by considering the exact sequence

$$0 \to C[p^n] \to C \xrightarrow{p^n} C \to 0$$

for $n \gg 0$, one sees that $H^1(F'_{v'}, C)/H^1(F'_{v'}, C)_{\mathrm{div}} \cong H^2(F'_{v'}, C[p^n])$. This last group is dual to $H^0(F'_{v'}, D^t[p^n])$ which coincides with $H^0(F'_{v'}, D^t)$ for $n \gg 0$. This gives the inequality in proposition 2.2. The second part is part of proposition 4.6 of [CG]. ■

Remark. If L denotes a fixed finite extension of F_v where A (and hence A^t) has good reduction, then an obvious bound for $|H^0(F'_{v'}, D^t)|$ is $|H^0(F'_{v'}L, D^t)| = |\widetilde{A}^t(k')_p|$ where k' denotes the residue field of $F'_{v'}L$. Since k' is a finite field, $\widetilde{A}^t(k')_p$ and $\widetilde{A}(k')_p$ have the same order, although they are not necessarily isomorphic. If A has good, ordinary reduction over $F'_{v'}$, then we have

$$\ker(a_{v'}) \cong H^0(F'_{v'}, \widetilde{A}^t[p^\infty]) = \widetilde{A}^t(f'_{v'})_p.$$

We need one more general result.

Proposition 2.3. *Assume that A has good reduction at v and that K_η/F_v is unramified. Then $\ker(r_{v'}) = 0$ for all F' and all v'.*

Proof. Here we use the following consequence of Tate's duality theorem for abelian varieties over local fields. For any extension $K_\eta/F'_{v'}$, we have

$$\ker(r_{v'})\widehat{\ } \cong (A^t(F'_{v'})/N_{K_\eta/F'_{v'}}(A^t))_p.$$

Thus it suffices to prove that $N_{K_\eta/F'_{v'}}(A^t) = A^t(F'_{v'})$ under the above hypotheses. We have an exact sequence

$$0 \to \mathcal{F}_{A^t}(\mathfrak{m}_{F'_{v'}}) \to A^t(F'_{v'}) \to \widetilde{A}^t(f'_{v'}) \to 0$$

where $f'_{v'}$ is the residue field for $F'_{v'}$ and $\mathcal{F}_{A^t}$ is the formal group for a Neron model of A^t over $\mathcal{O}_{F_v}$. By proposition 3.9, of [CG], the norm map for a formal group is surjective for unramified extensions. Thus $\mathcal{F}_{A^t}(\mathfrak{m}_{F'_{v'}})$ is contained in $N_{K_\eta/F'_{v'}}(A^t)$. Hence it suffices to verify that if f''/f' is any finite extension, where $f' = f'_{v'}$, then

$$N_{f''/f'}(\widetilde{A^t}(f'')) = \widetilde{A^t}(f').$$

This amounts to the assertion that $H^2(f''/f', \widetilde{A}^t(f''))=0$ since $G(f''/f')$ is cyclic. Perhaps the simplest way to verify this is to note that $H^2(f''/f', \widetilde{A}^t(f''))$ has the same order as $H^1(f''/f', \widetilde{A}^t(f''))$. To prove this is trivial, it is then enough to show that $H^1(f', \widetilde{A}^t(\overline{f}'))=0$, where $\overline{f}'$ denotes an algebraic closure of f'. But this is not hard to show by using the facts that $G(\overline{f}'/f') \cong \widehat{\mathbb{Z}}$ and $\widetilde{A}^t(\overline{f}')$ is a divisible group.

I. *K/F is a $\mathbb{Z}_p$-extension.*

Assume first that K_η/F_v is unramified. (This can occur!) If A has good reduction over F_v, then proposition 2.3 asserts that $\ker(r_{v'})=0$. If A has potentially good reduction, then proposition 2.3 easily implies that $|\ker(r_{v'})|$ is bounded as F' varies.

Assume now that K_η/F_v is ramified and that A has potentially ordinary reduction. The inertia group $I(K_\eta/F_v)$ must have finite index in $G(K_\eta/F_v)$. This means that the residue field $f'_{v'}$ is of bounded degree over f_v, as F' varies. Then by proposition 2.2 and the subsequent remark it follows that $\ker(a_{v'})$ has bounded order. (In the case of good ordinary reduction the obvious fact that $A(f'_{v'})$ stabilizes is enough.) Now consider

$$d_{v'} : H^1(F'_{v'}, D) \to H^1(K_\eta, D).$$

We have $\ker(d_{v'}) \cong H^1(K_\eta/F'_{v'}, D(K_\eta))$. Let L be again a fixed finite extension of F_v where A has good reduction. Let k be the residue field for LK_η, which is a finite field. Thus $D(LK_\eta)=\widetilde{A}(k)_p$ is finite and therefore so is $D(K_\eta)$. It is then obvious that $\ker(d_{v'})$ and hence $\ker(b_{v'})$ are finite and of bounded order as F' varies. Combining these observations, it follows that $\ker(r_{v'})$ is finite and has bounded order as F' varies.

Under certain hypotheses we can assert that $\ker(r_{v'})=0$ for all F'. We have already shown this if v is unramified in K/F and A has good reduction over F_v. Assume now that v is ramified in K/F. Assume also that A has good ordinary reduction at v and that the order of $\widetilde{A}(f_v)$ is not divisible by p. Since $f'_{v'}/f_v$ is a p-extension, it clearly follows that $\widetilde{A}(f'_{v'})_p=0$ for all F'. Hence, by proposition 2.2, $\ker(a_{v'})=0$. The residue field k of K_η is also a finite p-extension of f_v. Thus $D(K_\eta)=\widetilde{A}(k)=0$ again. It follows that $\ker(b_{v'})=0$. Therefore the hypotheses that K/F is a $\mathbb{Z}_p$-extension, A has good, ordinary reduction at v, and $\widetilde{A}(f_v)_p=0$ are sufficient to conclude that $\ker(r_{v'})=0$ for all intermediate fields F'.

II. $K=F(A[p^\infty])$.

In this case we will show that $\ker(r_{v'})$ is finite but of unbounded order as F' varies, under the assumption that A has potentially ordinary reduction at v. The finiteness of $\ker(a_{v'})$ is clear because it is isomorphic to $\mathrm{im}(\lambda_{v'})/\mathrm{im}(\lambda_{v'})_{\mathrm{div}}$ and $H^1(F'_{v'}, C)$ is cofinitely generated over $\mathbb{Z}_p$. Now A achieves good, ordinary reduction over $F_v(A[p])$ for odd p (and over $F_v(A[4])$ if $p=2$).

Proposition 2.2 implies that $|\ker(a_{v'})|$ is unbounded since the same is true of $|\widetilde{A}(f'_{v'})_p|$. In fact, if we take $F' = F_n = F(A[p^n])$ for any $n \geq 2$ and if v_n is a prime of F_n lying above v, then $|\widetilde{A}(f_{v_n})_p| \geq p^{gn}$, where f_{v_n} denotes the residue field for v_n. We have $\ker(a_{v_n}) \cong \widetilde{A}^t(f_{v_n})$ and one can verify that $\ker(a_{v_n}) \sim (\mathbb{Z}/p^n\mathbb{Z})^g$ as $n \to \infty$.

Now we consider the finiteness of $\ker(d_{v'})$. Note that $D(K_\eta) = D$. Assume that $\mathcal{U}$ is any open pro-p subgroup of $G(K_\eta/F_v)$ such that the action of $\mathcal{U}$ on D is unramified. (For example, $\mathcal{U} = G(K_\eta/F_v(A[p^n]))$ for $n \geq 2$. We will add a few more requirements on the choice of $\mathcal{U}$ below.) It suffices to show that $H^1(\mathcal{U}, D)$ is finite. Let $\mathcal{V}$ denote the inertia subgroup of $\mathcal{U}$. Then $\mathcal{U}/\mathcal{V} \cong \mathbb{Z}_p$. Let $u \in \mathcal{U}$ be chosen so that $u\mathcal{V}$ is a topological generator of $\mathcal{U}/\mathcal{V}$. Then $H^0(\mathcal{U}, D) = \ker(u-1)$ is finite (as pointed out in the proof of proposition 2.2) and therefore $H^1(\mathcal{U}/\mathcal{V}, D) = D/(u-1)D$ is trivial. Also clearly $H^2(\mathcal{U}/\mathcal{V}, D) = 0$. Therefore,

$$H^1(\mathcal{U}, D) \cong H^1(\mathcal{V}, D)^{\mathcal{U}/\mathcal{V}} = \mathrm{Hom}_{\mathcal{U}/\mathcal{V}}(\mathcal{V}/\mathcal{V}', D).$$

Now $\mathcal{U}$ acts faithfully on the vector space $V = T_p(A) \otimes \mathbb{Q}_p$. Let $\widetilde{V} = T_p(\widetilde{A}) \otimes \mathbb{Q}_p$. (We assume that A has good reduction over $K_\eta^{\mathcal{U}}$.) Let $W = \ker(V \longrightarrow \widetilde{V})$. We will assume that $\mathcal{U}/\ker(\chi) \cong \mathbb{Z}_p$, where χ: $\mathcal{U} \to 1+p\mathbb{Z}_p$ denotes the cyclotomic character. Let $N = \mathcal{V} \cap \ker(\chi)$. Then $N \subseteq \mathcal{V} \subseteq \mathcal{U}$ and $\mathcal{U}/N \cong \mathbb{Z}_p^2$ is abelian. Now $\mathcal{V}$ acts trivially on $\widetilde{V}$ and by $\chi\big|_{\mathcal{V}}$ on W. Hence N is a subgroup of $\mathrm{Aut}(V)$ which acts trivially on both $\widetilde{V}$ and W and so can be identified with a subgroup of $\mathrm{Hom}(\widetilde{V}, W)$. This shows that N is abelian, isomorphic to $\mathbb{Z}_p^m$ for some $m \geq 0$, and also that $\mathcal{V}/N$ acts on N by $\chi\big|_{\mathcal{V}}$. It follows that $[N{:}\mathcal{V}'] < \infty$. The finiteness of $H^1(\mathcal{U}, D)$ follows immediately because $\mathrm{Hom}_{\mathcal{U}/\mathcal{V}}(\mathcal{V}/N, D)$ is isomorphic to $H^0(\mathcal{U}, D)$.

We can take $\mathcal{U} = G(K_\eta/(F_n)_{v_n})$ for $n \gg 0$, where as before $F_n = F(A[p^n])$ and v_n is a prime above v. The above discussion shows that $H^0(\mathcal{U}, D) \cong \widetilde{A}(f_{v_n})_p$ is a homomorphic image of $\ker(d_{v_n}) = H^1(\mathcal{U}, D)$. It follows that $\ker(d_{v_n})$ contains a subgroup isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^g$. Also, it is not difficult to verify that $\ker(d_{v_n}) \sim (\mathbb{Z}/p^n\mathbb{Z})^g$ as $n \to \infty$. We noted previously that the same statement is true for $\ker(a_{v_n})$. By carefully studying the structure of the groups $H^1((F_n)_{v_n}, C)$, $H^1((F_n)_{v_n}, A[p^\infty])$ and $H^1((F_n)_{v_n}, D)$, one can show that $\ker(r_{v_n}) \sim (\mathbb{Z}/p^n\mathbb{Z})^{2g}$ as $n \to \infty$.

We remark that the preceding discussion shows that K/F is admissible if A has potentially ordinary reduction at all primes $\mathfrak{p}$ of F lying over p, as we will now explain. We already mentioned that $G(K/F)$ is a p-adic Lie group and that K/F is Σ-ramified for a finite set Σ of primes of F. Now if we take $v = \mathfrak{p}$, then $\mathfrak{d}_\mathfrak{p}$ and $\mathfrak{i}_\mathfrak{p}$ are the Lie algebras for $\mathcal{U}$ and $\mathcal{V}$, respectively. The Lie algebra for N is $\mathfrak{i}'_\mathfrak{p}$, which coincides with $\mathfrak{d}'_\mathfrak{p}$ since $\mathfrak{d}_\mathfrak{p}/\mathfrak{i}'_\mathfrak{p}$ is the Lie algebra for the abelian group $\mathcal{U}/N$.

III. *Arbitrary K/F.*

Let $\mathfrak{d}_v$ denote the Lie algebra for $G(K_\eta/F_v)$. Let $\mathfrak{i}_v$ be the Lie subalgebra corresponding to the inertia subgroup of $G(K_\eta/F_v)$. Let $D(K_\eta) = H^0(K_\eta, D)$. We prove the following results, assuming still that A has potentially ordinary reduction at v. Note that if A has good reduction at v, then $D(K_\eta) = \widetilde{A}_v(k_\eta)$, where $\widetilde{A}_v$ is the reduction of A at v and k_η denotes the residue field for η.

Proposition 2.4. *Assume that $D(K_\eta)$ is finite. Then* $\ker(r_{v'})$ *is finite and has bounded order as F' and v' vary. In particular, this is true if $\mathfrak{d}_v = \mathfrak{i}_v$.*

Proposition 2.5. *Assume that $\mathfrak{d}_v' = \mathfrak{i}_v'$. Then* $\ker(r_{v'})$ *is finite.*

Proof of Proposition 2.4. Since A and A^t are isogenous over F_v, there is a surjective G_{F_v}-homomorphism from D^t to D, with finite kernel. Hence $D^t(K_\eta)$ is finite. Proposition 2.2 implies that $|\ker(a_{v'})|$ is bounded by $|D^t(K_\eta)|$. By lemma 0.1, we see that $H^1(\mathcal{U}, D(K_\eta))$ is finite and has bounded order, where $\mathcal{U}$ varies over all closed subgroups of $G(K_\eta/F_v)$. Thus $\ker(d_{v'})$ is finite and has bounded order. Note that the bound depends only on v and not on the choice of η lying over v. If $\mathfrak{d}_v = \mathfrak{i}_v$, then the residue field k_η of K_η is finite. Since A^t has potentially good, ordinary reduction at v, one can bound $|D^t(K_\eta)|$ by $|D^t(K_\eta')| = |\widetilde{A}^t(k_\eta')|$, where K_η' is a finite extension of K_η such that A^t has good reduction over K_η' and k_η' denotes the corresponding residue field, which will still be finite. ∎

It is worth remarking that if $G(K_\eta/F_v)$ is a pro-p group and if both $H^0(F_v, D)$ and $H^0(F_v, D^t)$ vanish, then $D(K_\eta) = D^t(K_\eta) = 0$ and so the above proof shows that $\ker(r_{v'}) = 0$ for all F' and v'. In particular, this is true if A has good, ordinary reduction at v, $p \nmid |\widetilde{A}(f_v)|$, and $G(K_\eta/F_v)$ is pro-p. For in this case, $\widetilde{A}(f_v)$ and $\widetilde{A^t}(f_v)$ have the same order and $H^0(F_v, D) = \widetilde{A}(f_v)_p$, $H^0(F_v, D^t) = \widetilde{A^t}(f_v)_p$ are both trivial. Since $G(K_\eta/F_v)$ is pro-p, it follows easily that $D(K_\eta)$ and $D^t(K_\eta)$ are both trivial.

Proof of Proposition 2.5. We might as well assume that $D(K_\eta)$ is infinite. We know that $\ker(a_{v'})$ is finite. We must show that $\ker(d_{v'})$ is also finite. But this follows essentially as in II above, using the hypothesis that $\mathfrak{d}_v' = \mathfrak{i}_v'$. It suffices to show that $H^1(\mathcal{U}, D(K_\eta))$ is finite for all sufficiently small open subgroups $\mathcal{U}$ of $G(K_\eta/F_v)$. (This then is true for all open $\mathcal{U}$.) We assume that $\mathcal{U}$ is pro-p, that the inertia subgroup $\mathcal{V}$ of $\mathcal{U}$ acts trivially on $D(K_\eta)$, and that $[\mathcal{U}' : \mathcal{V}'] < \infty$. Now clearly $H^0(\mathcal{U}, D(K_\eta))$ is finite and $\mathcal{U}/\mathcal{V} \cong \mathbb{Z}_p$. As in II, the inflation-restriction sequence shows that $H^1(\mathcal{U}, D(K_\eta))$ is isomorphic to $\mathrm{Hom}_{\mathcal{U}/\mathcal{V}}(\mathcal{V}/\mathcal{V}', D(K_\eta))$. But since $\mathcal{U}'/\mathcal{V}'$ is finite, it is enough to show that $\mathrm{Hom}_{\mathcal{U}/\mathcal{V}}(\mathcal{V}/\mathcal{U}', D(K_\eta))$ is finite. But this is obvious because $\mathcal{U}/\mathcal{V}$ acts trivially on $\mathcal{V}/\mathcal{U}'$, $H^0(\mathcal{U}, D(K_\eta))$ is finite, and $\mathcal{V}$ is topologically finitely generated. ∎

In the proof of proposition 2.5, the key fact is the finiteness of $\mathrm{Hom}_{\mathcal{U}/\mathcal{V}}(\mathcal{V}/\mathcal{V}', D(K_\eta))$ for all sufficiently small open subgroups $\mathcal{U}$ of $G(K_\eta/F_v)$. This leads to a simple necessary and sufficient condition for the conclusion of that proposition. Suppose that $\mathcal{U}$ is an open pro-p subgroup of $G(K_\eta/F_v)$, that its inertia subgroup $\mathcal{V}$ acts trivially on $D(K_\eta)$, and that the Lie algebra of $\mathcal{V}'$ is $\mathfrak{i}'_v$. (It can happen that the Lie algebra of $\mathcal{V}'$ is bigger than $\mathfrak{i}'_v$.) These assumptions hold for any sufficiently small open subgroup of $G(K_\eta/F_v)$. Let $u \in \mathcal{U}$ be chosen so that $u\mathcal{V}$ is the Frobenius element of $\mathcal{U}/\mathcal{V}$. Now the map $x \to uxu^{-1}$ for $x \in \mathcal{V}$ induces a linear transformation of the vector space $(\mathcal{V}/\mathcal{V}') \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ over $\mathbb{Q}_p$ (of dimension $e = \dim(\mathfrak{i}_v) - \dim(\mathfrak{i}'_v) \geq 0$) with eigenvalues $\{\alpha_s\}$, $1 \leq s \leq e$. (Counting multiplicity, although that will be of no importance.) Also, u acts linearly on the vector space $T_p(D(K_\eta)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, with eigenvalues $\{\beta_t\}$, $1 \leq t \leq f$. Here $T_p(D(K_\eta))$ is the Tate module for $D(K_\eta)$ and $f = \mathrm{corank}_{\mathbb{Z}_p}(D(K_\eta))$. On the residue field of K_η, u induces the map $y \to y^q$, where $q = p^m$ for some $m \geq 1$. We denote m by $\deg(u)$. We define the following sets:

$$(6) \qquad \mathcal{A}_v = \{\log_p(\alpha_s)/\deg(u)\}_{1 \leq s \leq e}, \qquad \mathcal{B}_v = \{\log_p(\beta_t)/\deg(u)\}_{1 \leq t \leq f}.$$

These sets are independent of the choice of $\mathcal{U}$. The first set depends only on the Galois extension K_η/F_v (and, in fact, only on K_η, which is independent of $\eta|v$). The second set depends only on the $G(\overline{k}/k)$-representation space $T_p(D(K_\eta)) \otimes \mathbb{Q}_p$, where k is the residue field of any finite extension of F_v over which A achieves good reduction. This representation space is a subspace of the $G(\overline{k}/k)$-representation space $T_p(\widetilde{A}) \otimes \mathbb{Q}_p$. Thus the β_t's are algebraic numbers (in fact, Weil numbers), since they are contained in the set of eigenvalues of a Frobenius automorphism acting on $T_p(\widetilde{A}) \otimes \mathbb{Q}_p$ (where one must suitably adjust the residue field). These eigenvalues are just the p-adic unit eigenvalues associated to $T_l(\widetilde{A}) \otimes \mathbb{Q}_l$ for any prime $l \neq p$. We remark that $\mathcal{A}_v = \phi$ when $\mathfrak{i}_v = \mathfrak{i}'_v$ and $\mathcal{B}_v = \phi$ when $D(K_\eta)$ is finite.

We will prove the following result.

Proposition 2.6. *Assume that A has potentially ordinary reduction at v. Then the following statements are equivalent:*

- *(a) $\ker(r_{v'})$ is finite for all F' and v'.*
- *(b) $\mathcal{A}_v$ and $\mathcal{B}_v$ are disjoint.*

Proof. By proposition 2.2, $\ker(a_{v'})$ is always finite. Thus (a) is equivalent to the assertion that $\ker(d_{v'})$ is always finite. We might as well assume that $\mathcal{U}/\mathcal{V} \cong \mathbb{Z}_p$. (Otherwise, $\mathcal{U} = \mathcal{V}$ and one sees easily that $D(K_\eta)$ is finite. Then $\mathcal{B}_v$ is empty and $\ker(r_{v'})$ is finite by proposition 2.4.) The finiteness of $\ker(d_{v'})$ for all F' and v' is equivalent to the finiteness of $\mathrm{Hom}_{\mathcal{U}/\mathcal{V}}(\mathcal{V}/\mathcal{V}', D(K_\eta))$ for all $\mathcal{U}$ as described above. If this last group is infinite for some choice of $\mathcal{U}$, then clearly $\{\alpha_s\}$ and $\{\beta_t\}$ will fail to be disjoint. Thus $\mathcal{A}_v \cap \mathcal{B}_v$ will be nonempty. Conversely, if $\mathcal{A}_v \cap \mathcal{B}_v$ is nonempty, then we will have $\alpha_s^{p^k} = \beta_t^{p^k}$ for some s, t, and k, where $1 \leq s \leq e$, $1 \leq t \leq f$, and $k \geq 0$. (Since $\mathcal{U}$ is pro-p, the α_s's, β_t's are principal units in some finite extension of $\mathbb{Q}_p$.) We can assume that $k = 0$, i.e., that $\alpha_s = \beta_t$ (replacing $\mathcal{U}$ by $\mathcal{U}^{p^k}\mathcal{V}$ if necessary). Thus α_s and β_t have the same minimal polynomial over $\mathbb{Q}_p$. Then the $(\mathcal{U}/\mathcal{V})$-representation space $(\mathcal{V}/\mathcal{V}') \otimes \mathbb{Q}_p$ will have a nontrivial quotient which is isomorphic to a $(\mathcal{U}/\mathcal{V})$-invariant subspace of $T_p(D(K_\eta)) \otimes \mathbb{Q}_p$. This will imply that $\mathrm{Hom}_{\mathcal{U}/\mathcal{V}}(\mathcal{V}/\mathcal{V}', D(K_\eta))$ is infinite for suitably chosen $\mathcal{U}$. ■

Our final result about the case $v|p$ is the following.

Proposition 2.7. *Assume that there is a continuous representation $\rho_v : G_{F_v} \to GL_n(\mathbb{Q}_p)$ such that $K_\eta = \overline{F}_v^{\ker(\rho_v)}$ and such that ρ_v is Hodge-Tate. Then $\mathfrak{d}_v' = \mathfrak{i}_v'$.*

Proof. G_{F_v} acts on the $\mathbb{Q}_p$-vector space $\mathfrak{d}_v$ through the natural adjoint representation of $G(K_\eta/F_v)$ on its Lie algebra $\mathfrak{d}_v$. Let $\sigma_v : G_{F_v} \to \mathrm{Aut}_{\mathbb{Q}_p}(\mathfrak{d}_v/\mathfrak{i}_v')$ be the induced representation. We have an exact sequence

$$0 \to \mathfrak{i}_v/\mathfrak{i}_v' \to \mathfrak{d}_v/\mathfrak{i}_v' \to \mathfrak{d}_v/\mathfrak{i}_v \to 0$$

of finite-dimensional $\mathbb{Q}_p$-representation spaces for G_{F_v}. Of course, we can assume that $\mathfrak{d}_v \neq \mathfrak{i}_v$ and so $\dim_{\mathbb{Q}_p}(\mathfrak{d}_v/\mathfrak{i}_v) = 1$. Let $\mathcal{U}$ be an open subgroup of $G(K_\eta/F_v)$ and let $\mathcal{V}$ denote the inertia subgroup of $\mathcal{U}$. If $\mathcal{U}$ is sufficiently small, then the Lie algebra of $\mathcal{V}$ will be $\mathfrak{i}_v$ and the Lie algebra of $\mathcal{V}'$ will be $\mathfrak{i}_v'$. Also, the adjoint representation of $\mathcal{U}$ induces the trivial representation on $\mathfrak{d}_v/\mathfrak{i}_v$. The adjoint representation of $\mathcal{V}$ induces the trivial representation on $\mathfrak{i}_v/\mathfrak{i}_v'$. Thus, if $\mathcal{U}$ is chosen sufficiently small, $\mathcal{V}$ acts trivially on both $\mathfrak{i}_v/\mathfrak{i}_v'$ and $\mathfrak{d}_v/\mathfrak{i}_v$. Therefore, these $\mathbb{Q}_p$-representation spaces of G_{F_v} are Hodge-Tate and the corresponding Hodge-Tate weights are all 0's. (Remark: The Hodge-Tate property for a representation of G_{F_v} and the corresponding weights are unaffected by replacing F_v by a finite extension $K_\eta^{\mathcal{U}}$. The weights depend only on the restriction to the inertia subgroup $G_{K_\eta^{\mathcal{V}}}$. For these elementary facts, see [Fo].)

The assumption that ρ_v is Hodge-Tate turns out to imply that σ_v is also Hodge-Tate. The corresponding weights for σ_v would be all 0's. According to a theorem of Sen (corollary to theorem 11 in [Se]), the image of the inertia subgroup $G_{F_v^{\mathrm{unr}}}$ under σ_v must then be finite. It follows that if $\mathcal{U}$ is chosen sufficiently small, the natural action of $\mathcal{V}$ on $\mathcal{U}/\mathcal{V}'$ by inner automorphisms will be trivial. That is, $\mathcal{V}/\mathcal{V}'$ will be a subgroup of the center of $\mathcal{U}/\mathcal{V}'$. Since $\mathcal{U}/\mathcal{V}$ is topologically cyclic, it then follows that $\mathcal{U}/\mathcal{V}'$ is abelian. But then $\mathcal{U}' = \mathcal{V}'$ and so $\mathfrak{d}_v' = \mathfrak{i}_v'$, as claimed.

It remains to show that σ_v is Hodge-Tate. The category of Hodge-Tate representation is closed under tensor products, contragredients, subrepresentations and quotients. Let V_p be the underlying $\mathbb{Q}_p$-vector space for ρ_v. Let $\rho_v^\vee$ denote the contragredient of ρ_v. Then $\rho_v \otimes \rho_v^\vee$ is Hodge-Tate. This representation describes the action of G_{F_v} on $\mathrm{Hom}(V_p, V_p)$. The Lie algebras $\mathfrak{d}_v$, $\mathfrak{i}_v$, and $\mathfrak{i}'_v$ are $\mathbb{Q}_p$-subspaces which are invariant under the action of G_{F_v}. The action on $\mathfrak{d}_v$ is the adjoint representation of $G(K_\eta/F_v)$. It follows that σ_v, which gives the action of G_{F_v} on $\mathfrak{d}_v/\mathfrak{i}'_v$ induced by that on $\mathrm{Hom}(V_p, V_p)$, must indeed be Hodge-Tate. ■

(D) The kernel of $r_{K/F'}$.

We will conclude this section by combining the previous observations to study the kernels of the following maps:

$$r_{K/F'} : \mathcal{P}_A(F') \to \mathcal{P}_A(K)$$

where K/F is a given p-adic Lie extension, S-ramified for some finite set S of primes of F, and F' varies over all finite extensions of F contained in K. We assume always that A has potentially ordinary reduction at all primes $\mathfrak{p}$ of F lying over p. The kernel of $g_{K/F'}$ is just $\ker(r_{K/F'}) \cap \mathcal{G}_A(F')$. Let Σ be a finite set of primes of F containing S, all primes lying over p and ∞, and all primes where A has bad reduction. If $v \notin \Sigma$, then proposition 2.1 implies that $\ker(r_{v'}) = 0$. Thus, in fact,

$$\ker(r_{K/F'}) \subseteq \mathcal{P}_A^\Sigma(F')$$

where $\mathcal{P}_A^\Sigma(F') = \prod_{v'} \mathcal{H}_A(F'_{v'})$, v' running over the set $\Sigma(F')$ of primes of F' lying over the primes in Σ. We regard $\mathcal{P}_A^\Sigma(F')$ as a subgroup of $\mathcal{P}_A(F')$. We first discuss two special cases.

I. *K/F is a $\mathbb{Z}_p$-extension.*

Let $v \in \Sigma$. If v splits completely in K/F, then $\ker(r_{v'}) = 0$ for all F' and all $v'|v$. If v does not split completely, then the decomposition subgroup of $G(K/F)$ for v has finite index, i.e., v is finitely decomposed in K/F. But our previous observations show that $|\ker(r_{v'})|$ is finite and has bounded order for all such v (and $v'|v$). Hence it follows that $\ker(r_{K/F'})$ is finite and of bounded order as F' varies.

II. $K = F(A[p^\infty])$.

Since we have shown that the groups $\ker(r_{v'})$ are all finite in this case, it follows that $\ker(r_{K/F'})$ is finite for all F'. But its order is unbounded as F' varies. In fact, $\ker(r_{K/F'})[p]$ is often of unbounded order. To discuss this, we will consider the subfields $F' = F_n = F(A[p^n])$ for $n \geq 0$. The growth of $\ker(r_{K/F_n})$ exhibits some regularities. Let $m = m_A$ denote the dimension of the p-adic Lie group $G(K/F)$. For every nonarchimedean prime $v \in \Sigma$, let m_v

denote the dimension of a decomposition subgroup $G(K_\eta/F_v)$ (for any $\eta|v$). Here we can take Σ to consist of all primes of F which divide p or ∞ or where A has bad reduction. For $n \gg 0$, $G(F_n/F)$ has order ap^{mn} and the image of $G(K_\eta/F_v)$ in $G(F_n/F)$ has order $bp^{m_v n}$, where $a, b > 0$ are fixed positive constants. Thus the number of primes of F_n lying over v is $tp^{(m-m_v)n}$ for $n \gg 0$, where $t = t_v > 0$. We denote any of these primes by v_n. Since F_n/F and K/F are Galois, the structure of the group $\ker(r_{v_n})$ is the same for all primes v_n of F_n lying over v. There are several distinct cases:

(i) *$v|l$, $l \neq p$ or ∞, A has potentially good reduction at v.* Then A has good reduction over $(F_n)_{v_n}$ for $n \geq 1$ (or $n \geq 2$ if $p = 2$) and all $v_n|v$. Also, K/F_n is unramified at v_n. Thus, by proposition 2.1, we then have $\ker(r_{v_n}) = 0$.

(ii) *$v|l$, $l \neq p$ or ∞, A does not have potentially good reduction at v.* In this case $\ker(r_{v_n})$ coincides with the corresponding factor $H^1((F_n)_{v_n}, A[p^\infty])$ in $\mathcal{P}_A^\Sigma(F_n)$, which is isomorphic to $A^t((F_n)_{v_n})_p$. Thus, $\ker(r_{v_n})$ has unbounded exponent as n varies, but $\ker(r_{v_n})[p]$ has order p^{2g} for $n \gg 0$.. As pointed out earlier, $m_v = 2$. The number of such v_n's is $t_v p^{(m-2)n}$ for large n.

(iii) $v|p$. From our earlier discussion, it is clear that $\ker(r_{v_n})$ has unbounded exponent since that is true for $\ker(a_{v_n})$. But $\ker(a_{v_n})[p]$ has order p^g for $n \geq 1$ and $H^1(\mathcal{U}, D)[p]$ also has bounded order as $\mathcal{U}$ varies over open subgroups of $G(K_\eta/F_v)$. (See the remark preceding lemma 0.2.) Thus $|\ker(r_{v_n})[p]|$ is at least p^g, and is bounded as n varies. It is clear that $m_v \geq 2$.

(iv) $v|\infty$. The infinite primes of F_2 are complex. Thus $\ker(r_{v_n}) = 0$ when $n \geq 2$ in this case. Note however that, if v is real, then there will be subfields F' of K of arbitrarily high degree in which v splits completely. Then, if $e_v > 0$ and if $p = 2$, the archimedean contribution to $\ker(r_{K/F'})$ will be of exponent 2 but of unbounded order.

We have the following consequences. The exponent of $\ker(r_{K/F_n})$ is unbounded as $n \to \infty$. The order of $\ker(r_{K/F_n})[p]$ is also unbounded unless $m_v = m$ for all primes of F lying over p or where A does not have potentially good reduction. This condition is quite stringent, but it does hold, for example, when A is an elliptic curve with complex multiplication. In that case, A has potentially good reduction at all primes and $m_v = m = 2$ when $v|p$. It is possible that no examples exist with $m > 2$.

III. *Arbitrary K/F.*

We immediately have the following result.

Proposition 2.8. *Assume that K/F is admissible. Then* $\ker(r_{K/F'})$ *is finite for all finite extensions F' of F contained in K.*

Remark. The conclusion that $\ker(r_{K/F'})$ is always finite is valid under the following substantially weaker hypothesis: $\mathcal{A}_v \cap \mathcal{B}_v = \phi$ *for all primes v of F lying over p.* Here $\mathcal{A}_v$ and $\mathcal{B}_v$ are the sets $\mathcal{A}$ and $\mathcal{B}$ defined in (6), which depend only on A, v, and K/F.

Under various sets of hypotheses on A and on K/F, one can prove more precise statements about $\ker(r_{K/F'})$. To simplify our remarks, we assume that A has good, ordinary reduction at all v lying over p. We let $\Sigma = \Sigma_\infty \cup \Sigma_p \cup \Sigma_{\text{bad}} \cup \Sigma_{\text{ram}}$, where Σ_∞ denotes the set of archimedean primes of F, Σ_p the set of primes lying over p, Σ_{bad} the set of primes where A has bad reduction, and Σ_{ram} the set of primes ramified in K/F. We are assuming that $\Sigma_p \cap \Sigma_{\text{bad}} = \phi$, although it is likely that $\Sigma_p \cap \Sigma_{\text{ram}} \neq \phi$ and possible that $\Sigma_{\text{bad}} \cap \Sigma_{\text{ram}} \neq \phi$. We will discuss several types of behavior for $\ker(r_{K/F'})$, being content in each case to give convenient sufficient conditions for that behavior. For $v \notin \Sigma$, proposition 2.1 shows that the contributions of $\ker(r_{v'})$ to $\ker(r_{K/F'})$ is trivial for all $v'|v$. Hence it is enough to study the behavior of the contributions when $v \in \Sigma$, which our previous observations in this section determine.

(i) *When is* $\ker(r_{K/F'}) = 0$ *for all F'?* Here is a set of sufficient conditions:

> *For $v \in \Sigma_p$: $\widetilde{A}_v(k_\eta)_p = 0$, where k_η denotes the residue field for K corresponding to some $\eta|v$ and $\widetilde{A}_v$ denotes the reduction of A modulo v.*
>
> *For $v \in \Sigma$ but $\notin \Sigma_p \cup \Sigma_\infty$: $A(K_\eta)_p = 0$ if $v \in \Sigma_{\text{ram}}$; $A(K_\eta)_p$ is divisible if $v \notin \Sigma_{\text{ram}}$.*
>
> *For $v \in \Sigma_\infty$: If $p = 2$, $F_v \cong \mathbb{R}$, and $K_\eta \cong \mathbb{C}$, then $A(F_v)$ is connected. No condition if $p \neq 2$ or if $F_v = K_\eta$.*

The sufficiency of this set of conditions is easy to explain. For $v|\infty$, if $A(F_v)$ is connected, then the integer e_v defined in **B** is zero. For $v|p$, if $\widetilde{A}(k_\eta)_p = 0$, then $\ker(a_{v'}) = 0$ by proposition 2.2 and $\ker(d_{v'}) = 0$ simply because $D(K_\eta) = 0$. For $v \notin \Sigma_p \cup \Sigma_\infty \cup \Sigma_{\text{ram}}$, the triviality of $\ker(r_{v'})$ if $A(K_\eta)_p$ is divisible follows from the remark after the proof of proposition 2.1.

In the conditions for nonarchimedean $v \in \Sigma$, if $G(K_\eta/F_v)$ happens to be pro-p, then one can simply require that

$$\widetilde{A}(f_v)_p = 0 \textit{ for } v|p \textit{ and } A(F_v)_p = 0 \textit{ for } v \not| p,$$

which would be easier to verify.

(ii) *When is* $\ker(r_{K/F'}) \neq 0$ *for all F'?* Here are two sufficient conditions.

There is a $v \in \Sigma_p$ *such that* $\mathfrak{i}_v \neq 0$ *and* $\widetilde{A}_v(f_v)_p \neq 0$.

or

There is a $v \notin \Sigma_p$ *such that* $m_v = 2$ *and* $A^t(F_v)_p \neq 0$.

For the first condition, note that $\widetilde{A}_v(f'_{v'})_p \neq 0$ for any F' and any $v'|v$, where $f'_{v'}$ denotes the residue field for v'. Also, since $\mathfrak{i}_v \neq 0$, K_η/F_v is a deeply ramified extension. Then, by (4), we have $\ker(r_{v'}) \supset \ker(a_{v'})$ and, by proposition 2.2, we have $\ker(a_{v'}) \neq 0$. For the second condition, note that since $m_v = 2$, we have $\ker(r_{v'}) = H^1(F'_{v'}, A[p^\infty])$ and this group has the same order as $A^t(F'_{v'})_p$. Since $A^t(F_v)_p \subset A^t(F'_{v'})_p$, we have $\ker(r_{v'}) \neq 0$.

(iii) *When is the exponent of* $\ker(r_{K/F'})$ *bounded?* We give a set of necessary and sufficient conditions:

For $v \in \Sigma_p$, *either* $\mathfrak{i}_v = 0$ *or* $\widetilde{A}(k_\eta)_p$ *is finite.*

For $v \notin \Sigma_p \cup \Sigma_\infty$, *either* $m_v < 2$ *or* $m_v = 2$ *and* $A(K_\eta)_p = 0$.

If $\mathfrak{i}_v = 0$ for $v|p$, then the inertia subgroup of $G(K_\eta/F_v)$ is finite. One can then apply proposition 2.3 (first taking a suitably fixed finite extension of F_v). If $\mathfrak{i}_v \neq 0$, then K_η is deeply ramified. One can apply proposition 2.2. The finiteness of $\widetilde{A}(k_\eta)_p$ is equivalent to the assertion that $\ker(a_{v'})$ has bounded exponent. (Note: $|\ker(a_{v'})[p]|$ is bounded.) The finiteness of $\widetilde{A}(k_\eta)_p$ also implies that the order of $\ker(d_{v'})$ is bounded. If $\mathfrak{i}_v = \mathfrak{d}_v$, then k_η is itself finite and hence so is $\widetilde{A}(k_\eta)_p$. But if $\mathfrak{i}_v \neq \mathfrak{d}_v$, then G_{k_η} has profinite order prime to p. Hence $\widetilde{A}(k_\eta)_p$ is divisible. Thus $\widetilde{A}(k_\eta)_p$ is finite if and only if $\widetilde{A}(k_\eta)_p = 0$, in the case where $\mathfrak{i}_v \neq \mathfrak{d}_v$.

If $v \in \Sigma_\infty$, then $\ker(r_{v'})$ has exponent at most 2. Now assume that $v \notin \Sigma_p \cup \Sigma_\infty$. Then our remarks in (**A**), III show that $\ker(r_{v'})$ has bounded order if and only if either $m_v < 2$ or $m_v = 2$ and $A(K_\eta)_p$ is finite. The boundedness of the order and of the exponent are equivalent since $|\ker(r_{v'})[p]|$ is certainly bounded. If $m_v = 2$, then G_{K_η} has profinite order prime to p. Hence $A(K_\eta)_p$ must be divisible. Therefore, in this case, the finiteness of $A(K_\eta)_p$ is equivalent to $A(K_\eta)_p = 0$.

(iv) *When is* $\ker(r_{K/F'})[p]$ *of bounded order?* Here is a sufficient condition:

For all $v \in \Sigma$ *such that* $m_v < m$, *we have* $\ker(r_{v'}) = 0$ *for all* $v'|v$.

Note first that, for any fixed v, $|\ker(r_{v'})[p]|$ has bounded order. Also, note that the number of primes v' of F' lying over v is bounded (as F' varies) if and only if $m_v = m$.

Sufficient conditions for the triviality of $\ker(r_{v'})$ are described above (for the question about when $\ker(r_{K/F'}) = 0$). Note that $m_v = 0$ for archimedean primes, which can be important if $p = 2$. As we pointed out in the case $K = F(A[p^\infty])$ and as later examples will illustrate, it is often true that $\ker(r_{K/F'})[p]$ has unbounded order.

(E) The kernel of $g_{K/F'}$.

The above results help to study the behavior of $\ker(g_{K/F'}) = \ker(r_{K/F'}) \cap \mathcal{G}_A(F')$. Now, as mentioned at the beginning of **(D)**, we have $\ker(r_{K/F'}) \subset \mathcal{P}_A^\Sigma(F')$, where Σ is a finite set of primes of F containing $\Sigma_\infty, \Sigma_p, \Sigma_{\text{bad}}$, and Σ_{ram}. Then $K \subset F_\Sigma$, the maximal extension of F unramified outside Σ. We let $\mathcal{G}_A^\Sigma(F')$ denote the image of the map

$$\gamma_{F'} : H^1(F_\Sigma/F', A[p^\infty]) \to \mathcal{P}_A^\Sigma(F').$$

Then we have $\ker(g_{K/F'}) = \ker(r_{K/F'}) \cap \mathcal{G}_A^\Sigma(F')$. That is, $\ker(g_{K/F'})$ is just the kernel of the natural map

$$\ker(r_{K/F'}) \to \mathcal{P}_A^\Sigma(F')/\mathcal{G}_A^\Sigma(F').$$

One can study $\text{coker}(\gamma_{F'}) = \mathcal{P}_A^\Sigma(F')/\mathcal{G}_A^\Sigma(F')$ by using the global duality theorems of Poitou and Tate and hence obtain information about the structure of $\ker(r_{K/F'})/\ker(g_{K/F'})$. Referring to proposition 4.13 in [G1], which gives a rather general result about this, one has

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(\text{coker}(\gamma_{F'})[p]) \leq \rho_{F'} + 2\dim(A), \tag{7}$$

where $\rho_{F'} = \text{corank}_{\mathbb{Z}_p}(\text{Sel}_A(F')_p)$. Also, $\text{corank}_{\mathbb{Z}_p}(\text{coker}(\gamma_{F'})) \leq \rho_{F'}$. If $\rho_{F'} = 0$, then $\text{coker}(\gamma_{F'}) \cong \widehat{A^t(F')}_p$.

Assuming the finiteness of $\text{Ш}_A(F')_p$, we would have $\rho_{F'} = \text{corank}_{\mathbb{Z}}(A(F'))$. Very little is known about the behavior of this quantity as F' varies. (See chapter 1 of [G2] for a discussion of this in some cases.) On the other hand, it is relatively easy to study the behavior of $\ker(r_{K/F'})$. For example, if $K = F(A[p^\infty])$, then we remarked at the end of **D**II that $\dim_{\mathbb{Z}/p\mathbb{Z}}(\ker(r_{K/F_n})[p])$ is unbounded as $n \to \infty$ unless A satisfies a rather stringent condition. We do not know when $\dim_{\mathbb{Z}/p\mathbb{Z}}(\ker(g_{K/F_n})[p])$ is unbounded, but a sufficient condition for this would be that $\dim_{\mathbb{Z}/p\mathbb{Z}}(\ker(r_{K/F_n})[p]) - \rho_{F_n}$ is unbounded. We will discuss the behavior of $\ker(g_{K/F'})$ further in sections 3 and 4.

3 Control Theorems.

We can now discuss the kernels and cokernels of the maps $s_{K/F'}$. We first consider the two special cases.

I. *K/F is a $\mathbb{Z}_p$-extension.*

From section 1 we see that $\ker(h_{K/F'})$ is finite and of bounded order as F' varies. We also see that $\operatorname{coker}(h_{K/F'}) = 0$. Section 2 shows that $\ker(r_{K/F'})$ is finite and of bounded order, assuming of course that A has potentially ordinary reduction at all primes v of F lying over p. The exact sequence (1) then gives the following result, slightly generalizing proposition 6.4(i) of Mazur [M].

Proposition 3.1. *Assume that A has potentially ordinary reduction at all primes of F lying over p. Let K be any $\mathbb{Z}_p$-extension of F. Then the kernel and cokernel of $s_{K/F'}$ are finite and of bounded order as F' varies.*

If $A(F)_p = 0$, then $A(K)_p = 0$ also, and hence $\ker(h_{K/F'})$ is trivial. Therefore, $s_{K/F'}$ is injective for all F'. It is possible for $s_{K/F'}$ to be injective even if $A(F)_p \neq 0$. To simplify our discussion of this, we will assume that A has good ordinary reduction at all $v|p$. For such v, we define $\Phi_v = \ker\Big(A(F_v)_p \to \widetilde{A}_v(f_v)_p\Big)$, where f_v is the residue field of F_v and the map is reduction modulo v. For nonarchimedean primes v not lying over p, we define $\Phi_v = A(F_v) \cap (A(F_v^{\mathrm{unr}})_p)_{\mathrm{div}}$. For all v, Φ_v is a subgroup of $A(F_v)_p$. If $v \nmid p$ and A has good reduction at v, then $\Phi_v = A(F_v)_p$. We define the following subgroup of $A(F)_p$:

$$\Phi = \bigcap_v (A(F) \cap \Phi_v),$$

where the intersection is over all nonarchimedean primes v of F. (It suffices to let v run over $\Sigma_p \cup \Sigma_{\mathrm{bad}}$.) We then have the following result.

Proposition 3.2. *Assume that K/F is a $\mathbb{Z}_p$-extension in which every $v \in \Sigma_p$ is ramified and every $v \in \Sigma_{\mathrm{bad}}$ is finitely decomposed. (For example, the cyclotomic $\mathbb{Z}_p$-extension of F has these properties.) Assume that A has good, ordinary reduction at the primes of F lying above p. Suppose also that $\Phi = 0$. Then $s_{K/F'}$ is injective if $[F' : F] \gg 0$.*

Proof. For $v \in \Sigma_p$, let I_v denote the corresponding inertia subgroup of $\Gamma = G(K/F)$. For $v \in \Sigma_{\mathrm{bad}}$, let Γ_v denote the corresponding decomposition subgroup of Γ. (Note: $v \nmid p$ implies that v is unramified in K/F.) By assumption, the I_v's and Γ_v's have finite index in Γ. Now $A(K)_p$ is in fact finite. This follows easily from the hypothesis that I_v is nontrivial for all $v \in \Sigma_p$. Now choose an open subgroup $\mathcal{U}$ of Γ such that $\mathcal{U} \subseteq I_v$ for $v \in \Sigma_p$, $\mathcal{U} \subseteq \Gamma_v$ for $v \in \Sigma_{\mathrm{bad}}$, $\mathcal{U}$ acts trivially on $A(K)_p$, and on $A(K_\eta)_p/(A(K_\eta)_p)_{\mathrm{div}}$ for all $v \in \Sigma_{\mathrm{bad}}$, where η is any prime of K lying over v. Such a choice of $\mathcal{U}$ is clearly possible. Let F' be such that $G(K/F') \subseteq \mathcal{U}$. Then we will show that $\ker(s_{K/F'}) = 0$.

Suppose to the contrary that $\ker(s_{K/F'})$ contains a nonzero element σ. Now $A(K)_p = A(F')_p$ and so $\sigma \in \mathrm{Hom}(G(K/F'), A(F')_p)$. For each $v \in \Sigma_p \cup \Sigma_{\mathrm{bad}}$, and for any $v'|v$, let $\sigma_{v'} = \sigma\big|_{G_{F'_{v'}}}$, regarded as a 1-cocycle with values in $A[p^\infty]$. Also, for each such v', define a subgroup $\Phi_{v'}$ of $A(F'_{v'})_p$ just as Φ_v was defined above for F_v. For $v \in \Sigma_p$, we have $\sigma_{v'} \in \mathrm{im}(\lambda_{v'})$ since $\sigma \in \mathrm{Sel}_A(F')_p$. Now the inertia subgroup $I_{F'_{v'}}$ acts trivially on $\widetilde{A}[p^\infty]$, which implies that $\sigma_{v'}\big|_{I_{F'_{v'}}}$ has values in C_v. Since v' is totally ramified in K/F', it follows that $\mathrm{im}(\sigma') = \sigma_{v'}(I_{F'_{v'}})$ is contained in $A(F')_p \cap \Phi_{v'}$. Consider $v \in \Sigma_{\mathrm{bad}}$. Then $\sigma_{v'} = 0$ in $H^1(F_{v'}, A[p^\infty])$. But $\sigma_{v'}$ is in the subgroup $H^1(G(K_\eta/F'_{v'}), A(K_\eta)_p)$, which is canonically isomorphic to $\mathrm{Hom}(G(K_\eta/F'_{v'}), A(K_\eta)_p/(A(K_\eta)_p)_{\mathrm{div}})$. Thus, the values of $\sigma_{v'}$ are in $(A(K_\eta)_p)_{\mathrm{div}} = A(K_\eta) \cap (A(F_v^{\mathrm{unr}})_p)_{\mathrm{div}}$. (Note: $G(F_v^{\mathrm{unr}}/K_\eta)$ has profinite order prime to p.) Thus, the values of σ are in $\Phi' = \bigcap_{v'} (A(F')_p \cap \Phi_{v'})$. But one verifies easily that $\Phi = (\Phi')^{G(F'/F)}$. Hence $\Phi' = 0$ since $G(F'/F)$ is a p-group. Thus $\sigma' = 0$, showing that $s_{K/F'}$ is injective when $G(K/F') \subseteq \mathcal{U}$. ■

If $\Phi \neq 0$, then one can reverse the above proof to show that $\ker(r_{K/F'}) \neq 0$ when $[F' : F] \gg 0$ provided that $\mathrm{im}(\lambda_{v'})$ is divisible for all $v'|p$ (and so coincides with $\mathrm{im}(\kappa_{v'})$). This would be true if $\widetilde{A}_v(f_v)_p = 0$ for all primes v of F lying above p. For then we also have $\widetilde{A}_v(f_{v'})_p = 0$ for $v'|v$ and this means that $\mathrm{im}(\lambda_{v'})$ is indeed divisible (as a consequence of proposition 2.2).

It is possible for $s_{K/F}$ to have a nontrivial kernel even if $\Phi = 0$. For example, one might have $A(K)_p = A(F)_p$ and a nontrivial 1-cocycle in $H^1(\Gamma, A(K)_p) = \mathrm{Hom}(\Gamma, A(F)_p)$ could have trivial restrictions to some or all of the decomposition subgroups of Γ for primes in Σ_p or Σ_{bad}.

Consider the special case where $F = \mathbb{Q}$ and $K = \mathbb{Q}_\infty$, the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Then p is totally ramified in $\mathbb{Q}_\infty/\mathbb{Q}$. If p is odd, then $\Phi = 0$. This is clear since the inertia subgroup of $G_{\mathbb{Q}_p}$ acts on $\ker(A[p] \to \widetilde{A}_p[p])$ by the Teichmüller character ω, which has order $p - 1 > 1$. The proof of proposition 3.2 shows that $\ker(s_{\mathbb{Q}_\infty/\mathbb{Q}}) = 0$ too. But for $p = 2$, it is possible that $\Phi \neq 0$ and, nevertheless, it still turns out that $\ker(s_{\mathbb{Q}_\infty/\mathbb{Q}}) = 0$. (We will not go into the proof of this last assertion here. It involves identifying the elements of order p in $H^1(\mathbb{Q}_p, C_p)_{\mathrm{div}}$, where $C_p = \ker(A[p^\infty] \to \widetilde{A}_p[p^\infty])$.) An example where $\Phi \neq 0$ is the elliptic curve A defined by $y^2 + xy = x^3 - 784x - 8515$. The conductor of this curve is 21. It has good, ordinary reduction at $p = 2$ and multiplicative reduction at 3 and 7. One sees easily that $\Phi_v \neq 0$ for $v \in \{2, 3, 7\}$. The discriminant for this curve is $3 \cdot 7^2$ and so $\mathbb{Q}(A[2]) = \mathbb{Q}(\sqrt{3})$. Since $\sqrt{3} \notin \mathbb{Q}_v$ for $v = 2, 3$, and 7, it follows that $A(\mathbb{Q}_v)[2] \cong \mathbb{Z}/2\mathbb{Z}$ and hence $\Phi_v[2] = A(\mathbb{Q}_v)[2]$ for those primes. But $A(\mathbb{Q})$ has order 2 itself. Therefore, it is clear that $\Phi = A(\mathbb{Q})$ for the above elliptic curve A.

Our results in section 2 give a sufficient condition for $\mathrm{coker}(s_{K/F'}) = 0$ to hold for all F', namely: *If* $v \in \Sigma_p$ *and is ramified in* K/F, *then* $p \nmid |\widetilde{A}(f_v)|$. *If* $v \in \Sigma_{\mathrm{bad}}$, *then* $A(F_v^{\mathrm{unr}})_p$ *is divisible.* No condition is needed for $v|\infty$, since archimedean primes split completely in K/F. We also note that, for $v \in \Sigma_{\mathrm{bad}}$, it would suffice that $A(F_v)_p = 0$. For then $A(K_\eta)_p = 0$.

II. $K = F(A[p^\infty])$.

Applying the results of sections 1 and 2 to this case provides a proof of theorem 4 stated in the introduction. For we have shown that $\ker(h_{K/F'})$ and $\mathrm{coker}(h_{K/F'})$ are finite. With the hypothesis on the behavior of A at $v|p$, we have seen that $\ker(r_{K/F'})$, and hence $\ker(g_{K/F'})$, is finite. Therefore, diagram (1) again implies the finiteness of the kernel and cokernel of $s_{K/F'}$, proving theorem 4.

We noted in section 1 that $\ker(h_{K/F'})$ has unbounded order. But, nevertheless, we can prove the following result.

Proposition 3.3. *Suppose that* $\dim(A) = 1$ *and that* A *has potentially ordinary reduction at all* $v|p$. *For* $n \geq 0$, *let* $F_n = F(A[p^n])$. *Let* $K = F(A[p^\infty])$. *Then* $\ker(s_{K/F_n})$ *has bounded order as* n *varies.*

Proof. We will use the notation and observations given in section 1, II. Thus

$$\ker(h_{K/F_n}) = \mathrm{Hom}(G(M_n/F_n), A[p^n]).$$

Suppose that $\sigma : G(M_n/F_n) \to A[p^n]$ is an arbitrary element of $\ker(h_{K/F_n})$. We will show that if $\sigma \in \ker(s_{K/F_n}) = \ker(h_{K/F_n}) \cap \mathrm{Sel}_A(F_n)_p$, then the order of σ is bounded independently of n. (We will only use the local conditions for primes of F_n lying above p to show this.) This suffices because $\ker(h_{K/F_n})[p]$ is of bounded order too. Assuming that $n \gg 0$, σ will factor through $G(L_n/F_n)$, where $L_n = M_n \cap F_{2n}$. We have $G(L_n/F_n) \cong (\mathbb{Z}/p^n\mathbb{Z})^{m-1}$. If v_n is any prime of F_n lying above p, let I_{v_n} denote the corresponding inertia subgroup of $G(L_n/F_n)$. Replacing F by F_1 (or F_2 if $p = 2$) if necessary, we can assume that A has good, ordinary reduction at the primes of F lying above p. If v is the prime of F lying below v_n, let $\widetilde{A}_v$ denote A modulo v and let $C_{v_n} = \ker(A[p^n] \to \widetilde{A}_v[p^n])$, where the map is reduction modulo v_n. Since I_{v_n} acts trivially on $\widetilde{A}_v[p^n]$, it follows that if $\sigma \in \ker(s_{K/F_n})$, then

$$\sigma(I_{v_n}) \subset C_{v_n}$$

for all primes v_n of F lying above p.

Let $T_p(A)$ denote the Tate module for A. If η is any prime of K lying above v (a prime of F above p), let $U_\eta = \ker(T_p(A) \to T_p(\widetilde{A}_v))$. Then $U_\eta \cong \mathbb{Z}_p$, $T_p(A)/U_\eta \cong \mathbb{Z}_p$, and the action of $G(K_\eta/F_v)$ on this quotient is given by an unramified character $\psi : G(K_\eta/F_v) \to \mathbb{Z}_p^\times$ of infinite order. Now there must be a prime η' of K lying above p such that $U_{\eta'} \neq U_\eta$. For otherwise, $U = U_\eta$ would be invariant under the action of $G(K/F)$ and this Galois group would act on $T_p(A)/U$ by a character $\Psi : G(K/F) \to \mathbb{Z}_p^\times$ which has infinite order and is unramified at *all* primes of F lying above p. But it is easy to see that no such Ψ exists. Thus, we can choose η' so that $U_{\eta'} \neq U_\eta$. It follows that $U_\eta + U_{\eta'}$ is a subgroup of $T_p(A)$ of finite index p^k.

Suppose that v_n and v_n' are the primes of F_n lying below η and η', respectively. Then C_{v_n} and $C_{v_n'}$ are the images of U_η and $U_{\eta'}$ under the natural map $T_p(A) \to A[p^n]$. Now $|C_{v_n} \cap C_{v_n'}|$ is equal to the index of $C_{v_n} + C_{v_n'}$ in $A[p^n]$, and this is bounded by p^k for all n. Let $J = I_{v_n} \cap I_{v_n'}$. If $\sigma \in \ker(s_{K/F_n})$, we must have $\sigma(J) \subset C_{v_n} \cap C_{v_n'}$. That is, $\sigma|_J$ has order bounded by p^k. Furthermore, if $g \in G(F_n/F)$, then g acts on $G(L_n/F_n)$ as an inner automorphism. We have $I_{g(v_n)} = g(I_{v_n})$ and $C_{g(v_n)} = g(C_{v_n})$, and similarly for v_n'. It follows that $\sigma(g(J)) \subset g(C_{v_n} \cap C_{v_n'})$ if $\sigma \in \ker(s_{K/F_n})$, and hence $\sigma|_{g(J)}$ has order $\leq p^k$. Let V_n be the subgroup of $G(L_n/F_n)$ generated by the subgroups $g(J)$, $g \in G(F_n/F)$. Then if $\sigma \in \ker(s_{K/F_n})$, it follows that $\sigma|_{V_n}$ has order bounded by p^k. To prove the proposition, it is enough to show that $[G(L_n/F_n) : V_n\}$ is bounded as $n \to \infty$.

The action of $G(K_\eta/F_v)$ on $T_p(A)$ is triangular. If $g \in G(K_\eta/F_v)$, then g acts on $T_p(A)$ by a matrix $\begin{bmatrix} \varphi(g) & * \\ 0 & \psi(g) \end{bmatrix}$. Here ψ is an unramified character of infinite order and $\varphi = \chi\psi^{-1}$, where χ denotes the cyclotomic character. If A has complex multiplication, then this action is diagonalizable and $G(K_\eta/F_v)$ is a 2-dimensional p-adic Lie group. Its inertia subgroup $I(K_\eta/F_v)$ is 1-dimensional.. If A does not have complex multiplication, then it can be shown that $G(K_\eta/F_v)$ is a 3-dimensional p-adic Lie group and $I(K_\eta/F_v)$ is 2-dimensional. In both cases, if $\mathcal{Z}_\eta$ denotes the subgroup of $G(K_\eta/F_v)$ which acts on $T_p(A)$ as multiplication by a scalar, then $I(K_\eta/F_v) \cap \mathcal{Z}_\eta$ is trivial. We will identify $G(K_\eta/F_v)$ with the decomposition subgroup of $G(K/F)$ for η, and $I(K_\eta/F_v)$ with the inertia subgroup. If $\mathcal{Z}$ denotes the subgroup of $G(K/F)$ acting on $T_p(A)$ as scalars, then $I(K_\eta/F_v) \cap \mathcal{Z}$ is trivial. Thus the image of $I(K_\eta/F_v)$ in $G(M/F)$, which is the corresponding inertia subgroup of $G(M/F)$, is a p-adic Lie group of dimension 1 if A has complex multiplication, and of dimension 2 otherwise.

Assume that A has complex multiplication. If $n \gg 0$, then $G(K/F_n) \cong \mathbb{Z}_p^2$ and the inertia subgroup $I(K_\eta/F_v) \cap G(K/F_n)$ will be a direct summand. It follows that the inertia subgroup for v_n (the prime of F_n lying below η) in $G(F_{2n}/F_n) \cong (\mathbb{Z}/p^n\mathbb{Z})^2$ is cyclic of order p^n. Its intersection with $G(F_{2n}/L_n)$ is trivial and hence I_{v_n} is cyclic of order p^n. Thus, $I_{v_n} = G(L_n/F_n)$. The same will be true for $I_{v_n'}$. The proposition follows immediately from this.

If A does not have complex multiplication, then $G(F_{2n}/F_n) \cong (\mathbb{Z}/p^n\mathbb{Z})^4$ and the image of $I(K_\eta/F_v) \cap G(K/F_n)$ in this group will be isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^2$ for $n \gg 0$. The intersection with $G(F_{2n}/L_n)$ is trivial and so we have $I_{v_n} \cong (\mathbb{Z}/p^n\mathbb{Z})^2$. The same is true for $I_{v'_n}$. Since $G(L_n/F_n) \cong (\mathbb{Z}/p^n\mathbb{Z})^3$, it is not hard to see that $J = I_{v_n} \cap I_{v'_n}$ must contain a subgroup isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$ (for $n \gg 0$). It follows that the $G(F_n/F)$-module $G(L_n/F_n)$ has a quotient $W_n = G(L_n/F_n)/V_n$ which is isomorphic to $(\mathbb{Z}/p^{a_n}\mathbb{Z}) \times (\mathbb{Z}/p^{b_n}\mathbb{Z})$ for some $a_n, b_n \geq 0$. The proposition will follow if we show that a_n and b_n are bounded as $n \to \infty$.

By a well-known theorem of Serre, the image of the representation $G_F \to GL_2(\mathbb{Z}_p)$ giving the Galois action on $T_p(A)$ is of finite index in $GL_2(\mathbb{Z}_p)$. Let $V_p(A) = T_p(A) \otimes \mathbb{Q}_p$. Then the adjoint representation $\mathrm{Adj}(V_p(A)) = \mathrm{Sym}^2(V_p(A)) \otimes \det^{-1}$ of G_F will be irreducible. Now it is easy to define a natural isomorphism

$$G(L_n/F_n) \cong \mathrm{Adj}(A[p^n])$$

as modules for $G(F_n/F)$. Also $\mathrm{Adj}(A[p^n])$ can be identified with $\mathrm{Adj}(T_p(A))/p^n\mathrm{Adj}(T_p(A)$. Assume that a_n and/or b_n is unbounded as $n \to \infty$. This implies that the G_F-module $\mathrm{Adj}(T_p(A))$ has a sequence of quotients which are isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^e$ (as groups) for all $m \geq 1$, where e is either 1 or 2. It is not hard to deduce from this that $\mathrm{Adj}(T_p(A))$ must then have a G_F-quotient isomorphic to $\mathbb{Z}_p^e$ (as a $\mathbb{Z}_p$-module). This contradicts the fact that $\mathrm{Adj}(V_p(A))$ is irreducible. ■

It seems reasonable to believe that the hypotheses that A has potentially ordinary reduction at primes over p or that $\dim(A) = 1$ in proposition 3.3 are not necessary, although we have not looked at those questions closely. We also have not considered the behavior of $\ker(s_{K/F'})$ when F' is allowed to vary over *all* the finite extensions of F contained in K. But it is interesting to consider the infinite extensions M_n of F. We allow the dimension of A to be arbitrary. We assume that F has been replaced, if necessary, by F_1 (or F_2 if $p = 2$) so that A has good, ordinary reduction at all primes over F. Also we assume that F contains μ_p (or μ_4 if $p = 2$) so that K is just the compositum of M_n with the cyclotomic $\mathbb{Z}_p$-extension of F. Thus $G(K/M_n) \cong \mathbb{Z}_p$. Now K/M_n is unramified at all primes of M_n not lying over p. For the primes above p, the argument in the proof of Proposition 3.3 concerning inertia groups is easily adapted to show that the inertia subgroup of $G(K/M_n)$ for primes over p is trivial, i.e. K/M_n is unramified everywhere. The earlier arguments in 1,I show in this case that $\ker(h_{K/M_n})$ and $\mathrm{coker}(h_{K/M_n})$ are trivial. The local arguments are easily adapted to show that $\ker(r_{K/M_n})$ is trivial too. In fact, they are quite easy in this case because $A(K_\eta)_p$ is certainly divisible for any η. (In verifying the triviality of the contribution to $\ker(r_{K/M_n})$ for any η, one should note that $G(K_\eta/(M_n)_\eta)$ is either trivial or isomorphic to $\mathbb{Z}_p$. Also $(M_n)_\eta/F_v$ is a deeply ramified extension and so $\mathrm{im}(\kappa_{(M_n)_\eta}) = \mathrm{im}(\lambda_{(M_n)_\eta})$.) From these remarks, one obtains the following result.

Proposition 3.4. *Assume that A has good, ordinary reduction at all primes of F lying over p and that F contains μ_p (or μ_4 if $p = 2$). The natural map*

$$s_{K/M_n} : \mathrm{Sel}_A(M_n) \to \mathrm{Sel}_A(K)^{G(K/M_n)}$$

is an isomorphism for any $n \geq 0$.

It follows that $\ker(s_{K/F_n}) = \ker(s_{M_n/F_n})$ and $\mathrm{coker}(s_{K/F_n}) = \mathrm{coker}(s_{M_n/F_n})$ for all $n \geq 1$ (or $n \geq 2$ if $p = 2$). We have essentially used this observation to study $\ker(s_{K/F_n})$ above, but the behavior of $\mathrm{coker}(s_{K/F_n})$ is much more difficult. In fact, we cannot show that $\mathrm{coker}(s_{K/F_n})$ can be unbounded, although it seems likely that this sometimes happens. The main difficulty is that we don't understand how $\mathrm{rank}_{\mathbb{Z}}(A(F_n))$ grows as $n \to \infty$. We will now discuss this.

In **(E)** of section 2, we mentioned that $\ker(g_{K/F_n})[p]$ would be of unbounded dimension if $\dim_{\mathbb{Z}/p\mathbb{Z}}(\ker(r_{K/F_n})[p]) - \rho_n$ is unbounded, where $\rho_n = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_A(F_n)_p)$. If indeed this is so, then the exact sequence (1) together with the fact that both $\ker(h_{K/F_n})[p]$ and $\mathrm{coker}(h_{K/F_n})[p]$ have bounded dimension show that $\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathrm{coker}(s_{K/F_n})[p])$ is unbounded as $n \to \infty$. To state a more precise result, let Σ' denote the set of primes v of F such that either $v|p$ or A fails to have potentially good reduction at v. Let Σ'_n denote the primes of F_n lying above those in Σ' and let σ_n denote the cardinality of Σ'_n. Let $\tau_n = 2\dim(A)\sigma_n - \rho_n$. Then we have

Proposition 3.5. *Assume that $\tau_n \to \infty$ as $n \to \infty$. Then* $\mathrm{coker}(s_{K/F_n})$ *contains a subgroup isomorphic to $(\mathbb{Z}/p^{n-c}\mathbb{Z})^{\tau_n - c'}$ for all $n \gg 0$, where c and c' are constants.*

Proof. For every prime v_n in Σ'_n, the remarks in **A**II,(ii) and **C**II of section 2 show that $\ker(r_{v_n})$ contains a subgroup isomorphic to $(\mathbb{Z}/p^{n-c}\mathbb{Z})^{2\dim(A)}$ for all $n \gg 0$, where c is a constant depending only on the prime v of F lying below v_n. Since Σ' is finite, we can assume that c is independent of v and hence that $\ker(r_{K/F_n})$ contains a subgroup isomorphic to $(\mathbb{Z}/p^{n-c}\mathbb{Z})^{2\dim(A)\sigma_n}$ for all $n \gg 0$. The bound on $\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathrm{coker}(\gamma_n)[p])$ stated in (7) gives information about the structure of $\mathrm{coker}(\gamma_n)$. Taking that into account together with analogous information about $\ker(h_{K/F_n})$ and $\mathrm{coker}(h_{K/F_n})$ implies the stated result. ■

We will take up this topic again in section 4, suggesting a possible source of examples where the hypothesis in proposition 3.5 is satisfied.

III. Arbitrary K/F.

Theorem 1 follows immediately from propositions 1.1 and 2.8 by using the exact sequence (1). Thus, under the hypotheses of that theorem (or with the considerably weaker hypothesis that $\mathcal{A}_v \cap \mathcal{B}_v = \phi$ for all $v|p$), $\ker(s_{K/F'})$ is finite and of bounded order and $\mathrm{coker}(s_{K/F'})$ is finite. Theorem 2 follows from propositions 1.3 and 2.8. Theorem 3 is obtained as a corollary using proposition 2.7.

It is useful to know if $s_{K/F'}$ is an isomorphism for all F'. We will give one simple result, which will give sufficient conditions for this to happen and one useful corollary. We assume that $G(K/F)$ is pro-p, but it is not necessary to assume that it is a p-adic Lie group..

Proposition 3.6. *Assume that K/F is Galois and that $G(K/F)$ is a pro-p group. Assume that $A(F)_p$ is trivial. For all primes v of F lying over p, assume that A has good, ordinary reduction and that $\widetilde{A}_v(f_v)_p$ is trivial. For all primes v of F not dividing p which are ramified in K/F or where A has bad reduction, assume that $A(F_v)_p$ is trivial. Then $s_{K/F'}$ is an isomorphism for all extensions of F contained in K.*

Proof. Since $G(K/F)$ is pro-p and $A(F)_p = A(K)_p^{G(K/F)}$ is trivial, it follows that $A(K)_p$ is trivial. Hence so are $\ker(h_{K/F'})$ and $\mathrm{coker}(h_{K/F'})$ for all F'. Similarly, the triviality of $\widetilde{A}_v(f_v)_p$ for all $v|p$ implies that of $\widetilde{A}_v(f'_{v'})$ for all primes v' of F' lying above v. Thus $\ker(a_{v'}) = 0$ and $D(K_\eta) = 0$ for all primes η of K lying above v. Hence $\ker(r_{v'}) = 0$ for all $v'|p$. For $v \nmid p$, $\ker(r_{v'}) = 0$ for all primes v' of F lying over v if A has good reduction at v and v is unramified in K/F, by proposition 2.3. For the other primes, the assumption that $A(F_v)_p = 0$ implies that, for all $\eta|v$, $A(K_\eta) = 0$ (since $G(K_\eta/F_v)$ is pro-p). This implies that $\ker(r_{v'}) = 0$ for all $v'|v$. Hence the hypotheses in proposition 3.6 imply that $\ker(r_{K/F'}) = 0$ for all F'. Therefore, $\ker(g_{K/F'}) = 0$ too. The conclusion follows from the exact sequence (1). ■

Corollary 3.7. *Assume that K/F is Galois and that $G(K/F)$ is a pro-p group. Let A be an abelian variety defined over F satisfying the following hypotheses:*

(i) $A(F)_p = 0$ *and* $\mathrm{Sel}_A(F)_p = 0$.

(ii) For all primes v of F lying above p, A has good, ordinary reduction at v and $\widetilde{A}_v(f_v)_p$ is trivial, where f_v denotes the residue field for v.

(iii) For all primes v of F not lying over p which are ramified in K/F or where A has bad reduction, $A(F_v)_p$ is trivial.

Then $\mathrm{Sel}_A(F')_p = 0$ *for all extensions F' of F contained in K.*

Proof. The hypotheses imply that the map $s_{K/F}$ is an isomorphism. Since $\mathrm{Sel}_A(F)_p = 0$, it follows that $\mathrm{Sel}_A(K)_p^{G(K/F)} = 0$. Now $G(K/F)$ is a pro-p group acting continuously on the discrete, p-primary, abelian group $\mathrm{Sel}_A(K)_p$. It is easy to see that $\mathrm{Sel}_A(K)_p^{G(K/F)} = 0$ implies that $\mathrm{Sel}_A(K)_p = 0$. If $F \subset F' \subset K$, the map $s_{K/F'}$ is injective (since $A(K)_p = 0$) and so $\mathrm{Sel}_A(F')_p = 0$. ■

There are also results in the opposite direction which are consequences of the basic exact sequence (1) stated in the introduction and the observations in section 2 about $\ker(r_{K/F'})$. Under rather general hypotheses, one can show that $\mathrm{Sel}_A(K)_p$ must be "large."

Proposition 3.8. *Let K/F be any infinite Galois extension which is Σ-ramified for some finite set Σ of primes of F. Let A be any abelian variety defined over F. Let A^t denote the dual abelian variety. Suppose that $A(K)_p = A^t(K)_p = 0$ and that $\ker(r_{K/F'}) \neq 0$ for all finite extensions F' of F contained in K. Then $\mathrm{Sel}_A(K)_p$ is infinite.*

Proposition 3.9. *Let K/F be a Σ-ramified Galois extension such that $G(K/F)$ is a p-adic Lie group. Let A be any abelian variety defined over F.*

- *(a) Suppose that $\ker(r_{K/F'})[p]$ has unbounded order as F' varies over the finite extensions of F contained in K. Then $\mathrm{Sel}_A(K)_p[p]$ is infinite.*
- *(b) Suppose that for any $m, n \geq 1$, there is a finite extension F' of F contained in K such that $\ker(r_{K/F'})$ contains a subgroup isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^n$. Then $\mathrm{Sel}_A(K)_p$ contains a direct sum of infinitely many copies of $\mathbb{Q}_p/\mathbb{Z}_p$.*

Remark. Proposition 3.8 implies theorem 5 of the introduction. Suppose that $v = \mathfrak{p}$ satisfies the hypotheses of that theorem. Then, as explained in (ii) at the end of section 2, we do have $\ker(r_{v'}) \neq 0$ for all $v'|v$ and so $\ker(r_{K/F'}) \neq 0$ for all F'. Another condition guaranteeing this, and so implying that $\mathrm{Sel}_A(K)_p$ is infinite, is that there exists some prime v of F not lying over p such that v is infinitely ramified in K/F and such that $A^t(F_v)_p \neq 0$. If A has good reduction at v, $A^t(F_v)_p$ has the same order as $\widetilde{A}_v(f_v)$.

Proposition 3.9(b) implies theorem 6 of the introduction. For if $v = \mathfrak{p}$ satisfies the hypotheses in that theorem, then the residue field k_η for a prime η of K lying above v contains the unique $\mathbb{Z}_p$-extension of f_v. This implies that $\widetilde{A}_v(k_\eta)_p$ is divisible. Since $\widetilde{A}_v(f_v)_p \neq 0$, clearly $\widetilde{A}_v(k_\eta)_p$ is infinite, and so the exponent of $\widetilde{A}_v(f_{v'})_p$ is unbounded as F' varies over the finite Galois extensions of F contained in K and v' over the primes of F' dividing v. Since the number of such primes v' is unbounded and the exponent of $\ker(r_{v'})$ is also unbounded as F' varies, the hypothesis in proposition 3.9(b) indeed holds.

Proof of proposition 3.8. Since $A(K)_p = 0$, it follows that $\ker(h_{K/F'}) = 0$. Thus the maps $s_{K/F'}$ are injective. Now $\mathrm{Sel}_A(K)_p = \varinjlim \mathrm{Sel}_A(F')_p$ and so if $\mathrm{Sel}_A(K)_p$ were finite, then $h_{K/F'}$ would induce an isomorphism $\mathrm{Sel}_A(F')_p \to \mathrm{Sel}_A(K)_p$ for some finite extension F' of F contained in K. Then $\mathrm{coker}(s_{K/F'}) = 0$. It would follow from the exact sequence (1) that $\ker(g_{K/F'}) = 0$. But $\ker(r_{K/F'}) \neq 0$ by assumption. Since $\ker(r_{K/F'}) \neq \ker(g_{K/F'})$, the discussion in **(E)** of section 2 shows that $\mathrm{coker}(\gamma_{F'}) \neq 0$. Since $\mathrm{Sel}_A(K)_p$ is assumed to be finite, so is $\mathrm{Sel}_A(F')_p$. It then would follow that $\mathrm{coker}(\gamma_{F'}) \cong A^t(F')_p = 0$, which gives a contradiction. ■

Proof of proposition 3.9. For part (a), assume to the contrary that $\mathrm{Sel}_A(K)[p]$ is finite. Then $\mathrm{Sel}_A(K)_p \cong (\mathbb{Q}_p/\mathbb{Z}_p)^a \times$(a finite group) for some $a \geq 0$. It follows that $\mathrm{coker}(s_{K/F'})[p]$ is finite and of bounded order. By the remark preceding lemma 0.2, $\ker(h_{K/F'})[p]$ is also of bounded order. Using (1), we see that $\ker(g_{K/F'})[p]$ has bounded order too. Now $\ker(h_{K/F'})$ has bounded $\mathbb{Z}_p$-corank by lemma 0.2. Hence, it is clear that $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_A(F')_p)$ must be bounded. Using the same notation as in **(E)** of section 2, it follows that $\ker(r_{K/F'})/\ker(g_{K/F'})$ is isomorphic to a subgroup of $\mathcal{P}_A^{\Sigma}(F')/\mathcal{G}_A^{\Sigma}(F') = \mathrm{coker}(\gamma_{F'})$. Now $\mathrm{Sel}_A(F')_p$ and $\mathrm{Sel}_{A^t}(F')_p$ have the same $\mathbb{Z}_p$-corank. Since this is bounded, it follows from the inequality (7) that $\ker(r_{K/F'})[p]$ must be of bounded order, contradicting the hypothesis.

To show (b), consider $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$. It's a divisible p-primary abelian group and so must be a direct sum of copies of $\mathbb{Q}_p/\mathbb{Z}_p$. (See Theorem 23.1 in [Fu].) It turns out that $\mathrm{Sel}_A(K)_p/(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ has bounded exponent. To see this, we regard $\widehat{\mathrm{Sel}_A(K)_p}$ as a Λ-module, where Λ denotes the completed group algebra $\mathbb{Z}_p[[U]]$ for an open pro-p subgroup $\mathcal{U}$ of $G(K/F)$. It is known that Λ is a noetherian ring and that $\widehat{\mathrm{Sel}_A(K)_p}$ is a finitely generated Λ-module. The orthogonal complement of $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ is the torsion $\mathbb{Z}_p$-submodule T of $\widehat{\mathrm{Sel}_A(K)_p}$. This is a Λ-submodule of $\widehat{\mathrm{Sel}_A(K)_p}$ and so must be finitely generated as a Λ-module. Hence T and its Pontryagin dual $\mathrm{Sel}_A(K)_p/(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ must indeed have bounded exponent.

Assume that $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ is a direct sum of just finitely many copies of $\mathbb{Q}_p/\mathbb{Z}_p$. We will obtain a contradiction by showing that $\mathrm{Sel}_A(K)_p$ contains a subgroup isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^n$ for arbitrarily large m, n (and using the observation of the previous paragraph). It suffices to show that $\mathrm{coker}(s_{K/F'})$ contains such a subgroup for some F'. We will again use the exact sequence (1), taking advantage of the hypothesis concerning $\ker(r_{K/F'})$ and the freedom to vary m and n. By the remark preceding lemma 0.2, $\ker(h_{K/F'})[p]$ and $\mathrm{coker}(h_{K/F'})[p]$ are of bounded order as F' varies. This of course greatly restricts the structure of the groups $\ker(h_{K/F'})$ and $\mathrm{coker}(h_{K/F'})$. (Note however that these groups could be infinite.) It therefore clearly suffices to show that $\ker(g_{K/F'})$ contains a subgroup isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^n$ for arbitrarily large m and n (and for some F').

We are assuming that $(\mathrm{Sel}_A(K)_p)_{\mathrm{div}}$ has finite $\mathbb{Z}_p$-corank. By lemma 0.2, the $\mathbb{Z}_p$-corank of $\ker(h_{K/F'})$ is bounded. Hence $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_A(F')p)$ is also bounded. Referring to the proof of part (a), it follows that $\mathrm{coker}(\gamma_{F'})[p]$ has bounded order. This again restricts the structure of $\mathrm{coker}(\gamma_{F'})$ and hence of $\ker(r_{K/F'})/\ker(g_{K/F'})$. The hypothesis about $\ker(r_{K/F'})$ therefore implies what we need about $\ker(g_{K/F'})$, giving the desired contradiction. ■

4 Final remarks and examples.

$Ker(s_{K/F})$ can be infinite.

It is not hard to give examples of this phenomenon. Suppose that A is an abelian variety defined over a number field F and that the Mordell-Weil group $A(F)$ is infinite. Then $\mathrm{Sel}_A(F)_p$ contains the image of $A(F)\otimes(\mathbb{Q}_p/\mathbb{Z}_p)$ under the Kummer map κ. This is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$, where $r = \mathrm{rank}(A(F))$. Taking $\mathrm{im}(\kappa)$ as $\mathcal{H}_F$ in the final remarks of section 1, one can construct a p-adic Lie extension K/F such that $\mathrm{im}(\kappa) \subset \ker(h_{K/F})$. Then of course $\mathrm{im}(\kappa) \subset \ker(s_{K/F})$. One can describe K explicitly. Let

$$\mathcal{E} = \mathcal{E}_{A,F} = \{Q \in A(\overline{\mathbb{Q}}) \mid p^m Q \in A(F) \text{ for some } m \geq 1\}.$$

Then $K = F(\mathcal{E})$, the field generated by the coordinates of all elements of $\mathcal{E}$. Since $A[p^\infty] \subset \mathcal{E}$, one has $L = F(A[p^\infty]) \subset K$. It is also clear that $K \subset F_\Sigma$, where Σ is a finite set of primes of F containing the primes over p or ∞ and all primes where A has bad reduction.

Now $\ker(h_{L/F})$ is finite. Hence $h_{L/F}(\mathrm{im}(\kappa))$ is a subgroup of

$$H^1(L, A[p^\infty]) = \mathrm{Hom}(G(L^{\mathrm{ab}}/L), A[p^\infty])$$

isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$. A typical element of this subgroup is of the form $\varphi = \varphi_Q$ defined by $\varphi(g) = g(Q) - Q$ for $g \in G(L^{\mathrm{ab}}/L)$, $Q \in \mathcal{E}$. By definition, the intersection of the kernels of the φ_Q's is $G(L^{\mathrm{ab}}/K)$. Thus $G(K/L)$ can be identified with a closed subgroup of $\mathrm{Hom}((\mathbb{Q}_p/\mathbb{Z}_p)^r, A[p^\infty]) \cong T_p(A)^r$. This identification is compatible with the natural action of $G(L/F)$ on $G(K/L)$ and $T_p(A)^r$. In particular, if $r = 1$ and if the G_F-representation space $V_p(A)$ is irreducible, then $G(K/L)$ can be identified with a subgroup of $T_p(A)$ of finite index. The fact that $h_{K/F}(\mathrm{im}(\kappa)) = 0$ is clear since $A(F) \subset \mathcal{E}$ and $\mathcal{E} \otimes (\mathbb{Q}_p/\mathbb{Z}_p) = 0$.

$Coker(s_{K/F})$ can be infinite.

We will give an example where all the hypotheses in theorem 1 are satisfied except for the requirement that K/F be admissible. Since $A(K)_p$ will be finite, so will be $\ker(h_{K/F})$ and $\mathrm{coker}(h_{K/F})$. Hence all we need is to make $\ker(g_{K/F})$ infinite. In light of proposition 2.6, we must find an example where $\mathcal{A}_v$ and $\mathcal{B}_v$ fail to be disjoint for some prime $v|p$. We will choose an example such that $\mathrm{Sel}_A(F)_p$ is finite. Then, as mentioned previously, $\mathcal{G}_A^\Sigma(F)$ will be of finite index in $\mathcal{P}_A^\Sigma(F)$. It will therefore be enough to choose K so that $\ker(r_{K/F})$ is infinite. For that purpose, let v be a fixed prime of F lying above p. We will choose K so that the kernel of the map

$$r_v : \mathcal{H}_A(F_v) \to \mathcal{H}_A(K_\eta)$$

is infinite. Here η is a prime of K lying above v. Although it is not necessary, we will assume for simplicity that $\dim(A) = 1$ and that A has good reduction at v.

Now $\mathcal{H}_A(F_v)$ has $\mathbb{Z}_p$-corank $[F_v : \mathbb{Q}_p]$. Choose a subgroup $\mathcal{H}_v$ of $\mathcal{H}_A(F_v)$ isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. Let $a_v(\mathcal{H}_v)$ denote the image of $\mathcal{H}_v$ under the map a_v. Then $a_v(\mathcal{H}_v)$ is a subgroup of $H^1(F_v, D_v)$ isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ (since $\ker(a_v)$ is finite). One can apply the construction described at the end of section 1, taking $\mathcal{H}_{F_v}$ to be $a_v(\mathcal{H}_v)$ and obtaining a certain extension $K_{\mathcal{H}_v}$ of F_v. The action of G_{F_v} on D_v is given by a character $\psi_v : G_{F_v} \to \mathbb{Z}_p^\times$ of infinite order. Since A has good reduction at v, the character ψ_v is unramified and gives the action of $G(F_v^{\mathrm{unr}}/F_v)$ on $D_v = \widetilde{A}_v[p^\infty]$. Let $L_{\psi_v} = \overline{F}_v^{\ker(\psi_v)}$. Then $G(L_{\psi_v}/F_v) \cong \Delta \times \mathbb{Z}_p$, where Δ is a finite group. The restriction map

$$H^1(F_v, D_v) \to H^1(L_{\psi_v}, D_v)^{G(L_{\psi_v}/F_v)} = \mathrm{Hom}_{G(L_{\psi_v}/F_v)}(G(L_{\psi_v}^{\mathrm{ab}}/L_{\psi_v}), D_v)$$

is injective if p is odd (and has finite kernel if $p = 2$). The image of $a_v(\mathcal{H}_v)$ under this map is still isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ and coincides with $\mathrm{Hom}(G(K_{\mathcal{H}_v}/L_{\psi_v}), D_v)$, where $K_{\mathcal{H}_v}$ is a $\mathbb{Z}_p$-extension of L_{ψ_v} and is Galois over F_v. In fact, $G(K_{\mathcal{H}_v}/F_v)$ is a 2-dimensional p-adic Lie group and the inertia subgroup is of finite index in $G(K_{\mathcal{H}_v}/L_{\psi_v}) \cong \mathbb{Z}_p$. Thus $K_{\mathcal{H}_v}/F_v$ is deeply ramified.

If we can choose K so that K_η contains $K_{\mathcal{H}_v}$, then we will have

$$a_v(\mathcal{H}_v) \subset \ker(H^1(F_v, D_v) \to H^1(K_\eta, D_v)). \tag{8}$$

Therefore, we will have $\mathcal{H}_v \subset \ker(r_v)$, which makes $\ker(r_v)$ infinite. Conversely, assume that K/F is a p-adic Lie extension and that (8) holds. Then $K_{\mathcal{H}_v} \subset K_\eta$. To see this, first note that K_η/F_v must be infinitely ramified. Otherwise, it is easy to see that $H^1(K_\eta/F_v, D_v(K_\eta))$ would be finite, contradicting (8). Also, (8) implies that $D_v(K_\eta)$ must be infinite. Now $\mathrm{corank}_{\mathbb{Z}_p}(D_v) = 1$. Hence $D_v(K_\eta) = D_v$ and so $L_{\psi_v} \subset K_\eta$. It is then clear that $K_{\mathcal{H}_v} \subset K_\eta$ too.

To obtain such a field K, we will use an auxiliary elliptic curve E. Suppose that E is an elliptic curve defined over F satisfying all of the hypotheses that we have assumed for A. Assume that Σ' is the finite set of primes consisting of all primes of F lying over p or ∞ and all primes where E has bad reduction. Since $\mathrm{Sel}_E(F)_p$ is assumed to be finite, we know that $\mathcal{G}_E^{\Sigma'}(F)$ has finite index in $\mathcal{P}_E^{\Sigma'}(F)$. It follows easily from this that

$$H^1(F_v, \widetilde{E}_v[p^\infty])_{\mathrm{div}} \subset \mathrm{im}(H^1(F_{\Sigma'}/F, E[p^\infty]) \to H^1(F_v, \widetilde{E}_v[p^\infty])).$$

Referring to the construction at the end of section 1, we obtain a p-adic Lie extension K/F such that $F(E[p^\infty]) \subset K \subset F_{\Sigma'}$ and such that

$$H^1(F_{\Sigma'}/F, E[p^\infty]) = \ker(H^1(F, E[p^\infty]) \to H^1(K, E[p^\infty])).$$

With this choice of K, it follows that

$$H^1(F_v, \widetilde{E}_v[p^\infty])_{\mathrm{div}} \subset \ker(H^1(F_v, \widetilde{E}_v[p^\infty]) \to H^1(K_\eta, \widetilde{E}_v[p^\infty]). \tag{9}$$

Now, in addition to all the previous assumptions about E, we require that $\widetilde{E}_v \cong \widetilde{A}_v$ over f_v, the residue field for v. Then $\widetilde{E}_v[p^\infty] \cong \widetilde{A}_v[p^\infty] = D_v$ as G_{F_v}-modules. Since $a_v(\mathcal{H}_v)$ is divisible, it is a subgroup of $H^1(F_v, D_v)_{\mathrm{div}}$ and so (9) implies that (8) holds. Therefore, $K_{\mathcal{H}_v} \subset K_\eta$, as we wanted. It remains to show that A and E can be chosen so that $A(K)_p$ is finite. This is not hard to arrange. Assume that A does not have complex multiplication and that there is a prime λ of F such that A has bad reduction at λ, but E has good reduction at λ. Then $\lambda \notin \Sigma'$ and so λ is unramified in K/F. But the action of G_F on $V_p(A)$ is irreducible. This implies that if $A(K)_p$ is infinite, then $A(K)_p = A[p^\infty]$. That is, $F(A[p^\infty]) \subset K$. But then λ would necessarily be ramified in K/F. Hence $A(K)_p$ is indeed finite.

For the above choice of K/F, it is rather clear that $\mathcal{A}_v \cap \mathcal{B}_v \neq \phi$. Here we are using the notation of (6). For the action of $G(L_{\psi_v}/F_v)$ on $G(K_{\mathcal{H}_v}/L_{\psi_v})$ is given by the character ψ_v. The inertia subgroup of $G(K_{\mathcal{H}_v}/L_{\psi_v})$ is isomorphic to $\mathbb{Z}_p$ and L_{ψ_v}/F_v is an unramified extension. Since $K_{\mathcal{H}_v} \subset K_\eta$, it is clear that a Frobenius automorphism u will have $\psi_v(u)$ as one of its eigenvalues for its action on $\mathfrak{i}_v/\mathfrak{i}'_v$. By definition, $\psi_v(u)$ is also the eigenvalue of u acting on $T_p(D(K_\eta)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ since $D(K_\eta) = D_v$.

It is quite easy to find specific examples when $F = \mathbb{Q}$ and p is a small prime. If $p = 3$, we could take A to be defined by $y^2 + y = x^3 - x^2$, which is an elliptic curve of conductor 11. It has good, ordinary reduction at p. Take E to be defined by $y^2 + y = x^3 - x^2 - 33x + 93$, which has conductor 175. A theorem of Kolyvagin implies that the Selmer groups over $\mathbb{Q}$ for both A and E are finite (since the values at $s = 1$ of the Hasse-Weil L-functions are nonzero). They clearly have the same reduction modulo p. Also, A does not have complex multiplication, and we can take $\lambda = 11$, as above, to see that $A(K)_p$ is finite.

Coker$(s_{K/F'})$ *can have unbounded order even if* K/F *is admissible.*

Assume that $G(K/F) \cong \mathbb{Z}_p^m$, where $m \geq 2$. Suppose that A is an elliptic curve defined over F satisfying the following hypotheses: (i) $A(F)$ and $Ш_A(F)_p$ are both finite, (ii) A has potentially ordinary reduction at the primes of F lying over p, and (iii) there is a prime v of F not dividing p such that A has split, multiplicative reduction at v, the v-adic valuation of the j-invariant j_A of A is divisible by p, and v does not split completely in K/F. Then it follows that $\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathrm{coker}(s_{K/F'})[p])$ is unbounded. To see this, note that if η is a prime of K lying over p, then K_η/F_v must be the unramified $\mathbb{Z}_p$-extension of F_v (which is the only $\mathbb{Z}_p$-extension of F_v). Thus $G(K_\eta/F_v) \cong \mathbb{Z}_p$ and so it is clear that there exists a $\mathbb{Z}_p$-extension F_∞/F such that $F_\infty \subset K$ and v splits completely in F_∞/F. Hypothesis (i) implies that $\mathrm{Sel}_A(F)_p$ is finite. It then follows from theorem 2 that $\mathrm{Sel}_A(F_\infty)_p^{G(F_\infty/F)}$ is finite. This implies that $\mathrm{Sel}_A(F_\infty)_p$

is Λ-cotorsion, where $\Lambda = \mathbb{Z}_p[[G(F_\infty/F)]]$. Hence $(\mathrm{Sel}_A(F_\infty)_p)_{\mathrm{div}}$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ for some $\lambda \geq 0$ and therefore $\rho_{F'} = \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_A(F')_p) \leq \lambda$ for every subfield F' of F_∞. On the other hand, by hypothesis (iii), we have that $K_\eta/F'_{v'}$ is the unramified $\mathbb{Z}_p$-extension when $v'|v$ and $\eta|v'$ and that $\ker(r_{v'}) \neq 0$ since $A(K_\eta)_p$ will not be divisible. (The last assertion is a consequence of the assumption on j_A.) Thus $\dim_{\mathbb{Z}/p\mathbb{Z}}(\ker(r_{K/F'})[p]) \geq [F' : F]$. It then follows from the discussion in **(E)** of chapter 2 that $\dim_{\mathbb{Z}/p\mathbb{Z}}(\ker(g_{K/F'})[p])$ is unbounded as F' varies over the subfields of F_∞ containing F. Since $\ker(h_{K/F'})[p]$ and $\mathrm{coker}(h_{K/F'})[p]$ have bounded dimension, it is clear from the exact sequence (1) that $\dim_{\mathbb{Z}/p\mathbb{Z}}(\mathrm{coker}(s_{K/F'})[p])$ is also unbounded. It is not hard to find specific examples where the hypotheses (i)–(iii) hold.

We will now describe another possible kind of example. Let $K = F(A[p^\infty])$, where A is an abelian variety/F with good, ordinary reduction at the primes of F above p. We know that K/F is admissible. Let $F_n = F(A[p^n])$. For any prime v of F, the number of primes v_n of F_n lying above v is of course just the index of the decomposition subgroup for v_n in $G(F_n/F)$. If η is a prime of K lying above v, let m_v denote the dimension of the p-adic Lie group $G(K_\eta/F_v)$ and let $m = m_A$ denote the dimension of $G(K/F)$. Then, for $n \gg 0$, the number of v_n's lying above v will be $\alpha_v p^{(m-m_v)n}$, where α_v is a positive rational number. Let ρ_n, σ_n, and τ_n be as defined just before proposition 3.5. Then $\sigma_n = \sum_{v\in\Sigma'} \alpha_v p^{(m-m_v)n}$. To show that $\tau_n \to \infty$ as $n \to \infty$, which suffices to imply that $|\mathrm{coker}(s_{K/F_n})|$ is unbounded according to proposition 3.5, one must compare the growth of σ_n and ρ_n.

It is interesting to consider the case where A is an elliptic curve defined over $\mathbb{Q}$. Assume that A has good, ordinary reduction at p and split, multiplicative reduction at primes $l_1, \ldots, l_k$ where $k \geq 1$. Then A does not have complex multiplication. Let $F = \mathbb{Q}$, $F_n = \mathbb{Q}(A[p^n])$ and $K = \mathbb{Q}(A[p^\infty])$. We will assume that $G(K/\mathbb{Q}) \cong GL_2(\mathbb{Z}_p)$ and so $G_n = G(F_n/\mathbb{Q})$ is isomorphic to $GL_2(\mathbb{Z}/p^n\mathbb{Z})$. We have $m = 4$, $m_p = 3$, and $m_{l_i} = 2$ for $1 \leq i \leq k$. Then, by studying the index of a decomposition subgroup of G_n for each l_i and for p, one obtains the lower bound $\sigma_n > k(1-p^{-2})p^{2n} + (1+p^{-1})p^n$.

To give an upper bound on ρ_n, we will make a certain rather speculative (and perhaps questionable) hypothesis. For each $n \geq 0$, let $V_n = A(F_n) \otimes_{\mathbb{Z}} \mathbb{C}$. We regard V_n as a representation space over $\mathbb{C}$ for G_n. For each irreducible character χ of G_n, we let m_χ denote the multiplicity of the corresponding irreducible representation in V_n. Thus

$$\mathrm{rank}_{\mathbb{Z}}(A(F_n)) = \dim_{\mathbb{C}}(V_n) = \sum_\chi m_\chi d_\chi,$$

where χ runs over all irreducible characters of G_n. The hypothesis that we will make is that $m_\chi = 0$ if $\chi \neq \overline{\chi}$ and $m_\chi = 0$ or 1 if $\chi = \overline{\chi}$, with a number of exceptions which is bounded as $n \to \infty$. (For a discussion of this hypothesis and related examples, see chapter 1 of [G2].) Assuming also that $\text{Ш}_A(F_n)_p$ is finite for all n, it would follow that $\rho_n \leq \delta_n + c$, where $\delta_n = \sum_{\chi=\overline{\chi}} d_\chi$ and c is a fixed constant. (The sum is over all irreducible characters χ of G_n which are real-valued.) Note that δ_n is a purely group-theoretic quantity. One can show that $\delta_n < 2p^n$. In addition to the other hypotheses that we are making, let's assume that $k \geq 2$. It then would follow that $\tau_n = 2\sigma_n - \rho_n \to \infty$ as $n \to \infty$ and so the conclusion in proposition 3.5 would be valid.

The control theorem for Ш.

Assume that A is an abelian variety defined over F. For any algebraic extension L of F, we can define $\text{Ш}_A(L)$ by the exact sequence

$$0 \to A(L) \otimes_{\mathbb{Z}} (\mathbb{Q}/\mathbb{Z}) \to \mathrm{Sel}_A(L) \to \text{Ш}_A(L) \to 0.$$

Suppose that K/F is a p-adic Lie extension. One can ask about the behavior of the maps

$$\begin{aligned} m_{K/F'} &: A(F') \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p) \to A(K) \otimes_{\mathbb{Z}} (\mathbb{Q}_p/\mathbb{Z}_p)^{G(K/F')}, \\ t_{K/F'} &: \text{Ш}_A(F')_p \to \text{Ш}_A(K)_p^{G(K/F')}. \end{aligned}$$

Assuming that $\ker(s_{K/F'})$ and $\mathrm{coker}(s_{K/F'})$ are both finite and that $\text{Ш}_A(F')_p$ is finite, it follows easily that $\ker(m_{K/F'})$ and $\mathrm{coker}(m_{K/F'})$ are finite too. If $\text{Ш}_A(F')_p$ is finite, as conjectured, then obviously so is $\ker(t_{K/F'})$.

However, $\mathrm{coker}(t_{K/F'})$ can be infinite. Examples of this phenomenon are given in [Br] for the special case where K/F is a $\mathbb{Z}_p$-extension. In that paper, F is taken to be an imaginary quadratic field and A is an elliptic curve with complex multiplication by the ring of integers of F. The $\mathbb{Z}_p$-extension K/F is chosen so that a certain p-adic height pairing becomes degenerate. Specific examples are the curves A defined by $y^2 = x^3 - Dx$ for $D = 17$, -63, -33, and 117, where the CM-field is $F = \mathbb{Q}(i)$ and $p = 5$. In each case, there is a $\mathbb{Z}_p$ extension K/F such that $\text{Ш}_A(K)_p^{G(K/F)}$ is infinite even though $\text{Ш}_A(F)_p$ is finite. The rank of $A(F)$ over $\mathrm{End}(A)$ is 1. It is conjectured that this kind of phenomenon cannot occur if F is any number field, A is any abelian variety$/F$ with potentially ordinary reduction at the primes above p, and K/F is the cyclotomic $\mathbb{Z}_p$-extension. That is, under those hypotheses, $\text{Ш}_A(K)_p^{G(K/F')}$ should be finite and hence so will $\mathrm{coker}(t_{K/F'})$ for all finite extensions F' of F contained in K.

Multiplicative reduction at primes over p.

Suppose first that A is an elliptic curve defined over $\mathbb{Q}$ with split, multiplicative reduction at a prime p. Manin shows in [Ma] that the control theorem for the Selmer group of A in the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty/\mathbb{Q}$ follows from the assertion that q_A/p^a is not a root of unity, where $a = \mathrm{ord}_p(q_A)$. Here q_A denotes the Tate period for $A/\mathbb{Q}_p$, which is an element of $\mathbb{Q}_p^\times$.

The essential reason is that q_A is then not a universal norm for the extension $(\mathbb{Q}_\infty)_\pi/\mathbb{Q}_p$, where π is the unique prime of $\mathbb{Q}_\infty$ lying over p. Now it has recently been proven that q_A is actually transcendental. (See [BDGP].) The control theorem therefore holds for $\mathbb{Q}_\infty/\mathbb{Q}$ and, more generally, for the cyclotomic $\mathbb{Z}_p$-extension of an arbitrary number field F. But if K/F is an arbitrary $\mathbb{Z}_p$-extension, then the control theorem may fail. This can happen if q_A is a universal norm for K_η/F_v, where v is a prime of F lying above p which is infinitely ramified in K/F and η is a prime of K lying above v.

Assume more generally that A is an abelian variety/F. For every $v|p$, A achieves semistable reduction over a finite extension of F_v. Let h_v denote the height of the formal group for a Neron model of A over the integers in such a finite extension. The p-power torsion points on that formal group define a subgroup C_v of $A[p^\infty]$ which is G_{F_v}-invariant and isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{h_v}$ as a group. One can then define $D_v = A[p^\infty]/C_v$, which is a G_{F_v}-module isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^{2g-h_v}$ as a group, where $g = \dim(A)$. We will assume that $h_v = g$ for all $v|p$ so that the situation seems quite analogous to the case where A has potentially ordinary reduction at all $v|p$.

Let K/F be a p-adic Lie extension which is Σ-ramified for some finite set Σ of primes of F. Assume that either $A(K)_p$ is finite or that the Lie algebra $\mathfrak{g}$ of $G(K/F)$ is reductive (as in theorems 1, 2 stated in the introduction). Then $\ker(s_{K/F'})$ will be finite for all finite extensions F' of F contained in K. To prove that $\mathrm{coker}(s_{K/F'})$ is finite, one must show that $\ker(r_{v'})$ is finite for all $v'|p$. If $v'|v$ and A has potentially ordinary reduction at v, then the hypothesis $\mathfrak{d}'_v = \mathfrak{i}'_v$ suffices to imply this. (Proposition 2.5.) The key ingredient in proving that result is verifying that $\ker(d_{v'})$ is finite, where $d_{v'}$ is the map occurring in the commutative diagram (5). However, the hypothesis $\mathfrak{d}'_v = \mathfrak{i}'_v$ is not sufficient to imply the finiteness of $\ker(d_{v'})$ if we assume only that $h_v = g$.

Using the notation of part **C** of section 2, the assumption $h_v = g$ implies that $\mathrm{im}(\lambda_{v'})$ and $\mathrm{im}(\kappa_{v'})$ have the same $\mathbb{Z}_p$-corank. Since $\mathrm{im}(\kappa_{v'}) \subset \mathrm{im}(\lambda_{v'})$, we again have $\mathrm{im}(\kappa_{v'}) = \mathrm{im}(\lambda_{v'})_{\mathrm{div}}$. If K/F is infinitely ramified, then proposition 4.3 of [CG] states that $\mathrm{im}(\kappa_\eta) = \mathrm{im}(\lambda_\eta)$. It follows from these results that $\ker(a_{v'})$ is finite and that the finiteness of $\ker(r_{v'})$ is equivalent to that of $\ker(b_{v'})$. It is clear from (5) that

$$\ker(b_{v'}) \cong \ker(d_{v'}) \cap \mathrm{im}(\pi_{v'}).$$

Consequently, if $D_v(K_\eta) = D_v^{G_{K_\eta}}$ is finite, then $\ker(d_{v'}) = H^1(K_\eta/F'_{v'}, D_v(K_\eta))$ is finite and hence so is $\ker(b_{v'})$.

We will assume now that A is an elliptic curve defined over F which has split, multiplicative reduction at a prime $v|p$. In this case, $D_v \cong \mathbb{Q}_p/\mathbb{Z}_p$ and the action of G_{F_v} on D_v is trivial. For brevity, let $L = F'_{v'}$ and $\mathcal{U} = G(K_\eta/L)$, which is just an open subgroup of $G(K_\eta/F_v)$. We also let $\mathfrak{d}_v$ denote the Lie algebra of $G(K_\eta/F_v)$. Then $\ker(d_{v'}) \cong \mathrm{Hom}(\mathcal{U}/\mathcal{U}', D_v)$. If

$\mathcal{U}$ is a sufficiently small open subgroup of $G(K_\eta/F_v)$, then $\ker(d_{v'})$ has $\mathbb{Z}_p$-corank equal to $\dim_{\mathbb{Q}_p}(\mathfrak{d}_v/\mathfrak{d}'_v)$.

On the other hand, proposition 3.6 of [G1] provides a description of $\mathrm{im}(\pi_{v'})$. Let $q_A \in F_v^\times$ denote the Tate period for A. Then $\mathrm{im}(\pi_{v'})$ is a subgroup of $\mathrm{Hom}(G(L^{\mathrm{ab}}/L), D_v)$ and a homomorphism ϕ is in $\mathrm{im}(\pi_{v'})$ if and only if $\mathrm{rec}_L(q_A) \in \ker(\varphi)$. Here $\mathrm{rec}_L : L^\times \to G(L^{\mathrm{ab}}/L)$ denotes the reciprocity map of local class field theory. The difference between $\ker(b_{v'})$ and $\ker(d_{v'})$ depends therefore on the restriction of $\mathrm{rec}_L(q_A)$ to $G(L^{\mathrm{ab}} \cap K_\eta/L) = \mathcal{U}/\mathcal{U}'$. We have $\mathrm{corank}_{\mathbb{Z}_p}(\ker(b_{v'})) = \mathrm{rank}_{\mathbb{Z}_p}(\mathcal{U}/\mathcal{U}') - \epsilon$, where $\epsilon = 0$ if this restriction has finite order and $\epsilon = 1$ if this restriction has infinite order.

In particular, if $\dim_{\mathbb{Q}_p}(\mathfrak{d}_v/\mathfrak{d}'_v) \geq 2$, then $\ker(r_{v'})$ is infinite if $G(K_\eta/F'_{v'})$ is a sufficiently small open subgroup of $G(K_\eta/F_v)$. If $\mathfrak{d}_v = \mathfrak{d}'_v$, then $\ker(r_{v'})$ will always be finite. Consider the case where $\dim_{\mathbb{Q}_p}(\mathfrak{d}_v/\mathfrak{d}'_v) = 1$. One can then choose a normal, open subgroup $\mathcal{U}$ of $G(K_\eta/F_v)$ so that $\mathcal{U}/\mathcal{U}' \cong \mathbb{Z}_p$. Let $L = K_\eta^{\mathcal{U}}$ so that L is a finite Galois extension of F_v and K_η contains a unique $\mathbb{Z}_p$-extension L_∞ of L. If $G(L/F_v)$ acts nontrivially on $G(L_\infty/L)$ (by inner automorphisms), then it is not hard to see that $\mathrm{rec}_L(q_A)|_{L_\infty}$ is trivial. In this case, $\ker(r_{v'})$ will be infinite if $G(K_\eta/F'_{v'}) \subset \mathcal{U}$. But if $G(L/F_v)$ acts trivially on $G(L_\infty/L)$, then there exists a unique $\mathbb{Z}_p$-extension $F_{v,\infty}$ of F_v contained in K_η. If q_A is a universal norm for the $\mathbb{Z}_p$-extension $F_{v,\infty}/F_v$ (i.e. if $\mathrm{rec}_{F_v}(q_A)|_{F_{\infty,v}}$ is trivial), then $\ker(r_{v'})$ is always infinite. Otherwise, $\ker(r_{v'})$ is always finite. In the special case where $K = F(A[p^\infty])$, one has $\dim(\mathfrak{d}_v/\mathfrak{d}'_v) = 1$ and K_η contains the cyclotomic $\mathbb{Z}_p$-extension of F_v. The Tate period q_A is a universal norm for that $\mathbb{Z}_p$-extension if and only if $N_{F_v/\mathbb{Q}_p}(q_A)$ is of form ζp^a, where ζ is a root of unity. It is doubtful that this can happen, but not known.

References

[BDGP] K. Barré-Sirieix, G. Diaz, F. Gramain, G. Philibert, Une preuve de la conjecture de Mahler-Manin, *Invent. Math.* **124** (1996), 1–9.

[Br] G. Brattström, The invariants of the Tate-Shafarevich group in a $\mathbb{Z}_p$-extension can be infinite, *Duke Math. J.* **52** (1985), 149–156.

[CG] J. Coates, R. Greenberg, Kummer theory for abelian varieties over local fields, *Invent. Math.* **124** (1996), 129–174.

[CH1] J. Coates, S. Howson, Euler characteristics and elliptic curves, *Proc. Nat. Acad. Sci. U.S.A.* **94** (1997), 11115–11117.

[CH2] J. Coates, S. Howson, Euler characteristics and elliptic curves II, preprint.

[CM] J. Coates, G. McConnell, Iwasawa theory of modular elliptic curves of analytic rank at most 1, *J. London Math. Soc.* **50** (1994), 243–264.

[DSMS] J. D. Dixon, M. P. F. du Sautoy, A. Mann, D. Segal, Analytic pro-p groups, *London Math. Soc. Lecture Note Series* **157** Cambridge University Press, 1999.

[Fa1] G. Faltings, Hodge-Tate structures and modular forms, *Math. Annal.* **278** (1987), 133–149.

[Fa2] G. Faltings, p-adic Hodge theory, *Jour. of the AMS* **1** (1988), 255–299.

[Fo] J. M. Fontaine, Représentations p-adiques semistable, *Asterisque* **223** (1994), 113–184.

[Fu] L. Fuchs, Infinite Abelian Groups, Vol. 1, Academic Press, 1970.

[G1] R. Greenberg, Iwasawa Theory for Elliptic Curves, *Lecture Notes in Math.* **1716** (1999), 51–144.

[G2] R. Greenberg, Introduction to Iwasawa theory for elliptic curves, preprint.

[H] M. Harris, p-adic representations arising from descent on abelian varieties, *Comp. Math.* **39** (1979), 177–245.

[Ma] Y. I. Manin, Cyclotomic fields and modular curves, *Russian Math. Surveys* **26** no. 6 (1971), 7–78.

[M] B. Mazur, Rational points of abelian varieties with values in towers of number fields, *Invent. Math.* **18** (1972), 183–266.

[P] B. Perrin-Riou, Arithmetique des courbes elliptiques et théorie d'Iwasawa, *Mém. Soc. Math. France* **112** (1984).

[R] K. Ribet, Galois representations attached to eigenforms with Nebentypus, *Lecture Notes in Math.* **601** (1977), 17–52.

[Se] S. Sen, Continuous cohomology and p-adic Galois representations, *Invent. Math.* **62** (1980), 89–116.

[S1] J. P. Serre, Abelian l-adic representations and elliptic curves, Benjamin (1968).

[S2] J. P. Serre, Sur les groupes de congruence des variétés abéliennes II, *Izv. Akad. Nauk SSSR* **35** (1971), 731–735.

[S3] J. P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.

[ST] J. P. Serre, J. Tate, Good reduction of abelian varieties, *Ann. of Math.* **88** (1968), 492–517.

[Z1] Y. G. Zarhin, Torsion of abelian varieties over $GL(2)$-extensions of number fields, *Math. Ann.* **284** (1989), 631–696.

[Z2] Y. G. Zarhin, Torsion of abelian varieties, Weil classes and cyclotomic extensions, *Math. Proc. Camb. Phil. Soc.* **126** (1999), 1–15.