SELMER GROUPS AND CLASS GROUPS

KĘSTUTIS ČESNAVIČIUS

Abstract. Let A be an abelian variety over a global field K of characteristic $p \geqslant 0$. If A has nontrivial (resp. full) K-rational l-torsion for a prime $l \neq p$, we exploit the fppf cohomological interpretation of the l-Selmer group $\mathrm{Sel}_l A$ to bound $\#\mathrm{Sel}_l A$ from below (resp. above) in terms of the cardinality of the l-torsion subgroup of the ideal class group of K. Applied over families of finite extensions of K, the bounds relate the growth of Selmer groups and class groups. For function fields, this technique proves the unboundedness of l-ranks of class groups of quadratic extensions of every K containing a fixed finite field $\mathbb{F}_{p^n}$ (depending on l). For number fields, it suggests a new approach to the Iwasawa $\mu = 0$ conjecture through inequalities, valid when $A(K)[l] \neq 0$, between Iwasawa invariants governing the growth of Selmer groups and class groups in a $\mathbb{Z}_l$-extension.

1. Introduction

Fix a prime l, a number field K, an abelian variety $A \to \operatorname{Spec} K$ of dimension $g > 0$, and let L/K range in some family of finite extensions. Our goal is to relate, in favorable situations, the growth of the l-torsion subgroup $\mathrm{Pic}(\mathcal{O}_L)[l]$ of the ideal class group of L and that of the l-Selmer group $\mathrm{Sel}_l A_L$. Concrete expectations in the case of quadratic L/K are provided by folklore conjectures:

Conjecture 1.1. *As L/K ranges over quadratic extensions, $\#\mathrm{Pic}(\mathcal{O}_L)[l]$ is unbounded.*

Conjecture 1.2. *As L/K ranges over quadratic extensions, $\#\mathrm{Sel}_l A_L$ is unbounded.*

Remarks.

1.3. Conjecture 1.1 is known for $l = 2$ due to the genus theory of Gauss, but is open for every pair (K, l) with l odd; in the $K = \mathbb{Q}$ case, much more precise predictions are available through the Cohen-Lenstra heuristics [CL84]. The conjectured (but not universally believed) unboundedness of $\mathrm{rk}\, A(L)$ would imply Conjecture 1.2, which is known for $l = 2$ if $g = 1$ [CS10, Thm. 3][1] and for $l = 2$ in certain $g > 1$ cases (see Remarks 1.6 and 4.4), but is open for every pair (A, l) with l odd.

1.4. If Conjecture 1.1 (resp., 1.2) is known for (K, l), it follows for (K', l) for every finite extension K'/K, see Lemma 4.5 (resp., 4.6).

We relate the conjectures by proving their equivalence after replacing K by a finite extension:

Theorem 1.5 (Corollary 4.8)**.**

(a) If A has $\mathbb{Z}/l\mathbb{Z}$ or μ_l as a K-subgroup, then Conjecture 1.1 for K implies Conjecture 1.2 for A.

Date: August 8, 2013.

2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 11R23, 11R29, 11R58.

Key words and phrases. Selmer group, class group, fppf cohomology, Iwasawa theory.

[1]The case when A does not have potential complex multiplication is due to Bölling [Böl75, pp. 170-171]. Both papers concern the (stronger) unboundedness of cardinalities of 2-torsion subgroups of Shafarevich-Tate groups.

(b) If $A[l]$ has a filtration by K-subgroups with subquotients isomorphic to $\mathbb{Z}/l\mathbb{Z}$ or μ_l, then Conjecture 1.2 for A implies Conjecture 1.1 for K.

Remarks.

1.6. The known $l = 2$ case of Conjecture 1.1 therefore proves the $l = 2$ and $A(K)[2] \neq 0$ case of Conjecture 1.2. Restricting further to $g = 1$, this combines with the unboundedness of $\#\operatorname{Sel}_2 A_L$ proved by Klagsbrun, Mazur, and Rubin [Kla11, 1.2] under the $A(K)[2] = 0$ assumption to reprove Conjecture 1.2 in the $(g, l) = (1, 2)$ case.

1.7. Even though the idea that Selmer groups and class groups are related is not new (compare, e.g., [Sch96]), the relationship furnished by Theorem 1.5 is sharper than those available previously. Moreover, it is specific neither to quadratic L/K nor to number fields: §4, containing its proof, works in the setting of bounded degree extensions of any fixed global field K.

1.8. The method of the proof. Under the assumptions of (a) (resp., (b)) of Theorem 1.5, we prove lower (resp., upper) bounds for $\#\operatorname{Sel}_l A$ in terms of $\#\operatorname{Pic}(\mathcal{O}_K)[l]$ in §2 (resp., §3), which we apply after base change to L. As for the bounds themselves, the fppf cohomological interpretation of Selmer groups provides the idea. To explain it, assume for simplicity that $A[l] \cong (\mathbb{Z}/l\mathbb{Z})^g \oplus \mu_l^g$ over K, and let S be the spectrum of the ring of integers of K and $\mathcal{A} \to S$ the Néron model of A. The Néron property of $\mathcal{A}[l]_{S[\frac{1}{l}]}$ [Čes13, B.5] forces $\mathcal{A}[l]_{S[\frac{1}{l}]} \cong (\mathbb{Z}/l\mathbb{Z})^g \oplus \mu_l^g$. Passing to cohomology, both $\#H^1(S[\frac{1}{l}], \mathbb{Z}/l\mathbb{Z})$ and $\#H^1(S[\frac{1}{l}], \mu_l)$ relate to $\#\operatorname{Pic}(S)[l]$ (see Lemmas B.1 and B.2), whereas $H^1(S[\frac{1}{l}], \mathcal{A}[l]) \subset H^1(K, A[l])$ is defined by local conditions [Čes13, 4.2], which at finite places of good reduction agree with those defining $\operatorname{Sel}_l A \subset H^1(K, A[l])$ [Čes13, 2.5]; it remains to quantify the resulting relation between $\#H^1(S[\frac{1}{l}], \mathcal{A}[l])$ and $\#\operatorname{Sel}_l A$.

1.9. The function field case. The argument sketched in 1.8 continues to work for a global function field K of positive characteristic $p \neq l$. For such K, the analogue of Conjecture 1.2 is known in the case of a constant supersingular elliptic curve: $\operatorname{rk} A(L)$ is unbounded due to the work of Shafarevich and Tate [TŠ67]. With this input, we prove the analogue of Conjecture 1.1 for every K containing a fixed finite field $\mathbb{F}_{p^n}$ (depending on l) and consequently, for such K, also the analogue of Conjecture 1.2 for A that have $\mathbb{Z}/l\mathbb{Z}$ or μ_l as a K-subgroup. For precise statements, see Theorem 5.1 and Corollary 5.4. As in the number field case discussed in Remark 1.3, no case of the analogue of Conjecture 1.1 was previously known for odd l (for $l = 2$, see [Mad72, Thm. 3]).

1.10. Applications to Iwasawa theory. The bounds mentioned in 1.8 lead to inequalities of Propositions 7.1 and 7.3 between the Iwasawa invariants governing the growth of Selmer groups and class groups in the layers of a $\mathbb{Z}_p$-extension. These inequalities imply our main result concerning Iwasawa theory (for a detailed discussion and other results see §§6-8):

Theorem 1.11 (Theorem 8.4)**.** *For a prime p and a number field K, to prove the Iwasawa $\mu = 0$ conjecture for the cyclotomic $\mathbb{Z}_p$-extension K_∞/K, it suffices to find an abelian K-variety A such that*

(i) A has good ordinary reduction at all places above p,

(ii) A has $\mathbb{Z}/p\mathbb{Z}$ as a K-subgroup,

(iii) $\operatorname{Hom}(\operatorname{Sel}_{p^\infty} A_{K_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$ is a torsion module over the Iwasawa algebra and has μ-invariant 0.

Remark 1.12. In fact, it suffices to find such an A after replacing K by a finite extension, see Lemma 7.7. It is not clear, however, how to take advantage of the apparent flexibility of choice: for arbitrary K and p, (iii) alone seems nontrivial to fulfill. For $K = \mathbb{Q}$ and $p = 5$, the elliptic curve

11A3 satisfies (i)-(iii) [Gre99, pp. 120-124]; with this A, Theorem 1.11 reproves an easy case of the Ferrero-Washington theorem (which is not used in loc. cit., so the argument is not circular).

1.13. The contents of the paper. The bounds discussed in 1.8 are essential for all subsequent applications and are proved in §§2-3. These technical sections rely on (standard but crucial) auxiliary computations of appendices A and B. Theorem 1.5 is proved in §4, which applies the inequalities of §§2-3 in families of bounded degree extensions of K. Both §§2-4 and the appendix B work under the assumption that K is a global field. Special cases of function field analogues of Conjectures 1.1 and 1.2 are proved in §5. The remaining §§6-8 discuss Iwasawa theory (and assume that K is a number field). The introductory §6 records how Iwasawa invariants control the growth of $\mathrm{Pic}(\mathcal{O}_K)[p^m]$ and $\mathrm{Sel}_{p^m} A$; this deviates from the standard discussion that concerns $\mathrm{Pic}(\mathcal{O}_K)[p^\infty]$ and $\mathrm{Sel}_{p^\infty} A$. Inequalities between Iwasawa invariants of class groups and Selmer groups result from the bounds of §§2-3 and are the subject of §7. The final §8 summarizes the conclusions for the cyclotomic $\mathbb{Z}_p$-extension (§§6-7 allow an arbitrary $\mathbb{Z}_p$-extension).

1.14. Notation. The notation set in this paragraph is in place for the rest of the paper; deviations, if any, are recorded in the beginning of each section. Let l be a prime, m a positive integer, and K a global field. If $\mathrm{char}\, K = 0$, let S be the spectrum of the ring of integers of K; if $\mathrm{char}\, K > 0$, let S be the proper smooth curve with function field K. Let v be a place of K and K_v the corresponding completion; if $v \nmid \infty$, then v identifies with a closed point of S, and $\mathcal{O}_v$ and $\mathbb{F}_v$ denote the ring of integers and the residue field of K_v. Let r_1 and r_2 be the number of real and complex places of K. Let $A \to \mathrm{Spec}\, K$ be an abelian variety of dimension $g > 0$ and $\mathcal{A} \to S$ its Néron model. For $v \in S$, let Φ_v be the étale $\mathbb{F}_v$-group scheme of connected components of $\mathcal{A}_{\mathbb{F}_v}$. For a finite extension L/K, the formation of S, $\mathcal{A}$, Φ_v is *not* compatible with base change, and we denote by S^L, $\mathcal{A}^L$, Φ_w^L their analogues over L (note that S^L is the normalization of S in L).

1.15. Conventions. To simplify the computations, $\gtrsim_{A,L,\ldots}$ and $\lesssim_{A,L,\ldots}$ denote inequalities up to implied constants that depend only on the indicated parameters (note that A, being a morphism $A \to \mathrm{Spec}\, K$, includes dependence on K); when no parameters are indicated, the ones used last are taken. Also, $\sim$ stands for "$\gtrsim$ and $\lesssim$". When needed (e.g., for forming composita or intersections), a choice of a separable closure $\overline{F}$ of a field F is made implicitly (and compatibly for overfields). The étale fundamental group of an integral scheme is based at the generic point. Fppf cohomology is denoted by H^i; when the coefficient sheaf is a smooth group scheme, the identification with étale cohomology [Gro68, 11.7 1°)] is implicit and similarly for further identifications with Galois cohomology. Fppf cohomology with compact supports that takes into account infinite primes [Mil06, III.0.6 (a)] is denoted by H^i_c. All quotients are taken in the big fppf topos, and X_{fppf} denotes the big fppf site of the scheme X. The l^m-Selmer group $\mathrm{Sel}_{l^m} A$ is the preimage of $\prod_v A(K_v)/l^m A(K_v) \subset \prod_v H^1(K_v, A[l^m])$ in $H^1(K, A[l^m])$ regardless of $\mathrm{char}\, K$. For a nonempty open $U \subset S$, the number of closed points of S not in U is $\#(S \backslash U)$. If $\mathrm{char}\, K = 0$, then $\mathrm{Pic}_+(S)$ is the narrow ideal class group of K; if $\mathrm{char}\, K > 0$, then $\mathrm{Pic}_+(S) := \mathrm{Pic}(S)$. For an integer n and a scheme X, the open subscheme on which n is invertible is $X[\frac{1}{n}]$.

Acknowledgements. I thank Bjorn Poonen for many helpful discussions and suggestions. I thank Julio Brau, Pete Clark, Tim Dokchitser, Jordan Ellenberg, Zev Klagsbrun, Barry Mazur, Filip Najman, Karl Rubin, Doug Ulmer, Jeanine van Order, Larry Washington, and David Zureick-Brown for helpful conversations or correspondence regarding the material of the paper. Part of the research presented here was carried out during the author's stay at the Centre Interfacultaire Bernoulli (CIB) in Lausanne during the course of the program "Rational points and algebraic cycles".

I thank CIB, NSF, and the organizers of the program for a lively semester and the opportunity to take part.

2. Lower bounds for Selmer groups in terms of class groups

Mimicking [Mil06, p. 178], for a nonempty open $U \subset S$ and a sheaf $\mathcal{F}$ on U_{fppf}, we define

$$D^1(U,\mathcal{F}) := \mathrm{Im}(H^1_c(U,\mathcal{F}) \to H^1(U,\mathcal{F})).$$

Proposition 2.1. *If $U \subset S$ is a nonempty open subscheme for which A has semiabelian reduction at all $v \in U$ with $\operatorname{char}\mathbb{F}_v = l$, then*

$$\begin{array}{ccc} D^1(U,\mathcal{A}[l^m]) & \hookrightarrow & H^1(K,A[l^m]) \\ \downarrow & & \downarrow \\ \prod_{v\in U} H^1(\mathcal{O}_v,\mathcal{A}[l^m]) \times \prod_{v\notin U} 0 & \hookrightarrow & \prod_v H^1(K_v,A[l^m]), \end{array}$$

is Cartesian. If, moreover, $l \neq \operatorname{char} K$ or $U = S$, then, taking intersections inside $H^1(K,A[l^m])$,

$$\#\left(\frac{D^1(U,\mathcal{A}[l^m])}{D^1(U,\mathcal{A}[l^m]) \cap \mathrm{Sel}_{l^m} A}\right) \leqslant \prod_{v\in U} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(l^m\Phi_v)(\mathbb{F}_v)},$$

$$\#\left(\frac{\mathrm{Sel}_{l^m} A}{D^1(U,\mathcal{A}[l^m]) \cap \mathrm{Sel}_{l^m} A}\right) \leqslant \prod_{v\in U} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(l^m\Phi_v)(\mathbb{F}_v)} \cdot \prod_{v\in S\setminus U} \left(l^{mg[K_v:\mathbb{Q}_l]} \cdot \#A(K_v)[l^m]\right) \cdot \prod_{\substack{\text{real } v \\ l=2}} \#\pi_0(A(K_v)),$$

where $[K_v:\mathbb{Q}_l] := 0$ unless K_v is a finite extension of $\mathbb{Q}_l$.

Proof. For the diagram, use the similar description of $H^1(U,\mathcal{A}[l^m]) \subset H^1(K,A[l^m])$ [Česl3, 4.2 and B.4] and the compactly supported cohomology exact sequence [Mil06, III.0.6 (a)]. For the inequalities, compare the defining local conditions by means of [Česl3, 2.5 (a)] and Proposition A.1. □

Theorem 2.2. *Suppose that $A[l^m]$ has a K-subgroup $G \cong \bigoplus_{i\in I} \mathbb{Z}/l^{a_i}\mathbb{Z} \oplus \bigoplus_{j\in J} \mu_{l^{b_j}}$ with $a_i, b_j \geqslant 1$.*

(a) Set $r := r_1$ if $l = 2$, and $r := 0$ if $l \neq 2$; also $\{v \mid l\} := \varnothing$ if $\operatorname{char} K > 0$. If $l \neq \operatorname{char} K$, then

$$\#\,\mathrm{Sel}_{l^m} A \gtrsim_{g,l,m} \frac{\prod_i \#\,\mathrm{Pic}(S[\frac{1}{l}])[l^{a_i}] \prod_j \#\,\mathrm{Pic}_+(S)[l^{b_j}]}{2^{r\cdot\#J} \cdot l^{r_2\sum_j b_j} \cdot \prod_{v\in S[\frac{1}{l}]} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(l^m\Phi_v)(\mathbb{F}_v)} \cdot \prod_j \prod_{v\mid l} \#\mu_{l^{b_j}}(K_v)}.$$

(b) If $J = \varnothing$ and A has semiabelian reduction at all v with $\operatorname{char}\mathbb{F}_v = l$, then

$$\#\,\mathrm{Sel}_{l^m} A \gtrsim_{g,l,m} \frac{\prod_i \#\,\mathrm{Pic}(S)[l^{a_i}]}{\prod_{v\nmid\infty} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(l^m\Phi_v)(\mathbb{F}_v)}}.$$

Proof. We give the similar proofs together. For (a), set $U := S[\frac{1}{l}]$; for (b), set $U := S$. By Proposition 2.1, $\#\,\mathrm{Sel}_{l^m} A \geqslant \#D^1(U,\mathcal{A}[l^m]) \cdot \left(\prod_{v\in U} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(l^m\Phi_v)(\mathbb{F}_v)}\right)^{-1}$. Let $\mathcal{G} \to U$ be the group smoothening of the schematic image of $G \to \mathcal{A}_U$; by [BLR90, 7.1/6], $\mathcal{G}$ is the Néron model of G, hence $\mathcal{G} \cong \bigoplus_i \mathbb{Z}/l^{a_i}\mathbb{Z} \oplus \bigoplus_j \mu_{l^{b_j}}$. The U-homomorphism $\mathcal{G} \xrightarrow{f} \mathcal{A}[l^m]$ has generic fiber $G \hookrightarrow A[l^m]$; moreover, $H^1(U,\mathcal{G}) \subset H^1(K,G)$ and $H^1(U,\mathcal{A}[l^m]) \subset H^1(K,A[l^m])$ [Česl3, A.5 and B.4]. Therefore, $\#\operatorname{Ker} H^1(f) \lesssim 1$, giving $\#D^1(U,\mathcal{A}[l^m]) \gtrsim \#D^1(U,\mathcal{G})$. The conclusion follows by combining the obtained inequalities with Lemmas B.3 and B.4 and the exact sequence [Mil06, III.0.6 (a)]. □

3. Upper bounds for Selmer groups in terms of class groups

Assume in this section that $l \neq \operatorname{char} K$. Contrary to the lower bounds in Theorem 2.2, we do not use implied constants in the upper bounds in Theorem 3.1. This makes the inequalities less pleasant but has the advantage of providing explicit lower bounds on the cardinalities of l-torsion subgroups of class groups when Theorem 3.1 is applied to an abelian variety of high rank. For instance, one may hope for a practical approach to Theorem 1.5: by finding an elliptic curve $E \to \operatorname{Spec} \mathbb{Q}$ for which $E(\mathbb{Q})[l] \neq 0$ with l odd and a quadratic $F/\mathbb{Q}$ for which $\operatorname{rk} E(F)$ is large, one would get a quadratic number field with large class group l-rank $r_l := \dim_{\mathbb{F}_l} \operatorname{Pic}(S^F)[l]$. The current records (among quadratic F) $r_3 = 6$ [Que87] and $r_5 = 4$ [Sch83] exploit relations with elliptic curves.

Theorem 3.1. *Fix a nonempty open $U \subsetneq S[\frac{1}{l}]$ for which $\mathcal{A}_U \to U$ is an abelian scheme. Set $r := r_1$ if $l = 2$, and $r := 0$ if $l \neq 2$; also $[K : \mathbb{Q}] := 0$ if $\operatorname{char} K > 0$. If $A[l^m]$ has a filtration by K-subgroups N_j with subquotients isomorphic to $\mathbb{Z}/l^{a_i}\mathbb{Z}$ or $\mu_{l^{b_j}}$ with $a_i, b_j \geqslant 1$, then*

$$\#\operatorname{Sel}_{l^m} A \leqslant \prod_i \#(\operatorname{Pic}_+ S/l^{a_i} \operatorname{Pic}_+ S) \prod_j \#\operatorname{Pic}(U)[l^{b_j}] \cdot l^{[K:\mathbb{Q}]\sum_i a_i + (r_1+r_2+\#(S\setminus U)-1)\sum_j b_j} \cdot \prod_j \#\mu_{l^{b_j}}(K) \cdot \prod_i \prod_{v\in S\setminus U} \#\mu_{l^{a_i}}(K_v),$$

and also

$$\#\operatorname{Sel}_{l^m} A \leqslant \prod_i \#(\operatorname{Pic} U/l^{a_i} \operatorname{Pic} U) \prod_j \#(\operatorname{Pic}_+ S/l^{b_j} \operatorname{Pic}_+ S) \cdot l^{mg[K:\mathbb{Q}] + (\#(S\setminus U)-1)\sum_i a_i + (r_1+r_2-1)\sum_j b_j} \cdot \prod_i 2^r \cdot \prod_{\substack{\text{real } v \\ l=2}} \#\pi_0(A(K_v))^{-1} \cdot \#A[l^m](K) \cdot \prod_j \prod_{v\in S\setminus U} \#\mu_{l^{b_j}}(K_v).$$

Proof. Let $\mathcal{N}_j$ be the schematic image of $N_j \to \mathcal{A}[l^m]_U$. By [EGA I, 9.5.5-6], [EGA IV$_2$, 2.8.5-6], [TO70, p. 17 Lemma 5], and finiteness of $\mathcal{A}[l^m]_U$, the $\mathcal{N}_j$ filter $\mathcal{A}[l^m]_U$ by finite étale U-subgroups. Due to finiteness, the étale subquotients $\mathcal{N}_{j+1}/\mathcal{N}_j$ are the Néron models of the N_{j+1}/N_j and hence identify with $\mathbb{Z}/l^{a_i}\mathbb{Z}$ or $\mu_{l^{b_j}}$. Therefore, Lemmas B.1 to B.4 bound $\#H^1(U, \mathcal{A}[l^m])$ and $\#H^1_c(U, \mathcal{A}[l^m])$ through cohomology sequences, and the claimed inequalities follow by combining these bounds with the following observations:

(i) For the first inequality: by [Čes13, 2.5 (d) and 4.2], $\#\operatorname{Sel}_{l^m} A \leqslant \#H^1(U, \mathcal{A}[l^m])$;

(ii) For the second: by [Mil06, III.0.6 (a)] and Proposition 2.1, writing $\widehat{H}^i$ for Tate cohomology,

$$\#D^1(U, \mathcal{A}[l^m]) \leqslant \#H^1_c(U, \mathcal{A}[l^m]) \cdot \prod_{v\in S\setminus U} \#A(K_v)[l^m]^{-1} \cdot \prod_{v|\infty} \#\widehat{H}^0(K_v, A[l^m])^{-1} \cdot \#A[l^m](K), \text{ and}$$

$$\frac{\#\operatorname{Sel}_{l^m} A}{\#D^1(U, \mathcal{A}[l^m])} \leqslant l^{mg[K:\mathbb{Q}]} \cdot \prod_{v\in S\setminus U} \#A(K_v)[l^m] \cdot \prod_{\substack{\text{real } v \\ l=2}} \#\pi_0(A(K_v));$$

moreover, if $l = 2$ and v is real, by Proposition A.1(c) and [GH81, 1.3],

$$\#\widehat{H}^0(K_v, A[l^m]) = \#H^1(K_v, A[l^m]) = \#\pi_0(A(K_v))^2. \qquad \square$$

Remarks.

3.2. The two bounds are incomparable in general; they yield different bounds in Proposition 7.3.

3.3. When $\mathbb{Z}/l^{a_i}\mathbb{Z} \cong \mu_{l^{a_i}}$ over K, the two interpretations of the corresponding subquotient result in different right hand sides of the inequalities of Theorem 3.1, and hence also in the flexibility of choosing the best bound. Similarly for $\mu_{l^{b_j}}$.

4. Growth of Selmer groups and class groups in extensions of bounded degree

Theorem 4.1. *Let L/K be an extension of degree at most d.*

(a) If either

(i) A has $\mathbb{Z}/l\mathbb{Z}$ or μ_l as a K-subgroup, and $l \neq \operatorname{char} K$, or

(ii) A has everywhere semiabelian reduction and $\mathbb{Z}/l\mathbb{Z}$ as a K-subgroup,

then

$$\#\operatorname{Sel}_{l^m} A_L \gtrsim_{A,d,l} \#\operatorname{Pic}(S^L)[l].$$

(b) If $l \neq \operatorname{char} K$ and $A[l]$ has a filtration with subquotients isomorphic to $\mathbb{Z}/l\mathbb{Z}$ or μ_l, then

$$\#\operatorname{Sel}_l A_L \lesssim_{A,d,l} \#\operatorname{Pic}(S^L)[l]^{2g}.$$

Proof.

(a) This follows from Theorem 2.2 since, letting w denote a place of L, we have

(1) $\#\operatorname{Pic}(S^L[\frac{1}{l}])[l] \sim_{K,d,l} \#\operatorname{Pic}(S^L)[l]$ if $\operatorname{char} K \neq l$, because $\#(S^L \backslash S^L[\frac{1}{l}])$ is bounded;

(2) $\#\operatorname{Pic}_+(S^L)[l] \sim_{K,d} \#\operatorname{Pic}(S^L)[l]$, because the number of real w is bounded;

(3) There is a bounded number of w's of bad reduction for A; moreover, for each such w,

(α) If $\operatorname{char} K = 0$, up to isomorphism there are only finitely many possibilities for A_{L_w}.

(β) In general, $\frac{\#\Phi_w^L(\mathbb{F}_w)}{\#(l\Phi_w^L)(\mathbb{F}_w)} \leqslant \#\Phi_w^L[l]$, and, if $l \neq \operatorname{char}\mathbb{F}_w$ or the reduction is semiabelian, then $\#\Phi_w^L[l] \leqslant \#\mathcal{A}^L[l]_{\mathbb{F}_w} \sim_{g,l} 1$, as is seen by inspecting the finite part [EGA IV$_4$, 18.5.11 c)] of the quasi-finite separated $\mathcal{A}^L[l]_{\mathcal{O}_w}$.

(b) This follows from (either part of) Theorem 3.1: one argues as in (1) and (2) and uses

(4) $\#(\operatorname{Pic}_+ S^L/l\operatorname{Pic}_+ S^L) \sim_{K,d,l} \#\operatorname{Pic}(S^L)[l]$. □

Corollary 4.2. *If either (i) or (ii) of Theorem 4.1(a) hold, then $\#\operatorname{Sel}_l A_L$ is unbounded as L/K ranges over degree l extensions.*

Proof. Indeed, $\#\operatorname{Pic}(S^L)[l]$ is unbounded [Mad72, Thm. 3]. □

Corollary 4.3. *If $l \neq \operatorname{char} K$, then $\#\operatorname{Sel}_l A_L$ is unbounded as L/K ranges over extensions of degree at most $l^{2g+1} - l$.*

Proof. Indeed, A acquires a nontrivial l-torsion point over an extension of degree at most $l^{2g}-1$. □

Remark 4.4. There are several results in the literature concerned with proving the unboundedness of $\#Ш(A_L)[l]$ (and hence that of $\#\operatorname{Sel}_l A_L$) as L ranges over degree l extensions of K: [CS10, Thm. 3] treats the case $\dim A = 1$ and $l \neq \operatorname{char} K$, whereas [Cre11, Thm. 1.1], improving [Cla04, Thm. 7], allows arbitrary dimension but imposes restrictions (which are satisfied after passing to a finite extension) on the Néron-Severi group of A. In contrast, Corollary 4.2 has no dimension or Néron-Severi assumptions but constrains $A[l]$ and only gives Selmer growth.

If $l \neq \operatorname{char} K$, the assumptions of (a) and (b) in Theorem 4.1 are satisfied after passing to a suitable finite extension K'/K; standard lemmas 4.5 and 4.6, which are also used in §7, clarify in Corollary 4.8 how this affects the unboundedness questions.

Lemma 4.5. *Let L be a global field and L'/L an extension of degree at most d. Then*

$$\#\operatorname{Pic}(S^{L'})[n] \gtrsim_{d,n} \#\operatorname{Pic}(S^L)[n].$$

Proof. For number fields, the claim is clear from the theory of the Hilbert class field: if H/L is an unramified abelian extension with Galois group killed by n, then so is HL'/L', for which $[HL' : L'] \geqslant \frac{1}{d}[H : L]$. The proof in the function field case is the same – the link to unramified abelian extensions is provided by Lemma B.1(a) applied to the prime factors of n: $\#\operatorname{Pic}(S^L)[n] \sim_n \#H^1(S^L, \mathbb{Z}/n\mathbb{Z}) = \#\operatorname{Hom}(\pi_1^{\text{ét}}(S^L), \mathbb{Z}/n\mathbb{Z}) = [H_L : L]$ where H_L/L is the maximal (in $\overline{L}$) unramified abelian extension with Galois group killed by n, and similarly for L'. □

Lemma 4.6. *Let L be a global field, A a g-dimensional abelian variety over L, and L'/L an extension of degree at most d. If $\operatorname{char} L \nmid n$, then*

$$\#\operatorname{Sel}_n A_{L'} \gtrsim_{d,g,n} \#\operatorname{Sel}_n A.$$

Proof. Let $\mathrm{R}_{L'/L}$ denote the restriction of scalars. By [CGP10, A.5.1-2, A.5.4 (1), A.5.7],

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A[n] & \longrightarrow & A & \xrightarrow{n} & A & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathrm{R}_{L'/L}(A[n]_{L'}) & \longrightarrow & \mathrm{R}_{L'/L}(A_{L'}) & \xrightarrow{n} & \mathrm{R}_{L'/L}(A_{L'}) & \longrightarrow & 0 \end{array} \tag{1}$$

is a morphism of short exact (in the big étale site of L) sequences of smooth L-group schemes. Moreover, $\mathrm{R}_{L'/L}(A[n]_{L'})$ is finite étale with $\#\mathrm{R}_{L'/L}(A[n]_{L'}) \sim 1$: for separable L'/L, this is evident after base change to L', [CGP10, A.5.13] handles the purely inseparable case, and in general one uses the transitivity of $\mathrm{R}_{L'/L}$. Consequently, $\#\operatorname{Ker} H^1_{\text{ét}}(a) \sim 1$, and since $H^i_{\text{ét}}(L, \mathrm{R}_{L'/L}(A[n]_{L'})) \cong H^i_{\text{ét}}(L', A[n])$ [SGA $4\frac{1}{2}$, p. 24 II.3.6], it remains to see that $H^1_{\text{ét}}(a)$ respects the n-Selmer subgroups. This is evident from the compatibility of the formation of (1) with any base change and the well known $L' \otimes_L L_v \cong \prod_{w|v} L'_w$ [Ser79, II.§3 Thm. 1 (iii)] for a place v of L. □

Remark 4.7. For separable L'/L, one reduces to the Galois case and applies the inflation-restriction sequence in Galois cohomology to obtain another proof of Lemma 4.6.

Corollary 4.8. *Let L/K range in a family of finite extensions of bounded degree.*

- *(a) For a finite extension K'/K for which either (i) or (ii) of Theorem 4.1(a) hold, if $\#\operatorname{Pic}(S^L)[l]$ is unbounded, then so is $\#\operatorname{Sel}_l A_{K'L}$.*
- *(b) Assume that $l \neq \operatorname{char} K$. For a finite extension K'/K for which $A[l]_{K'}$ has a filtration with subquotients isomorphic to $\mathbb{Z}/l\mathbb{Z}$ or μ_l, if $\#\operatorname{Sel}_l A_L$ is unbounded, then so is $\#\operatorname{Pic}(S^{K'L})[l]$.*

Proof. Combine Theorem 4.1 with Lemmas 4.5 and 4.6. □

5. Special cases of the function field analogues of Conjectures 1.1 and 1.2

For this section, fix a prime p and suppose that $\operatorname{char} K = p$, i.e., K is a finite extension of $\mathbb{F}_p(t)$. The analogues in question assume that $l \neq p$ and predict that $\#\operatorname{Pic}(S^L)[l]$ and $\#\operatorname{Sel}_l A_L$ should be unbounded as L ranges over quadratic extensions of K. We show that this is indeed the case if one

replaces K by a finite extension depending on l (and also on A in the Selmer group case). The key input is the work of Shafarevich and Tate [TŠ67] on unboundedness of ranks of quadratic twists of a constant supersingular elliptic curve.

Theorem 5.1. *For each prime power l^m with $l \neq p$, there is a $q = p^{n(l,m)}$ such that if $\mathbb{F}_q \subset K$, then the number of $\mathbb{Z}/l^m\mathbb{Z}$-summands of $\mathrm{Pic}(S^L)[l^m]$ is unbounded as L/K ranges over quadratic extensions of the form $L = L'K$ for quadratic extensions $L'/\mathbb{F}_p(t)$. In particular, with $n := n(l,1)$, the analogue of Conjecture 1.1 holds for l and every global field containing $\mathbb{F}_{p^n}$.*

Proof. Take a supersingular elliptic curve $E \to \operatorname{Spec} \mathbb{F}_p$ (see [Wat69, 4.1 (5)] for its existence proved by Deuring). Let q be such that $E_{\mathbb{F}_q}[l^m] \cong \mathbb{Z}/l^m\mathbb{Z} \oplus \mu_{l^m}$, and hence also $E_{S^L}[l^m] \cong \mathbb{Z}/l^m\mathbb{Z} \oplus \mu_{l^m}$ for every L. By [Čes13, 5.4 (c)], $H^1(S^L, E_{S^L}[l^m]) = \mathrm{Sel}_{l^m} E_L$, and by the result of Shafarevich and Tate [Ulm07, 1.4], $\operatorname{rk} E(L)$ and hence also the number of $\mathbb{Z}/l^m\mathbb{Z}$-summands of $\mathrm{Sel}_{l^m} E_L$ are unbounded. It remains to note that by the proofs of Lemmas B.1 and B.2, $\mathrm{Sel}_{l^m} E_L \cong H^1(S^L, \mathbb{Z}/l^m\mathbb{Z} \oplus \mu_{l^m})$ admits a map to $\operatorname{Hom}(\mathrm{Pic}(S^L)/l^m \operatorname{Pic}(S^L), \mathbb{Z}/l^m\mathbb{Z}) \oplus \mathrm{Pic}(S^L)[l^m]$ with kernel of bounded size. □

Remarks.

5.2. For a composite $l_1^{m_1} \cdot \ldots \cdot l_k^{m_k}$ prime to p, the proof gives a $q = p^{n(l_1,m_1,\ldots,l_k,m_k)}$ such that for every finite extension $K/\mathbb{F}_q(t)$, the unbounded growth of the number of $\mathbb{Z}/l_i^{m_i}\mathbb{Z}$-summands of $\mathrm{Pic}(S^L)[l_i^{m_i}]$ is simultaneous as L/K ranges over quadratic extensions (of the form $L = L'K$ as in Theorem 5.1).

5.3. A possible choice for $n(l,m)$ is $2n$ with $(-p)^n \equiv 1 \bmod l^m$ (e.g., $n(l,m) := 2l^{m-1}(l-1)$): in the proof take the supersingular $E \to \operatorname{Spec} \mathbb{F}_p$ which has $x^2 + p$ as the characteristic polynomial of the p-power Frobenius Frob_p, so $\mathrm{Frob}_{p^{2n}}$ fixes $E[l^m]$.

Corollary 5.4. *If $l \neq p$, then there is a finite extension K'/K (depending on l and A) such that the analogue of Conjecture 1.2 holds for $A_{K''}$ and l for every finite extension K''/K', i.e., $\#\operatorname{Sel}_l A_L$ is unbounded as L/K'' ranges over quadratic extensions.*

Proof. Due to Theorems 4.1(a) and 5.1, it suffices to choose K' to contain $\mathbb{F}_{p^n}$ with $n = n(l,1)$ and satisfy either $\mathbb{Z}/l\mathbb{Z} \subset A[l]_{K'}$ or $\mu_l \subset A[l]_{K'}$. □

6. Iwasawa theory of class groups and Selmer groups

To keep the discussion focused, we assume in this and the next two sections that K is a number field, even though the question of function field analogues is an interesting one. Likewise, we set aside the possibility of more general p-adic Lie extensions and fix a $\mathbb{Z}_p$-extension K_∞/K. Concretely, K_∞/K is Galois with $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$; we fix a choice of the latter isomorphism, which identifies the Iwasawa algebra Λ of K_∞/K with $\mathbb{Z}_p[[T]]$. We denote by $v_1, \ldots, v_k$ the places of K ramified in K_∞, so $k \geqslant 1$ and $v_i \mid p$, and by K_n the subfield of K_∞ fixed by $p^n\mathbb{Z}_p$.

6.1. Iwasawa theory of class groups. Let M be the maximal unramified abelian pro-p extension of K_∞. Set $X := \mathrm{Gal}(M/K_\infty)$, which is a finitely generated torsion Λ-module (cf. [Ser58, Thm. 5 and §5]). The structure theory of such Λ-modules gives a Λ-homomorphism

$$X \to \bigoplus_i \Lambda/f_i^{l_i}\Lambda \oplus \bigoplus_j \Lambda/p^{m_j}\Lambda,$$

with finite kernel and cokernel (i.e., a *pseudo-isomorphism*) for uniquely determined $m_j \in \mathbb{Z}_{>0}$, monic polynomials $f_i \in \mathbb{Z}_p[[T]]$ that are monomials mod p, and $l_i \in \mathbb{Z}_{>0}$. The λ- and μ-invariants

of K_∞/K are

$$\lambda_{\mathrm{Pic}} := \sum l_i \deg f_i, \qquad \mu_{\mathrm{Pic}} := \sum m_j.$$

We also set $\mu_{\mathrm{Pic}}^{(m)} := \sum_j \min(m_j, m)$ for $m \geqslant 0$, which is of interest because it governs the growth of $\#\operatorname{Pic}(S^{K_n})[p^m]$ (as opposed to the customary in Iwasawa theory $\#\operatorname{Pic}(S^{K_n})[p^\infty]$):

Proposition 6.2. $\#\operatorname{Pic}(S^{K_n})[p^m] \sim_{K,K_\infty,m} p^{\mu_{\mathrm{Pic}}^{(m)} p^n}$.

Before giving the proof we record a trivial lemma that clarifies implicit computations in subsequent arguments involving pseudo-isomorphisms; the lemma will be used without explicit notice.

Lemma 6.3. *Let R be a commutative ring, and let $X \xrightarrow{f} Y$ be a homomorphism of R-modules with finite kernel and cokernel. For $r \in R$, the induced $X/rX \xrightarrow{f_{/r}} Y/rY$ and $X[r] \xrightarrow{f_{[r]}} Y[r]$ satisfy*

$$\#\operatorname{Ker} f_{/r} \leqslant \#\operatorname{Ker} f \cdot \#\operatorname{Coker} f, \qquad \#\operatorname{Coker} f_{/r} \leqslant \#\operatorname{Coker} f,$$
$$\#\operatorname{Ker} f_{[r]} \leqslant \#\operatorname{Ker} f, \qquad \#\operatorname{Coker} f_{[r]} \leqslant \#\operatorname{Ker} f \cdot \#\operatorname{Coker} f.$$

Proof. Apply the snake lemma twice. □

Proof of Proposition 6.2. Replacing K by K_n has the effect of multiplying $\mu_{\mathrm{Pic}}^{(m)}$ by p^n (since $\mathbb{Z}_p[[T]]$ is replaced by $\mathbb{Z}_p[[(T+1)^{p^n}-1]]$). By choosing n large, we are therefore reduced to the case when each v_i is totally ramified in K_∞.

In this case, by [Ser58, Thm. 4], as $\mathbb{Z}_p$-modules, $\operatorname{Pic}(S^{K_n})[p^\infty]$ is isomorphic to the quotient of the finitely generated $X/((T+1)^{p^n}-1)X$ by a submodule generated by k elements. Hence

$$\#\operatorname{Pic}(S^{K_n})[p^m] \sim \#(X/((T+1)^{p^n}-1)X)[p^m] \sim \prod_j \#(\Lambda/(p^{m_j}, (T+1)^{p^n}-1))[p^m] = p^{\mu_{\mathrm{Pic}}^{(m)} p^n}. \ \square$$

6.4. Iwasawa theory of Selmer groups. The *p^∞-Selmer group* of A_{K_n} is

$$\operatorname{Sel}_{p^\infty} A_{K_n} := \varinjlim_m \operatorname{Sel}_{p^m} A_{K_n},$$

and that of A_{K_∞} is

$$\operatorname{Sel}_{p^\infty} A_{K_\infty} := \varinjlim_n \operatorname{Sel}_{p^\infty} A_{K_n}.$$

For the compact Pontryagin dual $X' := \operatorname{Hom}(\operatorname{Sel}_{p^\infty} A_{K_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$, one knows

Claim 6.4.1. The Λ-module X' is finitely generated.

Proof. Fix a nonempty open $U \subset S[\frac{1}{p}]$ for which $\mathcal{A}_U \to U$ is an abelian scheme. Finiteness of $H^1_{\text{ét}}(U, \mathcal{A}[p])$ [Mil06, II.2.13] implies that of $H^1_{\text{ét}}(U, \mathcal{A}[p^\infty])[p]$: the exact sequences

$$0 \to \mathcal{A}[p]_U \to \mathcal{A}[p^n]_U \xrightarrow{p} \mathcal{A}[p^{n-1}]_U \to 0,$$
$$0 \to \mathcal{A}[p^{n-1}]_U \to \mathcal{A}[p^n]_U \xrightarrow{p^{n-1}} \mathcal{A}[p]_U \to 0$$

give $\#H^1_{\text{ét}}(U, \mathcal{A}[p^n])[p] \leqslant \#H^1_{\text{ét}}(U, \mathcal{A}[p]) \cdot \#A(K)[p]$. Consequently, $H^1_{\text{ét}}(U, \mathcal{A}[p^\infty])$ is $\mathbb{Z}_p$-cofinitely generated.

Let $U_\infty := \varprojlim U_{S^{K_n}}$ be the normalization of U in K_∞. Since U_∞/U is pro-(finite étale Galois), the Hochschild-Serre spectral sequence

$$H^i(\operatorname{Gal}(K_\infty/K), H^j_{\text{ét}}(U_\infty, \mathcal{A}[p^\infty])) \Rightarrow H^{i+j}_{\text{ét}}(U, \mathcal{A}[p^\infty])$$

shows that $H^1_{\text{ét}}(U_\infty, \mathcal{A}[p^\infty])^{\mathrm{Gal}(K_\infty/K)}$ is $\mathbb{Z}_p$-cofinitely generated. Therefore, so is

$$(\mathrm{Sel}_{p^\infty} A_{K_\infty})^{\mathrm{Gal}(K_\infty/K)} \subset H^1_{\text{ét}}(U_\infty, \mathcal{A}[p^\infty])^{\mathrm{Gal}(K_\infty/K)}.$$

Pontryagin duality then gives the finiteness of $X'/(T,p)$, and it remains to invoke the relevant version of Nakayama's lemma [Ser58, Lemme 4]. □

Claim 6.4.1 and the structure theory of finitely generated Λ-modules give a pseudo-isomorphism

$$X' \to \Lambda^\rho \oplus \bigoplus_s \Lambda/f_s^{l'_s}\Lambda \oplus \bigoplus_t \Lambda/p^{m'_t}\Lambda \tag{2}$$

as in 6.1 (with similar uniqueness claims). However, unlike X, the Λ-module X' need not be torsion, i.e., $\rho > 0$ is possible. As for class groups, set $\mu^{(m)}_{\mathrm{Sel}} := \sum_t \min(m'_t, m)$ for $m \geqslant 0$.

6.5. Controlled growth. We say that *the control theorem holds* for A and K_∞, if

$$\mathrm{Sel}_{p^\infty} A_{K_n} \to (\mathrm{Sel}_{p^\infty} A_{K_\infty})^{\mathrm{Gal}(K_\infty/K_n)} \quad \text{for } n \geqslant 0$$

has finite kernel and cokernel of order bounded independently of n. The first result of this type is due to Mazur [Maz72, 6.4 (i)]; it has subsequently been generalized by Greenberg [Gre03, 5.1]: potential good ordinary reduction of A at all $v \mid p$ is sufficient for the control theorem to hold. Such results play a purely axiomatic role in our computations:

Proposition 6.6. *$\#\,\mathrm{Sel}_{p^m} A_{K_n} \sim_{A,K_\infty,m} p^{(\rho m + \mu^{(m)}_{\mathrm{Sel}})p^n}$, if the control theorem holds for A and K_∞.*

To replace $\mathrm{Sel}_{p^m} A_{K_n}$ by $(\mathrm{Sel}_{p^\infty} A_{K_n})[p^m]$ we will need a quantitative version of [BKL+13, 5.9]:

Lemma 6.7. *Let $A \to \operatorname{Spec} K$ be an abelian variety over a global field, p a prime, and $a, b \in \mathbb{Z}_{>0}$.*

(a) The kernel and cokernel of $\mathrm{Sel}_a A \to (\mathrm{Sel}_{ab} A)[a]$ are of size at most $\#A[a](K)$.

(b) The kernel and cokernel of $\mathrm{Sel}_{p^m} A \to (\mathrm{Sel}_{p^\infty} A)[p^m]$ are of size at most $\#A[p^m](K)$.

Proof. Part (b) is obtained from (a) by taking direct limits. As for (a), the cohomology sequence of $0 \to A[a] \to A[ab] \xrightarrow{a} A[b] \to 0$ gives the kernel claim since $\frac{\#A[a](K)\cdot\#A[b](K)}{\#A[ab](K)} \leqslant \#A[a](K)$. Selmer groups consist of H^1-classes that vanish in every $H^1(K_v, A)$, so $\frac{(\mathrm{Sel}_{ab} A)[a]}{\mathrm{Im}(\mathrm{Sel}_a A)} \hookrightarrow \frac{H^1(K, A[ab])[a]}{\mathrm{Im}(H^1(K, A[a]))}$, and the cokernel claim results from the injection $\frac{H^1(K, A[ab])[a]}{\mathrm{Im}(H^1(K, A[a]))} \hookrightarrow \mathrm{Ker}\left(H^1(K, A[b]) \to H^1(K, A[ab])\right)$. □

Proof of Proposition 6.6. By Lemma 6.7(b), the control theorem, and the Pontryagin duality,

$$\#\,\mathrm{Sel}_{p^m} A_{K_n} \sim \#(\mathrm{Sel}_{p^\infty} A_{K_n})[p^m] \sim \#(\mathrm{Sel}_{p^\infty} A_{K_\infty})^{\mathrm{Gal}(K_\infty/K_n)}[p^m] \sim \#\left(X'/(p^m, (T+1)^{p^n} - 1)\right).$$

Therefore, the desired conclusion results from (2) (and Lemma 6.3). □

7. Relations between the Iwasawa invariants of Selmer groups and class groups

We keep the setup of §6 and denote by ord_p the p-adic valuation normalized by $\mathrm{ord}_p\, p = 1$.

Proposition 7.1. *Suppose that the control theorem holds for A and K_∞, and let Σ be the set of finite places of K that decompose completely in K_∞.*

(a) *If* $A[p^m]$ *has* $\bigoplus_i \mathbb{Z}/p^{a_i}\mathbb{Z} \oplus \bigoplus_j \mu_{p^{b_j}}$ *with* $a_i, b_j \geqslant 1$ *as a* K*-subgroup,* $p \neq 2$*, and each* $v \mid p$ *is finitely decomposed in* K_∞*, then*

$$\rho m + \mu_{\mathrm{Sel}}^{(m)} \geqslant \sum_i \mu_{\mathrm{Pic}}^{(a_i)} + \sum_j \mu_{\mathrm{Pic}}^{(b_j)} - r_2 \sum_j b_j - \sum_{v \in \Sigma} \mathrm{ord}_p \left(\frac{\#\Phi_v(\mathbb{F}_v)}{\#(p^m \Phi_v)(\mathbb{F}_v)} \right).$$

(b) *If* $A[p^m]$ *has* $\bigoplus_i \mathbb{Z}/p^{a_i}\mathbb{Z}$ *with* $a_i \geqslant 1$ *as a* K*-subgroup and* A *has semiabelian reduction at all* $v \mid p$*, then*

$$\rho m + \mu_{\mathrm{Sel}}^{(m)} \geqslant \sum_i \mu_{\mathrm{Pic}}^{(a_i)} - \sum_{v \in \Sigma} \mathrm{ord}_p \left(\frac{\#\Phi_v(\mathbb{F}_v)}{\#(p^m \Phi_v)(\mathbb{F}_v)} \right).$$

Proof. Combining Propositions 6.2 and 6.6 with Theorem 2.2 and using (1)-(4) below, we get

$$p^{(\rho m + \mu_{\mathrm{Sel}}^{(m)})p^n} \gtrsim_{A,K_\infty,m} p^{\left(\sum_i \mu_{\mathrm{Pic}}^{(a_i)} + \sum_j \mu_{\mathrm{Pic}}^{(b_j)} - r_2 \sum_j b_j\right)p^n} \cdot \left(\prod_{v \in \Sigma} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(p^m \Phi_v)(\mathbb{F}_v)} \right)^{-p^n} \quad \text{and}$$

$$p^{(\rho m + \mu_{\mathrm{Sel}}^{(m)})p^n} \gtrsim_{A,K_\infty,m} p^{\left(\sum_i \mu_{\mathrm{Pic}}^{(a_i)}\right)p^n} \cdot \left(\prod_{v \in \Sigma} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(p^m \Phi_v)(\mathbb{F}_v)} \right)^{-p^n}$$

in cases (a) and (b), respectively; the claimed inequalities follow by taking n large enough.

(1) $\#\operatorname{Pic}(S^{K_n}[\frac{1}{p}])[p^{a_i}] \sim \#\operatorname{Pic}(S^{K_n})[p^{a_i}]$ in (a), since $\#(S^{K_n} \backslash S^{K_n}[\frac{1}{p}])$ is bounded.

(2) The number of complex places of K_n is $r_2 p^n$.

(3) Since $S^{K_n}[\frac{1}{p}] \to S[\frac{1}{p}]$ is étale, $\prod_{\substack{w \nmid p\infty \\ w \text{ not above } \Sigma}} \#\Phi_w^{K_n} \sim 1$ where w denotes a place of K_n.

(4) For a place w of semiabelian reduction for A_{K_n}, one has $\frac{\#\Phi_w^{K_n}(\mathbb{F}_w)}{\#(p^m \Phi_w^{K_n})(\mathbb{F}_w)} \leqslant \#\Phi_w^{K_n}[p^m] \leqslant p^{2mg}$ where the last step uses surjectivity of multiplication by p^m on $(\mathcal{A}^{K_n})^0(\overline{\mathbb{F}}_w)$ and the consideration of the finite part [EGA IV$_4$, 18.5.11 c)] of the quasi-finite separated $(\mathcal{A}^{K_n}[p^m])_{\mathcal{O}_w}$. □

Remark 7.2. The control theorem can hold in presence of completely decomposed places of bad reduction for A, see [Gre03, 5.1].

Proposition 7.3. *Set* $r := r_1$ *if* $p = 2$*, and* $r := 0$ *if* $p \neq 2$*. Suppose that the control theorem holds for* A *and* K_∞*, and every place* v *above* p *or of bad reduction for* A *is finitely decomposed in* K_∞*. If* $A[p^m]$ *has a filtration by* K*-subgroups with subquotients isomorphic to* $\mathbb{Z}/p^{a_i}\mathbb{Z}$ *or* $\mu_{p^{b_j}}$ *with* $a_i, b_j \geqslant 1$*, then*

$$\rho m + \mu_{\mathrm{Sel}}^{(m)} \leqslant 2mg[K:\mathbb{Q}] - r_2 \sum_j b_j + \sum_i (\mu_{\mathrm{Pic}}^{(a_i)} + r) + \sum_j \mu_{\mathrm{Pic}}^{(b_j)},$$

and also

$$\rho m + \mu_{\mathrm{Sel}}^{(m)} \leqslant mg[K:\mathbb{Q}] + (r_1 + r_2) \sum_j b_j + \sum_i (\mu_{\mathrm{Pic}}^{(a_i)} + r) + \sum_j (\mu_{\mathrm{Pic}}^{(b_j)} + r) - \sum_{\substack{\text{real } v \\ p=2}} \mathrm{ord}_2(\#\pi_0(A(K_v))).$$

Proof. Combining Propositions 6.2 and 6.6 with Theorem 3.1 applied to $U_{S^{K_n}}$, where U is the largest open subscheme of $S[\frac{1}{p}]$ for which $\mathcal{A}_U \to U$ is an abelian scheme, and using (1)-(3) below,

we get

$$p^{(\rho m+\mu_{\mathrm{Sel}}^{(m)})p^n} \lesssim_{A,K_\infty,m} p^{\left(\sum_i(\mu_{\mathrm{Pic}}^{(a_i)}+r)+\sum_j \mu_{\mathrm{Pic}}^{(b_j)}+[K:\mathbb{Q}]\sum_i a_i+(r_1+r_2)\sum_j b_j\right)p^n} \quad \text{and}$$

$$p^{(\rho m+\mu_{\mathrm{Sel}}^{(m)})p^n} \lesssim_{A,K_\infty,m} p^{\left(\sum_i(\mu_{\mathrm{Pic}}^{(a_i)}+r)+\sum_j(\mu_{\mathrm{Pic}}^{(b_j)}+r)+mg[K:\mathbb{Q}]+(r_1+r_2)\sum_j b_j\right)p^n} \left(\prod_{\substack{\text{real } v\\ p=2}} \#\pi_0(A(K_v))\right)^{-p^n}.$$

The claimed inequalities follow by taking n large enough.

(1) Each infinite place of K is completely decomposed in K_∞.

(2) $\#(\mathrm{Pic}_+(S^{K_n})/p^{a_i}\,\mathrm{Pic}_+(S^{K_n})) \leqslant 2^{rp^n}\cdot \#\,\mathrm{Pic}(S^{K_n})[p^{a_i}]$.

(3) $\#\,\mathrm{Pic}(U_{S^{K_n}})[p^{b_j}] \sim_{A,K_\infty,m} \#\,\mathrm{Pic}(S^{K_n})[p^{b_j}]$, since $\#(S^{K_n}\backslash U_{S^{K_n}})$ is bounded. □

Corollary 7.4. *Suppose that the control theorem holds for A and K_∞, and every place v above p or of bad reduction for A is finitely decomposed in K_∞. If $A[p]$ has a filtration by K-subgroups with a subquotients isomorphic to $\mathbb{Z}/p\mathbb{Z}$ and b subquotients isomorphic to μ_p with $a+b=2g$, then*

$$\rho \leqslant g[K:\mathbb{Q}] + ar + 2g\mu_{\mathrm{Pic}}^{(1)} + \min\left(g[K:\mathbb{Q}] - r_2 b,\ b(r_1+r_2+r)\right).$$

Proof. Since $0 \subset A[p] \subset A[p^2] \subset \ldots \subset A[p^m]$ has subquotients $A[p]$, Proposition 7.3 applies. □

Remark 7.5. Remark 3.3 applies equally well to Proposition 7.3 and Corollary 7.4.

7.6. The assumptions on $A[p^m]$ in Propositions 7.1 and 7.3 are satisfied after replacing K by a finite extension K'. We record how this affects the Iwasawa invariants involved in the obtained inequalities. Set $K'_\infty := K'K_\infty$, and write K'_n, μ'_{Pic}, ρ', μ'_{Sel}, etc. for K'_∞/K' analogues of the familiar notation.

Lemma 7.7. *One has $\mu_{\mathrm{Pic}}^{(m)} \leqslant \mu_{\mathrm{Pic}}^{\prime(m)}$ for all $m \geqslant 0$. In particular, $\mu_{\mathrm{Pic}} \leqslant \mu'_{\mathrm{Pic}}$.*

Proof. If $K' \cap K_\infty = K_n$, then Lemma 4.5 and Proposition 6.2 give $p^n\mu_{\mathrm{Pic}}^{(m)} \leqslant \mu_{\mathrm{Pic}}^{\prime(m)}$. □

Lemma 7.8. *Suppose that the control theorem holds for A and K_∞ and also for $A_{K'}$ and K'_∞. Then $\rho m + \mu_{\mathrm{Sel}}^{(m)} \leqslant \rho' m + \mu_{\mathrm{Sel}}^{\prime(m)}$ for all $m \geqslant 0$. In particular, $\rho \leqslant \rho'$, and if $\rho' = 0$, then $\mu_{\mathrm{Sel}} \leqslant \mu'_{\mathrm{Sel}}$.*

Proof. If $K' \cap K_\infty = K_n$, then Lemma 4.6 and Proposition 6.6 give $p^n(\rho m + \mu_{\mathrm{Sel}}^{(m)}) \leqslant \rho' m + \mu_{\mathrm{Sel}}^{\prime(m)}$. □

8. Conclusions for the cyclotomic $\mathbb{Z}_p$-extension

Keeping the setup of §6, we now assume that K_∞/K is the cyclotomic $\mathbb{Z}_p$-extension, i.e., the unique $\mathbb{Z}_p$-subextension of $K(\mu_{p^\infty})/K$. No anomalies occur: every finite v is finitely decomposed in K_∞, and for a finite extension K'/K, the compositum $K'_\infty := K'K_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of K'.

Conjecture 8.1 (Iwasawa [Iwa71, p. 392], [Iwa73, p. 11])**.** $\mu_{\mathrm{Pic}} = 0$.

Conjecture 8.2 (Mazur [Maz72, p. 184])**.** *If A has good ordinary reduction at all $v \mid p$, then $\rho = 0$.*

8.3. Status of 8.1 and 8.2. Conjecture 8.1 is known for abelian $K/\mathbb{Q}$ [FW79]; Conjecture 8.2 is known for $A = E_K$, if p is odd, $E \to \operatorname{Spec} \mathbb{Q}$ is an elliptic curve with good ordinary reduction at p, and $K/\mathbb{Q}$ is abelian [Kat04, 17.4], [Roh84], and also for A with finite $\mathrm{Sel}_{p^\infty} A$, as the control theorem shows. Examples with $\mu_{\mathrm{Sel}} > 0$ are known, and in fact $\mu^{(1)}_{\mathrm{Sel}}$ can be arbitrarily large when K is allowed to vary, as Example 8.8 shows.

The inequalities of §7 allow one to relate Conjectures 8.1 and 8.2:

Theorem 8.4. *If $\rho + \mu_{\mathrm{Sel}} = 0$, the control theorem holds for A and K_∞, and*

(i) A has $\mathbb{Z}/p\mathbb{Z}$ as a K-subgroup and semiabelian reduction at all $v \mid p$, or

(ii) p is odd, and A has $\mathbb{Z}/p\mathbb{Z}$ as a K-subgroup, or

(iii) p is odd, K is totally real, and A has μ_p as a K-subgroup,

then $\mu_{\mathrm{Pic}} = 0$.

Proof. The conclusion is immediate from Proposition 7.1, because $\Sigma = \varnothing$. □

Adopting the notation of 7.6, one can use the results of §7 to study boundedness questions:

Theorem 8.5. *If $K = \mathbb{Q}$, the reduction of A at p is good ordinary, and $A[p]$ has a filtration by K-subgroups with subquotients isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or μ_p, then $\rho' \lesssim_{d,g} 1$ and $\mu'^{(1)}_{\mathrm{Sel}} \lesssim_{d,g} 1$ for an abelian extension $K'/\mathbb{Q}$ of degree d.*

Proof. Indeed, $\mu'_{\mathrm{Pic}} = 0$ (cf. 8.3), so Proposition 7.3 gives the claim. □

Remarks.

8.6. If one assumes Conjecture 8.1, then the abelian restriction on $K'/\mathbb{Q}$ is not needed; in fact, one can then also drop the assumption on $A[p]$ and get the $\rho', \mu'^{(1)}_{\mathrm{Sel}} \lesssim_{d,g,p} 1$ conclusion with the help of Lemma 7.8. Conversely, due to Proposition 7.1 and Lemma 7.8, such a conclusion for all d and a single A with good ordinary reduction at p would give $\mu'^{(1)}_{\mathrm{Pic}} \lesssim_{d,p} 1$. Due to Proposition 7.3 and Lemma 7.7, this would in turn imply $\rho', \mu'^{(1)}_{\mathrm{Sel}} \lesssim_{d,g,p} 1$ for *every* A with good ordinary reduction at p. Is there a way to prove $\rho', \mu'^{(1)}_{\mathrm{Sel}} \lesssim_{d,g,p} 1$ for a single such A without restricting to abelian $K'/\mathbb{Q}$ and relying on Conjecture 8.1?

8.7. If $d = g = 1$ and the reduction of A at p is good ordinary (but no assumption on $A[p]$), then Greenberg has conjectured that $\mu'^{(1)}_{\mathrm{Sel}} \leqslant 1$ [Gre99, 1.11 and p. 118 Remark]. We show that $\mu'^{(1)}_{\mathrm{Sel}}$ can grow unboundedly as d grows:

Example 8.8. Suppose that $\mathcal{A}[p] \cong (\mathbb{Z}/p\mathbb{Z})^g \oplus \mu_p^g$ over S and A has good reduction at all $v \mid p$. Then $\mathcal{A}^{K'}[p] \cong (\mathbb{Z}/p\mathbb{Z})^g \oplus \mu_p^g$ over $S^{K'}$ for every finite extension K'/K [Česl3, 3.4 and the proof of 3.3]. For instance, this is the case for $K = \mathbb{Q}$ and $A = X_0(11)$ with $p = 5$ [Česl3, 1.10].

Assume that $p > 2$. By [Česl3, 5.5 and the proof of 5.4] and Lemmas B.1 and B.2,

$$\#\operatorname{Sel}_p A_{K_n} \sim_{A,K_\infty} \#H^1(S^{K_n}, (\mathbb{Z}/p\mathbb{Z})^g \oplus \mu_p^g) \sim \#\operatorname{Pic}(S^{K_n})[p]^{2g} \cdot p^{gp^n(r_1+r_2)}. \tag{3}$$

If the reduction is ordinary at all $v \mid p$, then (3) combines with Propositions 6.2 and 6.6 to give

$$\rho + \mu^{(1)}_{\mathrm{Sel}} = 2g\mu^{(1)}_{\mathrm{Pic}} + g(r_1 + r_2).$$

The same reasoning applies with K replaced by a finite extension K'. In particular, if $p > 2$, the reduction of A at all $v \mid p$ is good ordinary, and $\mathcal{A}[p] \cong (\mathbb{Z}/p\mathbb{Z})^g \oplus \mu_p^g$, then

$$\rho' + \mu_{\mathrm{Sel}}^{\prime(1)} = 2g\mu_{\mathrm{Pic}}^{\prime(1)} + g(r_1' + r_2') \tag{4}$$

for every finite extension K'/K. In particular, under Conjectures 8.1 and 8.2, $\mu_{\mathrm{Sel}}^{\prime(1)} = g(r_1' + r_2')$, and for $K = \mathbb{Q}$, $A = X_0(11)$, $p = 5$, and $K'/\mathbb{Q}$ abelian, the same holds unconditionally (cf. 8.3).

Appendix A. Cardinalities of the images of local Kummer homomorphisms

Let K be a local field, A a g-dimensional abelian variety over K, and l a prime. Proposition A.1 summarizes standard computations in the form needed for the bounds of §§2-3.

Proposition A.1. *Fix an $m \in \mathbb{Z}_{>0}$. If K is nonarchimedean, let $\mathbb{F}_K$ be its residue field.*

(a) If K is nonarchimedean and $l \neq \operatorname{char} \mathbb{F}_K$, then $\#\left(A(K)/l^m A(K)\right) = \#A(K)[l^m]$.

(b) If K is a finite extension of $\mathbb{Q}_l$, then $\#\left(A(K)/l^m A(K)\right) = l^{mg[K:\mathbb{Q}_l]} \cdot \#A(K)[l^m]$.

(c) If $K \cong \mathbb{R}$ and $l = 2$, then $A(K)/l^m A(K) \cong \pi_0(A(K))$ (component group for the archimedean topology) and $\#\pi_0(A(K)) \leqslant 2^g$. In all other archimedean cases, $A(K)/l^m A(K) = 0$.

Proof.

(a) Let $\mathcal{O}_K$ be the ring of integers of K and $\mathcal{A} \to \operatorname{Spec} \mathcal{O}_K$ the Néron model of A. Since $\mathcal{A}$ is smooth over the Henselian $\mathcal{O}_K$, the reduction homomorphism $\mathcal{A}(\mathcal{O}_K) \to \mathcal{A}(\mathbb{F}_K)$ is surjective [BLR90, 2.2/14]; once we show that its kernel is uniquely divisible by l^m, the conclusion follows from the snake lemma because $\#(\mathcal{A}(\mathbb{F}_K)/l^m\mathcal{A}(\mathbb{F}_K)) = \#\mathcal{A}(\mathbb{F}_K)[l^m]$ due to finiteness of $\mathcal{A}(\mathbb{F}_K)$. Since $\mathcal{A} \xrightarrow{l^m} \mathcal{A}$ is separated étale [BLR90, 7.3/2(b)], so is its pullback over each $P \in \mathcal{A}(\mathcal{O}_K)$, and the claimed unique divisibility follows from [EGA IV$_4$, 18.5.12].

(b) The finite index inclusion $\mathbb{Z}_l^{g[K:\mathbb{Q}_l]} \subset A(K)$ of [Mat55, Thm. 7] with the snake lemma give

$$\frac{\#\operatorname{Coker}\left(A(K) \xrightarrow{l^m} A(K)\right)}{\#\operatorname{Ker}\left(A(K) \xrightarrow{l^m} A(K)\right)} = \frac{\#\operatorname{Coker}\left(\mathbb{Z}_l^{g[K:\mathbb{Q}_l]} \xrightarrow{l^m} \mathbb{Z}_l^{g[K:\mathbb{Q}_l]}\right)}{\#\operatorname{Ker}\left(\mathbb{Z}_l^{g[K:\mathbb{Q}_l]} \xrightarrow{l^m} \mathbb{Z}_l^{g[K:\mathbb{Q}_l]}\right)} = l^{mg[K:\mathbb{Q}_l]}.$$

(c) $H^1(K, A[l^m]) = 0$ unless $K \cong \mathbb{R}$ and $l = 2$, in which case [GH81, 1.1 (3)] applies. □

Remark A.2. Finiteness of quotients $A(K)/l^m A(K)$ fails for K of characteristic l: for instance, for the Tate elliptic curve $\mathbb{G}_m/q^{\mathbb{Z}}$, combine the snake lemma with the well-known infinitude of $K^\times/K^{\times l^m}$ [Iwa86, (2.2) and 2.8].

Appendix B. The flat cohomology of $\mathbb{Z}/l^a\mathbb{Z}$ and μ_{l^b}

Fix a nonempty open $U \subset S$. We work out the cardinalities of the (compactly supported) flat cohomology groups of U with $\mathbb{Z}/l^a\mathbb{Z}$ or μ_{l^b} coefficients, which are needed in §§2-3

Lemma B.1.

(a) $\#H^1(S, \mathbb{Z}/l^a\mathbb{Z}) = \#(\operatorname{Pic}_+ S/l^a \operatorname{Pic}_+ S)$.

(b) If $l \neq \operatorname{char} K$, then, interpreting $[K_v : \mathbb{Q}_l]$ as 0 unless $\operatorname{char} K = 0$ and $v \mid l$,

$$\#(\operatorname{Pic}_+ S/l^a \operatorname{Pic}_+ S) \leqslant \#H^1(U, \mathbb{Z}/l^a\mathbb{Z}) \leqslant \#(\operatorname{Pic}_+ S/l^a \operatorname{Pic}_+ S) \cdot \prod_{v \in S\setminus U} \left(\#\mu_{l^a}(K_v) \cdot l^{a[K_v:\mathbb{Q}_l]}\right).$$

Proof.

(a) Since $H^1(S, \mathbb{Z}/l^a\mathbb{Z}) \cong \operatorname{Hom}(\pi_1^{\text{ét}}(S), \mathbb{Z}/l^a\mathbb{Z})$, the theory of the narrow Hilbert class field gives the claim in the number field case. For function fields, one can (alternatively) use duality: by [Mil06, III.8.2], $H^1(S, \mathbb{Z}/l^a\mathbb{Z}) \cong H^2(S, \mu_{l^a})^*$, so, due to $0 \to \mu_{l^a} \to \mathbb{G}_m \xrightarrow{l^a} \mathbb{G}_m \to 0$ that is exact in S_{fppf}, the vanishing of the Brauer group of S gives the claim.

(b) The exact $0 \to H^1(S, \mathbb{Z}/l^a\mathbb{Z}) \to H^1(U, \mathbb{Z}/l^a\mathbb{Z}) \to \prod_{v\in S\setminus U} H^1(K_v, \mathbb{Z}/l^a\mathbb{Z})/H^1(\mathcal{O}_v, \mathbb{Z}/l^a\mathbb{Z})$, (a), and local class field theory give the bounds, because $H^1(K_v, \mathbb{Z}/l^a\mathbb{Z}) \cong \operatorname{Hom}(K_v^\times/K_v^{\times l^a}, \mathbb{Z}/l^a\mathbb{Z})$ and $H^1(\mathcal{O}_v, \mathbb{Z}/l^a\mathbb{Z}) \cong \operatorname{Hom}(\pi_1^{\text{ét}}(\mathcal{O}_v), \mathbb{Z}/l^a\mathbb{Z}) \cong \mathbb{Z}/l^a\mathbb{Z}$. □

Lemma B.2. $\#H^1(U, \mu_{l^b}) = \#\operatorname{Pic}(U)[l^b] \cdot l^{b\cdot\max(r_1+r_2+\#(S\setminus U)-1,0)} \cdot \#\mu_{l^b}(K)$.

Proof. Since $0 \to \mu_{l^b} \to \mathbb{G}_m \xrightarrow{l^b} \mathbb{G}_m \to 0$ is exact in U_{fppf}, its long exact cohomology sequence together with the unit theorem [AW45, p. 491, Thm. 6] give the claim. □

Lemma B.3. *Set $r := r_1$ if $l = 2$, and $r := 0$ if $l \neq 2$.*

(a) If $a \geqslant 1$, then $\#H^1_c(S, \mathbb{Z}/l^a\mathbb{Z}) = \#(\operatorname{Pic} S/l^a \operatorname{Pic} S) \cdot 2^{\max(r-1,0)}$.

(b) If $a \geqslant 1$ and $U \neq S$, then $\#H^1_c(U, \mathbb{Z}/l^a\mathbb{Z}) = \#(\operatorname{Pic} U/l^a \operatorname{Pic} U) \cdot l^{a(\#(S\setminus U)-1)} \cdot 2^r$.

Proof. By duality [Mil06, III.3.2, III.8.2], $\#H^1_c(U, \mathbb{Z}/l^a\mathbb{Z}) = \#H^2(U, \mu_{l^a})$, and the claim follows from the cohomology sequence of $0 \to \mu_{l^a} \to \mathbb{G}_m \xrightarrow{l^a} \mathbb{G}_m \to 0$ since the Brauer group of U is understood from the exact sequence $0 \to \operatorname{Br} U \to \bigoplus_{v\notin U} \operatorname{Br}(K_v) \xrightarrow{\sum \operatorname{inv}_v} \mathbb{Q}/\mathbb{Z}$ [Mil06, II.2.1]. □

Lemma B.4. *If $b \geqslant 1$ and l is invertible on $U \neq S$, then*

$$\#H^1_c(U, \mu_{l^b}) \geqslant \#(\operatorname{Pic}_+ S/l^b \operatorname{Pic}_+ S) \cdot l^{-b(r_2+1)},$$
$$\#H^1_c(U, \mu_{l^b}) \leqslant \#(\operatorname{Pic}_+ S/l^b \operatorname{Pic}_+ S) \cdot l^{b(r_1+r_2-1)} \cdot \prod_{v\in S\setminus U} \#\mu_{l^b}(K_v).$$

Proof. We replace compactly supported flat cohomology by its étale counterpart [Mil06, pp. 165-166]: by [Mil06, II.3.3, III.3.2, III.8.1] and [Gro68, 11.7 1°)], the two meanings of $H^i_c(U, \mu_{l^b})$ agree.

By the Euler characteristic formula [Mil06, II.2.13 (b)] and duality [Mil06, II.3.3],

$$\#H^1_c(U, \mu_{l^b}) = \frac{\#H^0_c(U, \mu_{l^b}) \cdot \#H^2_c(U, \mu_{l^b})}{2^r l^{br_2} \cdot \#H^3_c(U, \mu_{l^b})} = \frac{\#H^0_c(U, \mu_{l^b}) \cdot \#H^1(U, \mathbb{Z}/l^b\mathbb{Z})}{2^r l^{b(r_2+1)}}$$

with r as in Lemma B.3. By [Mil06, II.2.3 (a)] (we use the $U \neq S$ assumption to discard $H^0(U, \mu_{l^b})$),

$$H^0_c(U, \mu_{l^b}) \cong \bigoplus_{v|\infty} \widehat{H}^{-1}(K_v, \mu_{l^b}) \cong \bigoplus_{\text{real } v} H^1(K_v, \mu_{l^b}) \cong \bigoplus_{\text{real } v} \mathbb{R}^\times/\mathbb{R}^{\times l^b}$$

where $\widehat{H}^i$ denotes Tate cohomology. It remains to take into account Lemma B.1(b). □

References

[AW45] Emil Artin and George Whaples, *Axiomatic characterization of fields by the product formula for valuations*, Bull. Amer. Math. Soc. **51** (1945), 469–492. MR0013145 (7,111f)

[BKL+13] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra Jr., Bjorn Poonen, and Eric Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, preprint (2013). `http://arxiv.org/abs/1304.3971`.

[Böl75] Reinhard Bölling, *Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig groß werden*, Math. Nachr. **67** (1975), 157–179 (German). MR0384812 (52 #5684)

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)

[Čes13] Kęstutis Česnavičius, *Selmer groups as flat cohomology groups*, preprint (2013). `http://arxiv.org/abs/1301.4724`.

[CGP10] Brian Conrad, Ofer Gabber, and Gopal Prasad, *Pseudo-reductive groups*, New Mathematical Monographs, vol. 17, Cambridge University Press, Cambridge, 2010. MR2723571 (2011k:20093)

[CL84] H. Cohen and H. W. Lenstra Jr., *Heuristics on class groups*, Number theory (New York, 1982), Lecture Notes in Math., vol. 1052, Springer, Berlin, 1984, pp. 26–36, DOI 10.1007/BFb0071539, (to appear in print). MR750661

[Cla04] Pete L. Clark, *The period-index problem in WC-groups II: abelian varieties*, preprint (2004). `http://arxiv.org/abs/math/0406135`.

[Cre11] Brendan Creutz, *Potential Sh for abelian varieties*, J. Number Theory **131** (2011), no. 11, 2162–2174, DOI 10.1016/j.jnt.2011.05.013. MR2825120 (2012h:11089)

[CS10] Pete L. Clark and Shahed Sharif, *Period, index and potential. III*, Algebra Number Theory **4** (2010), no. 2, 151–174, DOI 10.2140/ant.2010.4.151. MR2592017 (2011b:11075)

[EGA I] A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique. I. Le langage des schémas*, Inst. Hautes Études Sci. Publ. Math. **4** (1960), 228. MR0217083 (36 #177a)

[EGA IV$_2$] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. II*, Inst. Hautes Études Sci. Publ. Math. **24** (1965), 231 (French). MR0199181 (33 #7330)

[EGA IV$_4$] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV*, Inst. Hautes Études Sci. Publ. Math. **32** (1967), 361 (French). MR0238860 (39 #220)

[FW79] Bruce Ferrero and Lawrence C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) **109** (1979), no. 2, 377–395, DOI 10.2307/1971116. MR528968 (81a:12005)

[GH81] Benedict H. Gross and Joe Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) **14** (1981), no. 2, 157–182. MR631748 (83a:14028)

[Gre99] Ralph Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144, DOI 10.1007/BFb0093453, (to appear in print). MR1754686 (2002a:11056)

[Gre03] ———, *Galois theory for the Selmer group of an abelian variety*, Compositio Math. **136** (2003), no. 3, 255–297, DOI 10.1023/A:1023251032273. MR1977007 (2004c:11097)

[Gro68] Alexander Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 88–188 (French). MR0244271 (39 #5586c)

[Iwa71] Kenkichi Iwasawa, *On some infinite Abelian extensions of algebraic number fields*, Actes du Congrès International des Mathématiciens (Nice, 1970), Gauthier-Villars, Paris, 1971, pp. 391–394. MR0422205 (54 #10197)

[Iwa73] ———, *On the μ-invariants of Z_l-extensions*, Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973, pp. 1–11. MR0357371 (50 #9839)

[Iwa86] ———, *Local class field theory*, Oxford Science Publications, The Clarendon Press Oxford University Press, New York, 1986. Oxford Mathematical Monographs. MR863740 (88b:11080)

[Kat04] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290 (English, with English and French summaries). Cohomologies p-adiques et applications arithmétiques. III. MR2104361 (2006b:11051)

[Kla11] Zev Klagsbrun, *Selmer Ranks of Quadratic Twists of Elliptic Curves*, ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.)–University of California, Irvine. MR2890124

[Mad72] Manohar L. Madan, *Class groups of global fields*, J. reine angew. Math. **252** (1972), 171–177. MR0296049 (45 #5110)

[Mat55] Arthur Mattuck, *Abelian varieties over p-adic ground fields*, Ann. of Math. (2) **62** (1955), 92–119. MR0071116 (17,87f)

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR0444670 (56 #3020)

[Mil06] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006. MR2261462 (2007e:14029)

[Que87] Jordi Quer, *Corps quadratiques de* 3*-rang* 6 *et courbes elliptiques de rang* 12, C. R. Acad. Sci. Paris Sér. I Math. **305** (1987), no. 6, 215–218 (French, with English summary). MR907945 (88j:11074)

[Roh84] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423, DOI 10.1007/BF01388636. MR735333 (86g:11038b)

[Sch83] R. J. Schoof, *Class groups of complex quadratic fields*, Math. Comp. **41** (1983), no. 163, 295–302, DOI 10.2307/2007782. MR701640 (84h:12005)

[Sch96] Edward F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56** (1996), no. 1, 79–114, DOI 10.1006/jnth.1996.0006. MR1370197 (97e:11068)

[Ser58] Jean-Pierre Serre, *Classes des corps cyclotomiques (d'après K. Iwasawa)*, Séminaire Bourbaki, Vol. 5, Soc. Math. France, Paris, 1995, pp. Exp. No. 174, 83–93 (French). MR1603459

[Ser79] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg. MR554237 (82e:12016)

[SGA $4\frac{1}{2}$] P. Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$; Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. MR0463174 (57 #3132)

[TO70] John Tate and Frans Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21. MR0265368 (42 #278)

[TŠ67] D. T. Tèit and I. R. Šafarevič, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), 770–773 (Russian). MR0237508 (38 #5790)

[Ulm07] Douglas Ulmer, *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields*, Invent. Math. **167** (2007), no. 2, 379–408, DOI 10.1007/s00222-006-0018-x. MR2270458 (2007k:11101)

[Wat69] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. MR0265369 (42 #279)

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

E-mail address: kestutis@math.mit.edu

URL: http://math.mit.edu/~kestutis/