J. Ramanujan Math. Soc. **31**, No.1 (2016) 31–61

Selmer groups as flat cohomology groups

Kęstutis Česnavičius

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

Communicated by: R. Sujatha

Received: April 2, 2015

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 known relationship between $\mathrm{Sel}_{p^m} A$ and $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[p^m])$ 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.

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

1. Introduction

Let K be a number field, let A be a g-dimensional abelian variety over K, and let p be a prime number. Fix a separable closure K^s of K. Tate conjectured [Tat66, p. 134] that the *p-adic Tate module* $T_pA := \varprojlim A[p^m](K^s)$ 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.

Consider now the p^∞-Selmer group

$$\mathrm{Sel}_{p^\infty} A \subset H^1(K, A[p^\infty]),$$

which consists of the classes of cocycles whose restrictions lie in

$$A(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_v, A[p^\infty])$$

for every place v of K. Note that $A[p^\infty](K^s) = V_pA/T_pA$ with $V_pA := T_pA \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, so T_pA determines the Galois cohomology groups appearing in the definition of $\mathrm{Sel}_{p^\infty} A$. Since an isogeny of degree prime to p induces an isomorphism on p^∞-Selmer groups, the theorem of Faltings implies that T_pA determines $\mathrm{Sel}_{p^\infty} A$ up to isomorphism. One may expect, however, a more direct and more explicit description of $\mathrm{Sel}_{p^\infty} A$ in terms of T_pA. For this, it suffices to give definitions of the subgroups $A(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p \subset H^1(K_v, A[p^\infty])$ in terms of T_pA.

Bloch and Kato found the desired definitions in [BK90, §3]: if $v \nmid p$, then $A(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p = 0$; if $v \mid p$, then, letting B_{cris} be the crystalline period ring of Fontaine and working with Galois cohomology groups formed using continuous cochains in the sense of [Tat76, §2], they define

$$H^1_f(K_v, V_pA) := \mathrm{Ker}(H^1(K_v, V_pA) \to H^1(K_v, V_pA \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})),$$

and prove that

$$\begin{aligned} A(K_v) \otimes \mathbb{Q}_p/\mathbb{Z}_p &= \mathrm{Im}(H^1_f(K_v, V_pA) \to H^1(K_v, V_pA/T_pA) \\ &= H^1(K_v, A[p^\infty])). \end{aligned}$$

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_pA), in the 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 the following theorem.

Theorem 1.1. *Fix an extension of number fields L/K, fix 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). For $v, w \nmid \infty$, let e_v and p_v be the absolute ramification index and the residue characteristic of v, and let $c_{A,v}$ and $c_{B,v}$ (resp., $c_{A,w}$ and $c_{B,w}$) be the local Tamagawa factors of A and B.*

(a) (i) *(Corollary 4.2, Remark 4.4, and Proposition B.3.) 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).) Assume that A has semiabelian reduction at all $v \mid \deg\phi$. 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.) If A has good reduction at all $v \mid \deg\phi$ and if $e_v < p_v - 1$ for every such v, then the $\mathcal{O}_L$-group scheme $\mathcal{A}^L[\phi]$ is determined up to isomorphism by the* $\mathrm{Gal}(L^s/K)$*-module $A[\phi](L^s)$.*

Thus, if

$$\left(\deg\phi, \prod_{w\nmid\infty} c_{A,w}c_{B,w}\right) = 1,$$

the reduction of A is good at all $v \mid \deg\phi$, and $e_v < p_v - 1$ for every such v (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 $\mathrm{Gal}(L^s/K)$*-module $A[\phi](L^s)$.*

Corollary 1.2. *If A has potential good reduction at every finite place of K 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. By a theorem of McCallum [ELL96, pp. 801–802], every prime q dividing some $c_{A,w}$ satisfies $q \le 2g+1$. Therefore, it suffices to consider those p with $p > \max(2g+1, [K:\mathbb{Q}]+1)$ for which A has good reduction at every place of K above p and to apply Theorem 1.1 to the multiplication by p^m isogeny. □

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) seems not to have appeared in the literature before, and consequently (ii) is more precise than what seems to be available.

In a more restrictive setup, the question of the extent to which $A[\phi]$ determines $\mathrm{Sel}_\phi A$ has also been discussed in [Gre10].

1.4. In the case of elliptic curves, Mazur and Rubin find in [MR15, 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 $Ш(A)$ in Proposition 4.5; such an interpretation is implicit already in the arguments of [Ray65, II.§3] and is proved in [Maz72, Appendix]. Our argument seems more direct: in the proof of loc. cit. the absence of Corollary 4.2 is circumvented with a diagram chase that uses 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 $e_v < p_v - 1$ 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 $A[\phi](L^s)$ as a $\mathrm{Gal}(L^s/K)$-module, rather than as a $\mathrm{Gal}(L^s/L)$-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 $e_v \geq p - 1$ for some place v of K above p.

1.10. In Theorem 1.1, is the subgroup $B(L)/\phi A(L)$ (equivalently, the quotient $Ш(A_L)[\phi]$) also determined by $A[\phi](L^s)$? The answer is 'no'. Indeed, in [CM00, p. 24] Cremona and Mazur report[1] that the

[1] Cremona and Mazur assume 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 $4592G1$.

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) in the case when the base is a global function field, one takes a (connected) proper smooth curve S over a finite field in the references indicated in the statement of Theorem 1.1 (a). Letting K be the function field of S, the analogue of Theorem 1.1 (b) is Corollary B.6: 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 (b),

$$H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \subset H^1(K, A[\phi])$$

is the subset 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 $A[\phi]$ determines the ϕ-Selmer subgroup

$$\mathrm{Sel}_\phi A \subset H^1(K, A[\phi]),$$

which, in fact, consists of the everywhere unramified cohomology classes of $H^1(K, A[\phi])$.

Example 1.12. We illustrate 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)); 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. Since $E[5] \cong \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$, the proof of Proposition 3.3 supplies an isomorphism

$$\mathcal{E}^K[5] \simeq \underline{\mathbb{Z}/5\mathbb{Z}}_{\mathcal{O}_K} \oplus \mu_5.$$

Therefore, the cohomology sequence of $0 \to \mu_5 \to \mathbb{G}_m \xrightarrow{5} \mathbb{G}_m \to 0$ together with the isomorphism $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathbb{Z}/5\mathbb{Z}) \simeq \mathrm{Cl}_K[5]$ gives

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

where Cl_K is the ideal class group, r_1^K and r_2^K are the numbers of real and complex places, and

$$h_5^K := \dim_{\mathbb{F}_5} \mathrm{Cl}_K[5], \quad u_5^K := \dim_{\mathbb{F}_5} \mu_5(\mathcal{O}_K).$$

The component groups of Néron models of elliptic curves with split multiplicative reduction are cyclic, so (1) and Remark 5.5 give the bounds

$$\begin{aligned}&2h_5^K + r_1^K + r_2^K - 1 + u_5^K - \#\{v \mid 11\} \\ &\quad \le \dim_{\mathbb{F}_5} \mathrm{Sel}_5 E_K \le 2h_5^K + r_1^K + r_2^K - 1 + u_5^K + \#\{v \mid 11\}. \end{aligned} \tag{2}$$

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

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

because the 5-parity conjecture is known for E_K by the results of [DD08]. When K ranges over the quadratic extensions of $\mathbb{Q}$, due to (2), the conjectured unboundedness of the 5-ranks h_5^K of the ideal class groups is equivalent to the unboundedness of $\dim_{\mathbb{F}_5} \mathrm{Sel}_5 E_K$. This equivalence is an instance of a general result [Čes15, 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 other authors, see, for instance, [Sch96].

It is curious to draw some concrete conclusions from (2) and (3).

(a) As is also well known, $\mathrm{rk}\, E(\mathbb{Q}) = 0$.
(b) If K is imaginary quadratic with $h_5^K = 0$ and 11 is inert or ramified in K, then $\mathrm{rk}\, E(K) = 0$.
(c) If K is imaginary quadratic with $h_5^K = 0$ and 11 splits in K, then either $\mathrm{rk}\, E(K) = 1$, or $\mathrm{rk}\, E(K) = 0$ and $\mathrm{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] = 1$, because, due to the Cassels–Tate pairing,

$$\mathrm{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] \equiv \dim_{\mathbb{F}_5} Ш(E_K)[5] \bmod 2.$$

Mazur in [Maz79, Thm. on p. 237] and Gross in [Gro82, Prop. 3] proved that $\mathrm{rk}\, E(K) = 1$.

(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 $\mathrm{rk}\, E(F) = 2$, or $Ш(E_F)[5^\infty]$ is infinite (one again uses the Cassels–Tate pairing).
(e) If K is real quadratic with $h_5^K = 0$ and 11 is inert or ramified in K, then either $\mathrm{rk}\, E(K) = 1$, or $\mathrm{rk}\, E(K) = 0$ and $\mathrm{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] = 1$. In the latter case $Ш(E_K)[p^\infty]$ is infinite for every prime p, because the p-parity conjecture is known for $E_{\bar{K}}$ for every p by [DD10, 1.4] (applied to E and its quadratic twist by K). Gross proved in [Gro82, Prop. 2] that if 11 is inert, then $\mathrm{rk}\, E(K) = 1$.
(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 $\mathrm{rk}\, E(K) = 1$, or $\mathrm{rk}\, E(K) = 0$ and $\mathrm{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] = 1$.

How can one construct the predicted rational points? In (c) and the inert case of (e), [Gro82] explains that Heegner point constructions account for the predicted rank growth.

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 results on fpqc descent, we apply them to prove Theorem 1.1 (b) and to reprove 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 $\mathrm{Sel}_\phi A$ and $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi])$ and to 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 PhD thesis of the author; we invite a reader interested in this to consult [Česl4a], which also discusses several tangentially related questions.

1.14 Conventions

When needed, a choice of a separable closure K^s of a field K will be made implicitly, as will be a choice of an embedding $K^s \hookrightarrow L^s$ 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}, $S_{\mathrm{Ét}}$, and $S_{\mathrm{ét}}$; the objects of S_{fppf} and $S_{\mathrm{Ét}}$ are all S-schemes, while those of $S_{\mathrm{ét}}$ are all schemes étale over S. The cohomology groups computed in $S_{\mathrm{ét}}$ and S_{fppf} are denoted by $H^i_{\mathrm{ét}}(S, -)$ and $H^i_{\mathrm{fppf}}(S, -)$; Galois cohomology merits no subscript: $H^i(K, -)$. An fppf torsor is a torsor under the group in question for the fppf topology. An algebraic group over a field K is a smooth K-group scheme of finite type.

2. Images of local Kummer homomorphisms as flat cohomology groups

Let $S = \operatorname{Spec} o$ for a Henselian discrete valuation ring o with a finite residue field $\mathbb{F}$, let $k = \operatorname{Frac} o$, 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 subgroup schemes of $\mathcal{A}$ and $\mathcal{B}$ discussed in §B.

2.1 The three subgroups

The first subgroup of $H^1_{\mathrm{fppf}}(k, A[\phi])$ is

$$B(k)/\phi A(k) \cong \operatorname{Im}(B(k) \xrightarrow{\kappa_\phi} H^1_{\mathrm{fppf}}(k, A[\phi])) \subset H^1_{\mathrm{fppf}}(k, A[\phi]).$$

The second subgroup is

$$H^1_{\mathrm{fppf}}(o, \mathcal{A}[\phi]) \cong \operatorname{Im}(H^1_{\mathrm{fppf}}(o, \mathcal{A}[\phi]) \xrightarrow{a} H^1_{\mathrm{fppf}}(k, A[\phi])) \subset H^1_{\mathrm{fppf}}(k, A[\phi]),$$

where the isomorphism results from the injectivity of a supplied by Proposition B.3, [GMB13, Prop. 3.1], and Proposition A.5 (even though $\mathcal{A}[\phi]$ may fail to be flat, loc. cit. proves that its category of fppf torsors is equivalent to the category of fppf torsors of the o-flat schematic image of $A[\phi]$ in $\mathcal{A}$, so Proposition A.5 nevertheless applies).

The third 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 $k^{sh} := \operatorname{Frac} o^{sh}$. The unramified subgroup is of most interest in the case when $A[\phi]$ is étale (for instance, when $\operatorname{char} k \nmid \deg \phi$); beyond this étale case, the unramified subgroup is often too small in comparison to the first two subgroups.

While $\operatorname{Im} \kappa_\phi$ is used to define the ϕ-Selmer group, $H^1_{\mathrm{fppf}}(o, \mathcal{A}[\phi])$ and $H^1_{\mathrm{nr}}(k, A[\phi])$ are easier to study because they depend only on $\mathcal{A}[\phi]$.

We investigate $\operatorname{Im}\kappa_\phi$ by detailing its relations with $H^1_{\text{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$ and $H^1_{\text{nr}}(k, A[\phi])$ in Propositions 2.5 and 2.7.

Lemma 2.2. *For a commutative connected algebraic group $G \to \operatorname{Spec}\mathbb{F}$, one has*

$$H^j(\mathbb{F}, G) = 0 \quad \text{for } j \geq 1.$$

Proof. In the case $j = 1$, the claimed vanishing is a well-known result of Lang [Lan56, Thm. 2]. In the case $j > 1$, the vanishing follows from the facts that $\mathbb{F}$ has cohomological dimension 1 and that $G(\mathbb{F}^s)$ is a torsion group (the latter results from the finiteness of $\mathbb{F}$). □

Lemma 2.3. *For an $\mathbb{F}$-subgroup $\Gamma \subset \Phi_A$, pullback induces isomorphisms*

$$H^j_{\text{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) \cong H^j(\mathbb{F}, \Gamma) \quad \text{for } j \geq 1.$$

In particular, $\#H^1_{\text{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) = \#\Gamma(\mathbb{F})$ and $H^j_{\text{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) = 0$ for $j \geq 2$.

Proof. By [Gro68, 11.7 2°)], pullback induces isomorphisms

$$H^j_{\text{fppf}}(\mathfrak{o}, \mathcal{A}^\Gamma) \cong H^j(\mathbb{F}, \mathcal{A}^\Gamma_{\mathbb{F}}) \quad \text{for } j \geq 1,$$

so it remains to apply Lemma 2.2 to the terms $H^j(\mathbb{F}, \mathcal{A}^0_{\mathbb{F}})$ in the long exact cohomology sequence of

$$0 \to \mathcal{A}^0_{\mathbb{F}} \to \mathcal{A}^\Gamma_{\mathbb{F}} \to \Gamma \to 0.$$ □

2.4 The local Tamagawa factors

These are

$$c_A := \#\Phi_A(\mathbb{F}) \quad \text{and} \quad c_B := \#\Phi_B(\mathbb{F}).$$

The sequences

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

are exact, so

$$\frac{\#\Phi_A(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \leq \#\Phi_A[\phi](\mathbb{F}) \quad \text{and} \quad \frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \leq \#\left(\frac{\Phi_B}{\phi(\Phi_A)}\right)(\mathbb{F}). \tag{4}$$

We now compare the subgroups $\operatorname{Im}\kappa_\phi$ and $H^1_{\text{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$ of $H^1_{\text{fppf}}(k, A[\phi])$ discussed in §2.

Proposition 2.5. *Suppose that* $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ *is flat (e.g., that* $\operatorname{char} \mathbb{F} \nmid \deg \phi$ *or that* A *has semiabelian reduction, see Lemma B.4).*

(a) *Then*

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

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

(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* $c_A c_B$*, 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.7 gives

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

where the injectivity of the vertical arrows follows from the Néron property, the 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 claimed equality follows.

On the other hand,

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

Moreover, Lemma 2.3 and the étale cohomology sequence of the short exact sequence

$$0 \to \mathcal{B}^{\phi(\Phi_A)} \to \mathcal{B} \to i_*(\Phi_B/\phi(\Phi_A)) \to 0$$

from Proposition B.2 give the exact sequence (see [Gro68, 11.7 1°)] for the identifications between different cohomology theories)

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

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

where we have used the exactness of i_* for the étale topology to obtain the last term. By combining (5) and (6), we obtain the remaining equality

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

$$= \frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})}.$$

(b) Let $\psi : B \to A$ be the isogeny with $\ker\psi = \phi(A[\deg\phi])$, so

$$\psi \circ \phi = \deg\phi, \quad \text{and thus also} \quad \phi \circ \psi = \deg\phi.$$

If $(\deg\phi, \#\Phi_B(\mathbb{F})) = 1$, then

$$\Phi_B(\mathbb{F}) = (\deg\phi)(\Phi_B(\mathbb{F})) \subset ((\deg\phi)(\Phi_B))(\mathbb{F}) \subset (\phi(\Phi_A))(\mathbb{F}) \subset \Phi_B(\mathbb{F}),$$

which gives the desired equality $\Phi_B(\mathbb{F}) = (\phi(\Phi_A))(\mathbb{F})$.

(c) We have the inclusion

$$\Phi_A[\phi] \subset \Phi_A[\deg\phi],$$

so if $(\deg\phi, \#\Phi_A(\mathbb{F})) = 1$, then $\Phi_A[\phi](\mathbb{F}) = 0$. The resulting injection

$$\Phi_A(\mathbb{F}) \hookrightarrow \phi(\Phi_A)(\mathbb{F})$$

is then surjective because $\#H^1(\mathbb{F}, \Phi_A[\phi]) = \#\Phi_A[\phi](\mathbb{F})$ due to the finiteness of $\mathbb{F}$.

(d) The claim follows by combining (b) and (c). □

(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

$$X_K = \bigcup_{i \in I} U_i \quad \text{and} \quad X_{R^h} = \bigcup_{i \in I} V_i$$

for quasi-affine open subschemes $U_i \subset X_K$ and $V_i \subset X_{R^h}$ 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

$$T = (Y, \mathcal{Y}, \tau : Y_{K^h} \xrightarrow{\sim} \mathcal{Y}_{K^h})$$

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 use limit considerations (for instance, as in [Ols06, proof of Prop. 2.2]) to descend $\mathcal{Y}$ to a $\mathcal{Y}' \to \operatorname{Spec} R'$ for some R' as above.

Similarly, $K^h = \varinjlim K'$ with $K' := \operatorname{Frac} R'$, so τ descends to a $\tau' : Y_{K'} \xrightarrow{\sim} \mathcal{Y}'_{K'}$ after possibly enlarging R'. We transport the K'/K-descent datum on $Y_{K'}$ along τ' to get a descent datum on $\mathcal{Y}'_{K'}$, which, as explained in [BLR90, §6.2, proof of Lemma C.2], extends uniquely to an R'/R-descent datum on $\mathcal{Y}'$. By [LMB00, 1.6.4], this descent datum is effective, and we get a quasi-separated R-algebraic space X; by construction, $F(X) \cong T$, and by [SP, 041V], X is of finite presentation.

The full faithfulness of F follows from a similar limit argument that uses étale descent for morphisms of sheaves on $R_{\text{Ét}}$ together with [LMB00, 4.18 (i)]. □

Let S be a connected Dedekind scheme (see §A for the definition), 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 $s_1, \ldots, s_n \in S$ be distinct nongeneric points, and let $V := S - \{s_1, \ldots, s_n\}$ be the complementary open subscheme. The functor*

$$F : \mathcal{G} \mapsto (\mathcal{G}_V, \mathcal{G}_{\mathcal{O}_{S,s_1}}, \ldots, \mathcal{G}_{\mathcal{O}_{S,s_n}}, \alpha_i : (\mathcal{G}_V)_{K_{S,s_i}} \xrightarrow{\sim} (\mathcal{G}_{\mathcal{O}_{S,s_i}})_{K_{S,s_i}} \text{ for } 1 \le i \le n)$$

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 $\alpha_1, \ldots, \alpha_n$ 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 localizations, the claim is a special case of fpqc descent. Thus, for henselizations and completions the claim follows from Lemma 3.1. □

Proposition 3.3 (Theorem 1.1 (b)). *Let L/K be an extension of number fields, and let $\phi\colon A \to B$ be a K-isogeny between abelian varieties. Assume that*

(i) *A has good reduction at all the places $v \mid \deg \phi$ of K;*
(ii) *For every place $v \mid \deg \phi$ of K, its absolute ramification index e_v satisfies*

$$e_v < p_v - 1,$$

where p_v is the residue characteristic of v.

Then the $\mathcal{O}_L$-group scheme $\mathcal{A}^L[\phi]$, defined as the kernel of the homomorphism induced by ϕ_L between the Néron models over $\mathcal{O}_L$, is determined up to isomorphism by the $\mathrm{Gal}(L^s/K)$*-module $A[\phi](L^s)$.*

Proof. By Corollary B.6, $\mathcal{A}^L[\phi]_{S\left[\frac{1}{\deg \phi}\right]}$ is the Néron model of the finite étale $A[\phi]_L$, and hence is determined by $A[\phi]$. By Corollary 3.2, it therefore suffices to prove that each $\mathcal{A}^L[\phi]_{\mathcal{O}_w}$ for a place $w \mid \deg \phi$ of L is also determined by $A[\phi]$. Moreover, if such a w lies above the place v of K, then the good reduction assumption implies that

$$\mathcal{A}^L[\phi]_{\mathcal{O}_w} \cong (\mathcal{A}^K[\phi]_{\mathcal{O}_v})_{\mathcal{O}_w},$$

so it suffices to prove that already $\mathcal{A}^K[\phi]_{\mathcal{O}_v}$ is determined by $A[\phi]$.

Let p be the residue characteristic of v. By Corollary B.5, $\mathcal{A}^K[\phi]_{\mathcal{O}_v}$ is finite flat, so it uniquely decomposes as a direct product of commutative finite flat $\mathcal{O}_v$-group schemes of prime power order. The prime-to-p factor is finite étale, so it is the Néron model of the prime-to-p factor of $A[\phi]$, and hence is determined by $A[\phi]$. The p-primary factor is also determined thanks to Raynaud's result [Ray74, Thm. 3.3.3] on uniqueness of finite flat models over Henselian discrete valuation rings of mixed characteristic and low absolute ramification index. □

Remark 3.4. Dropping (ii) but keeping (i), 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 by $A[\phi]$ for each $v \mid \deg\phi$.

Although the assumption (ii) excludes the cases when $2 \mid \deg\phi$, Remark 3.4 can sometimes be used to overcome this, as the following example illustrates.

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 reduction at all $v \mid 2$. Assume that $A[2](K_v) \neq (\mathbb{Z}/2\mathbb{Z})^2$ for every $v \mid 2$, so that $A[2]_{K_v}$ has at most one K_v-subgroup of order 2 for every such v. 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, then $A[2]$ determines the 2-Selmer group $\operatorname{Sel}_2 A$ by Theorem 1.1.

Remark 3.4 reduces us to proving that $A[2]_{K_v}$ determines $\mathcal{A}^K[2]_{\mathcal{O}_v}$ for each $v \mid 2$. We analyze the ordinary and the supersingular reduction cases separately. This is permissible because these cases are distinguishable: in the former, $A[2]_{K_v}$ is reducible, whereas in the latter it is not.

In the supersingular case, 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 $A[2]_{K_v}$. Fpqc descent along $\mathcal{O}_v^{sh}/\mathcal{O}_v$ then implies that $A[2]_{K_v}$ determines $\mathcal{A}^K[2]_{\mathcal{O}_v}$.

In the ordinary case, the connected-étale decomposition shows that $\mathcal{A}^K[2]_{\mathcal{O}_v}$ is an extension of $\underline{\mathbb{Z}/2\mathbb{Z}}_{\mathcal{O}_v}$ by $(\mu_2)_{\mathcal{O}_v}$. Therefore, since we assumed that $A[2]_{K_v}$ determines its subgroup $(\mu_2)_{K_v}$, it also determines $\mathcal{A}^K[2]_{\mathcal{O}_v}$ due to the injectivity of

$$\operatorname{Ext}^1_{\mathcal{O}_v}(\mathbb{Z}/2\mathbb{Z}, \mu_2) \cong H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mu_2) \to H^1_{\mathrm{fppf}}(K_v, \mu_2) \cong \operatorname{Ext}^1_{K_v}(\mathbb{Z}/2\mathbb{Z}, \mu_2)$$

(extensions in the category of fppf sheaves of $\mathbb{Z}/2\mathbb{Z}$-modules).

4. Selmer type descriptions of sets of torsors

The main result of this section is Corollary 4.2, which describes certain sets of torsors by local conditions and proves Theorem 1.1 (i). It leads to a short reproof of the 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, set $K := \operatorname{Frac} R$ 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. If $\mathcal{G}$ is a quasi-affine R-group scheme, then the same conclusion holds under analogous assumptions with R^h and K^h replaced by $\widehat{R}$ and $\widehat{K}$.

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 a flat and of finite presentation R-algebraic space $\mathcal{T}$, and various diagrams defining the $\mathcal{G}$-action descend, too. To conclude that $\mathcal{T}$ is a $\mathcal{G}$-torsor, it remains to note that

$$\mathcal{G} \times_R \mathcal{T} \to \mathcal{T} \times_R \mathcal{T}, \quad (g, t) \mapsto (gt, t) \tag{7}$$

is an isomorphism, as may be checked 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, see [SP, 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 an S-group scheme that is the Néron model of its generic fiber. Then the square*

$$\begin{array}{ccc} H^1_{\mathrm{fppf}}(S, \mathcal{G}) & \hookrightarrow & H^1_{\mathrm{fppf}}(K, \mathcal{G}_K) \\ \downarrow & & \downarrow \\ \prod_s H^1_{\mathrm{fppf}}(\mathcal{O}_{S,s}, \mathcal{G}_{\mathcal{O}_{S,s}}) & \hookrightarrow & \prod_s H^1_{\mathrm{fppf}}(K_{S,s}, \mathcal{G}_{K_{S,s}}), \end{array} \tag{8}$$

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 (8) results from Proposition A.5 and from the compatibility of the formation of the Néron model with localization, henselization, and completion (see [BLR90, §1.2, Prop. 4 and §7.2,

Thm. 1 (ii)] for these compatibilities). 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 (8) 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 $\mathcal{T}$ (these 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 (7) over U is bijective. Consequently, $\mathcal{T}_U$ is a $\mathcal{G}_U$-torsor.

To increase U by extending $\mathcal{T}_U$ over some $s \in S - U$, we 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 $U \cap W$, which permits us to glue them and to increase U. By iterating this process we arrive at the desired $U = S$. □

Remarks.

4.3. The closed subgroup assumption on the flat S-group scheme $\mathcal{G}$ is used only to deduce the indicated injectivity in (8). If one assumes instead that $\mathcal{G}$ is commutative finite flat, then the injectivity follows from the valuative criterion of properness; consequently, Corollary 4.2 also holds for such $\mathcal{G}$. For further extensions of Corollary 4.2, see [Čes14a, 7.2–7.4].

4.4. The flatness of $\mathcal{G}$ is actually not needed for Corollary 4.2 to hold. To justify this, let $\widetilde{\mathcal{G}}$ be the schematic image of $\mathcal{G}_K$ in $\mathcal{G}$, so that $\widetilde{\mathcal{G}}$ is S-flat and a closed S-subgroup scheme of the same Néron model. The formation of $\widetilde{\mathcal{G}}$ commutes with flat base change, in particular, with base change to $\mathcal{O}_{S,s}$, to $\mathcal{O}^h_{S,s}$, or to $\widehat{\mathcal{O}}_{S,s}$. By [Čes14a, 2.11] (or already by [GMB13, Prop. 3.1] if $\mathcal{G}$ is affine), the change of group maps

$$H^1_{\mathrm{fppf}}(S, \widetilde{\mathcal{G}}) \to H^1_{\mathrm{fppf}}(S, \mathcal{G}) \quad \text{and}$$

$$H^1_{\mathrm{fppf}}(\mathcal{O}_{S,s}, \widetilde{\mathcal{G}}_{\mathcal{O}_{S,s}}) \to H^1_{\mathrm{fppf}}(\mathcal{O}_{S,s}, \mathcal{G}_{\mathcal{O}_{S,s}})$$

are bijective, and likewise with $\mathcal{O}_{S,s}$ replaced by $\mathcal{O}^h_{S,s}$ or by $\widehat{\mathcal{O}}_{S,s}$. This reduces the claim of Corollary 4.2 for $\mathcal{G}$ to its claim for $\widetilde{\mathcal{G}}$, which is S-flat.

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

Proposition 4.5. *Suppose that S is a proper smooth curve over a finite field or that S is 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) *If c_s denotes the local Tamagawa factor of A at s (see §2 for the definition), then*

$$[H^1_{\text{ét}}(S, \mathcal{A}) : Ш(\mathcal{A})] \leq \prod_s c_s.$$

(b) *One has*

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

(c) *One has*

$$Ш(\mathcal{A}) = \operatorname{Im}(H^1_{\text{ét}}(S, \mathcal{A}^0) \to H^1_{\text{ét}}(S, \mathcal{A})).$$

(d) *Let $Ш(A)$ be the Shafarevich–Tate group of A. Then*

$$Ш(A) \subset Ш(\mathcal{A})$$

and

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

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

Proof.

(a) By Lemma 2.3 (see [Gro68, 11.7 1°)] for the identification between the étale and the fppf cohomology groups),

$$\#H^1_{\text{ét}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}_{\widehat{\mathcal{O}}_{S,s}}) = c_s,$$

so the claim results from the definition of $Ш(\mathcal{A})$.

(b) By [BLR90, §3.6, Cor. 10], if an $A_{K^h_{S,s}}$-torsor has a $\widehat{K}_{S,s}$-point, then it already has a $K^h_{S,s}$-point, i.e., the pullback map

$$H^1(K^h_{S,s}, A) \to H^1(\widehat{K}_{S,s}, A)$$

is injective, and hence, by Proposition A.5, so is the pullback map

$$H^1_{\text{ét}}(\mathcal{O}^h_{S,s}, \mathcal{A}_{\mathcal{O}^h_{S,s}}) \to H^1_{\text{ét}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}_{\widehat{\mathcal{O}}_{S,s}}).$$

Therefore, it suffices to prove that

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

This equality follows from the fact that the square

$$\begin{array}{ccc} H^1_{\text{ét}}(S, \mathcal{A}) & \hookrightarrow & H^1(K, A) \\ \downarrow & & \downarrow \\ \prod_s H^1_{\text{ét}}(\mathcal{O}^h_{S,s}, \mathcal{A}_{\mathcal{O}^h_{S,s}}) & \hookrightarrow & \prod_s H^1(K^h_{S,s}, A) \end{array}$$

is Cartesian by Corollary 4.2.

(c) In the notation of Proposition B.2, we have the exact sequence

$$0 \to \mathcal{A}^0 \to \mathcal{A} \to \bigoplus_s i_{s*}\Phi_s \to 0.$$

A segment of its associated long exact cohomology sequence reads

$$H^1_{\text{ét}}(S, \mathcal{A}^0) \to H^1_{\text{ét}}(S, \mathcal{A}) \to \bigoplus_s H^1_{\text{ét}}(k(s), \Phi_s),$$

so it remains to recall that the pullback maps

$$H^1_{\text{ét}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}_{\widehat{\mathcal{O}}_{S,s}}) \to H^1_{\text{ét}}(k(s), \Phi_s)$$

are isomorphisms by Lemma 2.3.

(d) The inclusion follows from (b). So does the bound on the index because for real v one has

$$H^1(K_v, A) \cong \pi_0(A(K_v)) \quad \text{and} \quad \#\pi_0(A(K_v)) \leq 2^{\dim A},$$

for instance, by [GH81, 1.1 (3) and 1.3]. The last claim also uses (a). □

5. Selmer groups as flat cohomology groups

The main goal of this section is the comparison of $\text{Sel}_\phi A$ 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 $\text{Gal}(K^s/K)$-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, $H^1_{\text{ur}}(K_v, M) \subset H^1(K_v, M)$ is chosen (compare with the definition [MR07, 1.2] in the number field case). The *Selmer group* of a Selmer structure 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, we let $S := \operatorname{Spec} \mathcal{O}_K$; if K is a function field, we let S be a connected proper smooth curve over a finite field with function field K. We let

$$A \xrightarrow{\phi} B \quad \text{and} \quad \mathcal{A} \xrightarrow{\phi} \mathcal{B}$$

be a K-isogeny between abelian varieties and the induced S-homomorphism between their Néron models. For a place $v \nmid \infty$, we get the induced map

$$\phi_v : \Phi_{A,v} \to \Phi_{B,v}$$

between the groups of connected components of the special fibers of $\mathcal{A}$ and $\mathcal{B}$ at v. We let

$$c_{A,v} := \#\Phi_{A,v}(\mathbb{F}_v) \quad \text{and} \quad c_{B,v} := \#\Phi_{B,v}(\mathbb{F}_v)$$

be the local Tamagawa factors.

5.3 Two sets of subgroups (compare with §2)

The first set of subgroups is

$$\operatorname{Im}(B(K_v) \xrightarrow{\kappa_{\phi,v}} H^1_{\text{fppf}}(K_v, A[\phi])) \cong B(K_v)/\phi A(K_v) \subset H^1_{\text{fppf}}(K_v, A[\phi]) \quad \text{for all } v.$$

Its Selmer group, defined as in §5, is the *ϕ-Selmer group*

$$\text{Sel}_\phi A \subset H^1_{\text{fppf}}(K, A[\phi]).$$

The second set of subgroups is

$$H^1_{\text{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \subset H^1_{\text{fppf}}(K_v, A[\phi]), \quad \text{if } v \nmid \infty, \quad \text{and}$$
$$H^1(K_v, A[\phi]) \subset H^1(K_v, A[\phi]), \quad \text{if } v \mid \infty;$$

the indicated injectivity for $v \nmid \infty$ has been discussed in §2 (even in the case when $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ fails to be flat!). By Corollary 4.2 and Remark 4.4 (together with Proposition B.3), its Selmer group is

$$H^1_{\text{fppf}}(S, \mathcal{A}[\phi]) \subset H^1_{\text{fppf}}(K, A[\phi]).$$

If $A[\phi]$ is étale, then $\mathcal{A}[\phi]$ is also étale over a sufficiently small nonempty open subset of S, so, by Proposition 2.7 (d), the above sets of subgroups are two Selmer structures on $A[\phi]$.

In general, without assuming that $A[\phi]$ is étale, the two sets of subgroups form two sets of Selmer conditions in the sense of [Čes14b, §3.1]; in particular, by [Čes14b, 3.2],

$$H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \quad \text{is always finite,}$$

even in the case when $A[\phi]$ is not étale and $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is not flat. (The notion of *Selmer conditions* generalizes the notion of a Selmer structure to the case when M of §5 is an arbitrary commutative finite K-group scheme, i.e., not necessarily étale.)

Proposition 5.4. *Suppose that $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (by Lemma B.4, this assumption holds if, for example, A has semiabelian reduction at all $v \nmid \infty$ for which* $\operatorname{char} \mathbb{F}_v \mid \deg \phi$*).*

(a) *If $\deg \phi$ is prime to $\prod_{v \nmid \infty} c_{B,v}$, then*

$$\mathrm{Sel}_\phi A \subset H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi])$$

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*

$$H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \subset \mathrm{Sel}_\phi A$$

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*

$$H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) = \mathrm{Sel}_\phi A$$

inside $H^1_{\mathrm{fppf}}(K, A[\phi])$.

Proof. By §5, setting $H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) := H^1(K_v, A[\phi])$ for $v \mid \infty$, we have injections

$$\begin{aligned} \frac{\mathrm{Sel}_\phi A}{H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \cap \mathrm{Sel}_\phi A} &\hookrightarrow \prod_{v \nmid \infty} \frac{\operatorname{Im} \kappa_{\phi,v}}{H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \cap \operatorname{Im} \kappa_{\phi,v}}, \\ \frac{H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi])}{H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \cap \mathrm{Sel}_\phi A} &\hookrightarrow \prod_{v} \frac{H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi])}{H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \cap \operatorname{Im} \kappa_{\phi,v}}. \end{aligned} \tag{9}$$

This together with Proposition 2.5 (b), (c), and (d) gives the claim because under the assumptions of (b) and (c) the factors of (9) 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 $\mathrm{Sel}_\phi A$ and $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi])$ quantitatively, one may combine (9) with Proposition 2.5 (a).

5.6. As in Proposition 2.7 (c) 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 to not restrict Proposition 5.4 to the case when A has semiabelian reduction at all $v \nmid \infty$ with $\mathrm{char}\,\mathbb{F}_v \mid \deg\phi$. 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 $\phi = \alpha \in \mathrm{End}_K(A) \subset F \subset K$. Then

$$\mathcal{A}_{\mathcal{O}_K\left[\frac{1}{\alpha}\right]} \xrightarrow{\phi} \mathcal{A}_{\mathcal{O}_K\left[\frac{1}{\alpha}\right]}$$

is flat (even étale) because it induces an automorphism of $\mathrm{Lie}\,\mathcal{A}_{\mathcal{O}_K\left[\frac{1}{\alpha}\right]}$, which is a line bundle on $\mathrm{Spec}\,\mathcal{O}_K\left[\frac{1}{\alpha}\right]$. On the other hand, $\deg\phi$ need not be invertible on $\mathrm{Spec}\,\mathcal{O}_K\left[\frac{1}{\alpha}\right]$. 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.

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 ≤ 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. *Every torsor (for the fppf or the étale topology) $\mathcal{T} \to S$ under a Néron model $\mathcal{X} \to S$ is a scheme that is separated, smooth, and has the Néron property.*

Proof. Representability of $\mathcal{T}$ by a scheme follows from [Ray70, Thm. XI 3.1 1)]. Its 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

$$\mathcal{Z} \subset \mathcal{Z} \times_S \mathcal{T}$$

that are mapped isomorphically to $\mathcal{Z}$ by the first projection ($\mathcal{Z}$ is the graph of f), and similarly for K-morphisms $\mathcal{Z}_K \to \mathcal{T}_K$. Such a $\mathcal{Z}$ is determined by $\mathcal{Z}_K$, being its schematic image in $\mathcal{Z} \times_S \mathcal{T}$ by [EGA IV_2, 2.8.5]. Bijectivity of the assignment $\mathcal{Z} \mapsto \mathcal{Z}_K$ for any $\mathcal{Z}$ as above is equivalent to the sought Néron property of $\mathcal{T}$.

To check this bijectivity, it remains to show that the schematic image $\mathcal{Z}' \subset \mathcal{Z} \times_S \mathcal{T}$ of any graph $\mathcal{Z}_K \subset \mathcal{Z}_K \times_K \mathcal{T}_K$ is projected isomorphically to $\mathcal{Z}$, as can be done étale locally on S (in the case of a Noetherian source, the formation of the schematic image commutes with flat base change by [EGA IV_3, 11.10.3 (iv), 11.10.5 (ii)]). By [EGA IV_4, 17.16.3 (ii)], there is an étale cover $S' \to S$ trivializing the torsor $\mathcal{T}$, so 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*

$$H^1_{\text{ét}}(S, \mathcal{X}) \xrightarrow{\iota} H^1_{\text{ét}}(K, \mathcal{X}_K) \cong H^1(K, \mathcal{X}_K) \tag{10}$$

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 (10):

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* (10) *is the unramified cohomology subset*

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

where $K^{sh} := \operatorname{Frac} R^{sh}$. In other words, an $\mathcal{X}_K$-torsor T extends to an $\mathcal{X}$-torsor if and only if $T(K^{sh}) \neq \emptyset$.

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 as follows.

Proposition A.5. *For an S-flat closed S-subgroup scheme $\mathcal{G}$ of a Néron model $\mathcal{X} \to S$, the pullback map*

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

is injective.

Proof. In terms of descent data with respect to a trivializing $S' \to S$ that is faithfully flat and locally of finite presentation, 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 $\mathcal{T}^{\mathcal{X}}$ by Proposition A.2.

Let $\mathcal{T}_1, \mathcal{T}_2$ be $\mathcal{G}$-torsors, and choose a common trivializing $S' \to S$. It suffices to show that a $\mathcal{G}_K$-torsor isomorphism $\alpha_K : (\mathcal{T}_1)_K \xrightarrow{\sim} (\mathcal{T}_2)_K$ extends to a $\mathcal{G}$-torsor isomorphism $\alpha : \mathcal{T}_1 \xrightarrow{\sim} \mathcal{T}_2$. 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 $\beta_K : (\mathcal{T}_1^{\mathcal{X}})_K \xrightarrow{\sim} (\mathcal{T}_2^{\mathcal{X}})_K$. By Proposition A.2, β_K extends to an $\mathcal{X}$-torsor isomorphism $\beta : \mathcal{T}_1^{\mathcal{X}} \xrightarrow{\sim} \mathcal{T}_2^{\mathcal{X}}$, which restricts to a desired α due to schematic dominance considerations for $(\mathcal{T}_i)_K \to \mathcal{T}_i$ (one uses [EGA IV$_2$, 2.8.5] and [EGA I, 9.5.5]). □

Remark A.6. The above results continue to hold for Néron lft models and without the flatness assumption in Proposition A.5, see [Čes14a, 2.19–2.21, 6.1] (an S-group scheme $\mathcal{X}$ is a *Néron lft model* (of $\mathcal{X}_K$) if it is separated, smooth, and satisfies the Néron property recalled in §A; a Néron lft model is not necessarily of finite type over S but is always locally of finite type due to smoothness).

B. Exact sequences involving Néron models of abelian varieties

In this appendix, we gather several standard facts about Néron models of abelian varieties used in the main body of the paper.

B.1 Open subgroups of Néron models of abelian varieties

Let S be a Dedekind scheme (defined in §A), and let K be its function field. Let

$$A \to \operatorname{Spec} K \quad \text{and} \quad \mathcal{A} \to S$$

be an abelian variety and 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 $k(s)$-subgroup $\Gamma_s \subset \Phi_s$. Then for all s but finitely many, $\Gamma_s = \Phi_s$, and we define the open subgroup

$$\mathcal{A}^{\Gamma} \subset \mathcal{A}$$

by removing for every s the connected components of $\mathcal{A}_s$ not in Γ_s. Letting $i_s\colon \operatorname{Spec} k(s) \to S$ denote the inclusion of the nongeneric point s, we have the homomorphism

$$\mathcal{A}^{\Gamma} \to \bigoplus_s i_{s*}\Gamma_s.$$

If $\Gamma_s = 0$ for every s, then the resulting $\mathcal{A}^0$ is the fiberwise identity component of $\mathcal{A}$.

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

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

the surjectivity of b follows from Hensel-lifting for the smooth $\mathcal{A}^{\Gamma}_{\mathcal{O}} \to \operatorname{Spec} \mathcal{O}$ (see [EGA IV_4, 18.5.17]), the surjectivity of c follows from the invariance of the component group of the smooth $\mathcal{A}^{\Gamma}_{k(s)^s} \to \operatorname{Spec} k(s)^s$ upon passage to a separably closed overfield, whereas the 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. □

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

Proposition B.3. *The kernel $\mathcal{A}[\phi] \to S$ is affine; every fppf torsor under $\mathcal{A}[\phi]$ is representable.*

Proof. Affineness of $\mathcal{A}[\phi]$ is a special case of [Ana73, 2.3.2]. Effectivity of fppf descent for affine schemes gives the torsor claim. □

Lemma B.4. *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 the nongeneric $s \in S$ for which* $\operatorname{char} k(s) \mid \deg \phi$.

Proof. Due to the fibral criterion of flatness [EGA IV_3, 11.3.11] for (c), the conditions (a)–(c) can be checked fiberwise on S. We will show that they are equivalent for the fiber over an $s \in S$.

Since $\mathcal{A}$ and $\mathcal{B}$ are faithfully flat and locally of finite type over S, [BLR90, §2.4, Prop. 4] supplies the equalities

$$\dim \mathcal{A}_s = \dim A \quad \text{and} \quad \dim \mathcal{B}_s = \dim B,$$

and hence also $\dim \mathcal{A}_s = \dim \mathcal{B}_s$. Moreover, by [SGA $3_{\text{I new}}$, VI_A, 6.7], every homomorphism between algebraic groups over a field factors through a flat surjection onto its closed image, so ϕ_s is surjective on identity components if and only if it is quasi-finite, i.e., (a)$\Leftrightarrow$(b). Furthermore, if $\phi_s(\mathcal{A}_s^0) = \mathcal{B}_s^0$, then ϕ_s is flat on identity components, i.e., (b)$\Rightarrow$(c). Conversely, if ϕ_s is flat, then, in addition to being closed, $\phi_s(\mathcal{A}_s^0)$ is also open, and hence equals $\mathcal{B}_s^0$, i.e., (c)$\Rightarrow$(b).

For the last claim, the consideration of the isogeny $\psi : B \to A$ with the kernel $\phi(A[\deg \phi])$ reduces to the case when ϕ is multiplication by an integer n. For such ϕ, the surjectivity of ϕ_s on the identity components 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.5. *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 quasi-finite, flat, and affine; it is also finite if A has good reduction at every nongeneric point of S.*

Proof. By Lemma B.4, $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is quasi-finite and flat; in the good reduction case, it is finite due to its properness, see [EGA IV_3, 8.11.1]. Affineness results from Proposition B.3. □

Corollary B.6. *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.5 and the degree hypothesis, the quasi-finite flat $\mathcal{A}[\phi] \to S$ is étale. On the other hand, by [BLR90, §7.1, Cor. 6], the Néron

model of $A[\phi]$ may be obtained as the group smoothening of the schematic image of $A[\phi]$ in $\mathcal{A}$. By [EGA IV_2, 2.8.5], this schematic image is $\mathcal{A}[\phi]$, so, since $\mathcal{A}[\phi] \to S$ is étale, no smoothening is needed. □

A choice of $k(s)$-subgroups $\Gamma_s \subset \Phi_s$ gives rise to their images $\phi_s(\Gamma_s)$. These images, in turn, give rise to the open subgroup $\mathcal{B}^{\phi(\Gamma)} \subset \mathcal{B}$ as in §B.

Corollary B.7. *Suppose that $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (e.g., that A has semiabelian reduction at all the nongeneric $s \in S$ with $\operatorname{char} k(s) \mid \deg \phi$). Then for every choice of $k(s)$-subgroups $\Gamma_s \subset \Phi_s$, 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. The S-morphism $\mathcal{A}^{\Gamma} \xrightarrow{\phi} \mathcal{B}^{\phi(\Gamma)}$ is faithfully flat and locally of finite presentation by Lemma B.4, whereas the exactness at the other terms is immediate from the definitions. □

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 the referee for helpful suggestions that improved the manuscript. I thank Rebecca Bellovin, Henri Darmon, Tim Dokchitser, Jessica Fintzen, Jean Gillibert, Benedict Gross, Mark Kisin, Chao Li, 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.

References

[Ana73] Sivaramakrishna Anantharaman, Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension 1, Sur les groupes algébriques, *Soc. Math.*, France, Paris, (1973) 5–79. *Bull. Soc. Math.*, France, Mém., 33 (French). MR0335524 (49 #305).

[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) 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).

[Čes14a] Kęstutis Česnavičius, Selmer groups as flat cohomology groups, ProQuest LLC, Ann Arbor, MI, 2014. Thesis (Ph.D.)–Massachusetts Institute of Technology. MR3279019.

[Čes14b] Kęstutis Česnavičius, p-Selmer growth in extensions of degree p, preprint (2014). Available at http: //arxiv.org/abs/1408.1151.

[Čes15] Kęstutis Česnavičius, Selmer groups and class groups, *Compos. Math.*, **151** (2015) no. 3, 416–434, DOI 10.1112/S0010437X14007441. MR3320567.

[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] Tim Dokchitser and Vladimir Dokchitser, 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).

[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] A. Grothendieck and J. Dieudonné, 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] A. Grothendieck and J. Dieudonné, 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] A. Grothendieck and J. Dieudonné, 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).

[GMB13] Philippe Gille and Laurent Moret-Bailly, Actions algébriques de groupes arithmétiques, Torsors, étale homotopy and applications to rational points, London Math. Soc. Lecture Note Ser., vol. 405, Cambridge Univ. Press, Cambridge, (2013) 231–249 (French, with English and French summaries). MR3077171.

[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).

[Gre10] Ralph Greenberg, Selmer groups and congruences, Proceedings of the International Congress of Mathematicians. Volume II, Hindustan Book Agency, New Delhi, (2010) 231–248. MR2827793 (2012j:11119).

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

[Gro82] Benedict H. Gross, Heegner points on $X_0(11)$, Seminar on Number Theory, 1981/1982, Univ. Bordeaux I, Talence, (1982), pp. Exp. No. 34, 5. MR695347 (84f:14019).

[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).

[Maz79] B. Mazur, On the arithmetic of special values of L functions, *Invent. Math.*, **55** (1979), no. 3, 207–240, DOI 10.1007/BF01406841. MR553997 (82e:14033).

[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).

[MR15] Barry Mazur and Karl Rubin, Selmer companion curves, *Trans. Amer. Math. Soc.*, **367** (2015) no. 1, 401–421, DOI 10.1090/S0002-9947-2014-06114-X. MR3271266.

[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).

[Ray65] Michel Raynaud, Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, (1995), pp. Exp. No. 286, 129–147 (French). MR1608794.

[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] Michel Raynaud, 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), 167–234, DOI 10.1007/BFb0093455. 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 $3_{\text{I new}}$] 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.

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

[Tat76] John Tate, Relations between K_2 and Galois cohomology, *Invent. Math.*, **36** (1976) 257–274. MR0429837 (55 #2847).