p-SELMER GROWTH IN EXTENSIONS OF DEGREE p

KĘSTUTIS ČESNAVIČIUS

Abstract. There is a known analogy between growth questions for class groups and for Selmer groups. If p is a prime, then the p-torsion of the ideal class group grows unboundedly in $\mathbb{Z}/p\mathbb{Z}$-extensions of a fixed number field K, so one expects the same for the p-Selmer group of a nonzero abelian variety over K. This Selmer group analogue is known in special cases and we prove it in general, along with a version for arbitrary global fields.

1. Introduction

1.1. Growth of class groups and of Selmer groups. It is a classical theorem of Gauss that the 2-torsion subgroup $\mathrm{Pic}(\mathcal{O}_L)[2]$ of the ideal class group of a quadratic number field L can be arbitrarily large. Although unboundedness of $\#\,\mathrm{Pic}(\mathcal{O}_L)[p]$ for an odd prime p is a seemingly inaccessible conjecture, [BCH$^+$66, VII-12, Thm. 4] explains how to extend Gauss' methods to prove that $\#\,\mathrm{Pic}(\mathcal{O}_L)[p]$ is unbounded if $L/\mathbb{Q}$ ranges over the $\mathbb{Z}/p\mathbb{Z}$-extensions instead.

As explained in [Čes15a], growth questions for ideal class groups and for Selmer groups of abelian varieties are often analogous. It is therefore natural to hope that for a prime p and a nonzero abelian variety A over $\mathbb{Q}$, the p-Selmer group $\mathrm{Sel}_p\, A_L$ can be arbitrarily large when $L/\mathbb{Q}$ ranges over the $\mathbb{Z}/p\mathbb{Z}$-extensions. Our main result confirms this expectation.

Theorem 1.2 (Theorem 5.6)**.** *Let p be a prime, K a global field, and A a nonzero abelian variety over K. If $A[p](\overline{K}) \neq 0$ (for instance, if $p \neq \mathrm{char}\, K$) or if A is supersingular, then*

$$\#\,\mathrm{Sel}_p\, A_L$$

is unbounded when L ranges over the $\mathbb{Z}/p\mathbb{Z}$-extensions of K.

Remarks.

1.3. In the excluded case when $A[p](\overline{K}) = 0$ and A is not supersingular (when also $\mathrm{char}\, K = p$ and $\dim A > 2$), there nevertheless is an $n \in \mathbb{Z}_{>0}$ that depends on A such that

$$\#\,\mathrm{Sel}_{p^n}\, A_L$$

is unbounded when L ranges over the $\mathbb{Z}/p^n\mathbb{Z}$-extensions of K, see Theorem 5.6.

1.4. See Corollary 5.5 for a version of Theorem 1.2 for Selmer groups of arbitrary isogenies.

1.5. The proof of Theorem 1.2 also reproves the unbounded growth of the p-torsion subgroup of the ideal class group in $\mathbb{Z}/p\mathbb{Z}$-extensions of K, see Corollary 5.3.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: kestutis@berkeley.edu.

Date: February 14, 2017.
2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 11R34, 11R58.
Key words and phrases. Abelian variety, Selmer group, arithmetic duality, Cassels–Poitou–Tate.

1.6. If K is a number field, then the analogue of Theorem 1.2 for $\mathbb{Z}/n\mathbb{Z}$-extensions with $1 < n < p$ seems to lie much deeper: by [Česl5a, 4.1 (b)], this analogue would imply the conjectured unboundedness of p-torsion of ideal class groups of $\mathbb{Z}/n\mathbb{Z}$-extensions of a finite extension of K. If $\operatorname{char} K > 0$, then [Česl5a, 5.5] proves an analogue of this type with $n = 2$ and $p \neq \operatorname{char} K$.

1.7. Previous investigations. Theorem 1.2 was known in a number of special cases:

- By Matsuno [Mat09, 4.5], if $K = \mathbb{Q}$ and $\dim A = 1$;
- By Clark and Sharif [CS10, Thm. 3], if $p \neq \operatorname{char} K$ and $\dim A = 1$;
- By Creutz [Cre11, 1.1] (which improves Clark [Cla04, Thm. 7]), if $\operatorname{char} K = 0$, Galois acts trivially on $\mathrm{NS}(A_{\overline{K}})$, and A has a principal polarization coming from a K-rational divisor;
- By [Česl5a, 4.2], if $p \neq \operatorname{char} K$ and A has $\mathbb{Z}/p\mathbb{Z}$ or μ_p as a K-subgroup, or if A has everywhere semiabelian reduction and $\mathbb{Z}/p\mathbb{Z}$ as a K-subgroup.

Unboundedness of p-Selmer sizes has also been observed in a number of other settings—typical variants include allowing arbitrary L/K as long as $[L : K]$ is bounded and/or also varying A as long as $\dim A$ is constant. For such results, see Cassels [Cas64], Bölling [Böl75], Kramer [Kra83], Fisher [Fis01, Cor. 2], Kloosterman and Schaefer [KS03, Thm. 2], Kloosterman [Klo05, 1.1], Matsuno [Mat07, 5.1], [Mat09, Thm. A], and Bartel [Bar10, 1.1 and 4.4]. For an attempt to understand p-Selmer behavior in $\mathbb{Z}/p\mathbb{Z}$-extensions of number fields in the elliptic curve case, see Brau [Bra14].

Question 1.8. *In Theorem 1.2, is $\#Ш(A_L)[p]$ also unbounded?*

In their respective special cases of Theorem 1.2, Clark–Sharif [CS10] and Creutz [Cre11] prove that the answer is 'yes'.

1.9. An overview of the proofs and of the paper. The proof of Theorem 1.2 is given in §5 and is based on arithmetic duality, the key input being a general version of the Cassels–Poitou–Tate exact sequence. In §4 we include a proof of this sequence that treats all global fields on an equal footing and circumvents well-known difficulties in positive characteristic by exploiting topologies carried by cohomology groups of local fields. The crucial topological input is closedness and discreteness of the image of a certain global-to-local pullback map. The analysis of this map in §2 rests in part on the results of [Česl5b] and leads to several improvements to the literature on arithmetic duality in positive characteristic, notably to [GA09, §4] and to [Mil70]. To be able to simultaneously prove the growth of class groups mentioned in Remark 1.5, in §3 we present a general framework for Selmer groups that extends the framework of Selmer structures of Mazur and Rubin to arbitrary global fields (in positive characteristic the unramified subgroups that play the decisive role in Selmer structures tend to be too small). For an overview of the auxiliary results isolated in Appendices A and B, see the introductions of the appendices.

1.10. Notation. The following notation is in place for the rest of the paper:

- K is a global field;
- If $\operatorname{char} K = 0$, then S is the spectrum of the ring of integers of K;
- If $\operatorname{char} K > 0$, then S is the proper smooth curve over a finite field such that the function field of S is K;
- A place of K is denoted by v, the resulting completion by K_v, the ring of integers and the residue field of K_v by $\mathcal{O}_v$ and $\mathbb{F}_v$, and the maximal ideal of $\mathcal{O}_v$ by $\mathfrak{m}_v$;

- A place of a finite extension K' of K is denoted by v'.

As usual, μ_n denotes $\mathrm{Ker}(\mathbb{G}_m \xrightarrow{n} \mathbb{G}_m)$ and α_p denotes the Frobenius kernel of the additive group $\mathbb{G}_a$ over $\mathbb{F}_p$. For an $n \in \mathbb{Z}_{\geqslant 0}$ and a p-divisible group (or a scheme) X over a base S of characteristic $p > 0$, we let $\mathrm{Frob}_{p^n,\, X/S} \colon X \to X^{(p^n)}$ denote the n-fold relative Frobenius morphism of X over S. Further notation is recorded in the beginning of each individual section.

As mentioned in §1.9, topology carried by cohomology groups of local fields will play an important role in treating all K at once. This topology is always taken to be the one defined in [Česnavičius15b, 3.1–3.2]. To avoid cluttering the proofs with repetitive citations, in §1.11 we gather the main topological properties that we will need. We will use these properties without explicit reference.

1.11. $H^n(K_v, G)$ **for a commutative finite** G. Fix a place v of K, a commutative finite K_v-group scheme G, and an $n \in \mathbb{Z}_{\geqslant 0}$. By [Čes15b, 3.5 (c), 3.6–3.8], $H^n(K_v, G)$ is a locally compact Hausdorff abelian topological group that is discrete if $n \neq 1$. By [Čes15b, 3.5 (b)], if G is étale (in particular, if $\mathrm{char}\, K = 0$), then $H^1(K_v, G)$ is also discrete. By [Čes15b, 3.10], if $v \nmid \infty$ and $\mathcal{G}$ is a commutative finite flat $\mathcal{O}_v$-model of G, then the pullback map identifies $H^n(\mathcal{O}_v, \mathcal{G})$ with a compact open subgroup of $H^n(K_v, G)$ (if $n \geqslant 2$, then $H^n(\mathcal{O}_v, \mathcal{G}) = 0$ by [Toë11, 3.4]). By [Čes15b, 4.2], if G fits into an exact sequence $0 \to H \to G \to Q \to 0$ of commutative finite K_v-group schemes, then the maps in the resulting cohomology sequence are continuous.

1.12. Conventions. We identify the nonarchimedean v with the closed points of S. For a nonempty open $U \subset S$, writing $v \notin U$ signifies that v does not correspond to a closed point of U (and hence could be archimedean). For a field F, a choice of its algebraic closure is denoted by $\overline{F}$. Fppf cohomology is denoted by H^n; identifications with étale cohomology are implicit and use [Gro68, 11.7 1°)]; further identifications with Galois cohomology are likewise implicit. If v is archimedean, then we implicitly make the Tate modification: $H^n(K_v, -)$ is our shorthand for $\widehat{H}^n(K_v, -)$ (this does not affect the H^n with $n \geqslant 1$). Compactness of a topological space does not entail Hausdorffness, and 'locally compact' means that every point has a compact neighborhood.

Acknowledgements. I thank Julio Brau, Pete L. Clark, Brendan Creutz, Bjorn Poonen, and Yunqing Tang for helpful conversations or correspondence.

2. Discreteness of the image of global cohomology

2.1. The setup. Throughout §2, we let U be a nonempty open subscheme of S and let $\mathcal{G}$ be a commutative finite flat U-group scheme. The objects of study are the pullback map

$$\mathrm{loc}^n(\mathcal{G}) \colon H^n(U, \mathcal{G}) \to \textstyle\bigoplus_{v \notin U} H^n(K_v, \mathcal{G}) \quad \text{for } n \in \mathbb{Z}_{\geqslant 0} \qquad \text{and its kernel} \qquad D^n(\mathcal{G}). \tag{2.1.1}$$

We seek to show in Theorem 2.18 that $\mathrm{Im}(\mathrm{loc}^n(\mathcal{G}))$ is closed and discrete and that $D^n(\mathcal{G})$ is finite.

Proposition 2.2. *The following square is Cartesian (with injective maps as indicated):*

$$\begin{tikzcd} H^1(U, \mathcal{G}) \arrow[r, hook] \arrow[d] & H^1(K, \mathcal{G}) \arrow[d] \\ \prod_{v \in U} H^1(\mathcal{O}_v, \mathcal{G}) \arrow[r, hook] & \prod_{v \in U} H^1(K_v, \mathcal{G}). \end{tikzcd}$$

Proof. This is a special case of [Čes16a, 4.3]. □

Proposition 2.3. *The image* $\mathrm{Im}\,(\mathrm{loc}^n(\mathcal{G}))$ *is closed for every* $n \in \mathbb{Z}_{\geqslant 0}$.

Proof. Let $\mathcal{H}$ be the Cartier dual of $\mathcal{G}$. By [Čes，16b, 5.3], the images of $\mathrm{loc}^n(\mathcal{G})$ and $\mathrm{loc}^{2-n}(\mathcal{H})$ are orthogonal complements under the sum of cup product pairings

$$H^n(K_v, \mathcal{G}) \times H^{2-n}(K_v, \mathcal{H}) \to H^2(K_v, \mathbb{G}_m) \xrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z}.$$

By Proposition A.3 and the discreteness of $H^2(K_v, \mathbb{G}_m)$ supplied by [Česk15b, 3.5 (b)], these pairings are continuous, so the claim follows. □

Proposition 2.4. *The image* $\mathrm{Im}(\mathrm{loc}^n(\mathcal{G}))$ *is discrete for* $n \neq 1$.

Proof. Even the target of $\mathrm{loc}^n(\mathcal{G})$ is discrete for $n \neq 1$. □

Lemma 2.5. *Let* $U' \subset U$ *be a nonempty open.*

(a) If $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}_{U'}))$ *is discrete, then so is* $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}))$.

(b) If $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}_{U'}))$ *is discrete and* $D^1(\mathcal{G}_{U'})$ *is finite, then* $D^1(\mathcal{G})$ *is finite.*

Proof. Let W be a compact neighborhood of 0 in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$, so

$$W' := W \times \textstyle\prod_{v \in U \setminus U'} H^1(\mathcal{O}_v, \mathcal{G})$$

is a compact neighborhood of 0 in $\bigoplus_{v \notin U'} H^1(K_v, \mathcal{G})$. By Proposition 2.3, the discrete $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}_{U'}))$ is closed in $\bigoplus_{v \notin U'} H^1(K_v, \mathcal{G})$, so $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}_{U'})) \cap W'$ is finite. Thus, $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G})) \cap W$ is finite, too, $W \backslash \left(\mathrm{Im}(\mathrm{loc}^1(\mathcal{G})) \cap (W \backslash \{0\})\right)$ exhibits 0 as an isolated point of $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}))$, and (a) follows.

For (b), Proposition 2.2 gives the inclusion $D^1(\mathcal{G}_{U'}) \subset D^1(\mathcal{G})$ in $H^1(U', \mathcal{G})$, whereas

$$[D^1(\mathcal{G}) : D^1(\mathcal{G}_{U'})] \leqslant \# \left(\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}_{U'})) \cap W'\right). \qquad \square$$

Lemma 2.6. *Let* K'/K *be a finite separable extension and* U' *the normalization of* U *in* K'.

(a) If $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}_{U'}))$ *is discrete, then so is* $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}))$.

(b) If $D^1(\mathcal{G}_{U'})$ *is finite, then so is* $D^1(\mathcal{G})$.

Proof. Let F'/F be either K'/K or $K'_{v'}/K_v$ for places $v' \mid v$ of K' and K. The kernel of the restriction

$$r \colon H^1(F, \mathcal{G}) \to H^1(F', \mathcal{G})$$

is finite, as one sees by using the separability to enlarge F'/F to a finite Galois extension, and then identifying $\mathrm{Ker}\, r$ with $H^1(\mathrm{Gal}(F'/F), \mathcal{G}(F'))$, which is finite by inspection.

(a) Let W' be a compact neighborhood of 0 in $\bigoplus_{v' \notin U'} H^1(K'_{v'}, \mathcal{G})$. By [Česk15b, 2.7 (viii)], the restriction $H^1(K_v, \mathcal{G}) \to H^1(K'_{v'}, \mathcal{G})$ is continuous for each $v' \mid v$, so there is a compact neighborhood W of 0 in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$ lying in the preimage of W'. As in the proof of Lemma 2.5, $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G}_{U'})) \cap W'$ is finite and it suffices to prove the finiteness of $\mathrm{Im}(\mathrm{loc}^1(\mathcal{G})) \cap W$, which follows by using in addition the finiteness of

$$\mathrm{Ker}(\textstyle\bigoplus_{v \notin U} H^1(K_v, \mathcal{G}) \to \bigoplus_{v' \notin U'} H^1(K'_{v'}, \mathcal{G})).$$

(b) The finite $\mathrm{Ker}(H^1(K, \mathcal{G}) \xrightarrow{r} H^1(K', \mathcal{G}))$ contains $\mathrm{Ker}(D^1(\mathcal{G}) \to D^1(\mathcal{G}_{U'}))$. □

Lemma 2.7. *Suppose that* $\mathcal{G}$ *fits into an exact sequence*

$$0 \to \mathcal{H} \to \mathcal{G} \to \mathcal{Q} \to 0$$

of commutative finite flat U*-group schemes.*

(a) If $\operatorname{Im}(\operatorname{loc}^1(\mathcal{H}))$ *and* $\operatorname{Im}(\operatorname{loc}^1(\mathcal{Q}))$ *are discrete and* $D^1(\mathcal{Q})$ *is finite, then* $\operatorname{Im}(\operatorname{loc}^1(\mathcal{G}))$ *is discrete.*

(b) If $D^1(\mathcal{H})$ *and* $D^1(\mathcal{Q})$ *are finite, then so is* $D^1(\mathcal{G})$.

Proof.

(a) Let $W_{\mathcal{Q}}$ be a compact neighborhood of 0 in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{Q})$. By the discreteness of $\operatorname{Im}\left(\operatorname{loc}^1(\mathcal{Q})\right)$ and Proposition 2.3,

$$\#\left(\operatorname{Im}\left(\operatorname{loc}^1(\mathcal{Q})\right) \cap W_{\mathcal{Q}}\right) < \infty.$$

We combine this with the Hausdorffness of $\bigoplus_{v \notin U} H^1(K_v, \mathcal{Q})$ to shrink $W_{\mathcal{Q}}$ to ensure that

$$\operatorname{Im}\left(\operatorname{loc}^1(\mathcal{Q})\right) \cap W_{\mathcal{Q}} = \{0\}.$$

We then let $W_{\mathcal{G}}$ be a compact neighborhood of 0 in the preimage of $W_{\mathcal{Q}}$ in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$.

Claim 2.7.1. The preimage $W_{\mathcal{H}}$ of $W_{\mathcal{G}}$ in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{H})$ is a compact neighborhood of 0.

Proof. Due to continuity, $W_{\mathcal{H}}$ is a closed neighborhood of 0, so only its compactness requires proof. Each $x \in W_{\mathcal{H}}$ has a compact neighborhood

$$W_x \subset \bigoplus_{v \notin U} H^1(K_v, \mathcal{H}).$$

By [Čes15b, 4.4 (c) (3)], the map

$$\bigoplus_{v \notin U} H^1(K_v, \mathcal{H}) \to \bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$$

is closed, and hence open onto its image. The image of $W_{\mathcal{H}}$ is a closed, and hence compact, subspace of $W_{\mathcal{G}}$, so it is contained in the image of the union Z of a finite number of the W_x. Since Z is compact, so is the union of its $\left(\bigoplus_{v \notin U} \mathcal{Q}(K_v)\right)$-translates. This union contains the closed subset $W_{\mathcal{H}}$, which is therefore compact. □

As in the proof of Lemma 2.5, Proposition 2.3 and Claim 2.7.1 ensure the finiteness of $\operatorname{Im}\left(\operatorname{loc}^1(\mathcal{H})\right) \cap W_{\mathcal{H}}$ and it suffices to prove the finiteness of $\operatorname{Im}\left(\operatorname{loc}^1(\mathcal{G})\right) \cap W_{\mathcal{G}}$.

Claim 2.7.2. The image I of $\operatorname{Im}(\operatorname{loc}^1(\mathcal{H}))$ in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$ is closed and discrete.

Proof. For the closedness, it suffices to combine Proposition 2.3 with loc. cit. For the discreteness, it suffices to use the finiteness of $I \cap W_{\mathcal{G}}$ inherited from $\operatorname{Im}\left(\operatorname{loc}^1(\mathcal{H})\right) \cap W_{\mathcal{H}}$. □

Claim 2.7.3. If $J \subset H^1(U, \mathcal{G})$ is the preimage of $D^1(\mathcal{Q})$, then $\operatorname{loc}^1(\mathcal{G})(J)$ is closed and discrete.

Proof. Since

$$[\operatorname{loc}^1(\mathcal{G})(J) : I] \leqslant \# D^1(\mathcal{Q}) < \infty,$$

every subset of $\operatorname{loc}^1(\mathcal{G})(J)$ is a union of finitely many translates of subsets of I, and hence is closed in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$ due to Claim 2.7.2. □

By construction,

$$\operatorname{Im}\left(\operatorname{loc}^1(\mathcal{G})\right) \cap W_{\mathcal{G}} = \operatorname{loc}^1(\mathcal{G})(J) \cap W_{\mathcal{G}},$$

so Claim 2.7.3 gives the finiteness.

(b) Since

$$[D^1(\mathcal{G}) : D^1(\mathcal{G}) \cap \operatorname{Im}(H^1(U, \mathcal{H}))] \leqslant \# D^1(\mathcal{Q}),$$

it suffices to prove that the preimage P of $D^1(\mathcal{G})$ in $H^1(U, \mathcal{H})$ is finite. For this, we use the inequality

$$[P : D^1(\mathcal{H})] \leqslant \prod_{v \notin U} \# \mathcal{Q}(K_v).$$

□

For use in the proof of Theorem 2.9, we recall the following well-known lemma.

Lemma 2.8. *For a field F and a commutative finite F-group scheme G, there is a finite separable extension F'/F such that $G_{F'}$ is a successive extension of F'-group schemes that are isomorphic to $\mathbb{Z}/m\mathbb{Z}$ with $m \in \mathbb{Z}_{>0}$, or to μ_m with $m \in \mathbb{Z}_{>0}$, or to α_p with $p = \operatorname{char} F$ (where $\alpha_0 := 0$).*

Proof. The claim is clear for étale G, and hence, by passing to Cartier duals, also for G of multiplicative type. Thus, the connected-étale sequence allows us to assume that G is connected and has a connected Cartier dual. By [SGA 3_{II}, XVII, 4.2.1 ii) $\Leftrightarrow$ iv)], such a G is a successive extension of α_p's. □

Theorem 2.9. *The image* $\operatorname{Im}(\operatorname{loc}^1(\mathcal{G}))$ *is discrete and the kernel* $D^1(\mathcal{G})$ *is finite.*

Proof. Lemmas 2.6 and 2.8 reduce to the case when $\mathcal{G}_K$ is a successive extension as in Lemma 2.8. We spread out and use Lemmas 2.5 and 2.7 to reduce further to the cases of $\mathcal{G} = \mathbb{Z}/m\mathbb{Z}$, of $\mathcal{G} = \mu_m$, and of $\mathcal{G} = \alpha_p$, and we use these formulas to extend $\mathcal{G}$ to a finite flat S-group scheme $\widetilde{\mathcal{G}}$.

We set

$$W := \textstyle\bigoplus_{v \notin U} H^1(\mathcal{O}_v, \widetilde{\mathcal{G}}) \qquad \text{(with } H^1(\mathcal{O}_v, \widetilde{\mathcal{G}}) := H^1(K_v, \mathcal{G}) \text{ for } v \mid \infty\text{)},$$

so W is an open neighborhood of 0 in $\bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$. By Proposition 2.2, the preimage of W in $H^1(U, \mathcal{G})$ is $H^1(S, \widetilde{\mathcal{G}})$. Since $H^1(S, \widetilde{\mathcal{G}})$ is finite, so are $D^1(\mathcal{G})$ and $\operatorname{Im}(\operatorname{loc}^1(\mathcal{G})) \cap W$. □

Remarks.

2.10. The finiteness of $D^1(\mathcal{G})$ proved in Theorem 2.9 improves [GA09, 4.3], which proved such finiteness after replacing $\mathcal{G}$ by $\mathcal{G}_{U'}$ for a sufficiently small nonempty open $U' \subset U$.

2.11. For the discreteness of $\operatorname{Im}(\operatorname{loc}^1(\mathcal{G}))$ to hold, not a single $v \notin U$ can be omitted from the direct sum in the target of $\operatorname{loc}^1(\mathcal{G})$. For instance, for a prime p, the image of

$$\mathbb{F}_p[t, t^{-1}]/\mathbb{F}_p[t, t^{-1}]^p \cong H^1(\mathbb{F}_p[t, t^{-1}], \alpha_p) \to H^1(\mathbb{F}_p((t)), \alpha_p) \cong \mathbb{F}_p((t))/\mathbb{F}_p((t))^p$$

is dense rather than discrete.[1]

Question 2.12. *Do the closedness and discreteness of the subset*

$$\operatorname{Im}(\operatorname{loc}^1(\mathcal{G})) \subset \textstyle\bigoplus_{v \notin U} H^1(K_v, \mathcal{G})$$

continue to hold for a larger class of U-group schemes $\mathcal{G}$ of finite type?

We turn to preliminaries needed for Theorem 2.16.

2.13. The cohomology with compact supports sequence. We let H^n_c denote the fppf cohomology with compact supports that takes into account the infinite primes, as defined in [Mil06, III.0.6 (a)]. Loc. cit. provides the promised exact sequence, which reads

$$\cdots \to H^n_c(U, \mathcal{G}) \xrightarrow{x^n_c(\mathcal{G})} H^n(U, \mathcal{G}) \xrightarrow{\operatorname{loc}^n(\mathcal{G})} \textstyle\bigoplus_{v \notin U} H^n(K_v, \mathcal{G}) \xrightarrow{\delta^n_c(\mathcal{G})} H^{n+1}_c(U, \mathcal{G}) \to \cdots \qquad (2.13.1)$$

and gives $D^n(\mathcal{G}) = \operatorname{Im}(x^n_c(\mathcal{G}))$ and $\operatorname{Im}(\operatorname{loc}^n(\mathcal{G})) = \operatorname{Ker}(\delta^n_c(\mathcal{G}))$.

2.14. Global duality. We let $\mathcal{H}$ be the Cartier dual of $\mathcal{G}$, so that [Mil06, III.3.2 and III.8.2] gives a bilinear pairing

$$H^n(U, \mathcal{G}) \times H^{3-n}_c(U, \mathcal{H}) \to H^3_c(U, \mathbb{G}_m) \xrightarrow{\operatorname{tr}} \mathbb{Q}/\mathbb{Z} \qquad (2.14.1)$$

that identifies $H^{3-n}_c(U, \mathcal{H})$ with the Pontryagin dual of the discrete $H^n(U, \mathcal{G})$.

[1] The isomorphism $H^1(\mathbb{F}_p((t)), \alpha_p) \cong \mathbb{F}_p((t))/\mathbb{F}_p((t))^p$ is a homeomorphism by [Česl15b, 4.3 (b) and 4.5].

Lemma 2.15. *In the setup of §§2.13–2.14, the homomorphism dual to* $\mathrm{loc}^n(\mathcal{G})$ *identifies with* $\delta_c^{2-n}(\mathcal{H})$*, i.e., the following diagram commutes*

$$\begin{tikzcd}
H^n(U, \mathcal{G}) \arrow[d, "\mathrm{loc}^n(\mathcal{G})"'] & \times & H_c^{3-n}(U, \mathcal{H}) \arrow[r, "(2.14.1)"] & H_c^3(U, \mathbb{G}_m) \arrow[r, "\mathrm{tr}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\
\bigoplus_{v \notin U} H^n(K_v, \mathcal{G}) & \times & \bigoplus_{v \notin U} H^{2-n}(K_v, \mathcal{H}) \arrow[u, "\delta_c^{2-n}(\mathcal{H})"] \arrow[r, "\sum_v - \cup -"] & \bigoplus_{v \notin U} H^2(K_v, \mathbb{G}_m) \arrow[u, "\delta_c^2(\mathbb{G}_m)"] \arrow[r, "\sum_v \mathrm{inv}_v"] & \mathbb{Q}/\mathbb{Z},
\end{tikzcd}$$

where the bottom row is the sum of Tate–Shatz local duality pairings.

Proof. We have proved this in the course of the proof of [Čes16b, 5.3]. □

Theorem 2.16. *The pairing* (2.14.1) *induces a perfect pairing of finite abelian groups*

$$D^n(\mathcal{G}) \times D^{3-n}(\mathcal{H}) \to \mathbb{Q}/\mathbb{Z}. \qquad (2.16.1)$$

Proof. Lemma 2.15 proves that

$$\mathrm{Ker}(\mathrm{loc}^n(\mathcal{G})) \qquad \text{and} \qquad \mathrm{Ker}(x_c^{3-n}(\mathcal{H}))$$

are orthogonal under (2.14.1), so (2.16.1) exists and is nondegenerate on the left. Consequently,

$$\#D^n(\mathcal{G}) \leqslant \#D^{3-n}(\mathcal{H}),$$

and, since $D^0(\mathcal{H})$ inherits finiteness from $H^0(U, \mathcal{H})$ and $D^1(\mathcal{H})$ is finite by Theorem 2.9, $D^2(\mathcal{G})$ and $D^3(\mathcal{G})$ are finite, too. Swapping the roles of $\mathcal{G}$ and $\mathcal{H}$, we learn that equalities must hold in the inequalities above, so (2.16.1) is also nondegenerate on the right. □

Remark 2.17. The deduction of Theorem 2.16 from Theorem 2.9 is the same as that of [GA09, 4.7] from [GA09, 4.3].

For ease of reference, we combine some of the results of §2 into the following theorem.

Theorem 2.18. *For* U *and* $\mathcal{G}$ *as in §2.1 and every* $n \in \mathbb{Z}_{\geqslant 0}$*, the image* $\mathrm{Im}(\mathrm{loc}^n(\mathcal{G}))$ *is closed and discrete in* $\bigoplus_{v \notin U} H^n(K_v, \mathcal{G})$ *and the kernel* $D^n(\mathcal{G})$ *is finite.*

Proof. The image claim is proved in Propositions 2.3 and 2.4 and Theorem 2.9. The kernel claim is proved in Theorems 2.9 and 2.16. □

3. Finiteness of Selmer groups

The results of §2 allow us to prove finiteness of Selmer groups without distinguishing between the number field and the function field cases (see Theorem 3.2). The key finiteness inputs to Theorem 3.2 are the finiteness of class groups and the Dirichlet Unit Theorem, both through the proof of Theorem 2.9. In the case of the ϕ-Selmer group for an isogeny ϕ between abelian varieties over K, Theorem 3.2 seems to improve the literature by treating all K and ϕ simultaneously, instead of resorting to [Mil70] that was tailored specifically to the $\mathrm{char}\, K \mid \deg \phi$ case. The approach of loc. cit. is close to ours: the key lemma of [Mil70] is a variant of Theorem 2.9 for $\mathbb{Z}/p\mathbb{Z}$, μ_p, and α_p.

Throughout §3, we fix a commutative finite K-group scheme G.

3.1. Selmer groups. *Selmer conditions* for G are compact subgroups

$$\mathrm{Sel}(G_{K_v}) \subset H^1(K_v, G), \qquad \text{one for each place } v \text{ of } K, \tag{3.1.1}$$

such that there is a nonempty open $U \subset S$ and a commutative finite flat U-model $\mathcal{G}$ of G for which

$$\mathrm{Sel}(G_{K_v}) \subset H^1(\mathcal{O}_v, \mathcal{G}) \quad \text{inside} \quad H^1(K_v, G) \qquad \text{for every} \quad v \in U$$

(the choice of $\mathcal{G}$ plays no role: two $\mathcal{G}$'s identify over a smaller U). The resulting *Selmer group*, $\mathrm{Sel}(G)$, is the fiber product

$$\begin{tikzcd} \mathrm{Sel}(G) \arrow[r, phantom, "\subset"] \arrow[d] & H^1(K, G) \arrow[d] \\ \prod_v \mathrm{Sel}(G_{K_v}) \arrow[r, phantom, "\subset"] & \prod_v H^1(K_v, G). \end{tikzcd}$$

(Implicitly, $\mathrm{Sel}(G)$ depends on the chosen Selmer conditions (3.1.1).)

Theorem 3.2. *For every choice of Selmer conditions,* $\mathrm{Sel}(G)$ *is finite.*

Proof. Let U and $\mathcal{G}$ be as in §3.1. By Proposition 2.2, imposing Selmer conditions at all $v \in U$ leaves us with a subgroup of $H^1(U, \mathcal{G})$. By Theorem 2.18 and the compactness of $\bigoplus_{v \notin U} \mathrm{Sel}(G_{K_v})$, imposing the further conditions at all $v \notin U$ leaves us with a finite group. □

Examples.

3.3. If $\mathrm{Sel}(G_{K_v}) = 0$ for all v, then Theorem 3.2 recovers the finiteness of

$$Ш^1(G) := \mathrm{Ker}(H^1(K, G) \to \textstyle\prod_v H^1(K_v, G)),$$

proved in [Mil06, I.4.9] in the number field case and in [GA09, 4.6] in the function field case.

3.4. If $\phi\colon A \to B$ is an isogeny of abelian varieties over K, then the subgroups

$$B(K_v)/\phi A(K_v) \subset H^1(K_v, A[\phi])$$

are compact due to the compactness of $B(K_v)$ and the continuity of the connecting map (supplied by [Česı15b, 4.2]). These subgroups are Selmer conditions—the U-model requirement is met due to [Česı16a, 2.5 (d)]. The resulting Selmer group is the ϕ*-Selmer group* $\mathrm{Sel}_\phi A$.

3.5. If $\mathcal{G}$ is a commutative finite flat S-group scheme, then Proposition 2.2 ensures that $H^1(S, \mathcal{G})$ is the Selmer group that results from the Selmer conditions

$$\begin{aligned} H^1(\mathcal{O}_v, \mathcal{G}) \subset H^1(K_v, \mathcal{G}) \qquad &\text{for } v \nmid \infty \quad \text{and} \\ H^1(K_v, \mathcal{G}) \subset H^1(K_v, \mathcal{G}) \qquad &\text{for } v \mid \infty. \end{aligned}$$

3.6. If $\mathrm{char}\, K = 0$ and in Example 3.5 one chooses $\mathcal{G} = \mathbb{Z}/m\mathbb{Z}$ for $m \in \mathbb{Z}_{\geqslant 0}$ but alters the Selmer conditions to be $0 \subset H^1(K_v, \mathcal{G})$ for $v \mid \infty$, then, by the theory of the Hilbert class field, the resulting Selmer group is the Pontryagin dual of the m-torsion of the ideal class group of K.

Remark 3.7. The notion of Selmer conditions extends the notion of a Selmer structure defined in [MR07, 1.2] in a number field setting. The role of the U-model $\mathcal{G}$ is analogous to the role of the unramified subgroups in loc. cit. (the unramified subgroups are too small when G is not étale), with the caveat that for added flexibility we do not insist that almost all of the inclusions $\mathrm{Sel}(G_{K_v}) \subset H^1(\mathcal{O}_v, \mathcal{G})$ be equalities.

4. Cassels–Poitou–Tate

In §5, our proof of unbounded Selmer growth is based on manipulating a generalization of the Cassels–Poitou–Tate sequence. This generalization is presented in Theorem 4.2, which extends [CS00, 1.5] to finite group schemes over global fields (loc. cit. focused on the case of finite group schemes of odd order over number fields). In (4.5.1) we write out the sequence of Theorem 4.2 in the special case of Selmer groups of dual isogenies between abelian varieties over a global field.

4.1. Selmer conditions that are orthogonal complements. Let $U \subset S$ be a nonempty open, $\mathcal{G}$ a commutative finite flat U-group scheme, and $\mathcal{H}$ its Cartier dual. For each $v \notin U$, let

$$\mathrm{Sel}(\mathcal{G}_{K_v}) \subset H^1(K_v, \mathcal{G}) \qquad \text{and} \qquad \mathrm{Sel}(\mathcal{H}_{K_v}) \subset H^1(K_v, \mathcal{H}) \tag{4.1.1}$$

be compact subgroups that are orthogonal complements under the Tate–Shatz local duality pairing

$$H^1(K_v, \mathcal{G}) \times H^1(K_v, \mathcal{H}) \to H^2(K_v, \mathbb{G}_m) \hookrightarrow \mathbb{Q}/\mathbb{Z}, \tag{4.1.2}$$

which is perfect by [Sha64, Duality theorem on p. 411] (alternatively, by [Mil06, I.2.3, I.2.13 (a), III.6.10]). We complete (4.1.1) to Selmer conditions by using the compact subgroups

$$H^1(\mathcal{O}_v, \mathcal{G}) \subset H^1(K_v, \mathcal{G}) \qquad \text{and} \qquad H^1(\mathcal{O}_v, \mathcal{H}) \subset H^1(K_v, \mathcal{H}) \qquad \text{for } v \in U. \tag{4.1.3}$$

By [Mil06, III.1.4 and III.7.2], (4.1.3) also concerns orthogonal complements, so shrinking U does not affect the setup. By Proposition 2.2, the resulting Selmer groups $\mathrm{Sel}(\mathcal{G})$ and $\mathrm{Sel}(\mathcal{H})$ fit into inclusions

$$\mathrm{Sel}(\mathcal{G}) \subset H^1(U, \mathcal{G}) \subset H^1(K, \mathcal{G}) \qquad \text{and} \qquad \mathrm{Sel}(\mathcal{H}) \subset H^1(U, \mathcal{H}) \subset H^1(K, \mathcal{H}); \tag{4.1.4}$$

by Theorem 3.2, they are finite. As in §2.1, we let

$$\mathrm{loc}^n(\mathcal{G})\colon H^n(U, \mathcal{G}) \to \textstyle\bigoplus_{v \notin U} H^n(K_v, \mathcal{G})$$

be the pullback map.

Theorem 4.2. *With the setup of §4.1 there is an exact sequence with continuous maps*

$$0 \to \mathrm{Sel}(\mathcal{G}) \to H^1(U, \mathcal{G}) \to \bigoplus_{v \notin U} \frac{H^1(K_v, \mathcal{G})}{\mathrm{Sel}(\mathcal{G}_{K_v})} \xrightarrow{y(\mathcal{G})} \mathrm{Sel}(\mathcal{H})^* \xrightarrow{x(\mathcal{G})} H^2(U, \mathcal{G}) \xrightarrow{\mathrm{loc}^2(\mathcal{G})} \bigoplus_{v \notin U} H^2(K_v, \mathcal{G}),$$

where $\mathrm{Sel}(\mathcal{G})$*,* $\mathrm{Sel}(\mathcal{H})$*,* $H^1(U, \mathcal{G})$*, and* $H^2(U, \mathcal{G})$ *are discrete and* $(-)^*$ *denotes the Pontryagin dual.*

Proof. Exactness up to $H^1(U, \mathcal{G})$ amounts to (4.1.4) and the definition of $\mathrm{Sel}(\mathcal{G})$. By [Čes16b, 5.3],

$$\mathrm{Im}(\mathrm{loc}^1(\mathcal{G})) \subset \textstyle\bigoplus_{v \notin U} H^1(K_v, \mathcal{G}) \qquad \text{and} \qquad \mathrm{Im}(\mathrm{loc}^1(\mathcal{H})) \subset \textstyle\bigoplus_{v \notin U} H^1(K_v, \mathcal{H})$$

are (closed) orthogonal complements under the sum of the pairings (4.1.2), and hence, by [BouTG, III.28, Cor. 1] and [HR79, 24.10], so are

$$\mathrm{Im}(\mathrm{loc}^1(\mathcal{G})) + \textstyle\bigoplus_{v \notin U} \mathrm{Sel}(\mathcal{G}_{K_v}) \subset \textstyle\bigoplus_{v \notin U} H^1(K_v, \mathcal{G}) \quad \text{and} \quad \mathrm{Im}(\mathrm{loc}^1(\mathcal{H})|_{\mathrm{Sel}(\mathcal{H})}) \subset \textstyle\bigoplus_{v \notin U} H^1(K_v, \mathcal{H}).$$

We therefore arrive at further orthogonal complements

$$\mathrm{Im}\left(H^1(U, \mathcal{G}) \to \textstyle\bigoplus_{v \notin U} \frac{H^1(K_v, \mathcal{G})}{\mathrm{Sel}(\mathcal{G}_{K_v})}\right) \quad \text{and} \quad \mathrm{Im}(\mathrm{loc}^1(\mathcal{H})|_{\mathrm{Sel}(\mathcal{H})}) \subset \textstyle\bigoplus_{v \notin U} \mathrm{Sel}(\mathcal{H}_{K_v}), \tag{$\dagger$}$$

which are closed because [HR79, 24.11] ensures the continuity of the pairings between $\frac{H^1(K_v, \mathcal{G})}{\mathrm{Sel}(\mathcal{G}_{K_v})}$ and $\mathrm{Sel}(\mathcal{H}_{K_v})$. Loc. cit. then allows us to define $y(\mathcal{G})$ to be the continuous map that factors through

$$\mathrm{Im}(\mathrm{loc}^1(\mathcal{H})|_{\mathrm{Sel}(\mathcal{H})})^* \to \mathrm{Sel}(\mathcal{H})^*.$$

This map is injective due to Theorem 2.18 and [HR79, 24.8–24.11], so exactness at $\bigoplus_{v \notin U} \frac{H^1(K_v, \mathcal{G})}{\mathrm{Sel}(\mathcal{G}_{K_v})}$ follows.

Loc. cit. also ensures the exactness of the sequence

$$0 \to \left(\tfrac{H^1(U,\mathcal{H})}{\mathrm{Sel}(\mathcal{H})}\right)^* \to H^1(U,\mathcal{H})^* \to \mathrm{Sel}(\mathcal{H})^* \to 0.$$

By Theorem 2.18 and [BouTG, III.28, Cor. 3], the image of

$$H^1(U,\mathcal{H}) \to \bigoplus_{v\notin U} \tfrac{H^1(K_v,\mathcal{H})}{\mathrm{Sel}(\mathcal{H}_{K_v})}$$

is discrete. By the analogue of (†) for $\mathcal{H}$, this image is also closed. Thus, by [HR79, 23.18, 24.8, and 24.11], the middle row of the diagram

$$\begin{tikzcd}
& & \bigoplus_{v\notin U} H^1(K_v,\mathcal{G}) \arrow[r, two heads] \arrow[d, "\mathrm{loc}^1(\mathcal{H})^*"] & \bigoplus_{v\notin U} \tfrac{H^1(K_v,\mathcal{G})}{\mathrm{Sel}(\mathcal{G}_{K_v})} \arrow[d, "y(\mathcal{G})"] & \\
\bigoplus_{v\notin U} \mathrm{Sel}(\mathcal{G}_{K_v}) \arrow[r, phantom, "\cong"] \arrow[urr, hook] & \bigoplus_{v\notin U} \left(\tfrac{H^1(K_v,\mathcal{H})}{\mathrm{Sel}(\mathcal{H}_{K_v})}\right)^* \arrow[r] & H^1(U,\mathcal{H})^* \arrow[r] \arrow[d, "x"] & \mathrm{Sel}(\mathcal{H})^* \arrow[r] \arrow[dl, dashed, "x(\mathcal{G})"] & 0 \\
& & H^2(U,\mathcal{G}) & &
\end{tikzcd}$$

is exact. Since $\mathrm{loc}^1(\mathcal{H})|_{\mathrm{Sel}(\mathcal{H})}$ factors through $\bigoplus_{v\notin U}\mathrm{Sel}(\mathcal{H}_{K_v})$, the top part of the diagram commutes. The map x is obtained from the map $x_c^2(\mathcal{H})$ of (2.13.1) by using (2.14.1), so the middle column is exact by Lemma 2.15. In conclusion, x factors through a unique $x(\mathcal{G})$ as indicated,

$$\mathrm{Ker}(x(\mathcal{G})) = \mathrm{Im}(y(\mathcal{G})), \qquad \text{and} \qquad \mathrm{Im}(x(\mathcal{G})) = \mathrm{Im}\, x = \mathrm{Ker}(\mathrm{loc}^2(\mathcal{G})).$$

Finiteness of $\mathrm{Sel}(\mathcal{H})^*$ ensures the continuity of $x(\mathcal{G})$. □

Remarks.

4.3. To extend the sequence of Theorem 4.2 to the right, combine (2.13.1), §2.14, and Lemma 2.15.

4.4. If $\mathcal{G}$ and $\mathcal{H}$ extend to Cartier dual finite flat S-group schemes $\widetilde{\mathcal{G}}$ and $\widetilde{\mathcal{H}}$, then one may take

$$\mathrm{Sel}(\mathcal{G}_{K_v}) = \begin{cases} H^1(\mathcal{O}_v,\widetilde{\mathcal{G}}), & \text{for } v \in S\backslash U, \\ H^1(K_v,\mathcal{G}), & \text{for } v \mid \infty, \end{cases} \quad \text{and} \quad \mathrm{Sel}(\mathcal{H}_{K_v}) = \begin{cases} H^1(\mathcal{O}_v,\widetilde{\mathcal{H}}), & \text{for } v \in S\backslash U, \\ 0, & \text{for } v \mid \infty. \end{cases}$$

With these choices, the sequence of Theorem 4.2 compares $H^1(S,\widetilde{\mathcal{G}})$ and $H^1(U,\mathcal{G})$.

Example 4.5. Let $\phi\colon A \to B$ and $\phi^\vee : B^\vee \to A^\vee$ be dual isogenies of abelian varieties over K, and let $\phi\colon \mathcal{A} \to \mathcal{B}$ and $\phi^\vee : \mathcal{B}^\vee \to \mathcal{A}^\vee$ be their extensions to dual isogenies of abelian schemes over a nonempty open $U \subset S$ of good reduction. As in Example 3.4,

$$B(K_v)/\phi A(K_v) \subset H^1(K_v, A[\phi]) \qquad \text{and} \qquad A^\vee(K_v)/\phi^\vee B^\vee(K_v) \subset H^1(K_v, B^\vee[\phi^\vee])$$

constitute Selmer conditions for $A[\phi]$ and $B^\vee[\phi^\vee]$ with Selmer groups $\mathrm{Sel}_\phi A$ and $\mathrm{Sel}_{\phi^\vee} B^\vee$. By Proposition 2.2 and [Česl6a, 2.5 (d)], these conditions for $v \in U$ cut out

$$H^1(U,\mathcal{A}[\phi]) \subset H^1(K, A[\phi]) \qquad \text{and} \qquad H^1(U,\mathcal{B}^\vee[\phi^\vee]) \subset H^1(K, B^\vee[\phi^\vee]).$$

By Proposition B.1, the remaining conditions at $v \notin U$ put us in the framework Theorem 4.2. Taking into account Remark 4.3, the resulting exact sequence reads

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_\phi A \arrow[r] & H^1(U,\mathcal{A}[\phi]) \arrow[r] & \bigoplus_{v\notin U} H^1(K_v, A)[\phi] \arrow[r] & (\mathrm{Sel}_{\phi^\vee} B^\vee)^* \arrow[dlll, rounded corners] \\
& H^2(U,\mathcal{A}[\phi]) \arrow[r] & \bigoplus_{v\notin U} H^2(K_v, A[\phi]) \arrow[r] & (B^\vee[\phi^\vee](K))^*. &
\end{tikzcd} \tag{4.5.1}$$

The last map is surjective if $H^3(U, \mathcal{A}[\phi]) = 0$. By §2.14, this is so if $H^0_c(U, \mathcal{B}^\vee[\phi^\vee]) = 0$, in particular, if $U \neq S$ and either $\operatorname{char} K = 0$ and $2 \nmid \deg \phi$, or $\operatorname{char} K > 0$.

5. Growth of Selmer groups

Theorems 5.2 and 5.6 along with Corollary 5.5 are the sought unbounded Selmer growth results. In §5, for a finite extension K'/K and an open $U \subset S$, we denote the normalization of U in K' by U'.

5.1. Selmer conditions over varying base fields. To fix the general setup, suppose that $U \subset S$ is a nonempty open, $\mathcal{G}$ and $\mathcal{H}$ are Cartier dual commutative finite flat U-group schemes, and $\mathscr{S}$ is a set of finite extensions of K such that $K \in \mathscr{S}$. Suppose also that for each $K' \in \mathscr{S}$ one has compact subgroups

$$\operatorname{Sel}(\mathcal{G}_{K'_{v'}}) \subset H^1(K'_{v'}, \mathcal{G}) \qquad \text{and} \qquad \operatorname{Sel}(\mathcal{H}_{K'_{v'}}) \subset H^1(K'_{v'}, \mathcal{H}) \qquad \text{for } v' \notin U' \tag{5.1.1}$$

that are orthogonal complements as in (4.1.1) and such that the restriction maps

$$H^1(K_v, \mathcal{G}) \to H^1(K'_{v'}, \mathcal{G}) \qquad \text{and} \qquad H^1(K_v, \mathcal{H}) \to H^1(K'_{v'}, \mathcal{H})$$

induce the maps

$$\operatorname{Sel}(\mathcal{G}_{K_v}) \to \operatorname{Sel}(\mathcal{G}_{K'_{v'}}) \qquad \text{and} \qquad \operatorname{Sel}(\mathcal{H}_{K_v}) \to \operatorname{Sel}(\mathcal{H}_{K'_{v'}}) \tag{5.1.2}$$

whenever $v' \notin U'$ and v is the place below v'. We write

$$\operatorname{Sel}(\mathcal{G}_{U'}) \qquad \text{and} \qquad \operatorname{Sel}(\mathcal{H}_{U'})$$

(resp., $\operatorname{Sel}(\mathcal{G})$ and $\operatorname{Sel}(\mathcal{H})$ if $K' = K$) for the Selmer groups that result by completing (5.1.1) to Selmer conditions as in (4.1.3). These Selmer groups are finite due to Theorem 3.2. Due to (5.1.2), for each $K' \in \mathscr{S}$ restriction maps induce the maps

$$\operatorname{Sel}(\mathcal{G}) \to \operatorname{Sel}(\mathcal{G}_{U'}) \qquad \text{and} \qquad \operatorname{Sel}(\mathcal{H}) \to \operatorname{Sel}(\mathcal{H}_{U'}).$$

As in §4.1, shrinking U affects neither the above setup, nor the Selmer groups.

Theorem 5.2. *In the setup of §5.1, if $\mathcal{G}_K$ is étale, p is a prime dividing $\#\mathcal{G}_K$, and $\mathscr{S}$ consists of the $\mathbb{Z}/p\mathbb{Z}$-subextensions of $\overline{K}/K$, then*

$$\# \operatorname{Sel}(\mathcal{G}_{U'})$$

is unbounded when K' ranges in $\mathscr{S}$.

Proof. Let $V \subset U$ be a nonempty open. Initial segments of the exact sequences of Theorem 4.2 for $\mathcal{G}_V$ and $\mathcal{G}_{V'}$ fit into the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Sel}(\mathcal{G}) \arrow[r] \arrow[d, "a"] & H^1(V, \mathcal{G}) \arrow[r, "l"] \arrow[d, "b"] & \left(\bigoplus_{v \notin U} \frac{H^1(K_v, \mathcal{G})}{\operatorname{Sel}(\mathcal{G}_{K_v})}\right) \oplus \left(\bigoplus_{v \in U \setminus V} \frac{H^1(K_v, \mathcal{G})}{H^1(\mathcal{O}_v, \mathcal{G})}\right) \arrow[r, "y(\mathcal{G}_V)"] \arrow[d, "c"] & \operatorname{Sel}(\mathcal{H})^* \\
0 \arrow[r] & \operatorname{Sel}(\mathcal{G}_{U'}) \arrow[r] & H^1(V', \mathcal{G}) \arrow[r, "l'"] & \left(\bigoplus_{v' \notin U'} \frac{H^1(K'_{v'}, \mathcal{G})}{\operatorname{Sel}(\mathcal{G}_{K'_{v'}})}\right) \oplus \left(\bigoplus_{v' \in U' \setminus V'} \frac{H^1(K'_{v'}, \mathcal{G})}{H^1(\mathcal{O}_{v'}, \mathcal{G})}\right) \arrow[r, "y(\mathcal{G}_{V'})"] & \operatorname{Sel}(\mathcal{H}_{U'})^*.
\end{tikzcd}$$

Claim 5.2.1. As V and K' vary, $\# \operatorname{Ker} b$ is bounded.

Proof. By the injectivity aspect of Proposition 2.2,

$$H^1(V, \mathcal{G}) \subset H^1(K, \mathcal{G}) \qquad \text{and} \qquad H^1(V', \mathcal{G}) \subset H^1(K', \mathcal{G}),$$

so $\operatorname{Ker} b \subset H^1(\operatorname{Gal}(K'/K), \mathcal{G}(K'))$. It remains to observe that the cardinality of $H^1(\operatorname{Gal}(K'/K), \mathcal{G}(K'))$ is bounded in terms of p and $\#\mathcal{G}$. □

Claim 5.2.2. As V and K' vary, $\#\operatorname{Ker} c$ is unbounded.

Proof. We fix an $m \in \mathbb{Z}_{>0}$. Since $\mathcal{G}$ is finite étale over a nonempty open of U, Čebotarev density theorem gives a set Σ of m closed points $v \in U$ for which $\mu_p(K_v) = \mu_p(\overline{K}_v)$ and $\mathcal{G}_{\mathcal{O}_v}$ is constant.

We fix a $v \in \Sigma$ and let $\underline{\mathbb{Z}/p^r\mathbb{Z}}_{\mathcal{O}_v}$ be a direct summand of $\mathcal{G}_{\mathcal{O}_v}$. Since $H^1(K_v, \mathbb{Z}/p^r\mathbb{Z})$ is the group of homomorphisms

$$h\colon \operatorname{Gal}(\overline{K}_v/K_v) \to \mathbb{Z}/p^r\mathbb{Z}$$

and $H^1(\mathcal{O}_v, \mathbb{Z}/p^r\mathbb{Z})$ is the subgroup of unramified h, every ramified $\mathbb{Z}/p\mathbb{Z}$-extension $K'_{v'}/K_v$ kills a nonzero element of $H^1(K_v, \mathcal{G})/H^1(\mathcal{O}_v, \mathcal{G})$. We fix such a $K'_{v'}/K_v$: there are many to choose from if $\operatorname{char} K_v = p$, and there is at least one if $\operatorname{char} K_v \neq p$ due to the $\mu_p(K_v) = \mu_p(\overline{K}_v)$ requirement.

We use [NSW08, 9.2.8] to find a $\mathbb{Z}/p\mathbb{Z}$-subextension $\overline{K}/K'/K$ that interpolates the chosen local extensions $K'_{v'}/K_v$ and set $V := U - \Sigma$ to arrive at a c with

$$\#\operatorname{Ker} c \geqslant p^m. \qquad \square$$

Since $\#\operatorname{Coker} l$ is bounded by $\#\operatorname{Sel}(\mathcal{H})$, unboundedness of $\#\operatorname{Ker} c$ supplied by Claim 5.2.2 implies that of $\#\operatorname{Ker}(c|_{\operatorname{Im} l})$. By Claim 5.2.1, $\#\operatorname{Ker} b$ stays bounded, so unboundedness of $\#\operatorname{Ker}(c|_{\operatorname{Im} l})$ implies that of $\#\operatorname{Coker} a$, i.e., that of $\#\operatorname{Sel}(\mathcal{G}_{U'})$ when K' ranges in $\mathscr{S}$. □

Corollary 5.3. *For a prime p, the cardinalities*

$$\#\operatorname{Pic}(S')[p]$$

are unbounded when K' ranges over the $\mathbb{Z}/p\mathbb{Z}$-extensions of K.

Proof. We use [Čes15a, B.1 (a)] to replace $\#\operatorname{Pic}(S')[p]$ by $\#H^1(S', \mathbb{Z}/p\mathbb{Z})$. Then it remains to apply Theorem 5.2 to $U = S$ and $\mathcal{G} = \mathbb{Z}/p\mathbb{Z}$ with $\operatorname{Sel}(\mathcal{G}_{K'_{v'}}) = H^1(K'_{v'}, \mathbb{Z}/p\mathbb{Z})$ for $v' \mid \infty$. □

Remark 5.4. For further results similar to Corollary 5.3, see, for instance, [Mad72].

Corollary 5.5. *For an isogeny $\phi\colon A \to B$ between abelian varieties over K and a prime p that divides the order of some K-étale subgroup $G \subset A[\phi]$ (if $p \neq \operatorname{char} K$, then the K-étaleness of G is automatic),*

$$\#\operatorname{Sel}_\phi A_{K'}$$

is unbounded when K' ranges over the $\mathbb{Z}/p\mathbb{Z}$-extensions of K.

Proof. Let $\psi\colon A \to C$ be an isogeny with kernel G. Since

$$\#\operatorname{Ker}(\operatorname{Sel}_\psi A_{K'} \to \operatorname{Sel}_\phi A_{K'})$$

is bounded by $\#(A[\phi]/G)$, we may assume that $\psi = \phi$. In this case, we let $\phi^\vee$ be the dual isogeny and choose U and (5.1.1) as in Example 4.5 (using Proposition B.1) to argue that Theorem 5.2 applies. □

In characteristic p, Corollary 5.5 may be supplemented by the following result.

Theorem 5.6. *For a prime p and a nonzero abelian variety A over K, there is an $n \in \mathbb{Z}_{>0}$ for which*

$$\#\operatorname{Sel}_{p^n} A_{K'}$$

is unbounded when K' ranges over the $\mathbb{Z}/p^n\mathbb{Z}$-extensions of K. Moreover, one may choose $n = 1$ if $A[p](\overline{K}) \neq 0$ (for instance, if $\operatorname{char} K \neq p$) or if A is supersingular (for instance, if $A[p](\overline{K}) = 0$ and $\dim A \leqslant 2$).

Remark 5.7. For every $N \geqslant n$, the sizes of the kernel and the cokernel of the map

$$\mathrm{Sel}_{p^n} A_{K'} \to (\mathrm{Sel}_{p^N} A_{K'})[p^n]$$

are bounded by p^{2ng}, see [Čes15a, 6.7 (a)]. Therefore, Theorem 5.6 also shows that $\# \mathrm{Sel}_{p^N} A_{K'}$ is unbounded when K' ranges over the $\mathbb{Z}/p^n\mathbb{Z}$-extensions of K.

In the case when $A[p](\overline{K}) = 0$, the proof of Theorem 5.6 will use the following lemmas.

Lemma 5.8. *For a connected-connected p-divisible group G over a field k of characteristic p, there exist integers $x > y > 0$ and $z \geqslant 0$ such that*

$$\mathrm{Ker}(\mathrm{Frob}_{p^{xt},\, G/k}) \subset G[p^{yt+z}] \qquad \textit{for every} \quad t \in \mathbb{Z}_{\geqslant 0}.$$

Proof. For any x, y, and z, the indicated inclusions may be tested over the algebraic closure of k, so we lose no generality by assuming that $k = \overline{k}$. Since G is connected-connected, all its Dieudonné–Manin slopes lie in the open interval $(0, 1)$.

If G is isoclinic of slope $\frac{r}{s}$, then its s-fold relative Frobenius morphism $\mathrm{Frob}_{p^s,\, G/k}$ identifies with multiplication by p^r, so it suffices to set $x := s$, $y := r$, and $z := 0$ (with these choices the indicated inclusions are even equalities). Thus, more generally, if G is a product of isoclinic p-divisible groups G_i with slopes $\{\frac{r_i}{s_i}\}$ and we set $x := \prod s_i$, then

$$\mathrm{Ker}(\mathrm{Frob}_{p^{xt},\, G_i/k}) = G_i[p^{r_i \cdot \frac{x}{s_i} \cdot t}] \qquad \text{for every } i \text{ and every } t \in \mathbb{Z}_{\geqslant 0},$$

so it suffices to in addition set $y := \max_i \{ r_i \cdot \prod_{i' \neq i} s_{i'} \}$ and $z := 0$.

In general, thanks to the Dieudonné–Manin classification and the assumption $k = \overline{k}$, there is a k-isogeny $f \colon G \to G'$ towards a p-divisible group G' that is a product of isoclinic p-divisible groups. Thus, if x and y are chosen for G' as in the previous paragraph, then, in order to obtain the sought triple x, y, z for G, it remains to let z be any nonnegative integer such that $\mathrm{Ker}\, f \subset G[p^z]$. □

Lemma 5.9. *For every $n, \ell \in \mathbb{Z}_{\geqslant 1}$, a nonarchimedean local field k of characteristic $p > 0$ has infinitely many totally ramified $\mathbb{Z}/p^n\mathbb{Z}$-extensions $\widetilde{k}/k$ such that $\mathrm{Gal}(\widetilde{k}/k)$ acts trivially on $\widetilde{\mathfrak{o}}/\widetilde{\mathfrak{m}}^\ell$, where $\widetilde{\mathfrak{o}}$ denotes the ring of integers of $\widetilde{k}$ and $\widetilde{\mathfrak{m}} \subset \widetilde{\mathfrak{o}}$ denotes the maximal ideal.*

Proof. The condition on the triviality of the action means that the ramification subgroup $\mathrm{Gal}(\widetilde{k}/k)_{\ell-1}$ equals the entire $\mathrm{Gal}(\widetilde{k}/k)$. In terms of the upper numbering, this means that

$$\mathrm{Gal}(\widetilde{k}/k)^{\varphi_{\widetilde{k}/k}(\ell-1)} = \mathrm{Gal}(\widetilde{k}/k), \qquad \text{where} \quad \varphi_{\widetilde{k}/k}(\ell-1) = \int_0^{\ell-1} \frac{dx}{[\mathrm{Gal}(\widetilde{k}/k)_0 : \mathrm{Gal}(\widetilde{k}/k)_x]}.$$

Thus, since $\varphi_{\widetilde{k}/k}(\ell-1) \leqslant \ell-1$, it suffices to ensure that

$$\mathrm{Gal}(\widetilde{k}/k)^{\ell-1} = \mathrm{Gal}(\widetilde{k}/k), \qquad \text{or that even} \qquad \mathrm{Gal}(\widetilde{k}/k)^{\ell} = \mathrm{Gal}(\widetilde{k}/k).$$

Local class field theory then reduces us to finding infinitely many continuous $\mathbb{Z}/p^n\mathbb{Z}$-quotients of $\mathfrak{o}^\times$ onto which $1 + \mathfrak{m}^\ell$ maps surjectively, where $\mathfrak{o}$ denotes the ring of integers of k and $\mathfrak{m} \subset \mathfrak{o}$ denotes the maximal ideal. By [Neu99, II.5.7 (ii) and its proof], there is a topological group isomorphism

$$\mathfrak{o}^\times \simeq (\mathfrak{o}/\mathfrak{m})^\times \times \prod_{i=1}^{\infty} \mathbb{Z}_p$$

such that the image of the subgroup $1 + \mathfrak{m}^\ell \subset \mathfrak{o}^\times$ contains the subgroup $\prod_{i=1}^{f(\ell)} 0 \times \prod_{i=f(\ell)+1}^{\infty} \mathbb{Z}_p$ for some $f(\ell) \in \mathbb{Z}_{\geqslant 1}$. It remains to observe that the quotient $\mathbb{Z}_p/p^n\mathbb{Z}_p$ of the i^{th} copy of $\mathbb{Z}_p$ with $i > f(\ell)$ gives rise to a sought quotient of $\mathfrak{o}^\times$. □

Proof of Theorem 5.6. Corollary 5.5 settles the case $\operatorname{char} K \neq p$, so we assume that $\operatorname{char} K = p$.

The overall structure of the argument will be similar to the one used to prove Theorem 5.2. Namely, we let $V \subset U \subset S$ be nonempty opens such that A extends to an abelian scheme $\mathcal{A} \to U$, and we use the sequence (4.5.1) with $\phi = [p^n]_A$ (and an n to be fixed later) to obtain the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \operatorname{Sel}_{p^n} A \arrow[r] \arrow[d, "a"] & H^1(V, \mathcal{A}[p^n]) \arrow[r, "l"] \arrow[d, "b"] & \bigoplus_{v \notin V} H^1(K_v, A)[p^n] \arrow[r] \arrow[d, "c"] & (\operatorname{Sel}_{p^n} A^\vee)^* \\
0 \arrow[r] & \operatorname{Sel}_{p^n} A_{K'} \arrow[r] & H^1(V', \mathcal{A}[p^n]) \arrow[r, "l'"] & \bigoplus_{v' \notin V'} H^1(K'_{v'}, A)[p^n] &
\end{tikzcd}$$

with exact rows. As in the final paragraph of the proof of Theorem 5.2, due to the uniform boundedness of $\# \operatorname{Ker} b$ supplied by the proof of Claim 5.2.1, it suffices to prove that there is an n subject to the constraints of the last sentence of the claim such that $\# \operatorname{Ker} c$ is unbounded when V and K' vary. Moreover, since we may use [NSW08, 9.2.8] to interpolate any finite set of local $\mathbb{Z}/p^n\mathbb{Z}$-extensions by a global $\mathbb{Z}/p^n\mathbb{Z}$-extension, it suffices to show that for some n satisfying the constraints and for infinitely many $v \in U$ there is a $\mathbb{Z}/p^n\mathbb{Z}$-extension $K'_{v'}/K_v$ such that

$$\operatorname{Ker}(H^1(K_v, A)[p^n] \to H^1(K'_{v'}, A)[p^n]) \neq 0. \tag{5.9.1}$$

By Tate local duality, the requirement (5.9.1) is equivalent to the requirement that the norm map

$$\mathcal{N} \colon A^\vee(K'_{v'}) \to A^\vee(K_v) \qquad \text{is not surjective.} \tag{5.9.2}$$

To find infinitely many $v \in U$ satisfying (5.9.2) for some $K'_{v'}$, we split the argument into cases.

The case when $A[p](\overline{K}) \neq 0$. In this case, neither of the isogenous p-divisible groups $A[p^\infty]$ and $A^\vee[p^\infty]$ is connected, so $A^\vee[p](\overline{K}) \neq 0$, too. Therefore, at the cost of shrinking U, we may assume that $\mathcal{A}^\vee[p]$ is an extension of a nonzero finite étale U-group scheme $\mathcal{Q}$ by a finite flat U-group scheme $\mathcal{H}$ that has connected fibers. By the Čebotarev density theorem, there are infinitely many $v \in U$ such that $\mathcal{Q}(\mathbb{F}_v) \neq 0$. For such v, due to the vanishing of $H^1(\mathbb{F}_v, \mathcal{H})$ supplied, for instance, by [Čes15b, 5.7 (b)], one also has $\mathcal{A}^\vee(\mathbb{F}_v)[p] \neq 0$.

We choose $n = 1$, let v be such that $\mathcal{A}^\vee(\mathbb{F}_v)[p] \neq 0$, and let $K'_{v'}/K_v$ be any ramified $\mathbb{Z}/p\mathbb{Z}$-extension. The norm map $\mathcal{N}$ of (5.9.2) reduces to multiplication by p on $\mathcal{A}^\vee(\mathbb{F}_v)$, so cannot be surjective because $\#(\mathcal{A}^\vee(\mathbb{F}_v)/p\mathcal{A}^\vee(\mathbb{F}_v)) = \#\mathcal{A}^\vee(\mathbb{F}_v)[p]$.

The case when A is supersingular. We choose $n = 1$ and for any $v \in U$ use Lemma 5.9 to choose a ramified $\mathbb{Z}/p\mathbb{Z}$-extension $K'_{v'}/K_v$ for which $\operatorname{Gal}(K'_{v'}/K_v)$ acts trivially on $\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^2}$. For proving that the norm map $\mathcal{N}$ of (5.9.2) is not surjective, we consider the formal group of $A^\vee_{K_v}$, i.e., the formal completion of $\mathcal{A}^\vee_{\mathcal{O}_v}$ along the identity section of the special fiber. The $\mathcal{O}_v$-points of this formal group identify with

$$\varprojlim_{n \geqslant 1} \operatorname{Ker}(\mathcal{A}^\vee(\mathcal{O}_v/\mathfrak{m}_v^n) \twoheadrightarrow \mathcal{A}^\vee(\mathbb{F}_v)),$$

and hence also with the kernel

$$\operatorname{Ker}\left(\mathcal{A}^\vee(\mathcal{O}_v) \twoheadrightarrow \mathcal{A}^\vee(\mathbb{F}_v)\right)$$

of the reduction map, and likewise over $\mathcal{O}_{v'}$. We seek to show that

$$\mathcal{N}\left(\operatorname{Ker}(\mathcal{A}^\vee(\mathcal{O}_{v'}) \twoheadrightarrow \mathcal{A}^\vee(\mathbb{F}_{v'}))\right) \subset \operatorname{Ker}(\mathcal{A}^\vee(\mathcal{O}_v) \twoheadrightarrow \mathcal{A}^\vee(\mathcal{O}_v/\mathfrak{m}_v^p)) \tag{5.9.3}$$

(the indicated surjectivity results from the $\mathcal{O}_v$-smoothness of $\mathcal{A}^\vee_{\mathcal{O}_v}$). Once this is done, it will follow that $\mathcal{N} \colon \mathcal{A}^\vee(\mathcal{O}_{v'}) \to \mathcal{A}^\vee(\mathcal{O}_v)$ cannot be surjective because $\#\mathcal{A}^\vee(\mathbb{F}_{v'}) < \#\mathcal{A}^\vee(\mathcal{O}_v/\mathfrak{m}_v^p)$.

Since $\mathcal{A}^\vee(\mathcal{O}_v/\mathfrak{m}_v^p) \subset \mathcal{A}^\vee(\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^2})$, for (5.9.3) it suffices to show that $\mathcal{N}$ induces the zero map on

$$\mathrm{Ker}(\mathcal{A}^\vee(\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^2}) \to \mathcal{A}^\vee(\mathbb{F}_{v'})).$$

This induced map agrees with multiplication by p because $\mathrm{Gal}(K'_{v'}/K_v)$ acts trivially on $\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^2}$. Moreover, since A is supersingular, so is $A^\vee$, and hence the p-divisible group $A^\vee[p^\infty]$ is isoclinic of slope $\frac{1}{2}$. In particular, the multiplication by p map of $A^\vee$ identifies with the relative p^2-Frobenius morphism $\mathrm{Frob}_{p^2,\, A^\vee/K}$. Therefore, the map induced by $\mathcal{N}$ on $\mathrm{Ker}(\mathcal{A}^\vee(\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^2}) \to \mathcal{A}^\vee(\mathbb{F}_v))$ agrees with the map induced by the relative p^2-Frobenius of $\mathcal{A}^\vee_{\mathcal{O}_{v'}}$, and hence vanishes.

The case when $A[p](\overline{K}) = 0$. In this case, the isogenous p-divisible groups $A[p^\infty]$ and $A^\vee[p^\infty]$ are connected-connected, so Lemma 5.8 provides integers $x > y > 0$ and $z \geqslant 0$ such that

$$\mathrm{Ker}(\mathrm{Frob}_{p^{xt},\, A^\vee/k}) \subset A^\vee[p^{yt+z}] \qquad \text{for every} \quad t \in \mathbb{Z}_{\geqslant 0}. \tag{5.9.4}$$

We choose a t for which $xt > yt + z$, set $n := yt + z$, and for a $v \in U$ use Lemma 5.9 to choose a totally ramified $\mathbb{Z}/p^n\mathbb{Z}$-extension $K'_{v'}/K_v$ for which $\mathrm{Gal}(K'_{v'}/K_v)$ acts trivially on $\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^{xt}}$. Similarly to the proof of the supersingular case, we seek to show that

$$\mathcal{N}(\mathrm{Ker}(\mathcal{A}^\vee(\mathcal{O}_{v'}) \twoheadrightarrow \mathcal{A}^\vee(\mathbb{F}_{v'}))) \subset \mathrm{Ker}(\mathcal{A}^\vee(\mathcal{O}_v) \twoheadrightarrow \mathcal{A}^\vee(\mathcal{O}_v/\mathfrak{m}_v^{p^{xt-n}})), \tag{5.9.5}$$

which will prove the sought nonsurjectivity of $\mathcal{N}$ because $\#\mathcal{A}^\vee(\mathbb{F}_{v'}) < \#\mathcal{A}^\vee(\mathcal{O}_v/\mathfrak{m}_v^{p^{xt-n}})$. To prove (5.9.5), it suffices to prove that the map induced by $\mathcal{N}$ on

$$\mathrm{Ker}(\mathcal{A}^\vee(\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^{xt}}) \to \mathcal{A}^\vee(\mathbb{F}_{v'})).$$

is zero. Since $\mathrm{Gal}(K'_{v'}/K_v)$ acts trivially on $\mathcal{O}_{v'}/\mathfrak{m}_{v'}^{p^{xt}}$, this induced map is multiplication by p^n, so, due to (5.9.4), it factors through the zero map induced by the relative p^{xt}-Frobenius of $\mathcal{A}^\vee_{\mathcal{O}_{v'}}$. □

Remark 5.10. Since the sequence

$$0 \to (\mathrm{Sel}_{p^n} A_{K'})^{\mathrm{Gal}(K'/K)} \to H^1(V', \mathcal{A}[p^n])^{\mathrm{Gal}(K'/K)} \xrightarrow{l'} \left(\mathrm{Im}\, l'\right)^{\mathrm{Gal}(K'/K)}$$

is exact, the proof of Theorem 5.6 shows that even $\#(\mathrm{Sel}_{p^n} A_{K'})^{\mathrm{Gal}(K'/K)}$ is unbounded (and similarly in Corollary 5.5).

Appendix A. Continuity of cup products

The goal of this appendix is to prove that cup product pairings on local cohomology groups are continuous, see Proposition A.3 for a precise statement. Such continuity is implied by the assertion [Mil06, III.6.5 (e)] (whose proof is omitted in loc. cit.) and is crucial for this paper through its roles in the Tate–Shatz local duality [Mil06, III.6.10] and in the proof of Proposition 2.3.

As always, the topology on cohomology is that defined in [Čes15b, 3.1–3.2]. However, we also use [Čes15b, 5.11 and 6.5 (with 3.5 (d))], which guarantee agreement with the "Čech topology." In Lemma A.2, we recall the needed Čech-theoretic notation; see [Čes15b, 5.1] for further recollections.

Lemma A.1. *For a local field k, a k-group scheme G locally of finite type, and an $x \in H^1(k, G)$, there is a finite extension k'/k such that the image of $H^1(k'/k, G) \hookrightarrow H^1(k, G)$ (consisting of classes of right G-torsors that become trivial over k') contains an open neighborhood of x.*

Proof. By [SGA $3_{\text{I new}}$, VII$_\text{A}$, 8.3], G is an extension

$$1 \to H \to G \to Q \to 1$$

of a smooth k-group scheme Q by a finite connected H. By [Čes15b, 3.5 (a) and 4.2], the map

$$H^1(k,G) \to H^1(k,Q)$$

has open fibers, so a k'/k killing the fiber containing x would suffice. To arrive at such a k', we replace k by a finite extension to kill the image of x in $H^1(k,Q)$ and apply [Čes15b, 5.7 (b)], which supplies a finite extension of k that kills the entire $H^1(k,H)$. □

Lemma A.2. *For a finite extension k'/k of local fields and a finite k-group scheme G, the map*

$$H^1(k'/k,G) \hookrightarrow H^1(k,G)$$

is a closed embedding (as in [Čes15b, 5.1], we let $Z^1_{k'/k,G}$ be the k-scheme of 1-cocycles and endow $H^1(k'/k,G)$ with the quotient topology via $Z^1_{k'/k,G}(k) \twoheadrightarrow H^1(k'/k,G)$).

Proof. We fix an algebraic closure $\overline{k}$ containing k', so

$$H^1(k,G) = \varinjlim_{\overline{k}/\widetilde{k}/k'} H^1(\widetilde{k}/k,G),$$

where $\widetilde{k}$ ranges over the indicated finite subextensions. By [Čes15b, 5.11], if each $H^1(\widetilde{k}/k,G)$ is topologized analogously to $H^1(k'/k,G)$, then the topology on $H^1(k,G)$ agrees with the direct limit topology. It therefore suffices to show, as we do below, that each

$$H^1(k'/k,G) \hookrightarrow H^1(\widetilde{k}/k,G)$$

is closed.

For $n \geqslant 0$, we set $\widetilde{k}_n := \otimes_{i=0}^n \widetilde{k}$ (tensor product over k) and let

$$C^n_{\widetilde{k}/k,G} := \mathrm{Res}_{\widetilde{k}_n/k}(G_{\widetilde{k}_n})$$

be the scheme of n-cochains (for G with respect to $\widetilde{k}/k$). Since G is finite, $C^n_{\widetilde{k}/k,G}$ is an affine k-group scheme of finite type. Thus,

$$C^1_{k'/k,G} \hookrightarrow C^1_{\widetilde{k}/k,G}$$

is a closed immersion by [SGA $3_{\mathrm{I\ new}}$, $\mathrm{VI_B}$, 1.4.2], so

$$Z^1_{k'/k,G} \hookrightarrow Z^1_{\widetilde{k}/k,G}$$

is one, too. It remains to note that the $C^0_{\widetilde{k}/k,G}(k)$-orbit quotient map

$$Z^1_{\widetilde{k}/k,G}(k) \twoheadrightarrow H^1(\widetilde{k}/k,G)$$

is closed because $C^0_{\widetilde{k}/k,G}(k)$ is finite. □

Proposition A.3. *For a local field k and a bilinear pairing $G \times_k H \to F$ of commutative k-group schemes locally of finite type with G and H finite, the cup product induces a continuous map*

$$H^n(k,G) \times H^m(k,H) \to H^{n+m}(k,F) \qquad \textit{for every} \qquad n,m \in \mathbb{Z}_{\geqslant 0}.$$

Proof. By [Sha72, p. 208, Thm. 42], every element of $H^n(k,G)$ lies in the image of $H^n(k'/k,G)$ for some finite extension k'/k, and likewise for $H^m(k,H)$. Moreover, $H^n(k,G)$ and $H^m(k,H)$ are discrete except for H^1. Working in neighborhoods of fixed elements of $H^n(k,G)$ and $H^m(k,H)$ and using Lemmas A.1 and A.2, we therefore reduce to proving the continuity of the composition

$$H^n(k'/k,G) \times H^m(k'/k,H) \xrightarrow{-\cup-} H^{n+m}(k'/k,F) \xrightarrow{y} H^{n+m}(k,F) \qquad \text{for every } k'/k.$$

Continuity of y is part of the agreement with the Čech topology, whereas the cup product lifts to a map

$$Z^n_{k'/k,G}(k) \times Z^m_{k'/k,H}(k) \to Z^{n+m}_{k'/k,F}(k)$$

that is continuous because it is induced by a k-scheme morphism. □

Appendix B. Selmer conditions for dual isogenies are orthogonal complements

We seek to justify the legitimacy of the choice of Selmer conditions in Example 4.5 by proving Proposition B.1, which is standard but seems to lack a reference.

Proposition B.1. *For a local field k and dual isogenies $\phi\colon A \to B$ and $\phi^\vee : B^\vee \to A^\vee$ between abelian varieties over k, the subgroups*

$$B(k)/\phi A(k) \subset H^1(k, A[\phi]) \qquad \text{and} \qquad A^\vee(k)/\phi^\vee B^\vee(k) \subset H^1(k, B^\vee[\phi^\vee])$$

are orthogonal complements under the Tate-Shatz local duality pairing

$$H^1(k, A[\phi]) \times H^1(k, B^\vee[\phi^\vee]) \to \mathbb{Q}/\mathbb{Z}.$$

Proof. Due to the commutativity of diagrams such as the first one in [Mil06, III.7.8], the case $\phi = n_A$ for $n \in \mathbb{Z}_{>0}$ is an implicit corollary of the proofs [Mil06, I.3.4, I.3.7, and III.7.8] of Tate local duality for abelian varieties. Thus, we assume the $\phi = n_A$ case to be known and deduce the general case.

By symmetry, it suffices to show that $B(k)/\phi A(k)$ is the annihilator of $A^\vee(k)/\phi^\vee B^\vee(k)$. We set $n := \deg \phi$ and let $\psi\colon B \to A$ be the isogeny for which $\psi \circ \phi = n_A$. In the diagram

$$\begin{tikzcd}
B(k)/\phi A(k) \arrow[r, hook] \arrow[d, "\psi"] & H^1(k, A[\phi]) \arrow[d] & \times & H^1(k, B^\vee[\phi^\vee]) \arrow[rr, bend left] & A^\vee(k)/\phi^\vee B^\vee(k) \arrow[l, hook'] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\
A(k)/nA(k) \arrow[r, hook] & H^1(k, A[n]) & \times & H^1(k, A^\vee[n]) \arrow[u, "H^1(k,\psi^\vee)"'] \arrow[rr, bend right] & A^\vee(k)/nA^\vee(k) \arrow[l, hook'] \arrow[u, two heads] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd} \tag{B.1.1}$$

in which $\psi^\vee$ is the isogeny dual to ψ, the curved arrows are the Tate–Shatz local duality cup product pairings, and the wing squares commute. By [Oda69, 1.1], the inclusion $A[\phi] \hookrightarrow A[n]$ identifies with the Cartier dual of $\psi^\vee : A^\vee[n] \to B^\vee[\phi^\vee]$, so the commutativity of the pairing square results from using [GH71, 3.1] to identify cup product pairings with Ext-product pairings, using [GH70, 4.5] to identify Ext-product pairings with Yoneda edge product pairings, and using the commutativity of

$$\begin{tikzcd}
\mathrm{Ext}^1(B^\vee[\phi^\vee], \mathbb{G}_m) \arrow[d, "\mathrm{Ext}^1(\psi^\vee, \mathbb{G}_m)"'] & \times & \mathrm{Ext}^1(\mathbb{Z}, B^\vee[\phi^\vee]) \arrow[r] & \mathrm{Ext}^2(\mathbb{Z}, \mathbb{G}_m) \arrow[d, equal] \\
\mathrm{Ext}^1(A^\vee[n], \mathbb{G}_m) & \times & \mathrm{Ext}^1(\mathbb{Z}, A^\vee[n]) \arrow[u, "\mathrm{Ext}^1(\mathbb{Z},\psi^\vee)"] \arrow[r] & \mathrm{Ext}^2(\mathbb{Z}, \mathbb{G}_m)
\end{tikzcd}$$

that results from interpreting Ext's as Hom's in a derived category.

The commutativity of (B.1.1) and the assumed $\phi = n_A$ case show that $B(k)/\phi A(k)$ kills $A^\vee(k)/\phi^\vee B^\vee(k)$. Moreover, an $x \in H^1(k, A[\phi])$ that kills $A^\vee(k)/\phi^\vee B^\vee(k)$ maps to $A(k)/nA(k)$ in $H^1(k, A[n])$, so $x \in B(k)/\phi A(k)$ due to the commutativity of the following diagram with exact rows:

$$\begin{tikzcd}
B(k)/\phi A(k) \arrow[r, hook] \arrow[d, "\psi"] & H^1(k, A[\phi]) \arrow[r, two heads] \arrow[d] & H^1(k, A)[\phi] \arrow[d, hook] \\
A(k)/nA(k) \arrow[r, hook] & H^1(k, A[n]) \arrow[r, two heads] & H^1(k, A)[n].
\end{tikzcd}$$

□

References

[Bar10] Alex Bartel, *Large Selmer groups over number fields*, Math. Proc. Cambridge Philos. Soc. **148** (2010), no. 1, 73–86, DOI 10.1017/S0305004109990132. MR2575373 (2011a:11109)

[BCH$^+$66] A. Borel, S. Chowla, C. S. Herz, K. Iwasawa, and J.-P. Serre, *Seminar on complex multiplication*, Seminar held at the Institute for Advanced Study, Princeton, N.J., 1957-58. Lecture Notes in Mathematics, No. 21, Springer-Verlag, Berlin-New York, 1966. MR0201394 (34 #1278)

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

[BouTG] Nicolas Bourbaki, *Éléments de mathématique. Topologie generale*, chap. I-IV, Hermann (1971); chap. V-X, Hermann (1974) (French).

[Bra14] Julio Brau, *Selmer groups of elliptic curves in degree p extensions*, preprint (2014). Available at http://arxiv.org/abs/1401.3304.

[Cas64] J. W. S. Cassels, *Arithmetic on curves of genus* 1. *VI. The Tate-Šafarevič group can be arbitrarily large*, J. reine angew. Math. **214/215** (1964), 65–70. MR0162800 (29 #104)

[Čes15a] Kęstutis Česnavičius, *Selmer groups and class groups*, Compos. Math. **151** (2015), no. 3, 416–434, DOI 10.1112/S0010437X14007441. MR3320567

[Čes15b] Kęstutis Česnavičius, *Topology on cohomology of local fields*, Forum Math. Sigma **3** (2015), e16, 55, DOI 10.1017/fms.2015.18.

[Čes16a] ———, *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc. **31** (2016), no. 1, 31–61.

[Čes16b] ———, *The ℓ-parity conjecture over the constant quadratic extension*, preprint (2016). Available at http://arxiv.org/abs/1402.2939.

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

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

[CS00] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, 88, Published by Narosa Publishing House, New Delhi, 2000. MR1759312 (2001b:11046)

[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)

[Fis01] Tom Fisher, *Some examples of 5 and 7 descent for elliptic curves over* **Q**, J. Eur. Math. Soc. (JEMS) **3** (2001), no. 2, 169–201, DOI 10.1007/s100970100030. MR1831874 (2002m:11045)

[GA09] Cristian D. González-Avilés, *Arithmetic duality theorems for 1-motives over function fields*, J. reine angew. Math. **632** (2009), 203–231, DOI 10.1515/CRELLE.2009.055. MR2544149 (2010i:11169)

[GH70] J. Gamst and K. Hoechsmann, *Products in sheaf-cohomology*, Tôhoku Math. J. (2) **22** (1970), 143–162. MR0289605 (44 #6793)

[GH71] ———, *Ext-products and edge-morphisms*, Tôhoku Math. J. (2) **23** (1971), 581–588. MR0302741 (46 #1884)

[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)

[HR79] Edwin Hewitt and Kenneth A. Ross, *Abstract harmonic analysis. Vol. I*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 115, Springer-Verlag, Berlin, 1979. Structure of topological groups, integration theory, group representations. MR551496 (81k:43001)

[Klo05] Remke Kloosterman, *The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large*, J. Théor. Nombres Bordeaux **17** (2005), no. 3, 787–800 (English, with English and French summaries). MR2212126 (2006k:11102)

[Kra83] Kenneth Kramer, *A family of semistable elliptic curves with large Tate-Shafarevitch groups*, Proc. Amer. Math. Soc. **89** (1983), no. 3, 379–386, DOI 10.2307/2045480. MR715850 (85d:14059)

[KS03] Remke Kloosterman and Edward F. Schaefer, *Selmer groups of elliptic curves that can be arbitrarily large*, J. Number Theory **99** (2003), no. 1, 148–163, DOI 10.1016/S0022-314X(02)00054-9. MR1957249 (2003m:11081)

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

[Mat07] Kazuo Matsuno, *Construction of elliptic curves with large Iwasawa λ-invariants and large Tate-Shafarevich groups*, Manuscripta Math. **122** (2007), no. 3, 289–304, DOI 10.1007/s00229-006-0068-9. MR2305419 (2008h:11106)

[Mat09] ———, *Elliptic curves with large Tate-Shafarevich groups over a number field*, Math. Res. Lett. **16** (2009), no. 3, 449–461, DOI 10.4310/MRL.2009.v16.n3.a6. MR2511625 (2010e:11053)

[Mil70] J. S. Milne, *Elements of order p in the Tate-Šafarevič group*, Bull. London Math. Soc. **2** (1970), 293–296. MR0277507 (43 #3240)

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

[MR07] Barry Mazur and Karl Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612, DOI 10.4007/annals.2007.166.579. MR2373150 (2009a:11127)

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher; With a foreword by G. Harder. MR1697859 (2000m:11104)

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR2392026 (2008m:11223)

[Oda69] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135. MR0241435 (39 #2775)

[SGA $3_{\mathrm{I\ new}}$] Philippe Gille and Patrick Polo (eds.), *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*, Documents Mathématiques (Paris) [Mathematical Documents (Paris)], 7, Société Mathématique de France, Paris, 2011 (French). Séminaire de Géométrie Algébrique du Bois Marie 1962–64. [Algebraic Geometry Seminar of Bois Marie 1962–64]; A seminar directed by M. Demazure and A. Grothendieck with the collaboration of M. Artin, J.-E. Bertin, P. Gabriel, M. Raynaud and J-P. Serre; Revised and annotated edition of the 1970 French original. MR2867621

[SGA 3_{II}] *Schémas en groupes. II: Groupes de type multiplicatif, et structure des schémas en groupes généraux*, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Dirigé par M. Demazure et A. Grothendieck. Lecture Notes in Mathematics, Vol. 152, Springer-Verlag, Berlin-New York, 1970 (French). MR0274459 (43 #223b)

[Sha64] Stephen S. Shatz, *Cohomology of artinian group schemes over local fields*, Ann. of Math. (2) **79** (1964), 411–449. MR0193093 (33 #1314)

[Sha72] ———, *Profinite groups, arithmetic, and geometry*, Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1972. Annals of Mathematics Studies, No. 67. MR0347778 (50 #279)

[Toë11] Bertrand Toën, *Descente fidèlement plate pour les n-champs d'Artin*, Compos. Math. **147** (2011), no. 5, 1382–1412, DOI 10.1112/S0010437X10005245 (French, with English and French summaries). MR2834725