SELMER GROUPS AS FLAT COHOMOLOGY GROUPS

KĘSTUTIS ČESNAVIČIUS

Abstract. Given a prime number p, Bloch and Kato showed how the p^∞-Selmer group of an abelian variety A over a number field K is determined by the p-adic Tate module. In general, the p^m-Selmer group $\mathrm{Sel}_{p^m} A$ need not be determined by the mod p^m Galois representation $A[p^m]$; we show, however, that this is the case if p is large enough. More precisely, we exhibit a finite explicit set of rational primes Σ depending on K and A, such that $\mathrm{Sel}_{p^m} A$ is determined by $A[p^m]$ for all $p \notin \Sigma$. In the course of the argument we describe the flat cohomology group $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[p^m])$ of the ring of integers of K with coefficients in the p^m-torsion $\mathcal{A}[p^m]$ of the Néron model of A by local conditions for $p \notin \Sigma$, compare them with the local conditions defining $\mathrm{Sel}_{p^m} A$, and prove that $\mathcal{A}[p^m]$ itself is determined by $A[p^m]$ for such p. Our method sharpens the relationship between $\mathrm{Sel}_{p^m} A$ and $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[p^m])$ which was first observed by Mazur and continues to work for other isogenies ϕ between abelian varieties over global fields provided that $\deg \phi$ is constrained appropriately. To illustrate it, we exhibit resulting explicit rank predictions for the elliptic curve $11A1$ over certain families of number fields.

1. Introduction

Let K be a number field, let $A \to \operatorname{Spec} K$ be a dimension g abelian variety, and let p be a prime number. Fix a separable closure $\overline{K}$ of K. Tate conjectured [Tat66, p. 134] that the *p-adic Tate module* $T_p A := \varprojlim A[p^m](\overline{K})$ determines A up to an isogeny of degree prime to p, and Faltings proved this in [Fal83, §1 b)]. One can ask whether $A[p]$ alone determines A to some extent. Consideration of the case $g = 1$, $p = 2$ shows that for small p one cannot expect much in this direction. However, at least if $g = 1$ and $K = \mathbb{Q}$, for p large enough (depending on A) the Frey-Mazur conjecture [Kra99, Conj. 3] predicts that $A[p]$ should determine A up to an isogeny of degree prime to p.

Let $\mathrm{Sel}_{p^\infty} A \subset H^1(K, A[p^\infty])$ be the p^∞-Selmer group. The theorem of Faltings implies that $T_p A$ determines $\mathrm{Sel}_{p^\infty} A$ up to isomorphism, and a direct description of $\mathrm{Sel}_{p^\infty} A$ in terms of $T_p A$ was given by Bloch and Kato [BK90] using ideas from p-adic Hodge theory. Considering the p-Selmer group $\mathrm{Sel}_p A$ and $A[p]$ instead of $\mathrm{Sel}_{p^\infty} A$ and $A[p^\infty]$ (equivalently, $\mathrm{Sel}_{p^\infty} A$ and $T_p A$), in light of the Frey-Mazur conjecture, one may expect a direct description of $\mathrm{Sel}_p A$ in terms of $A[p]$ for large p. We give such a description as a special case of

Theorem 1.1. *Fix an extension of number fields L/K, a K-isogeny $\phi\colon A \to B$ between abelian varieties, and let $\mathcal{A}[\phi]$ and $\mathcal{A}^L[\phi]$ be the kernels of the induced homomorphisms between the Néron models over the rings of integers $\mathcal{O}_K$ and $\mathcal{O}_L$. Let v (resp., w) denote a place of K (resp., L), let $c_{A,v}$ and $c_{B,v}$ (resp., $c_{A,w}$ and $c_{B,w}$) denote the local Tamagawa factors for $v, w \nmid \infty$ (cf. 2.4), let e_v be the absolute ramification index if $v \nmid \infty$, set $e_p := \max_{v|p} e_v$, and see 1.14 for other notation.*

(a) Assume that A has semiabelian reduction at all $v \mid \deg \phi$.

Date: September 9, 2013.

2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 14F20, 14K02, 14L15.

Key words and phrases. Abelian variety, Selmer group, fppf cohomology, torsor, Néron model.

(i) (Corollaries 4.2 and B.4.) *The pullback map* $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi]) \to H^1(K, A[\phi])$ *is an isomorphism onto the preimage of* $\prod_{v\nmid\infty} H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \subset \prod_{v\nmid\infty} H^1(K_v, A[\phi])$.

(ii) (Proposition 5.4(c).) *If* $\deg\phi$ *is prime to* $\prod_{v\nmid\infty} c_{A,v}c_{B,v}$ *and either* $2 \nmid \deg\phi$ *or* $A(K_v)$ *is connected for all real* v*, then* $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi]) = \mathrm{Sel}_\phi A$ *inside* $H^1(K, A[\phi])$.

(b) (Proposition 3.3.) *Assume that* A *has good reduction at all* $v \mid \deg\phi$*. If* $e_p < p-1$ *for every prime* $p \mid \deg\phi$*, then the* $\mathcal{O}_L$*-group scheme* $\mathcal{A}^L[\phi]$ *is determined up to isomorphism by the* $\mathrm{Gal}(\overline{L}/K)$*-module* $A[\phi](\overline{L})$.

Thus, if $(\deg\phi, \prod_{w\nmid\infty} c_{A,w}c_{B,w}) = 1$*, the reduction of* A *is good at all* $v \mid \deg\phi$*, and* $e_p < p-1$ *for every* $p \mid \deg\phi$ *(in particular,* $2 \nmid \deg\phi$*), then the* ϕ*-Selmer group* $\mathrm{Sel}_\phi A_L \subset H^1(L, A[\phi])$ *is determined by the* $\mathrm{Gal}(\overline{L}/K)$*-module* $A[\phi](\overline{L})$.

Corollary 1.2. *If* A *has potential good reduction everywhere and* p *is large enough (depending on* A*), then* $A[p^m]$ *determines* $\mathrm{Sel}_{p^m} A_L$ *for every finite extension* L/K.

Proof. Indeed, by a theorem of McCallum [ELL96, pp. 801-802], $q \leqslant 2g+1$ for a prime $q \mid c_{A,w}$. □

Remarks.

1.3. Relationships similar to (ii) between Selmer groups and flat cohomology groups are not new and have been (implicitly) observed already in [Maz72] and subsequently used by Mazur, Schneider, Kato, and others (often after passing to p^∞-Selmer groups as is customary in Iwasawa theory). However, the description of $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi])$ by local conditions in (i) is new, and consequently (ii) is more precise than what seems to be available in the literature.

1.4. In the case of elliptic curves, Mazur and Rubin find in [MR13, Thm. 3.1 and 6.1] (see also [AS05, 6.6] for a similar result of Cremona and Mazur) that under assumptions different from those of Theorem 1.1, p^m-Selmer groups are determined by mod p^m Galois representations together with additional data including the set of places of potential multiplicative reduction. It is unclear to us whether their results can be recovered from the ones presented in this paper.

1.5. The Selmer type description as in (i) continues to hold for $H^1_{\text{ét}}(\mathcal{O}_K, \mathcal{A})$, where $\mathcal{A} \to \operatorname{Spec}\mathcal{O}_K$ is the Néron model of A. This leads to a reproof of the étale cohomological interpretation of the Shafarevich-Tate group $Ш(A)$ observed by Mazur [Maz72, Appendix], see Proposition 4.3. Our argument is more direct: in the proof of loc. cit. the absence of Corollary 4.2 is circumvented with a diagram chase using cohomology with supports exact sequences.

1.6. In Theorem 1.1(a), it is possible to relate $\mathrm{Sel}_\phi A$ and $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi])$ under weaker hypotheses than those of (ii) by combining Proposition 2.5 with Corollary 4.2 as in the proof of Proposition 5.4 (see also Remark 5.5).

1.7. The interpretation of Selmer groups as flat cohomology groups is useful beyond the case when ϕ is multiplication by an integer. For an example, see the last sentence of Remark 5.7.

1.8. Theorem 1.1 is stronger than its restriction to the case $L = K$. Indeed, the analogue of $e_p < p-1$ may fail for L but hold for K. This comes at the expense of $\mathcal{A}^L[\phi]$ and $\mathrm{Sel}_\phi A_L$ being determined by $A[\phi](\overline{L})$ as a $\mathrm{Gal}(\overline{L}/K)$-module, rather than as a $\mathrm{Gal}(\overline{L}/L)$-module.

1.9. Taking $L = K$ and $A = B$ in Theorem 1.1, we get the set Σ promised in the abstract by letting it consist of all primes below a place of bad reduction for A, all primes dividing a local Tamagawa factor of A, the prime 2, and all odd primes p ramified in K for which $e_p \geqslant p-1$.

1.10. In Theorem 1.1, is the subgroup $B(L)/\phi A(L)$ (equivalently, the quotient $Ш(A_L)[\phi]$) also determined by $A[\phi](\overline{L})$? The answer is 'no'. Indeed, in [CM00, p. 24] Cremona and Mazur report[1] that the elliptic curves $2534E1$ and $2534G1$ over $\mathbb{Q}$ have isomorphic mod 3 representations, but $2534E1$ has rank 0, whereas $2534G1$ has rank 2. Since 3 is prime to the conductor 2534 and the local Tamagawa factors $c_2 = 44$, $c_7 = 1$, $c_{181} = 2$ (resp., $c_2 = 13$, $c_7 = 2$, $c_{181} = 1$) of $2534E1$ (resp., $2534G1$), Theorem 1.1 indeed applies to these curves. Another example (loc. cit.) is the pair $4592D1$ and $4592G1$ with $\phi = 5$ and ranks 0 and 2.

For an odd prime p and elliptic curves E and E' over $\mathbb{Q}$ with $E[p] \cong E'[p]$ and prime to p conductors and local Tamagawa factors, Theorem 1.1, expected finiteness of Ш, and Cassels-Tate pairing predict that $\operatorname{rk} E(\mathbb{Q}) \equiv \operatorname{rk} E'(\mathbb{Q}) \bmod 2$. Can one prove this directly?

1.11. For the analogue of Theorem 1.1(a) for global function fields, one takes a (connected) proper smooth curve S over a finite field in the indicated references. Letting K be the function field of S, the analogue of Theorem 1.1(b) is Corollary B.5: if $\operatorname{char} K \nmid \deg \phi$, then $\mathcal{A}[\phi] \to S$ is the Néron model of $A[\phi] \to \operatorname{Spec} K$ (L plays no role); in this case, due to Proposition 2.7(c), $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \subset H^1(K, A[\phi])$ consists of the everywhere unramified cohomology classes. The final conclusion becomes: if $(\deg \phi, \operatorname{char} K \prod_s c_{A,s} c_{B,s}) = 1$ (the product of the local Tamagawa factors is indexed by the closed $s \in S$), then $\operatorname{Sel}_\phi A \subset H^1(K, A[\phi])$ is determined by $A[\phi]$ and in fact consists of the everywhere unramified cohomology classes of $H^1(K, A[\phi])$.

Example 1.12. We illustrate the utility of our methods and results by estimating the 5-Selmer group of the base change E_K of the elliptic curve $E = 11A1$ to any number field K. This curve has also been considered by Tom Fisher, who described in [Fis03, 2.1] the ϕ-Selmer groups of E_K for the two degree 5 isogenies ϕ of E_K defined over $\mathbb{Q}$. We restrict to $11A1$ for the sake of concreteness (and to get precise conclusions (a)-(f)), although our argument leads to estimates analogous to (2) for every elliptic curve A over $\mathbb{Q}$ and an odd prime p of good reduction for A such that $A[p] \cong \mathbb{Z}/p\mathbb{Z} \oplus \mu_p$.

Let $\mathcal{E}^K \to \operatorname{Spec} \mathcal{O}_K$ be the Néron model of E_K. As $E[5] \cong \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$, by the proof of Proposition 3.3, $\mathcal{E}^K[5] \cong \underline{\mathbb{Z}/5\mathbb{Z}}_{\mathcal{O}_K} \oplus \mu_5$, so $0 \to \mu_5 \to \mathbb{G}_m \xrightarrow{5} \mathbb{G}_m \to 0$ together with $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathbb{Z}/5\mathbb{Z}) \cong \operatorname{Cl}_K[5]$ give

$$\dim_{\mathbb{F}_5} H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{E}^K[5]) = 2 \dim_{\mathbb{F}_5} \operatorname{Cl}_K[5] + \dim_{\mathbb{F}_5} \mathcal{O}_K^\times / \mathcal{O}_K^{\times 5} = 2h_5^K + r_1^K + r_2^K - 1 + u_5^K, \qquad (1)$$

where Cl_K is the ideal class group, r_1^K and r_2^K are the numbers of real and complex places, and $h_5^K := \dim_{\mathbb{F}_5} \operatorname{Cl}_K[5]$, $u_5^K := \dim_{\mathbb{F}_5} \mu_5(\mathcal{O}_K)$. Since component groups of Néron models of elliptic curves with split multiplicative reduction are cyclic, (1) and Remark 5.5 give

$$2h_5^K + r_1^K + r_2^K - 1 + u_5^K - \#\{v \mid 11\} \leqslant \dim_{\mathbb{F}_5} \operatorname{Sel}_5 E_K \leqslant 2h_5^K + r_1^K + r_2^K - 1 + u_5^K + \#\{v \mid 11\}. \quad (2)$$

Thus, the obtained estimate is most precise when K has a single place above 11. Also,

$$\dim_{\mathbb{F}_5} \operatorname{Sel}_5 E_K \equiv r_1^K + r_2^K - 1 + u_5^K + \#\{v \mid 11\} \bmod 2, \qquad (3)$$

because the 5-parity conjecture is known for E_K [DD08]. When K ranges over the quadratic extensions of $\mathbb{Q}$, due to (2), the conjectured unboundedness of 5-ranks h_5^K of ideal class groups is equivalent to the unboundedness of $\dim_{\mathbb{F}_5} \operatorname{Sel}_5 E_K$. This equivalence is an instance of a general result [Česl3b, 1.5] that gives a precise relation between unboundedness questions for Selmer groups and class groups. That a relation of this sort may be feasible has also been (at least implicitly) observed by various other authors; see, for instance, [Sch96].

It is curious to draw some concrete conclusions that (2) and (3) offer:

[1] Assuming the Birch and Swinnerton-Dyer conjecture to compute Shafarevich-Tate groups analytically. This is unnecessary for us, since full 2-descent finds provably correct ranks of $2534E1$, $2534G1$, $4592D1$, and $4592G1$.

(a) As is also well known, $\operatorname{rk} E(\mathbb{Q}) = 0$.

(b) If K is imaginary quadratic with $h_5^K = 0$ and 11 is inert or ramified in K, then $\operatorname{rk} E(K) = 0$.

(c) If K is imaginary quadratic with $h_5^K = 0$ and 11 splits in K, then either $\operatorname{rk} E(K) = 1$, or $\operatorname{rk} E(K) = 0$ and $\operatorname{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] = 1$. In the latter case $Ш(E_K)[p^\infty]$ is infinite for every prime p, because the p-parity conjecture is known for E_K for every p by [DD10, 1.4] (applied to E and its quadratic twist by K).

(d) If F is a quadratic extension of a K as in (c) in which none of the places of K above 11 split and $h_5^F = 0$, then either $\operatorname{rk} E(F) = 2$, or $Ш(E_F)[5^\infty]$ is infinite.

(e) If K is real quadratic with $h_5^K = 0$ and 11 is inert or ramified in K, then either $\operatorname{rk} E(K) = 1$, or $\operatorname{rk} E(K) = 0$ and $\operatorname{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] = 1$. In the latter case $Ш(E_K)[p^\infty]$ is infinite for every prime p for the same reason as in (c).

(f) If K is cubic with a complex place (or quartic totally imaginary), a single place above 11, and $h_5^K = 0$, then either $\operatorname{rk} E(K) = 1$, or $\operatorname{rk} E(K) = 0$ and $\operatorname{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] = 1$.

How can one construct the predicted rational points? In (c) and the inert case of (e) one could hope that Heegner and Stark-Heegner point constructions would account for the predicted rank growth; for some numerical evidence of this for (e), see [DG02, Tables 1 and 2] and [DP06, §4 pp. 347-348]. However, (d) and (f) concern situations that seem to be beyond the scope of applicability of the existing methods for systematic construction of rational points of infinite order.

1.13. The contents of the paper. We begin by restricting to local bases in §2 and comparing the subgroups $B(K_v)/\phi(A(K_v))$, $H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi])$, and $H^1_{\mathrm{nr}}(K_v, A[\phi])$ of $H^1(K_v, A[\phi])$ under appropriate hypotheses. In §3, after recording some standard fpqc descent results, we apply them to prove Theorem 1.1(b) and obtain a new proof of the étale cohomological interpretation of Shafarevich-Tate groups. In §4, exploiting the descent results of §3, we take up the question of H^1_{fppf} with appropriate coefficients over Dedekind bases being described by local conditions and prove Theorem 1.1(i). The final §5 uses the local analysis of §2 to compare $\operatorname{Sel}_\phi A$ and $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi])$ and complete the proof of Theorem 1.1. The two appendices collect various results concerning torsors and exact sequences of Néron models used in the main body of the text. Some of the results presented in this paper are worked out in somewhat more general settings in the corresponding chapter of the PhD thesis of the author; we invite a reader interested in this to consult [Česl3a], which also discusses several tangentially related questions.

1.14. Conventions. When needed, a choice of a separable closure $\overline{K}$ of a field K will be made implicitly, as will be a choice of an embedding $\overline{K} \hookrightarrow \overline{L}$ for an overfield L/K. If v is a place of a global field K, then K_v is the corresponding completion; for $v \nmid \infty$, the ring of integers and the residue field of K_v are denoted by $\mathcal{O}_v$ and $\mathbb{F}_v$. If K is a number field, $\mathcal{O}_K$ is its ring of integers. For $s \in S$ with S a scheme, $\mathcal{O}_{S,s}$, $\mathfrak{m}_{S,s}$, and $k(s)$ are the local ring at s, its maximal ideal, and its residue field. For a local ring R, its henselization, strict henselization, and completion are R^h, R^{sh}, and $\widehat{R}$. The fppf, big étale, and étale sites of S are S_{fppf}, $S_{\acute{\mathrm{E}}\mathrm{t}}$, and $S_{\text{ét}}$; the objects of S_{fppf} and $S_{\acute{\mathrm{E}}\mathrm{t}}$ are all S-schemes, while those of $S_{\text{ét}}$ are all schemes étale over S. The cohomology groups computed in $S_{\text{ét}}$ and S_{fppf} are denoted by $H^i_{\text{ét}}(S, -)$ and $H^i_{\mathrm{fppf}}(S, -)$; Galois cohomology merits no subscript: $H^i(K, -)$. We frequent the shorthand X_T for the base change of $X \to S$ along $T \to S$. An algebraic group over a field K is a finite type smooth K-group scheme.

Acknowledgements. I thank Bjorn Poonen for many helpful discussions, suggestions, and for reading various drafts. I thank Brian Conrad for reading the manuscript and suggesting numerous

improvements. I thank Rebecca Bellovin, Henri Darmon, Tim Dokchitser, Jessica Fintzen, Jean Gillibert, Mark Kisin, Dino Lorenzini, Barry Mazur, Martin Olsson, Michael Stoll, and David Zureick-Brown for helpful conversations or correspondence regarding the material of this 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. Images of local Kummer homomorphisms as flat cohomology groups

Let $S = \operatorname{Spec} \mathfrak{o}$ for a Henselian discrete valuation ring $\mathfrak{o}$ with a finite residue field $\mathbb{F}$, let $k = \operatorname{Frac} \mathfrak{o}$, let $i\colon \operatorname{Spec} \mathbb{F} \to S$ be the closed point, let $\phi\colon A \to B$ be a k-isogeny of abelian varieties, let $\phi\colon \mathcal{A} \to \mathcal{B}$ be the induced S-homomorphism between the Néron models, which gives rise to the homomorphism $\phi\colon \Phi_A \to \Phi_B$ between the étale $\mathbb{F}$-group schemes of connected components of $\mathcal{A}_{\mathbb{F}}$ and $\mathcal{B}_{\mathbb{F}}$. We use various open subgroups of $\mathcal{A}$ and $\mathcal{B}$ discussed in B.1.

2.1. The three subgroups. The first one is $\operatorname{Im}(B(k) \xrightarrow{\kappa_\phi} H^1_{\mathrm{fppf}}(k, A[\phi])) \cong B(k)/\phi A(k)$.

The second subgroup is defined if $\operatorname{char} \mathbb{F} \nmid \deg \phi$ or A has semiabelian reduction; it is the image of $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \xrightarrow{a} H^1_{\mathrm{fppf}}(k, A[\phi])$. By Proposition A.5 (see also the proof of Proposition 2.5(a)), a is injective, and we identify $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \cong \operatorname{Im} a \subset H^1_{\mathrm{fppf}}(k, A[\phi])$.

The third subgroup is defined if $\operatorname{char} k \nmid \deg \phi$ (so $A[\phi]$ is étale); it is the unramified subgroup $H^1_{\mathrm{nr}}(k, A[\phi]) := \operatorname{Ker}(H^1(k, A[\phi]) \to H^1(k^{sh}, A[\phi])) \subset H^1(k, A[\phi])$, where $k^{sh} := \operatorname{Frac} \mathfrak{o}^{sh}$.

While $\operatorname{Im} \kappa_\phi$ is used to define the ϕ-Selmer group, $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$ and $H^1_{\mathrm{nr}}(k, A[\phi])$ are easier to study as they depend only on $\mathcal{A}[\phi]$. We investigate $\operatorname{Im} \kappa_\phi$ by detailing its relations with $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$ and $H^1_{\mathrm{nr}}(k, A[\phi])$ in Propositions 2.5 and 2.7.

Lemma 2.2. *For a commutative connected algebraic group $G \to \operatorname{Spec} \mathbb{F}$ and $j \geqslant 1$, $H^j(\mathbb{F}, G) = 0$.*

Proof. The case $j > 1$ holds since $\mathbb{F}$ has cohomological dimension 1 and $G(\overline{\mathbb{F}})$ is a torsion group (as $\mathbb{F}$ is finite), and the case $j = 1$ is a well-known result of Lang [Lan56, Thm. 2]. □

Lemma 2.3. *For a subgroup $\Gamma \subset \Phi_A$ and $j \geqslant 1$, pullback induces isomorphisms $H^j_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) \cong H^j(\mathbb{F}, \Gamma)$. In particular, $\#H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) = \#\Gamma(\mathbb{F})$ and $H^j_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) = 0$ for $j \geqslant 2$.*

Proof. Combine pullback isomorphisms $H^j_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) \cong H^j(\mathbb{F}, \mathcal{A}^\Gamma_{\mathbb{F}})$ for $j \geqslant 1$ [Gro68, 11.7], the long exact cohomology sequence of $0 \to \mathcal{A}^0_{\mathbb{F}} \to \mathcal{A}^\Gamma_{\mathbb{F}} \to \Gamma \to 0$, and Lemma 2.2. □

2.4. The local Tamagawa factors. These are $c_A := \#\Phi_A(\mathbb{F})$ and $c_B := \#\Phi_B(\mathbb{F})$. The sequences

$$0 \to \Phi_A[\phi](\overline{\mathbb{F}}) \to \Phi_A(\overline{\mathbb{F}}) \to (\phi(\Phi_A))(\overline{\mathbb{F}}) \to 0,$$
$$0 \to (\phi(\Phi_A))(\overline{\mathbb{F}}) \to \Phi_B(\overline{\mathbb{F}}) \to (\Phi_B/\phi(\Phi_A))(\overline{\mathbb{F}}) \to 0$$

are exact, and hence

$$\frac{\#\Phi_A(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \leqslant \#\Phi_A[\phi](\mathbb{F}), \qquad \frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \leqslant \#\left(\frac{\Phi_B}{\phi(\Phi_A)}\right)(\mathbb{F}). \tag{4}$$

We now compare the subgroups $\operatorname{Im} \kappa_\phi$ and $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$ of $H^1_{\mathrm{fppf}}(k, A[\phi])$ discussed in 2.1:

Proposition 2.5. *Suppose that $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (e.g., that A has semiabelian reduction if $\operatorname{char}\mathbb{F} \mid \deg\phi$, cf. Lemma B.3).*

(a) Then

$$\#\left(\frac{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])}{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])\cap\operatorname{Im}\kappa_\phi}\right) = \frac{\#\Phi_A(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \overset{(4)}{\leqslant} \#\Phi_A[\phi](\mathbb{F}),$$
$$\#\left(\frac{\operatorname{Im}\kappa_\phi}{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])\cap\operatorname{Im}\kappa_\phi}\right) = \frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \overset{(4)}{\leqslant} \#\left(\frac{\Phi_B}{\phi(\Phi_A)}\right)(\mathbb{F}).$$

(b) If $\deg\phi$ is prime to c_B, then $\Phi_B(\mathbb{F}) = (\phi(\Phi_A))(\mathbb{F})$, and hence, by (a), $\operatorname{Im}\kappa_\phi \subset H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])$.

(c) If $\deg\phi$ is prime to c_A, then $\Phi_A(\mathbb{F}) = (\phi(\Phi_A))(\mathbb{F})$, and hence, by (a), $H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi]) \subset \operatorname{Im}\kappa_\phi$.

(d) If $\deg\phi$ is prime to c_Ac_B, then $\operatorname{Im}\kappa_\phi = H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])$.

Proof.

(a) The short exact sequence $0 \to \mathcal{A}[\phi] \to \mathcal{A} \xrightarrow{\phi} \mathcal{B}^{\phi(\Phi_A)} \to 0$ of Corollary B.6 gives

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})/\phi\mathcal{A}(\mathfrak{o}) & \longrightarrow & H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi]) & \longrightarrow & \operatorname{Ker}(H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}) \xrightarrow{H^1_{\mathrm{fppf}}(\phi)} H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{B}^{\phi(\Phi_A)})) & \longrightarrow & 0 \\
 & & \big\downarrow & & \big\downarrow a & & \big\downarrow & & \\
0 & \longrightarrow & B(k)/\phi A(k) & \xrightarrow{\kappa_\phi} & H^1_{\mathrm{fppf}}(k,A[\phi]) & \longrightarrow & H^1_{\mathrm{fppf}}(k,A)[\phi] & \longrightarrow & 0,
\end{array}$$

where the injectivity of the vertical arrows follows from the Néron property, snake lemma, and Corollary A.3. By Lemma 2.3, $H^1_{\mathrm{fppf}}(\phi)$ identifies with $H^1(\mathbb{F},\Phi_A) \xrightarrow{h} H^1(\mathbb{F},\phi(\Phi_A))$ induced by ϕ; moreover, h is onto. Since $\frac{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])}{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])\cap\operatorname{Im}\kappa_\phi} \cong \operatorname{Ker} H^1_{\mathrm{fppf}}(\phi) \cong \operatorname{Ker} h$, and $\#\operatorname{Ker} h = \frac{\#H^1(\mathbb{F},\Phi_A)}{\#H^1(\mathbb{F},\phi(\Phi_A))} = \frac{\#\Phi_A(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})}$, the first claim follows. On the other hand,

$$\frac{\operatorname{Im}\kappa_\phi}{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])\cap\operatorname{Im}\kappa_\phi} \cong \frac{B(k)/\phi A(k)}{\mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})/\phi\mathcal{A}(\mathfrak{o})} \cong \frac{\mathcal{B}(\mathfrak{o})}{\mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})}. \tag{5}$$

Lemma 2.3 and the étale cohomology sequence of $0 \to \mathcal{B}^{\phi(\Phi_A)} \to \mathcal{B} \to i_*(\Phi_B/\phi(\Phi_A)) \to 0$ from Proposition B.2 give the exact sequence (cf. also [Gro68, 11.7 1°])

$$0 \to \frac{\mathcal{B}(\mathfrak{o})}{\mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})} \to \left(\frac{\Phi_B}{\phi(\Phi_A)}\right)(\mathbb{F}) \to H^1(\mathbb{F},\phi(\Phi_A)) \to H^1(\mathbb{F},\Phi_B) \twoheadrightarrow H^1\left(\mathbb{F},\frac{\Phi_B}{\phi(\Phi_A)}\right), \tag{6}$$

where we have used the exactness of i_* for the étale topology to obtain the last term. Combining (5) and (6) yields the remaining

$$\#\left(\frac{\operatorname{Im}\kappa_\phi}{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])\cap\operatorname{Im}\kappa_\phi}\right) = \frac{\#(\Phi_B/\phi(\Phi_A))(\mathbb{F})\cdot\#H^1(\mathbb{F},\Phi_B)}{\#H^1(\mathbb{F},\phi(\Phi_A))\cdot\#H^1(\mathbb{F},\Phi_B/\phi(\Phi_A))} = \frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})}.$$

(b) Let $\psi\colon B \to A$ be the isogeny with $\ker\psi = \phi(A[\deg\phi])$, so $\psi\circ\phi = \deg\phi$, and thus $\phi\circ\psi = \deg\phi$. If $(\deg\phi, \#\Phi_B(\mathbb{F})) = 1$, then $\Phi_B(\mathbb{F}) = (\deg\phi)(\Phi_B(\mathbb{F})) \subset ((\deg\phi)(\Phi_B))(\mathbb{F}) \subset (\phi(\Phi_A))(\mathbb{F}) \subset \Phi_B(\mathbb{F})$, giving the desired $\Phi_B(\mathbb{F}) = (\phi(\Phi_A))(\mathbb{F})$.

(c) Considering ψ as in the proof of (b), $\Phi_A[\phi] \subset \Phi_A[\deg\phi]$, so if $(\deg\phi, \#\Phi_A(\mathbb{F})) = 1$, then $\Phi_A[\phi](\mathbb{F}) = 0$. The resulting $\Phi_A(\mathbb{F}) \hookrightarrow \phi(\Phi_A)(\mathbb{F})$ is onto, since $\#H^1(\mathbb{F}, \Phi_A[\phi]) = \#\Phi_A[\phi](\mathbb{F})$.

(d) Combine (b) and (c). □

Remark 2.6. In the case $\dim A = 1$ and $\phi = p^m$, Proposition 2.5(d) has also been observed by Mazur and Rubin [MR13, Prop. 5.8].

We now compare the third subgroup $H^1_{\mathrm{nr}}(k, A[\phi]) \subset H^1(k, A[\phi])$ of 2.1 to $\operatorname{Im}\kappa_\phi$ and $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$:

Proposition 2.7. *Suppose that* $\operatorname{char} k \nmid \deg\phi$*, and let* $\mathcal{G} \to S$ *be the Néron model of* $A[\phi] \to \operatorname{Spec} K$ *(it exists, for instance, by* [BLR90, §7.1 Cor. 6]*).*

(a) The image of $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \to H^1(k, A[\phi])$ *contains* $H^1_{\mathrm{nr}}(k, A[\phi])$*.*

(b) One has $H^1_{\mathrm{nr}}(k, A[\phi]) \subset \operatorname{Im}\kappa_\phi$*, if one assumes in addition that*

(i) $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ *is flat if* $\operatorname{char}\mathbb{F} \mid \deg\phi$*, and*

(ii) $\deg\phi$ *is prime to* c_A *or, more generally (cf. Proposition 2.5(c)),* $\#\Phi_A(\mathbb{F}) = \#(\phi(\Phi_A))(\mathbb{F})$*.*

(c) If $\operatorname{char}\mathbb{F} \nmid \deg\phi$*, then* $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) = H^1_{\mathrm{nr}}(k, A[\phi])$*.*

(d) One has $\operatorname{Im}\kappa_\phi = H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) = H^1_{\mathrm{nr}}(k, A[\phi])$*, if one assumes in addition that*

(i) $\operatorname{char}\mathbb{F} \nmid \deg\phi$*, and*

(ii) $\deg\phi$ *is prime to* $c_A c_B$ *or, more generally,* $\#\Phi_A(\mathbb{F}) = \#(\phi(\Phi_A))(\mathbb{F}) = \#\Phi_B(\mathbb{F})$*.*

Proof.

(a) By Proposition A.4, it suffices to find an S-homomorphism $\mathcal{G} \to \mathcal{A}[\phi]$ inducing an isomorphism on generic fibers, which is provided by [BLR90, §7.1 Cor. 6].

(b) By Proposition 2.5(a), $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \subset \operatorname{Im}\kappa_\phi$, so the conclusion results from (a).

(c) This follows from Proposition A.4, because if $\operatorname{char}\mathbb{F} \nmid \deg\phi$, then $\mathcal{G} = \mathcal{A}[\phi]$ by Corollary B.5.

(d) By Proposition 2.5, $\operatorname{Im}\kappa_\phi = H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$, so the conclusion results from (c). □

Remark 2.8. Proposition 2.7(d) generalizes a well-known lemma of Cassels [Cas65, 4.1], which yields $\operatorname{Im}\kappa_\phi = H^1_{\mathrm{nr}}(k, A[\phi])$ under the additional good reduction assumption (when $c_A = c_B = 1$). If $\dim A = 1$, such generalization has also been observed by Schaefer and Stoll [SS04, 4.5]. From this standpoint, Proposition 2.5(d) extends Cassels' lemma further to all residue characteristics.

3. Assembling $\mathcal{A}[\phi]$ by glueing

A standard descent lemma 3.1 (whose proof is included for completeness) is crucial for glueing $\mathcal{A}[\phi]$ together in the proof of Proposition 3.3; it will also be key in Selmer type descriptions of sets of torsors in §4. Its more technical part (b) involving algebraic spaces is needed to avoid a quasi-affineness hypothesis in Corollary 4.2, which enables us to glue torsors under a Néron model in the proof of Proposition 4.3: even though *a posteriori* such torsors are schemes, we glue them as algebraic spaces (because the description of the essential image in Lemma 3.1(a) is not practical beyond the quasi-affine case). For the proof of Theorem 1.1, however, there is no need to resort to algebraic spaces: Lemma 3.1(a) is sufficient due to affineness of $\mathcal{A}[\phi]$ guaranteed by Corollary B.4.

Lemma 3.1. *Let R be a discrete valuation ring, let $K := \operatorname{Frac} R$ and $K^h := \operatorname{Frac} R^h$, and consider*

$$F\colon X \mapsto (X_K, X_{R^h}, \tau\colon (X_K)_{K^h} \xrightarrow{\sim} (X_{R^h})_{K^h}),$$

a functor from the category of R-algebraic spaces to the category of triples consisting of a K-algebraic space, an R^h-algebraic space, and an isomorphism between their base changes to K^h.

(a) When restricted to the full subcategory of R-schemes, F is an equivalence onto the full subcategory of triples of schemes that admit a quasi-affine open covering (see the proof for the definition). The same conclusion holds with R^h and K^h replaced by $\widehat{R}$ and $\widehat{K} := \operatorname{Frac} \widehat{R}$.

(b) When restricted to the full subcategory of R-algebraic spaces of finite presentation, F is an equivalence onto the full subcategory of triples involving only algebraic spaces of finite presentation.

Proof.

(a) This is proved in [BLR90, §6.2 Prop. D.4 (b)]. A triple of schemes admits a quasi-affine open covering if $X_K = \bigcup_{i\in I} U_i$ and $X_{R^h} = \bigcup_{i\in I} V_i$ for quasi-affine open subschemes U_i, V_i for which τ restricts to isomorphisms $(U_i)_{K^h} \xrightarrow{\sim} (V_i)_{K^h}$.

(b) The method of proof was suggested to me by Brian Conrad. By construction, R^h is a filtered direct limit of local étale R-algebras R' which are discrete valuation rings sharing the residue field and a uniformizer with R. Given a $T = (Y, \mathcal{Y}, \tau\colon Y_{K^h} \xrightarrow{\sim} \mathcal{Y}_{K^h})$ with $Y \to \operatorname{Spec} K$ and $\mathcal{Y} \to \operatorname{Spec} R^h$ of finite presentation, to show that it is in the essential image of the restricted F we first descend $\mathcal{Y}$ to $\mathcal{Y}' \to \operatorname{Spec} R'$ for some R' as above using limit considerations (compare [Ols06, proof of Prop. 2.2]). Similarly, $K^h = \varinjlim K'$ with $K' = \operatorname{Frac} R'$ and τ descends to $\tau'\colon Y_{K'} \xrightarrow{\sim} \mathcal{Y}'_{K'}$ after possibly increasing R'. Transporting the descent datum on $Y_{K'}$ with respect to K'/K along τ', one gets a descent datum on $\mathcal{Y}'_{K'}$, which, as explained in [BLR90, §6.2 proof of Lemma C.2], extends uniquely to a descent datum on $\mathcal{Y}'$ with respect to R'/R. By [LMB00, 1.6.4], the descent datum is effective, giving a quasi-separated R-algebraic space X; by construction, $F(X) \cong T$, and by [SP, Lemma 041V], X is of finite presentation. The full faithfulness of F follows from a similar limit argument using étale descent for morphisms of sheaves on $R_{\text{Ét}}$ and [LMB00, 4.18 (i)]. □

Let S be a Dedekind scheme (cf. A.1), let K be its function field. For $s \in S$, set $K_{S,s} := \operatorname{Frac} \mathcal{O}_{S,s}$. The purpose of this convention (note that $K_{S,s} = K$) is to clarify the statement of Corollary 3.2 by making $\mathcal{O}_{S,s}$ and $K_{S,s}$ notationally analogous to $\mathcal{O}^h_{S,s}$ and $K^h_{S,s}$.

Corollary 3.2. *Let S be a Dedekind scheme, let $s_1, \dots, s_n \in S$ be distinct nongeneric points, and let $V := S - \{s_1, \dots, s_n\}$ be the complementary open subscheme. The functor*

$$F\colon \mathcal{G} \mapsto (\mathcal{G}_V, \mathcal{G}_{\mathcal{O}_{S,s_1}}, \dots, \mathcal{G}_{\mathcal{O}_{S,s_n}}, \alpha_i\colon (\mathcal{G}_V)_{K_{S,s_i}} \xrightarrow{\sim} (\mathcal{G}_{\mathcal{O}_{S,s_i}})_{K_{S,s_i}} \text{ for } 1 \leqslant i \leqslant n) \tag{7}$$

is an equivalence of categories from the category of quasi-affine S-group schemes to the category of tuples consisting of a quasi-affine V-group scheme, a quasi-affine $\mathcal{O}_{S,s_i}$-group scheme for each i, and isomorphisms $\alpha_1, \dots, \alpha_n$ of base changed group schemes as indicated. The same conclusion holds with $\mathcal{O}_{S,s_i}$ and K_{S,s_i} replaced by $\mathcal{O}^h_{S,s_i}$ and K^h_{S,s_i} or by $\widehat{\mathcal{O}}_{S,s_i}$ and $\widehat{K}_{S,s_i}$.

Proof. For henselizations and completions the claim follows from Lemma 3.1, since for localizations it is a special case of fpqc descent. □

Proposition 3.3 (Theorem 1.1(b))**.** *Let L/K be an extension of number fields, let $\phi\colon A \to B$ be a K-isogeny between abelian varieties, set $S := \operatorname{Spec} \mathcal{O}_L$, and let $\mathcal{A}^L[\phi]$ be the kernel of the homomorphism induced by ϕ_L between the Néron models over S. Assume that*

(i) A has good reduction at all places $v \mid \deg \phi$ of K;

(ii) $e_p < p - 1$ for every prime $p \mid \deg \phi$ (see Theorem 1.1 for the definition of e_p).

Then the $\mathcal{O}_L$-group scheme $\mathcal{A}^L[\phi]$ is determined up to isomorphism by the $\operatorname{Gal}(\overline{L}/K)$-module $A[\phi](\overline{L})$.

Proof. By Corollaries B.4 and B.5, $\mathcal{A}^L[\phi]_{\mathcal{O}_w}$ is finite flat for every place $w \mid \deg \phi$ of L, whereas $\mathcal{A}^L[\phi]_{S[\frac{1}{\deg \phi}]}$ is the Néron model of the finite étale $A[\phi]_L$ and hence is determined by $A[\phi]$. If $L = K$, each $\mathcal{A}^K[\phi]_{\mathcal{O}_w}$ is also determined: in the prime power order case this follows either from the Néron property of finite étale $\mathcal{O}_w$-group schemes or [Ray74, Thm. 3.3.3]; in general, $\mathcal{A}^K[\phi]_{\mathcal{O}_w}$ decomposes as a product of finite flat $\mathcal{O}_w$-group schemes of prime power order. For arbitrary L and $w \mid v$, good reduction at v gives $\mathcal{A}^L[\phi]_{\mathcal{O}_w} \cong (\mathcal{A}^K[\phi]_{\mathcal{O}_v})_{\mathcal{O}_w}$ and thus an analogous conclusion. An application of Corollary 3.2 finishes the proof. □

Remark 3.4. Dropping (ii) but keeping (i) (or assuming instead of (i) and (ii) that A has semi-abelian reduction at all $v \mid \deg \phi$ and $L = K$), the proof continues to give the same conclusion as long as one argues that in the situation at hand $\mathcal{A}^K[\phi]_{\mathcal{O}_v}$ is determined for each $v \mid \deg \phi$.

Although (ii) excludes the $2 \mid \deg \phi$ cases, Remark 3.4 can sometimes overcome this:

Example 3.5. Let K be a number field of odd discriminant, and let $A \to \operatorname{Spec} K$ be an elliptic curve with good supersingular reduction at all $v \mid 2$. We show that the conclusion of Proposition 3.3 holds for $2\colon A \to A$, so, in particular, if $\prod_{v \nmid \infty} c_{A,v}$ is odd and K is totally imaginary, $A[2]$ determines $\operatorname{Sel}_2 A$ by Theorem 1.1.

Remark 3.4 reduces to proving that $\mathcal{A}^K[2]_{\mathcal{O}_v}$ is determined by $A[2]_{K_v}$ for each $v \mid 2$. By [Ser72, p. 275, Prop. 12], $A[2]_{K_v^{sh}}$ with $K_v^{sh} := \operatorname{Frac} \mathcal{O}_v^{sh}$ is irreducible and also an $\mathbb{F}_4$-vector space scheme of dimension 1. By [Ray74, 3.3.2 3°], $\mathcal{A}^K[2]_{\mathcal{O}_v^{sh}}$ is its unique finite flat $\mathcal{O}_v^{sh}$-model. By schematic density considerations, the descent datum on $\mathcal{A}^K[2]_{\mathcal{O}_v^{sh}}$ with respect to $\mathcal{O}_v^{sh}/\mathcal{O}_v$ is uniquely determined by its restriction to the generic fiber, which in turn is determined by $A[2]_{K_v}$. We conclude by fpqc descent along $\mathcal{O}_v^{sh}/\mathcal{O}_v$ that $\mathcal{A}^K[2]_{\mathcal{O}_v}$ is determined by $A[2]_{K_v}$.

4. Selmer type descriptions of sets of torsors

The main result of this section is Corollary 4.2 describing certain sets of torsors by local conditions and proving Theorem 1.1(i). It leads to a short reproof of a result of Mazur that gives étale (or fppf) cohomological interpretation of Shafarevich-Tate groups and also forms the basis of our approach to fppf cohomological interpretation of Selmer groups.

Lemma 4.1. *Let R be a discrete valuation ring, let $K := \operatorname{Frac} R$ and $K^h := \operatorname{Frac} R^h$, and let $\mathcal{G}$ be a flat R-group algebraic space of finite presentation. If the horizontal arrows are injective in*

$$\begin{array}{ccc} H^1_{\mathrm{fppf}}(R, \mathcal{G}) & \hookrightarrow & H^1_{\mathrm{fppf}}(K, \mathcal{G}_K) \\ \downarrow & & \downarrow \\ H^1_{\mathrm{fppf}}(R^h, \mathcal{G}_{R^h}) & \hookrightarrow & H^1_{\mathrm{fppf}}(K^h, \mathcal{G}_{K^h}), \end{array}$$

then the square is Cartesian. The same conclusion holds under analogous assumptions with R^h and K^h replaced by $\widehat{R}$ and $\widehat{K}$ if $\mathcal{G}$ is a quasi-affine R-group scheme.

Proof. We first treat the case of R^h and K^h. We need to show that every $\mathcal{G}_K$-torsor $\mathcal{T}_K$ which, when base changed to K^h, extends to a $\mathcal{G}_{R^h}$-torsor $\mathcal{T}_{R^h}$, already extends to a $\mathcal{G}$-torsor $\mathcal{T} \to \operatorname{Spec} R$. By Lemma 3.1(b), $\mathcal{T}_{R^h}$ descends to an fppf R-algebraic space $\mathcal{T}$, and various diagrams defining the $\mathcal{G}$-action descend, too. To argue that $\mathcal{T}$ is a $\mathcal{G}$-torsor, it remains to note that

$$\mathcal{G} \times_R \mathcal{T} \to \mathcal{T} \times_R \mathcal{T}, \quad (g,t) \mapsto (gt,t) \tag{8}$$

is an isomorphism, because it is so over R^h. In the similar proof for $\widehat{R}$ and $\widehat{K}$, to apply Lemma 3.1 one recalls that if $\mathcal{G}$ is a quasi-affine scheme, then so are its torsors [SP, Lemma 0247]. □

Let S be a Dedekind scheme, let K be its function field. As in §3, to clarify analogies in Corollary 4.2, we set $K_{S,s} := \operatorname{Frac} \mathcal{O}_{S,s}$ for a nongeneric $s \in S$.

Corollary 4.2. *Let $\mathcal{G}$ be a flat closed S-subgroup scheme of a Néron model. Then*

$$\begin{array}{ccc} H^1_{\mathrm{fppf}}(S,\mathcal{G}) & \hookrightarrow & H^1_{\mathrm{fppf}}(K,\mathcal{G}_K) \\ \downarrow & & \downarrow \\ \prod_s H^1_{\mathrm{fppf}}(\mathcal{O}_{S,s},\mathcal{G}_{\mathcal{O}_{S,s}}) & \hookrightarrow & \prod_s H^1_{\mathrm{fppf}}(K_{S,s},\mathcal{G}_{K_{S,s}}), \end{array} \tag{9}$$

is Cartesian (the products are indexed by the nongeneric $s \in S$), and similarly with $\mathcal{O}_{S,s}$ and $K_{S,s}$ replaced by $\mathcal{O}^h_{S,s}$ and $K^h_{S,s}$ (resp., $\widehat{\mathcal{O}}_{S,s}$ and $\widehat{K}_{S,s}$ if $\mathcal{G} \to S$ is quasi-affine).

Proof. The indicated injectivity in (9) results from Proposition A.5 and the compatibility of the formation of the Néron model with localization, henselization, and completion [BLR90, §1.2 Prop. 4 and §7.2 Thm. 1 (ii)]. By Lemma 4.1, the diagram

$$\begin{array}{ccc} \prod_s H^1_{\mathrm{fppf}}(\mathcal{O}_{S,s},\mathcal{G}_{\mathcal{O}_{S,s}}) & \hookrightarrow & \prod_s H^1_{\mathrm{fppf}}(K_{S,s},\mathcal{G}_{K_{S,s}}) \\ \downarrow & & \downarrow \\ \prod_s H^1_{\mathrm{fppf}}(\mathcal{O}^h_{S,s},\mathcal{G}_{\mathcal{O}^h_{S,s}}) & \hookrightarrow & \prod_s H^1_{\mathrm{fppf}}(K^h_{S,s},\mathcal{G}_{K^h_{S,s}}) \end{array}$$

is Cartesian, and likewise for $\widehat{\mathcal{O}}_{S,s}$ and $\widehat{K}_{S,s}$. It remains to argue that (9) is Cartesian.

We need to show that every $\mathcal{G}_K$-torsor $\mathcal{T}_K$ which extends to a $\mathcal{G}_{\mathcal{O}_{S,s}}$-torsor $\mathcal{T}_{\mathcal{O}_{S,s}}$ for every nongeneric $s \in S$, already extends to a $\mathcal{G}$-torsor $\mathcal{T}$ (the torsors are schemes, see the proof of Proposition A.5). Since $\mathcal{T}_K \to \operatorname{Spec} K$ inherits finite presentation from $\mathcal{G}_K$, for some open dense $U \subset S$ it spreads out to a $\mathcal{T}_U \to U$ which is faithfully flat, of finite presentation, has a $\mathcal{G}_U$-action, and for which the analogue of (8) over U is bijective. Consequently, $\mathcal{T}_U$ is a $\mathcal{G}_U$-torsor.

To increase U by extending $\mathcal{T}_U$ over some $s \in S - U$, spread out $\mathcal{T}_{\mathcal{O}_{S,s}}$ to a $\mathcal{G}_W$-torsor $\mathcal{T}_W$ over some open neighborhood $W \subset S$ of s. By Proposition A.5, the torsors $\mathcal{T}_U$ and $\mathcal{T}_W$ are isomorphic over $U \cap W$, permitting us to glue them and increase U. Iterating we arrive at the desired $U = S$. □

We now give an alternative proof of the results of [Maz72, Appendix] using Corollary 4.2.

Proposition 4.3. *Suppose that S is a proper smooth curve over a finite field or the spectrum of the ring of integers of a number field. Let $A \to \operatorname{Spec} K$ be an abelian variety, and let $\mathcal{A} \to S$ be its Néron model. Letting the product run over the nongeneric $s \in S$, set*

$$Ш(\mathcal{A}) := \operatorname{Ker}\left(H^1_{\text{ét}}(S, \mathcal{A}) \to \prod_s H^1_{\text{ét}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}_{\widehat{\mathcal{O}}_{S,s}}) \right).$$

(a) Let c_s be the local Tamagawa factor of A at s (cf. 2.4). Then $[H^1_{\text{ét}}(S, \mathcal{A}) : Ш(\mathcal{A})] \leqslant \prod_s c_s$.

(b) $\operatorname{Ker}(H^1(K, A) \to \prod_s H^1(\widehat{K}_{S,s}, A)) = Ш(\mathcal{A}) = \operatorname{Im}(H^1_{\text{ét}}(S, \mathcal{A}^0) \to H^1_{\text{ét}}(S, \mathcal{A}))$.

(c) Let $Ш(A)$ be the Shafarevich-Tate group of $A \to \operatorname{Spec} K$. Then $Ш(A) \subset Ш(\mathcal{A})$ and

$$[Ш(\mathcal{A}) : Ш(A)] \leqslant \prod_{\text{real } v} \#\pi_0(A(K_v)) \leqslant 2^{\#\{\text{real } v\} \cdot \dim A}.$$

In particular, $Ш(A)$ is finite if and only if so is $H^1_{\text{ét}}(S, \mathcal{A})$.

Proof.

(a) Indeed, $\#H^1_{\text{ét}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}_{\widehat{\mathcal{O}}_{S,s}}) = c_s$ by Lemma 2.3.

(b) The first equality follows from Corollary 4.2 with $\mathcal{G} = \mathcal{A}$: working with henselizations suffices thanks to the injectivity of $H^1(K^h_{S,s}, A) \to H^1(\widehat{K}_{S,s}, A)$ [BLR90, §3.6 Cor. 10] and the bijectivity of $H^1_{\text{ét}}(\mathcal{O}^h_{S,s}, \mathcal{A}_{\mathcal{O}^h_{S,s}}) \to H^1_{\text{ét}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}_{\widehat{\mathcal{O}}_{S,s}})$ [Gro68, 11.7]. For the second equality, combine the cohomology sequence of the sequence of Proposition B.2 with Lemma 2.3.

(c) The claim follows from the first equality in (b), as for real v one has $H^1(K_v, A) \cong \pi_0(A(K_v))$ and $\#\pi_0(A(K_v)) \leqslant 2^{\dim A}$ (compare [GH81, 1.1 (3) and 1.3]). □

5. Selmer groups as flat cohomology groups

The main objective of this section is the comparison of $\operatorname{Sel}_\phi A$ and $H^1_{\text{fppf}}(S, \mathcal{A}[\phi])$ in Proposition 5.4.

5.1. Selmer structures. Let K be a global field, and let M be a finite discrete $\operatorname{Gal}(\overline{K}/K)$-module. A *Selmer structure* on M is a choice of a subgroup of $H^1(K_v, M)$ for each place v such that for all v but finitely many, $H^1_{\text{nr}}(K_v, M) \subset H^1(K_v, M)$ is chosen (compare [MR07, Def. 1.2]); its *Selmer group* is the subgroup of $H^1(K, M)$ obtained by imposing the chosen local conditions, i.e., it consists of the cohomology classes whose restrictions to every $H^1(K_v, M)$ lie in the chosen subgroups.

5.2. The setup. If K is a number field, let $S = \operatorname{Spec} \mathcal{O}_K$; if K is a function field, let S be the proper smooth curve with function field K. Let $A \xrightarrow{\phi} B$ be a K-isogeny between abelian varieties, and let $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ be the induced S-homomorphism between their Néron models, which, for $v \nmid \infty$, induces $\phi_v \colon \Phi_{A,v} \to \Phi_{B,v}$ between the groups of connected components of the special fibers of $\mathcal{A}$ and $\mathcal{B}$ at v. Let $c_{A,v} := \#\Phi_{A,v}(\mathbb{F}_v)$ and $c_{B,v} := \#\Phi_{B,v}(\mathbb{F}_v)$ be the local Tamagawa factors.

5.3. Two sets of subgroups (compare 2.1). The first one is $\operatorname{Im}(B(K_v) \xrightarrow{\kappa_{\phi,v}} H^1_{\text{fppf}}(K_v, A[\phi])) \cong B(K_v)/\phi A(K_v)$ for all v; its Selmer group, defined as in 5.1, is the *ϕ-Selmer group* $\operatorname{Sel}_\phi A \subset H^1_{\text{fppf}}(K, A[\phi])$.

The second one is defined only if $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (e.g., if A has semiabelian reduction at all $v \nmid \infty$ with $\operatorname{char} \mathbb{F}_v \mid \deg \phi$, cf. Lemma B.3); it is

$$\begin{aligned} H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \subset H^1_{\mathrm{fppf}}(K_v, A[\phi]), &\qquad \text{if } v \nmid \infty, \text{ and} \\ H^1(K_v, A[\phi]) \subset H^1(K_v, A[\phi]), &\qquad \text{if } v \mid \infty, \end{aligned}$$

and has the corresponding Selmer group $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \subset H^1_{\mathrm{fppf}}(K, A[\phi])$ by Corollary 4.2.

If $\operatorname{char} K \nmid \deg \phi$ and $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat, these are two Selmer structures on $A[\phi]$ by Proposition 2.7(d).

Proposition 5.4. *Suppose that $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (e.g., that A has semiabelian reduction at all $v \nmid \infty$ with $\operatorname{char} \mathbb{F}_v \mid \deg \phi$, cf. Lemma B.3).*

(a) If $\deg \phi$ is prime to $\prod_{v \nmid \infty} c_{B,v}$, then $\operatorname{Sel}_\phi A \subset H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi])$ inside $H^1_{\mathrm{fppf}}(K, A[\phi])$.

(b) If $\deg \phi$ is prime to $\prod_{v \nmid \infty} c_{A,v}$ and either $2 \nmid \deg \phi$ or $A(K_v)$ equipped with its archimedean topology is connected for all real v, then $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \subset \operatorname{Sel}_\phi A$ inside $H^1_{\mathrm{fppf}}(K, A[\phi])$.

(c) If $\deg \phi$ is prime to $\prod_{v \nmid \infty} c_{A,v} c_{B,v}$ and either $2 \nmid \deg \phi$ or $A(K_v)$ equipped with its archimedean topology is connected for all real v, then $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) = \operatorname{Sel}_\phi A$ inside $H^1_{\mathrm{fppf}}(K, A[\phi])$.

Proof. By 5.3, setting $H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) := H^1(K_v, A[\phi])$ for $v \mid \infty$, there are injections

$$\begin{aligned} \frac{\operatorname{Sel}_\phi A}{H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \cap \operatorname{Sel}_\phi A} &\hookrightarrow \prod_{v \nmid \infty} \frac{\operatorname{Im} \kappa_{\phi,v}}{H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \cap \operatorname{Im} \kappa_{\phi,v}}, \\ \frac{H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi])}{H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \cap \operatorname{Sel}_\phi A} &\hookrightarrow \prod_{v} \frac{H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi])}{H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \cap \operatorname{Im} \kappa_{\phi,v}}. \end{aligned} \tag{10}$$

This together with Proposition 2.5(b), (c), and (d) give the claim, since under the assumptions of (b) and (c) the factors of (10) for $v \mid \infty$ vanish: $H^1(K_v, A[\phi]) = 0$ unless $2 \mid \deg \phi$ and v is real, and also, by [GH81, 1.3], $H^1(K_v, A) \cong \pi_0(A(K_v))$. □

Remarks.

5.5. To compare $\operatorname{Sel}_\phi A$ and $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi])$ quantitatively, combine (10) with Proposition 2.5(a).

5.6. As in Proposition 2.7(b) and (d), the assumptions on $c_{A,v}$ and $c_{B,v}$ in Proposition 5.4(a), (b), and (c) (and hence also in Theorem 1.1(ii)) can be weakened to, respectively,

$$\begin{aligned} &\#\Phi_{B,v}(\mathbb{F}_v) = \#(\phi_v(\Phi_{A,v}))(\mathbb{F}_v) \text{ for all } v \nmid \infty, \\ &\#\Phi_{A,v}(\mathbb{F}_v) = \#(\phi_v(\Phi_{A,v}))(\mathbb{F}_v) \text{ for all } v \nmid \infty, \text{ and} \\ &\#\Phi_{A,v}(\mathbb{F}_v) = \#(\phi_v(\Phi_{A,v}))(\mathbb{F}_v) = \#\Phi_{B,v}(\mathbb{F}_v) \text{ for all } v \nmid \infty. \end{aligned}$$

5.7. In practice, it is useful not to restrict Proposition 5.4 to the case when A has semiabelian reduction at all $v \nmid \infty$ with $\operatorname{char} \mathbb{F}_v \mid \deg \phi$. For instance, suppose that K is a number field, A is an elliptic curve that has complex multiplication by an imaginary quadratic field $F \subset K$, and $\phi = \alpha \in \operatorname{End}_K(A) \subset F \subset K$. Then $\mathcal{A}_{\mathcal{O}_K[\frac{1}{\alpha}]} \xrightarrow{\phi} \mathcal{A}_{\mathcal{O}_K[\frac{1}{\alpha}]}$ is flat (even étale) because it induces an automorphism of $\operatorname{Lie} \mathcal{A}_{\mathcal{O}_K[\frac{1}{\alpha}]}$, which is a line bundle on $\operatorname{Spec} \mathcal{O}_K[\frac{1}{\alpha}]$. On the other hand, $\deg \phi$ need not be invertible on $\operatorname{Spec} \mathcal{O}_K[\frac{1}{\alpha}]$. Proposition 5.4 applied to this example leads to a different proof of [Rub99, 6.4], which facilitates the analysis of Selmer groups of elliptic curves with complex multiplication by relating them to class groups.

Appendix A. Torsors under a Néron model

A.1. Dedekind schemes and Néron models. A *Dedekind scheme* S is a connected Noetherian normal scheme of dimension $\leqslant 1$. The connectedness is not necessary, but it simplifies the notation. We let K denote the function field of S. An S-group scheme $\mathcal{X}$ is a *Néron model* (of $\mathcal{X}_K$) if it is separated, of finite type, smooth, and satisfies the *Néron property*: the restriction to the generic fiber map $\mathrm{Hom}_S(\mathcal{Z},\mathcal{X}) \to \mathrm{Hom}_K(\mathcal{Z}_K,\mathcal{X}_K)$ is bijective for every smooth S-scheme $\mathcal{Z}$.

Proposition A.2. *A torsor (for fppf or étale topology) $\mathcal{T} \to S$ under a Néron model $\mathcal{X} \to S$ (by* [Ray70, Thm. XI 3.1 1)]*, $\mathcal{T}$ is a scheme) is separated, smooth, and has the Néron property.*

Proof. Separatedness and smoothness are inherited from $\mathcal{X}$ by descent. In checking the Néron property, one can restrict to quasi-compact $\mathcal{Z}$. Since $\mathcal{T}$ is separated, S-morphisms $\mathcal{Z} \xrightarrow{f} \mathcal{T}$ are in bijection with closed subschemes $\mathfrak{Z} \subset \mathcal{Z} \times_S \mathcal{T}$ mapped isomorphically to $\mathcal{Z}$ by the first projection ($\mathfrak{Z}$ is the graph of f), and similarly for K-morphisms $\mathcal{Z}_K \to \mathcal{T}_K$. Such a $\mathfrak{Z}$ is determined by $\mathfrak{Z}_K$, being its schematic image in $\mathcal{Z} \times_S \mathcal{T}$ [EGA IV_2, 2.8.5]. Bijectivity of $\mathfrak{Z} \mapsto \mathfrak{Z}_K$ for any $\mathcal{Z}$ as above is equivalent to the Néron property of $\mathcal{T}$. To check it, it remains to show that the schematic image $\mathfrak{Z}' \subset \mathcal{Z} \times_S \mathcal{T}$ of any graph $\mathfrak{Z}_K \subset \mathcal{Z}_K \times_K \mathcal{T}_K$ is projected isomorphically to $\mathcal{Z}$, as can be done étale locally on S (in the case of a Noetherian source, formation of schematic image commutes with flat base change [EGA IV_3, 11.10.3 (iv), 11.10.5 (ii)]). But if $S' \to S$ is an étale cover trivializing the smooth $\mathcal{T}$ [EGA IV_4, 17.16.3 (ii)], the claim follows from the Néron property of $\mathcal{T}_{S'} \cong \mathcal{X}_{S'}$. □

Corollary A.3. *For a Néron model $\mathcal{X} \to S$, the pullback map*

$$H^1_{\text{ét}}(S,\mathcal{X}) \xrightarrow{\iota} H^1_{\text{ét}}(K,\mathcal{X}_K) \cong H^1(K,\mathcal{X}_K) \tag{11}$$

is injective.

Proof. Indeed, by Proposition A.2, a torsor under $\mathcal{X}$ is determined by its generic fiber. □

If S is local, it is possible to determine the image of (11):

Proposition A.4. *Suppose that $S = \operatorname{Spec} R$ for a discrete valuation ring R, and let $\mathcal{X} \to S$ be a Néron model. The image of the injection ι from* (11) *is the unramified cohomology subset*

$$I := \operatorname{Ker}(H^1(K,\mathcal{X}_K) \to H^1(K^{sh},\mathcal{X}_{K^{sh}}))$$

where $K^{sh} :=$ $\operatorname{Frac} R^{sh}$; i.e., an $\mathcal{X}_K$-torsor T extends to an $\mathcal{X}$-torsor if and only if $T(K^{sh}) \neq \varnothing$.

Proof. Due to smoothness, every torsor $\mathcal{T}$ under $\mathcal{X}$ trivializes over an étale cover $U \to \operatorname{Spec} R$, and hence over R^{sh}, giving $\operatorname{Im}\iota \subset I$. The inclusion $I \subset \operatorname{Im}\iota$ is a special case of [BLR90, §6.5 Cor. 3]. □

Corollary A.3 can be strengthened slightly:

Proposition A.5. *Let $\mathcal{G}$ be a flat closed S-subgroup scheme of a Néron model $\mathcal{X} \to S$. Then*

$$H^1_{\text{fppf}}(S,\mathcal{G}) \to H^1_{\text{fppf}}(K,\mathcal{G}_K)$$

is injective.

Proof. In terms of descent data with respect to a trivializing fppf $S' \to S$, a $\mathcal{G}$-torsor $\mathcal{T}$ is described by the automorphism of the trivial right $\mathcal{G}_{S'\times_S S'}$-torsor given by left translation by a $g \in \mathcal{G}(S' \times_S S')$. The image of g in $\mathcal{X}(S' \times_S S')$ describes an $\mathcal{X}$-torsor $\mathcal{T}^{\mathcal{X}}$, and the $\mathcal{G}$-equivariant closed immersion $\mathcal{T} \subset \mathcal{T}^{\mathcal{X}}$ of (a priori) algebraic spaces shows that $\mathcal{T}$ is a scheme, since so is $\mathcal{T}^{\mathcal{X}}$ (cf. Proposition A.2).

Let $\mathcal{T}_1, \mathcal{T}_2$ be $\mathcal{G}$-torsors, and take a common trivializing $S' \to S$. It suffices to show that a $\mathcal{G}_K$-torsor isomorphism $\alpha_K \colon (\mathcal{T}_1)_K \xrightarrow{\sim} (\mathcal{T}_2)_K$ extends to a $\mathcal{G}$-torsor isomorphism $\alpha \colon \mathcal{T}_1 \xrightarrow{\sim} \mathcal{T}_2$. In terms of descent data, α_K is described as left multiplication by a certain $h \in \mathcal{G}(S'_K)$, whose image in $\mathcal{X}(S'_K)$ extends α_K to an $\mathcal{X}_K$-torsor isomorphism $\beta_K \colon (\mathcal{T}_1^{\mathcal{X}})_K \xrightarrow{\sim} (\mathcal{T}_2^{\mathcal{X}})_K$. By Proposition A.2, β_K extends to an $\mathcal{X}$-torsor isomorphism $\beta \colon \mathcal{T}_1^{\mathcal{X}} \xrightarrow{\sim} \mathcal{T}_2^{\mathcal{X}}$, which restricts to a desired α due to schematic dominance considerations for $(\mathcal{T}_i)_K \to \mathcal{T}_i$ [EGA IV$_2$, 2.8.5], [EGA I, 9.5.5]. □

Remark A.6. The above results continue to hold for Néron lft models, see [Česl3a, 2.16–2.18, 6.1].

Appendix B. Exact sequences involving Néron models of abelian varieties

We gather several standard facts about Néron models of abelian varieties used in the paper.

B.1. Open subgroups of Néron models of abelian varieties. Let S be a Dedekind scheme (see A.1), let K be its function field; let $A \to \operatorname{Spec} K$ be an abelian variety, let $\mathcal{A} \to S$ be its Néron model. For $s \in S$, let $\Phi_s := \mathcal{A}_s/\mathcal{A}_s^0$ be the étale $k(s)$-group scheme of connected components of $\mathcal{A}_s$. For each nongeneric $s \in S$, choose a subgroup $\Gamma_s \subset \Phi_s$; for all s but finitely many, $\Gamma_s = \Phi_s$. Define the open subgroup $\mathcal{A}^\Gamma \subset \mathcal{A}$ by removing for each s the connected components of $\mathcal{A}_s$ not in Γ_s for each s, and note the homomorphisms $\mathcal{A}^\Gamma \to \bigoplus_s i_{s*}\Gamma_s$ with $i_s \colon \operatorname{Spec} k(s) \to S$. If $\Gamma_s = 0$ for each s, the resulting $\mathcal{A}^0$ consists fiberwise of connected components of identity.

Proposition B.2. *For all choices $\widetilde{\Gamma}_s \subset \Gamma_s \subset \Phi_s$, the sequence*

$$0 \to \mathcal{A}^{\widetilde{\Gamma}} \to \mathcal{A}^\Gamma \xrightarrow{a} \bigoplus_s i_{s*}(\Gamma_s/\widetilde{\Gamma}_s) \to 0$$

is exact in $S_{\text{ét}}$, $S_{\text{Ét}}$, and S_{fppf}.

Proof. Left exactness is clear, whereas to check the remaining surjectivity of a in $S_{\text{Ét}}$ on stalks, it suffices to consider strictly local $(\mathcal{O}, \mathfrak{m})$ centered at a nongeneric $s \in S$ with $\widetilde{\Gamma}_s \neq \Gamma_s$. Let $\mathfrak{a} \subset \mathfrak{m}$ be the ideal generated by the image of $\mathfrak{m}_{S,s}$; in the commutative diagram

$$\begin{array}{ccc} \mathcal{A}^\Gamma(\mathcal{O}) & \xrightarrow{a(\mathcal{O})} & (\Gamma_s/\widetilde{\Gamma}_s)(\mathcal{O}/\mathfrak{a}) \\ \downarrow b & & \wr \downarrow d \\ \mathcal{A}^\Gamma(\mathcal{O}/\mathfrak{m}) & \xrightarrow{c} & (\Gamma_s/\widetilde{\Gamma}_s)(\mathcal{O}/\mathfrak{m}) \end{array}$$

surjectivity of b follows from Hensel-lifting for the smooth $\mathcal{A}^\Gamma_{\mathcal{O}} \to \operatorname{Spec} \mathcal{O}$, surjectivity of c follows from invariance of the component group of the smooth $\mathcal{A}^\Gamma_{\overline{k(s)}} \to \operatorname{Spec} \overline{k(s)}$ upon passage to a separably closed overfield, whereas bijectivity of d is immediate from $(\Gamma_s/\widetilde{\Gamma}_s)_{\mathcal{O}/\mathfrak{a}}$ being finite étale over the Henselian local $(\mathcal{O}/\mathfrak{a}, \mathfrak{m}/\mathfrak{a})$. The desired surjectivity of $a(\mathcal{O})$ follows immediately. □

Let $A \xrightarrow{\phi} B$ be a K-isogeny of abelian varieties, inducing $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ on Néron models over S.

Lemma B.3. *The following are equivalent:*

(a) $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is quasi-finite,

(b) $\mathcal{A}^0 \xrightarrow{\phi} \mathcal{B}^0$ is surjective (as a morphism of schemes),

(c) $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat,

and are implied by

(d) A has semiabelian reduction at all nongeneric $s \in S$ with $\operatorname{char} k(s) \mid \deg \phi$.

Proof. Every homomorphism between algebraic groups over a field factors through a flat surjection onto its closed image [SGA $3_{\text{I new}}$, VI_A 6.7], rendering (a), (b), and (c) equivalent due to the fibral criterion of flatness [EGA IV_3, 11.3.11] and the constancy of the fiber dimension of $\mathcal{A}^0$ (resp., $\mathcal{B}^0$).

For the last claim, consideration of the isogeny $\psi\colon B \to A$ with kernel $\phi(A[\deg \phi])$ reduces to the case when ϕ is multiplication by an integer n, in which case the surjectivity of ϕ_s is clear if the reduction at s is semiabelian and follows by inspection of Lie algebras if $\operatorname{char} k(s) \nmid n$. □

Corollary B.4. *Suppose that $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (e.g., that A has semiabelian reduction at every nongeneric $s \in S$ with* $\operatorname{char} k(s) \mid \deg \phi$*). Then $\mathcal{A}[\phi] \to S$ is separated quasi-finite flat and affine; it is also finite if A has good reduction everywhere. In particular, every torsor under $\mathcal{A}[\phi]$ is representable.*

Proof. By Lemma B.3, $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is separated quasi-finite flat; thus, it is also affine by [SGA $3_{\text{I new}}$, XXV, 4.1] and, in the good reduction case, finite due to properness [EGA IV_3, 8.11.1]. Effectivity of fppf descent for affine schemes gives the torsor claim. □

Corollary B.5. *If* $\operatorname{char} k(s) \nmid \deg \phi$ *for all $s \in S$, then $\mathcal{A}[\phi]$ is the Néron model of $A[\phi]$.*

Proof. Due to Corollary B.4 and the degree hypothesis, the quasi-finite flat $\mathcal{A}[\phi] \to S$ is étale, and hence the conclusion by [BLR90, §7.1 Cor. 6] and [EGA IV_2, 2.8.5]. □

A choice of $\Gamma_s \subset \Phi_s$ yields $\phi_s(\Gamma_s)$, which give rise to the open subgroup $\mathcal{B}^{\phi(\Gamma)} \subset \mathcal{B}$ as in B.1.

Corollary B.6. *Suppose that $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (e.g., that A has semiabelian reduction at all nongeneric $s \in S$ with* $\operatorname{char} k(s) \mid \deg \phi$*). For all choices $\Gamma_s \subset \Phi_s$, the sequence*

$$0 \to \mathcal{A}^\Gamma[\phi] \to \mathcal{A}^\Gamma \xrightarrow{\phi} \mathcal{B}^{\phi(\Gamma)} \to 0$$

is exact in S_{fppf}.

Proof. Indeed, the S-morphism $\mathcal{A}^\Gamma \xrightarrow{\phi} \mathcal{B}^{\phi(\Gamma)}$ is fppf by Lemma B.3. □

References

[AS05] Amod Agashe and William Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484, DOI 10.1090/S0025-5718-04-01644-8. With an appendix by J. Cremona and B. Mazur. MR2085902 (2005g:11119)

[BK90] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400. MR1086888 (92g:11063)

[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)

[Cas65] J. W. S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **217** (1965), 180–199. MR0179169 (31 #3420)

[Čes13a] Kęstutis Česnavičius, *PhD thesis chapter "Selmer groups as flat cohomology groups"* (2013). Available at `http://math.mit.edu/~kestutis`.

[Čes13b] ———, *Selmer groups and class groups*, preprint (2013). `http://arxiv.org/abs/1307.4261`.

[CM00] John E. Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR1758797 (2001g:11083)

[DD08] Tim Dokchitser and Vladimir Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), no. 3, 662–679, DOI 10.1016/j.jnt.2007.02.008. MR2389862 (2009c:11079)

[DD10] ———, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596, DOI 10.4007/annals.2010.172.567. MR2680426 (2011h:11069)

[DG02] Henri Darmon and Peter Green, *Elliptic curves and class fields of real quadratic fields: algorithms and evidence*, Experiment. Math. **11** (2002), no. 1, 37–55. MR1960299 (2004c:11112)

[DP06] Henri Darmon and Robert Pollack, *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel J. Math. **153** (2006), 319–354, DOI 10.1007/BF02771789. MR2254648 (2007k:11077)

[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_3] ———, *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III*, Inst. Hautes Études Sci. Publ. Math. **28** (1966), 255. MR0217086 (36 #178)

[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)

[ELL96] Bas Edixhoven, Qing Liu, and Dino Lorenzini, *The p-part of the group of components of a Néron model*, J. Algebraic Geom. **5** (1996), no. 4, 801–813. MR1486989 (98m:14051)

[Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432 (German). MR718935 (85g:11026a)

[Fis03] Tom Fisher, *Descent calculations for the elliptic curves of conductor 11*, Proc. London Math. Soc. (3) **86** (2003), no. 3, 583–606, DOI 10.1112/S0024611502013977. MR1974391 (2004e:11059)

[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)

[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)

[Kra99] Alain Kraus, *On the equation $x^p + y^q = z^r$: a survey*, Ramanujan J. **3** (1999), no. 3, 315–333, DOI 10.1023/A:1009835521324. MR1714945 (2001f:11046)

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR0086367 (19,174a)

[LMB00] Gérard Laumon and Laurent Moret-Bailly, *Champs algébriques*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 39, Springer-Verlag, Berlin, 2000 (French). MR1771927 (2001f:14006)

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

[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)

[MR13] ———, *Selmer companion curves*, Trans. Amer. Math. Soc., to appear; available at `http://arxiv.org/abs/1203.0620`.

[Ols06] Martin C. Olsson, Hom*-stacks and restriction of scalars*, Duke Math. J. **134** (2006), no. 1, 139–164, DOI 10.1215/S0012-7094-06-13414-2. MR2239345 (2007f:14002)

[Ray70] Michel Raynaud, *Faisceaux amples sur les schémas en groupes et les espaces homogènes*, Lecture Notes in Mathematics, Vol. 119, Springer-Verlag, Berlin, 1970 (French). MR0260758 (41 #5381)

[Ray74] ———, *Schémas en groupes de type $(p, \dots, p)$*, Bull. Soc. Math. France **102** (1974), 241–280 (French). MR0419467 (54 #7488)

[Rub99] Karl Rubin, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 167–234, DOI 10.1007/BFb0093455, (to appear in print). MR1754688 (2001j:11050)

[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)

[SS04] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231 (electronic), DOI 10.1090/S0002-9947-03-03366-X. MR2021618 (2004g:11045)

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (French). MR0387283 (52 #8126)

[SGA $3_{\text{I new}}$] 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

[SP] *The Stacks Project*. `http://stacks.math.columbia.edu`.

[Swa98] Richard G. Swan, *Néron-Popescu desingularization*, Algebra and geometry (Taipei, 1995), Lect. Algebra Geom., vol. 2, Int. Press, Cambridge, MA, 1998, pp. 135–192. MR1697953 (2000h:13006)

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR0206004 (34 #5829)

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/`