Selmer groups as flat cohomology groups

by

Kęstutis Česnavičius

Bachelor of Science, Jacobs University, 2010

Submitted to the Department of Mathematics
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2014

Author ..... Signature redacted

Department of Mathematics
May 2, 2014

Certified by ..... Signature redacted .....

Bjorn Poonen
Claude Shannon Professor of Mathematics
Thesis Supervisor

Accepted by ..... Signature redacted .....

Alexei Borodin
Chairman, Department Committee on Graduate Students

Selmer groups as flat cohomology groups

by

Kęstutis Česnavičius

Submitted to the Department of Mathematics
on May 2, 2014, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

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 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. Standard glueing techniques developed in the course of the proofs have applications to finite flat group schemes over global bases, permitting us to transfer many of the known local results to the global setting.

Thesis Supervisor: Bjorn Poonen
Title: Claude Shannon Professor of Mathematics

Acknowledgments

I thank Bjorn Poonen for his guidance and support, many helpful discussions and suggestions, and for feedback on various drafts. I thank Brian Conrad for helpful comments on an early draft of this manuscript. I thank Rebecca Bellovin, Henri Darmon, Johan de Jong, 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 thesis. 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. I thank MIT for excellent conditions for my PhD work.

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* $T_pA := \varprojlim A[p^m](\overline{K})$ determines A up to an isogeny of degree prime to p, and Faltings proved this in [Fal83, §1 b)][1]. 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[2] prime to p.

Consider now the p^∞-Selmer group $\operatorname{Sel}_{p^\infty} A \subset H^1(K, A[p^\infty])$, 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 $A[p^\infty](\overline{K}) = V_pA/T_pA$ 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 $\operatorname{Sel}_{p^\infty} A$. Since an isogeny of degree prime to p induces an isomorphism on p^∞-Selmer groups, the theorem of Faltings implies that T_pA determines $\operatorname{Sel}_{p^\infty} A$ up to isomorphism. One may expect, however, a more direct and more explicit description of $\operatorname{Sel}_{p^\infty} A$ 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]: 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

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

and prove that

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

Considering the p-Selmer group $\operatorname{Sel}_p A$ and $A[p]$ instead of $\operatorname{Sel}_{p^\infty} A$ and $A[p^\infty]$ (equivalently, $\operatorname{Sel}_{p^\infty} A$ and T_pA), in light of the Frey–Mazur conjecture, one may expect a direct description of $\operatorname{Sel}_p A$ 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 $c_{B,w}$) be the corresponding local Tamagawa factors for $v, w \nmid \infty$ (cf. §8.7), let e_v be the absolute ramification index if $v \nmid \infty$, set $e_p := \max_{v|p} e_v$, and see §1.17 for other notation.*

(a) (i) (Corollary 7.3.) *The pullback map*

$$H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi]) \to H^1(K, A[\phi]) \tag{1.1.1}$$

is an isomorphism onto the preimage of $\prod_{v\nmid\infty} H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \subset \prod_{v\nmid\infty} H^1(K_v, A[\phi])$.

---

[1] By [Tat66, Lemmas 1 and 3], the quoted result of Faltings implies the bijectivity of

$$\mathbb{Z}_p \otimes \operatorname{Hom}(A, B) \to \operatorname{Hom}_{\operatorname{Gal}(\overline{K}/K)}(T_pA, T_pB)$$

for all abelian varieties A, B over K. In particular, if $\iota\colon T_pA \xrightarrow{\sim} T_pB$, there is an isogeny $\phi\colon A \to B$ whose reduction mod p agrees with ι mod p, hence $p \nmid \deg \phi$.

[2] The degree condition can be added, since up to isomorphism only finitely many abelian varieties are K-isogenous to A [Zar85, Thm. 1].

(ii) (Proposition 9.8 (d).) *If the reduction of A at all $v \mid \deg\phi$ is semiabelian, $\deg\phi$ 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 $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi]) = \mathrm{Sel}_\phi A$ inside $H^1(K, A[\phi])$.*

(b) (Proposition 5.9.) *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 works even if $\mathcal{A}[\phi]$ is not $\mathcal{O}_K$-flat thanks to Proposition 2.11; 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 here.

1.5. The Selmer type description of a flat cohomology group as in (i) continues to hold with other $\mathcal{O}_K$-group schemes $\mathcal{G}$ as coefficients. For instance, $\mathcal{G}$ can be a finite flat group scheme or a Néron model; see Theorem 7.2 for a general result of this type. Choosing $\mathcal{G} = \mathcal{A}$ to be the Néron model of A leads to a reproof of the étale cohomological interpretation of the Shafarevich–Tate group $Ш(A)$ in Proposition 7.5; such interpretation is implicit already in the arguments of [Ray65, II.§3] and is proved in [Maz72, Appendix]. Our argument is more direct: in the proof of loc. cit. the absence of Theorem 7.2 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), see Proposition 9.8 (a).

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 9.10.

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. To determine an explicit finite set of rational primes Σ depending on K, L, A, and B such that $\mathrm{Sel}_\phi A_L$ is determined by the $\mathrm{Gal}(\overline{L}/K)$-module $A[\phi](\overline{L})$ whenever $\deg\phi$ is coprime to the elements of Σ, let Σ consist of all primes below a place of bad reduction for A, all primes

dividing a local Tamagawa factor of A_L or B_L, the prime 2, and all odd primes p ramified in K for which $e_p \geqslant p-1$ (since $e_p \leqslant [K:\mathbb{Q}]$, one can include all the primes $p \leqslant [K:\mathbb{Q}]+1$ for simplicity). Taking $L = K$ and $A = B$ yields the set Σ promised in the abstract.

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[3] 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?

The analogue of Theorem 1.1 in the function field case is

Theorem 1.11. *Let S be a (connected) proper smooth curve over a finite field, let K be its function field, let $\phi\colon A \to B$ be a K-isogeny between abelian varieties, and let $\mathcal{A}[\phi] \to S$ be the kernel of the induced homomorphism between the Néron models over S. For a closed point $s \in S$, let $\widehat{\mathcal{O}}_{S,s}$ be the completion of the local ring at s, let $\widehat{K}_{S,s}$ be the fraction field of $\widehat{\mathcal{O}}_{S,s}$, and let $c_{A,s}$ and $c_{B,s}$ be the corresponding local Tamagawa factors (cf. §8.7).*

(a) *(i)* (Corollary 7.3.) *The pullback map $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \to H^1_{\mathrm{fppf}}(K, A[\phi])$ is an isomorphism onto the preimage of $\prod_s H^1_{\mathrm{fppf}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}[\phi]) \subset \prod_s H^1_{\mathrm{fppf}}(\widehat{K}_{S,s}, A[\phi])$ where the products are indexed by the closed $s \in S$.*

(ii) (Proposition 8.9 (e).) *If $\operatorname{char} K \nmid \deg \phi$, then $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) \subset H^1(K, A[\phi])$ consists of the everywhere unramified cohomology classes.*

(iii) (Proposition 9.8 (d).) *If the reduction of A is semiabelian everywhere and $\deg \phi$ is prime to $\prod_s c_{A,s}c_{B,s}$, then $H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) = \operatorname{Sel}_\phi A$ inside $H^1_{\mathrm{fppf}}(K, A[\phi])$.*

(b) (Corollary 3.9.) *If $\operatorname{char} K \nmid \deg \phi$, then the S-group scheme $\mathcal{A}[\phi]$ is determined up to isomorphism by $A[\phi]$; actually, $\mathcal{A}[\phi] \to S$ is just the Néron model of $A[\phi] \to \operatorname{Spec} K$.*

Thus, if $(\deg \phi, \operatorname{char} K \prod_s c_{A,s}c_{B,s}) = 1$, then the ϕ-Selmer subgroup $\operatorname{Sel}_\phi A \subset H^1(K, A[\phi])$ is determined by $A[\phi]$ and in fact consists of the everywhere unramified cohomology classes of $H^1(K, A[\phi])$.

Remarks.

1.12. The prevalence of the unramified condition in the final conclusion of Theorem 1.11 is due to the following extension of a well-known lemma of Cassels [Cas65, 4.1] proved in Proposition 8.9 (f): for a nonarchimedean place v of a global field K and a K-isogeny $\phi\colon A \to B$, if $(\deg \phi, c_{A,v}c_{B,v} \operatorname{char} \mathbb{F}_v) = 1$, then the condition at v defining the ϕ-Selmer group is the unramified cohomology subgroup $H^1_{\mathrm{nr}}(K_v, A[\phi]) \subset H^1(K_v, A[\phi])$; Cassels assumes in addition that v is a place of good reduction (when $c_{A,v} = c_{B,v} = 1$). If A is an elliptic curve and K is a number field, this generalization has also been observed by Schaefer and Stoll [SS04, 4.5].

[3] 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 $4592G1$.

If $(\deg\phi, c_{A,v}c_{B,v}\operatorname{char}\mathbb{F}_v) = 1$, then $H^1_{\mathrm{nr}}(K_v, A[\phi]) = H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi])$ inside $H^1(K_v, A[\phi])$ by Proposition 8.9 (f). Thus, a further extension of Cassels' lemma to all residue characteristics is Proposition 8.8 (e): if $(\deg\phi, c_{A,v}c_{B,v}) = 1$ and A has semiabelian reduction at v in case $\operatorname{char}\mathbb{F}_v \mid \deg\phi$, then the condition at v defining $\mathrm{Sel}_\phi A$ is $H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{A}[\phi]) \subset H^1(K_v, A[\phi])$. This conclusion has also been observed by Mazur and Rubin [MR13, Prop. 5.8] in the case $\dim A = 1$ and $\phi = p^m$.

1.13. Injectivity of the pullback maps in Theorems 1.1 (i) and 1.11 (i) are special cases of Theorem 6.1: such injectivity continues to hold with a closed subgroup of a Néron model as coefficients for the cohomology groups (or pointed sets in the noncommutative case).

1.14. Models of finite group schemes over global bases. The glueing techniques developed in §4 with the purpose of proving Theorem 1.1 (b) apply to the study of finite flat group schemes over global bases. More precisely, let K be a number field, let $\mathcal{O}_K$ be its ring of integers, and fix a rational prime p. An *$\mathcal{O}_K$-model* (of its generic fiber) is a commutative quasi-finite flat separated $\mathcal{O}_K$-group scheme $\mathcal{G}$ killed by a power of p such that $\mathcal{G}_{\mathcal{O}_K[\frac{1}{p}]} \to \operatorname{Spec}\mathcal{O}_K[\frac{1}{p}]$ is a Néron model (cf. §2.2 for Néron models) and $\mathcal{G}_{\mathcal{O}_v} \to \operatorname{Spec}\mathcal{O}_v$ is finite flat for each $v \mid p$; see §5.1 for the definition in the general setting. A commutative finite flat $\mathcal{O}_K$-group scheme $\mathcal{G}$ of p-power order is precisely a finite $\mathcal{O}_K$-model, which in turn is nothing else than an $\mathcal{O}_K$-model $\mathcal{G}$ for which the $\mathrm{Gal}(\overline{K}/K)$-module $\mathcal{G}(\overline{K})$ is unramified away from p (cf. §5.1). Studying general $\mathcal{O}_K$-models amounts to allowing ramification away from p.

Our main results concerning $\mathcal{O}_K$-models $\mathcal{G}$ are Corollary 4.4 together with Theorem 5.4, which say that $\mathcal{G}$ is determined by $\mathcal{G}_K$ together with $(\mathcal{G}_{\mathcal{O}_v})_{v|p}$; moreover, a compatible tuple $(\mathcal{G}_K, (\mathcal{G}_{\mathcal{O}_v})_{v|p})$ glues to an $\mathcal{O}_K$-model $\mathcal{G}$. Effectively, the study of $\mathcal{O}_K$-models of a fixed generic fiber G amounts to the study of finite flat $\mathcal{O}_v$-models of G_{K_v} for $v \mid p$, permitting us to transfer many of the known local results to the global setting. For instance, we obtain uniqueness of $\mathcal{O}_K$-models of a fixed generic fiber G for K of low ramification at places above p (Proposition 5.7 (c)), show that the product over all $v \mid p$ of Kisin's moduli of finite flat group schemes varieties continues to parametrize models over global bases (Proposition 5.17), and show that a p-divisible group over K extends (uniquely) to $\mathcal{O}_K$ if and only if all its layers have finite $\mathcal{O}_K$-models (§5.19 and Proposition 5.21); see §5 for other results of this sort. The description of $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{G}) \subset H^1(K, \mathcal{G}_K)$ by local conditions as in Remark 1.5 holds for every $\mathcal{O}_K$-model $\mathcal{G}$; see §§9.2–9.5 for a discussion of this.

Example 1.15. 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 (1.15.2) 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 $E[5] \cong \mathbb{Z}/5\mathbb{Z} \oplus \mu_5$ (compare [Gre99, pp. 120–121]), by Proposition 5.9 and its proof, $\mathcal{E}^K[5] \cong \underline{\mathbb{Z}/5\mathbb{Z}}_{\mathcal{O}_K} \oplus \mu_5$. Thus, exploiting the exact sequence $0 \to \mu_5 \to \mathbb{G}_m \xrightarrow{5} \mathbb{G}_m \to 0$ together with Example 9.3,

$$\dim_{\mathbb{F}_5} H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{E}^K[5]) = 2\dim_{\mathbb{F}_5}\mathrm{Cl}_K[5] + \dim_{\mathbb{F}_5}\mathcal{O}_K^\times/\mathcal{O}_K^{\times 5} = 2h_5^K + r_1^K + r_2^K - 1 + u_5^K, \quad (1.15.1)$$

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

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

Since component groups of Néron models of elliptic curves with split multiplicative reduction are cyclic, (1.15.1) and Proposition 9.8 (a) give

$$2h_5^K+r_1^K+r_2^K-1+u_5^K-\#\{v \mid 11\} \leqslant \dim_{\mathbb{F}_5} \mathrm{Sel}_5 E_K \leqslant 2h_5^K+r_1^K+r_2^K-1+u_5^K+\#\{v \mid 11\}. \quad (1.15.2)$$

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

$$\dim_{\mathbb{F}_5} \mathrm{Sel}_5 E_K \equiv r_1^K + r_2^K - 1 + u_5^K + \#\{v \mid 11\} \bmod 2, \quad (1.15.3)$$

because the 5-parity conjecture is known for E_K [DD08]. When K ranges over the quadratic extensions of $\mathbb{Q}$, due to (1.15.2), the conjectured unboundedness of 5-ranks h_5^K of ideal class groups (which a priori has nothing to do with E) is equivalent to the unboundedness of $\dim_{\mathbb{F}_5} \mathrm{Sel}_5 E_K$; in particular, it is implied by the folklore[4] conjecture that the ranks of quadratic twists of a fixed elliptic curve over $\mathbb{Q}$ (in our case, E) are unbounded.

It is curious to observe some concrete conclusions that (1.15.2) and (1.15.3) offer (note that precise rank expectations are possible due to (1.15.2)—the sole growth follows already from parity considerations):

(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 $\mathrm{cork}_{\mathbb{Z}_5} Ш(E_K)[5^\infty] = 1$. 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.

(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_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. 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.

1.16. The contents of the paper. We begin by collecting several general results concerning Néron models and their torsors in §2 and proceed in §3 by proving various short exact sequences involving open subgroups of Néron models of abelian varieties. These give appropriate analogues of Kummer sequences when working with Néron models. We devote §4 to a standard fpqc descent result enabling us to glue schemes over global bases from their local base changes, which leads in §5 to global analogues of familiar local results concerning finite flat group schemes. Injectivity of (1.1.1) and related maps is argued in §6, which also discusses embeddings of finite flat group schemes into Néron models. In §7, exploiting §4, we study the question of H^1_{fppf} with appropriate coefficients over Dedekind bases being described by local conditions. We restrict to local bases in §8 to compare 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 $H^1(K_v, A[\phi])$

[4]Which does not mean "widely believed".

under appropriate hypotheses. The local analysis is used in §9 to compare the ϕ-Selmer group and $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathcal{A}[\phi])$. For cross-reference purposes, several known results from algebraic geometry are gathered in Appendix A.

1.17. 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 a local ring R, its henselization, strict henselization, and completion are R^h, R^{sh}, and $\widehat{R}$. 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. We call a morphism *fppf* if it is flat, surjective, and locally of finite presentation. An *fppf torsor* is a torsor for the fppf topology (as opposed to a torsor that itself is fppf over the base). The fppf, big étale, and étale sites of S are S_{fppf}, $S_{\text{É}\mathrm{t}}$, and $S_{\text{ét}}$; the objects of S_{fppf} and $S_{\text{É}\mathrm{t}}$ 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 $H^i_{\text{ét}}(S, \mathcal{G})$ and $H^i_{\mathrm{fppf}}(S, \mathcal{G})$; usually $\mathcal{G}$ will be represented by a commutative S-group algebraic space locally of finite presentation. Galois cohomology groups are denoted by H^i. For $\mathcal{G}$ as above, the δ-functorial identification $H^i_{\text{ét}}(K, \mathcal{G}) \cong H^i(K, \mathcal{G}(\overline{K}))$ is made implicitly (similarly in the noncommutative case for $i \leqslant 1$, cf. §A.4). So is $H^i_{\text{ét}}(S, \mathcal{G}) \cong H^i_{\mathrm{fppf}}(S, \mathcal{G})$ for smooth $\mathcal{G}$ as in Proposition A.2 (see Proposition A.6 for the noncommutative case); it is δ-functorial as well. In the presence of $f\colon S' \to S$, it is understood that $H^i_{\mathrm{fppf}}(S, \mathcal{G}) \to H^i_{\mathrm{fppf}}(S', f^*\mathcal{G})$ is the δ-functorial pullback. 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. For an integer n and a scheme S, the open subscheme on which n is invertible is $S[\frac{1}{n}]$.

Since [SP, Definition 025Y] is our definition of an algebraic space (see also [SP, Lemma 076M]), when citing other references we need to make sure that the implicit quasi-separatedness assumption is met. Better behavior under descent is our reason for resorting to algebraic spaces. The reader only interested in Theorems 1.1 and 1.11 can stick to schemes: due to affineness of $\mathcal{A}[\phi]$, its torsors are schemes (see Proposition 3.3).

2. Néron models

Our analysis of Selmer groups will be based on a study of Néron models of abelian varieties. This section is devoted to various concepts and results in the theory of Néron models. We set notation in §§2.1–2.2, record ways to recognize and construct Néron models in §§2.3–2.17, and investigate their torsors in §§2.18–2.21.

2.1. Dedekind schemes. These are the connected Noetherian normal schemes S of dimension $\leqslant 1$. Connectedness (due to which $S \neq \varnothing$) is not necessary but simplifies the notation (though not the proofs). A nonempty open $U \subset S$ as well as $\operatorname{Spec} \mathcal{O}_{S,s}$, $\operatorname{Spec} \mathcal{O}^h_{S,s}$, and $\operatorname{Spec} \widehat{\mathcal{O}}_{S,s}$ for $s \in S$ are Dedekind schemes as well. The main cases of interest are S being a (connected) proper smooth curve and $S = \operatorname{Spec} \mathcal{O}_K$ for the ring of integers $\mathcal{O}_K$ of a number field or a nonarchimedean local field K.

Let K be the function field of S. If $\mathcal{X}$ is an S-scheme, $\mathcal{X}_K$ is the *generic fiber* of $\mathcal{X}$. A nongeneric $s \in S$ is closed, and the complement of a nonempty open subscheme $U \subset S$ is a finite union of closed points. A normal Noetherian local ring of dimension $\leqslant 1$, such as $\mathcal{O}_{S,s}$ for $s \in S$, is either a discrete valuation ring or a field. The fraction fields of $\mathcal{O}^h_{S,s}$, $\mathcal{O}^{sh}_{S,s}$, and $\widehat{\mathcal{O}}_{S,s}$ will be denoted by $K^h_{S,s}$, $K^{sh}_{S,s}$, and $\widehat{K}_{S,s}$, respectively. Note that $\mathcal{O}_{S,s}$, $\mathcal{O}^h_{S,s}$, $\mathcal{O}^{sh}_{S,s}$, and $\widehat{\mathcal{O}}_{S,s}$ are either fields (if s is the

generic point) or discrete valuation rings sharing a common uniformizer [BLR90, §2.3 Prop. 10]. In the latter case, $\mathcal{O}_{S,s}$, $\mathcal{O}^h_{S,s}$, and $\widehat{\mathcal{O}}_{S,s}$ share the residue fields (cf. [EGA IV$_4$, 18.6.6 (iii)] for $\mathcal{O}^h_{S,s}$). The introduced notation will be in force in this section.

2.2. Néron (lft) models. 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 $\mathcal{Z}$ (which determines $\mathcal{X}$ from $\mathcal{X}_K$ up to a unique isomorphism). Dropping the finite type requirement, one obtains the definition of a *Néron lft model*, which is locally of finite type because of smoothness. Of course, a Néron model is also a Néron lft model. No further generality is obtained if $\mathcal{X}$ is an algebraic space in these definitions: a separated group algebraic space locally of finite type over a locally Noetherian base of dimension $\leqslant 1$ is a scheme [Ana73, 4.B].

Proposition 2.3.

(a) A finite type (resp., locally of finite type) $\mathcal{X} \to S$ is a Néron model (resp., Néron lft model) if and only if so is $\mathcal{X}_{\mathcal{O}_{S,s}} \to \operatorname{Spec}\mathcal{O}_{S,s}$ for every closed $s \in S$.

(b) If $\mathcal{X} \to S$ is a Néron model (resp., Néron lft model), then so are

$$\mathcal{X}_{\mathcal{O}^h_{S,s}} \to \operatorname{Spec}\mathcal{O}^h_{S,s}, \quad \mathcal{X}_{\widehat{\mathcal{O}}_{S,s}} \to \operatorname{Spec}\widehat{\mathcal{O}}_{S,s}, \quad \text{and} \quad \mathcal{X}_{\mathcal{O}^{sh}_{S,s}} \to \operatorname{Spec}\mathcal{O}^{sh}_{S,s}$$

for a closed $s \in S$.

Proof.

(a) See [BLR90, §1.2 Prop. 4] and [BLR90, p. 290].

(b) Combine (a) and [BLR90, §10.1 Prop. 3]. □

Proposition 2.4. *A proper smooth S-group scheme $\mathcal{G}$ is a Néron model.*

Proof. Proposition 2.3 (a) reduces to the local case $S = \operatorname{Spec}\mathcal{O}_{S,s}$, when the conclusion is clear due to [BLR90, §7.1 Thm. 1] as $\mathcal{G}(\mathcal{O}^{sh}_{S,s}) \to \mathcal{G}(K^{sh}_{S,s})$ is bijective by the valuative criterion of properness. □

Proposition 2.5. *Let $\mathcal{G}$ and $\mathcal{H}$ be Néron models over S. A sheaf of groups $\mathcal{E}$ on S_{fppf} that is an extension $1 \to \mathcal{H} \to \mathcal{E} \to \mathcal{G} \to 1$ is represented by a Néron model.*

Proof. By Proposition A.8, the S-group algebraic space $\mathcal{E}$ is separated, of finite type, and smooth, and so in fact a scheme [BLR90, §6.6 Cor. 3]. The proof of [BLR90, §7.5 Prop. 1 (b)] based on the same method as the proof of Proposition 2.4 now shows that $\mathcal{E}$ is a Néron model. □

Remark 2.6. One can use Proposition 2.5 to reduce Proposition 2.4 to the familiar cases of $\mathcal{G}$ being an abelian scheme or finite étale. Indeed, as we now show, a proper smooth group scheme $\mathcal{G}$ over a connected base scheme S is an extension of a finite étale S-group scheme by an abelian scheme. Let $\mathcal{G}^0 \subset \mathcal{G}$ be the open S-subgroup scheme such that $(\mathcal{G}^0)_s$ is the identity component of $\mathcal{G}_s$ for every $s \in S$ [EGA IV$_3$, 15.6.5]. We claim that $\mathcal{G}^0 \subset \mathcal{G}$ is also closed, rendering the smooth $\mathcal{G}^0 \to S$ proper. Granting this, due to the constancy of fiber dimension of $\mathcal{G}$ [EGA IV$_3$, 15.6.6 (iii) β)] (this is the only place where connectedness of S is used), $\mathcal{G}^0 \to S$ is an abelian scheme, and, by Proposition A.13 (c)–(d), $\mathcal{G}/\mathcal{G}^0$ is a separated smooth S-algebraic space of finite type. Working fiberwise, $\mathcal{G}/\mathcal{G}^0 \to S$ is quasi-finite by [SP, Lemma 06RW], and hence a scheme by [LMB00, A.2]. It then inherits properness from $\mathcal{G}$ [EGA II, 5.4.3 (ii)], and hence is finite étale [EGA IV$_3$, 8.11.1]. To complete the argument we now show that $\mathcal{G}^0 \subset \mathcal{G}$ is closed. Since $\mathcal{G} \to S$ is of finite presentation and the formation $\mathcal{G}^0$ commutes with arbitrary base change, due to the usual limit arguments, we

can assume that S is affine, then Noetherian, then also local, and finally also complete (using fpqc descent in this last step). In the latter case, [EGA III_1, 5.5.2] applied to the connected $\mathcal{G}^0$ shows that $\mathcal{G}^0 \to S$ inherits properness from its special fiber. The desired properness of $\mathcal{G}^0 \subset \mathcal{G}$ follows.

An important source of Néron models is Theorem 2.13; for its formulation, we recall the notions of

2.7. Schematic image and schematic dominance. For a scheme morphism $X \xrightarrow{f} Y$, its *schematic image* is the initial closed subscheme $Y' \to Y$ through which f factors. By [SP, Lemma 01R6], the schematic image exists. If for each open $U \subset Y$ the schematic image of f_U is U, then f is *schematically dominant* [EGA IV_3, 11.10.2]. If f is quasi-compact, then the induced $X \to Y'$ is schematically dominant [SP, Lemma 01R8], and in this case the formation of Y' commutes with flat base change [EGA IV_3, 11.10.5 (ii) a)].

The schematic image of a morphism of algebraic spaces is defined analogously to the case of schemes; its existence is guaranteed by [SP, Lemma 082X]. If the morphism is in addition quasi-compact, then the formation of the schematic image again commutes with flat base change [SP, Lemma 089E].

Lemma 2.8 (Transitivity of schematic images for algebraic spaces). *For a scheme T and morphisms of T-algebraic spaces $f\colon X \to Y$ and $g\colon Y \to Z$, let $Y' \hookrightarrow Y$ and $Z' \hookrightarrow Z$ be the schematic images of f and $g|_{Y'}$. Then $Z' \hookrightarrow Z$ is also the schematic image of $g \circ f$.*

Proof. Since a section of a closed immersion of algebraic spaces is an isomorphism, the proof of [EGA I, 9.5.5] given for schemes continues to work for algebraic spaces. □

Lemma 2.9. *Let T be a scheme and $f\colon X \to Y$ and $g_1, g_2\colon Y \to Z$ morphisms of T-algebraic spaces. If $Z \to T$ is separated, $g_1 \circ f = g_2 \circ f$, and the schematic image of f is Y, then $g_1 = g_2$.*

Proof. The proof of [EGA I, 9.5.6] given for schemes continues to work for algebraic spaces. □

Recall that S is a connected Dedekind scheme with function field K.

Proposition 2.10. *Let $\mathcal{Y}$ be an S-algebraic space and H a closed subalgebraic space of $\mathcal{Y}_K$.*

(a) The schematic image $\mathcal{H}$ of $H \to \mathcal{Y}$ is the unique S-flat closed subalgebraic space of $\mathcal{Y}$ with generic fiber H. In particular, a flat $\mathcal{Y}$ is the schematic image of its generic fiber.

(b) For an S-algebraic space $\mathcal{Y}'$ and a closed subalgebraic space $H' \subset \mathcal{Y}'_K$ whose schematic image in $\mathcal{Y}'$ is denoted by $\mathcal{H}'$, the schematic image of $H \times_K H' \to \mathcal{Y} \times_S \mathcal{Y}'$ is $\mathcal{H} \times_S \mathcal{H}'$.

(c) For a flat S-algebraic space $\mathcal{X}$, an S-morphism $f\colon \mathcal{X} \to \mathcal{Y}$ factors through $\mathcal{H}$ if and only if f_K factors through H.

(d) If $\mathcal{Y}$ is an S-group and H is a K-subgroup, then $\mathcal{H}$ is an S-subgroup of $\mathcal{Y}$.

(e) If $\mathcal{X}$ is a flat S-algebraic space and $\mathcal{Y}$ is separated, then there is at most one S-morphism $\mathcal{X} \to \mathcal{Y}$ extending a given $\mathcal{X}_K \to \mathcal{Y}_K$.

(f) If $\mathcal{Y}$ is a separated S-group and H is a K-subgroup, then the closed S-subgroup $\mathcal{H}$ is separated. Moreover, $\mathcal{H}$ is killed by n (resp., is commutative) if so is H.

(g) If $\mathcal{Y}$ is a finite type S-group and H is a finite K-group, then $\mathcal{H}$ is a quasi-finite S-group.

Proof.

(a) Choose an étale surjection $U \to \mathcal{Y}$ for some scheme U. By the known scheme case [EGA IV_2, 2.8.5] and the flat base change aspect of §2.7, $\mathcal{H} \times_{\mathcal{Y}} U$ is the unique S-flat closed subscheme of U with generic fiber $H \times_{\mathcal{Y}_K} U_K$. Its S-flatness implies that of $\mathcal{H}$ thanks to [SP, Lemma 06ET].

For the uniqueness claim, the interpretation in [SP, Lemma 03MB] of closed subalgebraic spaces in terms of their quasi-coherent sheaves of ideals reduces to showing that S-flat closed subalgebraic spaces $\mathcal{H}_1 \subset \mathcal{H}_2 \subset \mathcal{Y}$ sharing H as their generic fiber are equal. Due to [SP, Lemma 041Y], this can be checked étale locally on $\mathcal{Y}$, and it holds after base change to U.

(b) This results from the S-flatness and uniqueness claims of (a).

(c) Combine the definition of $\mathcal{H}$, Lemma 2.8 applied to the composition $\mathcal{X}_K \to \mathcal{X} \xrightarrow{f} \mathcal{Y}$, and (a).

(d) The diagrams giving the group scheme structure of $\mathcal{Y}$ restrict to $\mathcal{H}$ due to (a), (b), and (c).

(e) Combine (a) and Lemma 2.9.

(f) Separatedness is inherited from $\mathcal{Y}$. The rest follows from (e).

(g) By (a) and (d), $\mathcal{H}$ is a finite type flat S-group with $\mathcal{H}_K = H$. Choose an étale surjection $U \to \mathcal{H}$ with U a locally of finite type flat S-scheme. The generic fiber U_K is locally quasi-finite. By [SP, Definition 03XJ], it remains to check that U is also locally quasi-finite. For this, working locally on U, we assume that $U \xrightarrow{u} S$ is affine. Since we seek to show that the fibers of u are finite, we may also assume that S is local.

Due to flatness and (a), U is the scheme-theoretic union of the schematic images of the irreducible components of U_K. To show the finiteness of the special fiber of U, we can therefore pass to these S-flat schematic images and assume that U is irreducible, in which case the conclusion results from [BLR90, §2.4 Prop. 4]. □

Proposition 2.10 enables us to extend [GMB13, Prop. 3.1] beyond the affine case:

Proposition 2.11. *Let S be a connected Dedekind scheme, K its function field, $\mathcal{G} \to S$ a separated S-group algebraic space, and $\widetilde{\mathcal{G}} \subset \mathcal{G}$ the schematic image of $\mathcal{G}_K \to \mathcal{G}$, so $\widetilde{\mathcal{G}}$ is an S-flat closed subgroup of $\mathcal{G}$ by Proposition 2.10 (a) and (d). For a torsor $\mathcal{X} \to S$ under $\mathcal{G}$ for the fppf topology, the schematic image $\widetilde{\mathcal{X}}$ of $\mathcal{X}_K \to \mathcal{X}$ is a torsor under $\widetilde{\mathcal{G}}$ for the fppf topology. The assignment $\mathcal{X} \mapsto \widetilde{\mathcal{X}}$ is functorial and furnishes an equivalence of categories between torsors under $\mathcal{G}$ and those under $\widetilde{\mathcal{G}}$. The "change of group" functor resulting from $\widetilde{\mathcal{G}} \subset \mathcal{G}$ is quasi-inverse to $\mathcal{X} \mapsto \widetilde{\mathcal{X}}$. In particular, $H^1_{\mathrm{fppf}}(S, \widetilde{\mathcal{G}}) \to H^1_{\mathrm{fppf}}(S, \mathcal{G})$ is bijective.*

Proof. Torsor sheaves are the same as torsor algebraic spaces thanks to Proposition A.5.

The action morphism $\mathcal{G} \times_S \mathcal{X} \to \mathcal{X}$ restricts to $\widetilde{\mathcal{G}} \times_S \widetilde{\mathcal{X}} \to \widetilde{\mathcal{X}}$ thanks to Proposition 2.10 (c), which also shows that $\widetilde{\mathcal{X}}(T) = \mathcal{X}(T)$ for every fppf $T \to S$, so $\widetilde{X}(T) \neq \varnothing$ for some such T. Since $\mathcal{X}$, and hence also $\widetilde{\mathcal{X}}$, inherits separatedness from $\mathcal{G}$, employing in addition Proposition 2.10 (b) and (e), we see that the isomorphism $\mathcal{G} \times_S \mathcal{X} \xrightarrow{(g,x)\mapsto(gx,x)} \mathcal{X} \times_S \mathcal{X}$ and its inverse restrict to the analogous isomorphism $\widetilde{\mathcal{G}} \times_S \widetilde{\mathcal{X}} \to \widetilde{\mathcal{X}} \times_S \widetilde{\mathcal{X}}$ and its inverse. In conclusion, $\widetilde{\mathcal{X}}$ is a torsor under $\widetilde{\mathcal{G}}$ for the fppf topology. The functoriality of $\mathcal{X} \mapsto \widetilde{\mathcal{X}}$ also results from Proposition 2.10 (c).

We turn to the remaining quasi-inverse claim. For a torsor $\mathcal{X}'$ under $\widetilde{\mathcal{G}}$ for the fppf topology, the natural map $i\colon \mathcal{X}' \hookrightarrow \mathcal{X}' \times^{\widetilde{\mathcal{G}}} \mathcal{G} =: \mathcal{X}$ is a closed immersion, as one checks fppf locally on S. Moreover, i_K is an isomorphism and $\mathcal{X}'$ inherits flatness from $\widetilde{\mathcal{G}}$. Thus, due to Proposition 2.10 (a) and (c),

$\mathcal{X}' = \widetilde{\mathcal{X}}$ inside $\mathcal{X}$ functorially in $\mathcal{X}'$. Conversely, for a torsor $\mathcal{X}$ under $\mathcal{G}$, the natural $\widetilde{\mathcal{X}} \times^{\widetilde{\mathcal{G}}} \mathcal{G} \to \mathcal{X}$ is an isomorphism, as can be checked fppf locally on S; this isomorphism is functorial in $\mathcal{X}$. □

2.12. Group smoothenings. For a finite type S-group scheme $\mathcal{G}$ with smooth generic fiber, its *group smoothening* is an S-homomorphism $\mathcal{G}' \xrightarrow{t} \mathcal{G}$ with a finite type smooth S-group scheme $\mathcal{G}'$ satisfying: for a finite type smooth $\mathcal{Z} \to S$, every S-morphism $\mathcal{Z} \to \mathcal{G}$ factors uniquely through t. If a group smoothening of $\mathcal{G}$ exists, it is unique up to a unique isomorphism. Due to spreading out (applied to $\mathcal{Z}$), the formation of $\mathcal{G}'$ commutes with localization on S, so t_K is an isomorphism.

Theorem 2.13 ([BLR90, §7.1 Cor. 6]). *A closed K-smooth subgroup scheme $G \subset \mathcal{X}_K$ of the generic fiber of a Néron model $\mathcal{X} \to S$ admits a Néron model, which is given by the group smoothening of the schematic image $\overline{G}$ of $G \to \mathcal{X}$. Consequently, $\overline{G}$ is a Néron model if and only if it is S-smooth.*

Corollary 2.14. *A smooth S-group scheme $\mathcal{G}$ is a closed subgroup of a Néron model if and only if it is a Néron model itself.*

Proof. To see that $\mathcal{G}$ inherits the Néron property, use Proposition 2.10 (c) for smooth schemes $\mathcal{X}$. □

Étale Néron models are particularly pleasant to deal with due to

Proposition 2.15. *Let G be a finite étale K-group scheme.*

(a) The Néron model $\mathcal{G} \to S$ of G exists and is separated quasi-finite étale.

(b) $\mathcal{G} \to S$ is finite if and only if $G(\overline{K})$ is unramified at all nongeneric $s \in S$ (i.e., if and only if the finite $(\widehat{K}_{S,s})^{\mathrm{nr}}$-group $G_{(\widehat{K}_{S,s})^{\mathrm{nr}}}$ is constant for all such s, where $(\widehat{K}_{S,s})^{\mathrm{nr}} := \mathrm{Frac}(\widehat{\mathcal{O}}_{S,s})^{sh}$).

(c) $\mathcal{G} \mapsto \mathcal{G}_K$ is an equivalence between the category of étale Néron models over S and that of finite étale K-group schemes that is compatible with kernels and finite products. When restricted to the full subcategory of finite étale $\mathcal{G}$, it is also compatible with quotients.

(d) Commutative finite étale S-group schemes form an abelian subcategory of the category of abelian sheaves on $S_{\text{ét}}$ that is equivalent by the exact generic fiber functor to the category of finite discrete $\mathrm{Gal}(\overline{K}/K)$-modules that are unramified at all nongeneric points of S.

Proof. The Néron property of a finite étale S-group scheme can be verified directly by reducing to the constant case (alternatively, use Proposition 2.4). Thus, for existence in (a), spreading-out and [BLR90, §1.4 Prop. 1 and §6.5 Cor. 3] reduces to the case of a strictly local S, when $\mathcal{G} \to S$ is obtained from G by extending the constant subgroup $\underline{G(K)}_K \subset G$ to a constant subgroup over S [BLR90, §7.1 Thm. 1]. The other claims of (a), as well as (b), are immediate from construction. Since a quotient of finite étale group schemes is finite étale, (c) follows, and it implies (d). □

Remarks.

2.16. The existence in (a) can also be argued with the help of restriction of scalars and normalization to reduce to the constant case.

2.17. Without restricting to finite étale $\mathcal{G}$ in (c), compatibility with quotients fails. Indeed, short exactness of a sequence of $\mathrm{Gal}(\overline{K}/K)$-modules does not imply that of the corresponding sequence of Néron models. An example is a nonsemisimple ramified extension H of two trivial mod p characters: by (b), the Néron model of H is not finite, whereas every extension of finite S-group schemes must again be finite due to Proposition A.8.

We now consider fppf (equivalently, étale, cf. Proposition A.6) torsors under a Néron (lft) model.

Proposition 2.18 ([Ray70, Thm. XI 3.1 1)]). *Every fppf torsor under a Néron model is representable by a scheme.*

We do not know whether representability by schemes fails for torsors under Néron lft models.

Proposition 2.19. *An fppf torsor $\mathcal{T} \to S$ under a Néron lft model $\mathcal{X} \to S$ is a separated smooth S-algebraic space that has the Néron property for smooth S-algebraic spaces. If $\mathcal{X}$ is a Néron model, then $\mathcal{T} \to S$ is of finite type.*

Proof. By Propositions A.5 and A.6, $\mathcal{T}$ trivializes over an étale cover $S' \to S$ and is representable by an S-algebraic space. Every S-algebraic space $\mathcal{Z}$ is the quotient of an étale equivalence relation of schemes, so in checking Néron bijectivity of $\mathcal{T}(\mathcal{Z}) \to \mathcal{T}(\mathcal{Z}_K)$, one is reduced to the case of a smooth S-scheme Z. As Néron property is preserved under étale base change, in the commutative diagram

$$\begin{array}{ccccc} \mathcal{T}(Z) & \longrightarrow & \mathcal{T}(Z_{S'}) & \rightrightarrows & \mathcal{T}(Z_{S'\times_S S'}) \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} \\ \mathcal{T}(Z_K) & \longrightarrow & \mathcal{T}((Z_{S'})_K) & \rightrightarrows & \mathcal{T}((Z_{S'\times_S S'})_K) \end{array}$$

with equalizer rows, b and c are bijective, hence so is a, giving the Néron property of $\mathcal{T}$. The other claimed properties are inherited from $\mathcal{X}$ by descent [SP, Lemmas 0421, 0429, and 041U]. □

Corollary 2.20. *For a Néron lft model $\mathcal{X} \to S$,*

$$H^1_{\mathrm{fppf}}(S, \mathcal{X}) \xrightarrow{\iota} H^1_{\mathrm{fppf}}(K, \mathcal{X}_K) \overset{\S 1.17}{\cong} H^1(K, \mathcal{X}_K) \tag{2.20.1}$$

is injective (cf. §A.4 for the notation).

Proof. An fppf torsor under $\mathcal{X}$ is determined by its generic fiber due to Proposition 2.19. □

If S is local, it is possible to determine the image of (2.20.1):

Proposition 2.21. *Let R be a discrete valuation ring, and set $K := \operatorname{Frac} R$ and $K^{sh} := \operatorname{Frac} R^{sh}$. For a Néron lft model $\mathcal{X}$ over $S = \operatorname{Spec} R$, the image of the injection ι from (2.20.1) is the unramified cohomology subset*

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

which consists of all the $\mathcal{X}_K$-torsors that trivialize over K^{sh}. In other words, an $\mathcal{X}_K$-torsor T extends to an $\mathcal{X}$-torsor if and only if $T(K^{sh}) \neq \varnothing$.

Proof. By Proposition A.6, every $\mathcal{X}$-torsor $\mathcal{T}$ trivializes over an étale cover $U \to S$. Moreover, $\operatorname{Spec} R^{sh} \to \operatorname{Spec} R$ factors through U, so $\mathcal{T}$ trivializes over R^{sh}. This yields $\operatorname{Im} \iota \subset I$.

By construction, R^{sh} is a filtered direct limit of local étale R-algebras R' which are discrete valuation rings sharing a uniformizer with R; if $K' = \operatorname{Frac} R'$, then $K^{sh} = \varinjlim K'$. Let T be an $\mathcal{X}_K$-torsor with $T(K^{sh}) \neq \varnothing$; we will show that it extends to an $\mathcal{X}$-torsor $\mathcal{T}$, thus proving $I \subset \operatorname{Im} \iota$. Since T is locally of finite presentation, $T(K^{sh}) = \varinjlim T(K')$ [LMB00, 4.18 (i)], so T trivializes over some K'; we fix the corresponding R'. The descent datum on $T_{K'}$ with respect to K'/K transports along an isomorphism of torsors to $\mathcal{X}_{K'}$ and then, since Néron property is preserved under étale base change, to a descent datum on $\mathcal{X}_{R'}$ with respect to R'/R, all compatibly with the torsor structure. This compatibility together with the effectivity of the descent datum on $\mathcal{X}_{R'}$ for algebraic spaces [LMB00, 1.6.4], equips the descended $\mathcal{T} \to \operatorname{Spec} R$ with the structure of an $\mathcal{X}$-torsor trivialized over R'. By construction, $\mathcal{T}_K \cong T$ as $\mathcal{X}_K$-torsors. □

3. Exact sequences involving Néron models of abelian varieties

The short exact sequences gathered in this section are crucial for the fppf cohomological approach to Selmer groups and have been used repeatedly in the literature, but their proofs seem hard to locate.

3.1. Open subgroups of $\mathcal{A}$. Let S be a connected Dedekind scheme (cf. §2.1), let K be its function field, let $A \to \operatorname{Spec} K$ be an abelian variety, and let $\mathcal{A} \to S$ be its Néron model. For a nongeneric $s \in S$, let Φ_s be the finite étale $k(s)$-group scheme $\mathcal{A}_s/\mathcal{A}_s^0$ of connected components of the special fiber $\mathcal{A}_s$. For each s, choose a $k(s)$-subgroup $\Gamma_s \subset \Phi_s$ (equivalently, a $\operatorname{Gal}(\overline{k(s)}/k(s))$-submodule $\Gamma_s(\overline{k(s)}) \subset \Phi_s(\overline{k(s)})$). For all s but finitely many, $\mathcal{A}_s$ is an abelian variety, so $\Phi_s = 0$ and $\Gamma_s = \Phi_s$. Consequently, one obtains the open S-subgroup scheme $\mathcal{A}^\Gamma \subset \mathcal{A}$ by removing for each s the connected components of $\mathcal{A}_s$ not in Γ_s. By construction, for each S-scheme T, the sections in $\mathcal{A}^\Gamma(T)$ are those $T \xrightarrow{f} \mathcal{A}$ for which the composition of $f_s\colon T_s \to \mathcal{A}_s$ and $\mathcal{A}_s \to \Phi_s$ factors through $\Gamma_s \subset \Phi_s$. If $\Gamma_s = 0$ for each s, one obtains the open S-subgroup $\mathcal{A}^0 \subset \mathcal{A}$ that fiberwise consists of connected components of identity. Of course, $\Gamma_s = \Phi_s$ for all s leads to $\mathcal{A}^\Phi = \mathcal{A}$. For $s \in S$, we denote the base change $(\mathcal{A}^\Gamma)_s$ by $\mathcal{A}_s^\Gamma$.

For a closed $s \in S$, denote by $i_s\colon \operatorname{Spec} k(s) \to S$ the resulting closed immersion. Since $i_s^*\mathcal{A}^\Gamma = \mathcal{A}_s^\Gamma$, under the adjunction $i_s^* \dashv i_{s*}$ the homomorphism $\mathcal{A}_s^\Gamma \xrightarrow{\pi_s} \Gamma_s$ corresponds to the homomorphism $\mathcal{A}^\Gamma \to i_{s*}\mathcal{A}_s^\Gamma \xrightarrow{i_{s*}(\pi_s)} i_{s*}\Gamma_s$ mapping $f \in \mathcal{A}^\Gamma(T)$ to $\pi_s \circ f_s$. In particular, for every choice of $\widetilde{\Gamma}_s \subset \Gamma_s$, there is a Cartesian square

$$\begin{array}{ccc} \mathcal{A}^{\widetilde{\Gamma}} & \hookrightarrow & \mathcal{A}^\Gamma \\ \downarrow & & \downarrow \\ \bigoplus_s i_{s*}\widetilde{\Gamma}_s & \hookrightarrow & \bigoplus_s i_{s*}\Gamma_s. \end{array} \tag{3.1.1}$$

Proposition 3.2. *For all choices of subgroups $\widetilde{\Gamma}_s \subset \Gamma_s \subset \Phi_s$, 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 from (3.1.1) and left exactness of i_{s*}, whereas to check the remaining surjectivity of a in $S_{\text{Ét}}$ on stalks, it suffices to consider strictly local rings $(\mathcal{O}, \mathfrak{m})$ of $S_{\text{Ét}}$ 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

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

b is surjective due to Hensel-lifting for the smooth $\mathcal{A}_{\mathcal{O}}^\Gamma \to \operatorname{Spec}\mathcal{O}$ [BLR90, §2.3 Prop. 5], c is surjective due to invariance of the rational component group of the smooth $\mathcal{A}_{\overline{k(s)}}^\Gamma \to \operatorname{Spec}\overline{k(s)}$ upon passage to a separably closed overfield [EGA IV_4, 17.16.3 (ii)], whereas d is bijective since $(\Gamma_s/\widetilde{\Gamma}_s)_{\mathcal{O}/\mathfrak{a}}$ is finite étale over the Henselian local $(\mathcal{O}/\mathfrak{a}, \mathfrak{m}/\mathfrak{a})$ [EGA IV_4, 18.5.15]. The desired surjectivity of $a(\mathcal{O})$ follows (by limit arguments [EGA IV_3, 8.14.2], a induces $a(\mathcal{O})$ on the stalk at $\mathcal{O}$). □

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

Proposition 3.3. *The kernel $\mathcal{A}[\phi] \to S$ is affine. Every torsor under $\mathcal{A}[\phi]$ for the fppf topology is representable.*

Proof. Affineness is a special case of [Ana73, 2.3.2]. Representability of torsors is a special case of Proposition A.7. □

Lemma 3.4. *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.

When the equivalent conditions hold, $\mathcal{A}^0 \xrightarrow{\phi} \mathcal{B}^0$ is a surjection of fppf sheaves.

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

Since $\mathcal{A}$, $\mathcal{B}$ are fppf over S, by [BLR90, §2.4 Prop. 4], $\dim \mathcal{A}_s = \dim A$, $\dim \mathcal{B}_s = \dim B$, and hence $\dim \mathcal{A}_s = \dim \mathcal{B}_s$. Therefore, by [SGA $3_{\text{I new}}$, VI_B, 1.2 et 1.3], (a)⇔(b). If ϕ_s is flat, then $\phi_s(\mathcal{A}_s^0)$ is both open and closed (loc. cit.), and hence equals $\mathcal{B}_s^0$. Thus, (c)⇒(b). Conversely, if ϕ_s is surjective, it is flat [SGA $3_{\text{I new}}$, VI_A 5.4.1], so (b)⇒(c).

For the last claim, by (b) and (c), ϕ is fppf, and hence a surjection of represented fppf sheaves. □

3.5. Semiabelian reduction. One says that A has *semiabelian reduction* at a nongeneric $s \in S$ if $\mathcal{A}_s^0$ is an extension of an abelian variety by a torus.

Lemma 3.6. *The equivalent conditions of Lemma 3.4 hold if*

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

If ϕ is multiplication by n, then (d) is equivalent to the conditions of Lemma 3.4.

Proof. For a commutative connected algebraic group G over a field k, multiplication by n is surjective on G, provided that G is a semiabelian variety if $\operatorname{char} k \nmid n$: it is surjective on abelian varieties and tori for every k and induces an isomorphism on $\operatorname{Lie} G$ if $\operatorname{char} k \nmid n$, so [SGA $3_{\text{I new}}$, VI_B 1.2] applies. This gives (d)⇒(b) by considering the isogeny $\psi\colon B \to A$ with kernel $\phi(A[\deg \phi])$, so $\phi \circ \psi = \deg \phi$.

To argue that (a)⇒(d) if $\phi = n$, take an $s \in S$ with $\operatorname{char} k(s) \mid n$. Quasi-finiteness of multiplication by n prevents $\mathcal{A}^0_{k(s)^{\mathrm{alg}}}$ from having $\mathbb{G}_a$ as a subgroup, so $\mathcal{A}^0_{k(s)^{\mathrm{alg}}}$ is of unipotent rank 0, and hence $\mathcal{A}_s^0$ is a semiabelian variety as explained in [BLR90, §7.3 p. 178]. □

Remark 3.7. For an arbitrary ϕ, (d) is not equivalent to (a)–(c) of Lemma 3.4: take

$$\phi = \mathrm{id}_{A_1} \times n\colon A_1 \times A_2 \to A_1 \times A_2$$

for an n for which (d) holds for A_2; (c) holds for this ϕ, but (d) fails in general since A_1 is arbitrary.

Corollary 3.8. *Suppose that $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (due to Lemma 3.6, this is the case if 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 everywhere.*

Proof. By Lemma 3.4, $\mathcal{A} \to \mathcal{B}$ is quasi-finite flat, and $\mathcal{A}[\phi] \to S$ inherits these properties. Affineness results from Proposition 3.3 (or also from [SGA $3_{\text{I new}}$, XXV, 4.1]). If A has good reduction, then $\mathcal{A}$ is proper over S, and hence so is its closed subscheme $\mathcal{A}[\phi]$, which then is finite due to quasi-finiteness [EGA IV_3, 8.11.1]. □

Corollary 3.9. *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. By Proposition 2.10 and Corollary 3.8, $\mathcal{A}[\phi]$ is the schematic image of $A[\phi] \to \mathcal{A}$ and is killed by $\deg \phi$. Thus, due to Corollary 3.8 and Proposition A.9, $\mathcal{A}[\phi] \to S$ is étale, and one invokes Theorem 2.13. □

The analogue of $0 \to A[\phi] \to A \xrightarrow{\phi} B \to 0$ for $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ faces complications due to possibly disconnected closed fibers. To state it in Proposition 3.10 (a), note that a choice of $\Gamma_s \subset \Phi_s$ yields $\phi_s(\Gamma_s)$, which give the open subgroup $\mathcal{B}^{\phi(\Gamma)} \subset \mathcal{B}$ as in §3.1, and $\phi\colon \mathcal{A}^\Gamma \to \mathcal{B}$ factors through $\mathcal{B}^{\phi(\Gamma)} \hookrightarrow \mathcal{B}$.

Proposition 3.10. *If* $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ *is flat (e.g., if* A *has semiabelian reduction at all nongeneric* $s \in S$ *with* $\operatorname{char} k(s) \mid \deg \phi$*, cf. Lemma 3.6), then for all choices* $\Gamma_s \subset \Phi_s$ *the sequences*

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

(b) $0 \to \mathcal{A}^0[\phi] \to \mathcal{A}^\Gamma[\phi] \to \bigoplus_s i_{s*}(\Gamma_s[\phi_s]) \to 0$

are exact in S_{fppf}.

Proof. In the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{A}^0[\phi] & \longrightarrow & \mathcal{A}^\Gamma[\phi] & \longrightarrow & \bigoplus_s i_{s*}(\Gamma_s[\phi_s]) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{A}^0 & \longrightarrow & \mathcal{A}^\Gamma & \longrightarrow & \bigoplus_s i_{s*}\Gamma_s & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \oplus_s i_{s*}\phi_s} & & \\
0 & \longrightarrow & \mathcal{B}^0 & \longrightarrow & \mathcal{B}^{\phi(\Gamma)} & \longrightarrow & \bigoplus_s i_{s*}(\phi_s(\Gamma_s)) & \longrightarrow & 0,
\end{array}$$

the bottom horizontal sequences are short exact by Proposition 3.2, the left bottom ϕ is surjective by Lemma 3.4, and the right vertical sequence is short exact in S_{fppf} because it is so in $S_{\text{Ét}}$ due to exactness of each i_{s*} in the étale topology. Both claims follow by invoking snake lemma. □

Corollary 3.11. *Suppose that* $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ *is flat. For an isogeny* $B \xrightarrow{\psi} C$ *of abelian varieties, which induces* $\mathcal{B} \xrightarrow{\psi} \mathcal{C}$ *on Néron models, and for every choice of* $\Gamma_s \subset \Phi_s$*, the sequence*

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

is exact in S_{fppf}.

Proof. Due to universality of quotients [Ray67, §3 iii)], pulling back Proposition 3.10 (a) along $\mathcal{B}^{\phi(\Gamma)}[\psi] \hookrightarrow \mathcal{B}^{\phi(\Gamma)}$ gives the claim. □

Remark 3.12. Corollary 3.11 requires no assumption on $\mathcal{B} \xrightarrow{\psi} \mathcal{C}$. For instance, it applies when $\phi = n$ and $\psi = m$ are multiplication by n and m isogenies and A has semiabelian reduction at all nongeneric $s \in S$ with $\operatorname{char} k(s) \mid n$.

4. Glueing schemes over global bases

Let S be a connected Dedekind scheme and K its function field. For a nongeneric $s \in S$, 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 Lemma 4.1 by making $\mathcal{O}_{S,s}$ and $K_{S,s}$ notationally analogous to $\mathcal{O}^h_{S,s}$ and $K^h_{S,s}$.

A standard descent lemma 4.1 formalizes the idea that an S-scheme amounts to a V-scheme for a nonempty open $V \subset S$ together with a compatible $\widehat{\mathcal{O}}_{S,s}$-scheme for every $s \in S - V$. We use it in §5 through Corollary 4.4 to reduce questions about group schemes over global bases to the local case. Its special case Claim 4.1.1 is key for Selmer type descriptions of sets of fppf torsors in §7.

Lemma 4.1. *Let $s_1, \ldots, s_n \in S$ be distinct nongeneric points, $V := S - \{s_1, \ldots, s_n\}$ the complementary open subscheme, and F the functor*

$$X \mapsto (X_V, X_{\mathcal{O}_{S,s_1}}, \ldots, X_{\mathcal{O}_{S,s_n}}, \alpha_i \colon (X_V)_{K_{S,s_i}} \xrightarrow{\sim} (X_{\mathcal{O}_{S,s_i}})_{K_{S,s_i}} \text{ for } 1 \leqslant i \leqslant n)$$

from the category of S-algebraic spaces to the category of tuples consisting of a V-algebraic space, an $\mathcal{O}_{S,s_i}$-algebraic space for each i, and isomorphisms $\alpha_1, \ldots, \alpha_n$ as indicated ("glueing data"). Morphisms in the target category are tuples of morphisms of V- and $\mathcal{O}_{S,s_i}$-algebraic spaces that are compatible with the α_i's.

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

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

Proof. In (a), we say that a tuple of schemes admits a quasi-affine open covering if $X_V = \bigcup_{j \in J} U_j$ and $X_{\mathcal{O}_{S,s_i}} = \bigcup_{j \in J} U_{i,j}$ for $1 \leqslant i \leqslant n$ with quasi-affine (over respective bases) open U_j, $U_{i,j}$ for which the α_i restrict to isomorphisms $(U_j)_{K_{S,s_i}} \xrightarrow{\sim} (U_{i,j})_{K_{S,s_i}}$. The definition is analogous in the case of henselizations or completions, or for various categories of tuples considered below. Note that F takes values in the claimed subcategory: an affine open covering of X gives a quasi-affine open covering $F(X)$.

Since F is the composite of $X \mapsto (X_{S-\{s_1\}}, X_{\mathcal{O}_{S,s_1}}, \alpha_1)$ and its analogue for $s_2, \ldots, s_n \in S - \{s_1\}$ (and similarly for henselizations and completions), induction reduces us to the $n = 1$ case (in (a), a quasi-affine open covering of an n-tuple descends to a quasi-affine open covering of the first entry of the triple due to the inductive hypothesis applied to the schemes in the covering). In the sequel $s_1 = s$, $\alpha_1 = \alpha$, $V = S - \{s\}$, and we stop writing $K_{S,s}$ for K.

Postponing the cases of henselizations and completions, we now prove (a) and (b):

(a) Giving a descent datum with respect to the fpqc $V \bigsqcup \operatorname{Spec} \mathcal{O}_{S,s} \to S$ amounts to giving α because there are no nontrivial triple intersections. Thus, F is fully faithful [BLR90, §6.1 Thm. 6 (a)]. For essential surjectivity, by [SP, Lemma 0247], the quasi-affine open cover descends and glues along descended quasi-affine open intersections to a desired X.

(b) Let $\pi \in K$ be a uniformizer of $\mathcal{O}_{S,s}$; note that $\mathcal{O}_{S,s}$ is a filtered direct limit $\varinjlim R$ of coordinate rings of affine open subschemes of S containing s on which π is regular and vanishes only at s. For essential surjectivity, given a $(Y, \mathcal{Y}, \alpha \colon Y_K \xrightarrow{\sim} \mathcal{Y}_K)$ with $Y \to V$ and $\mathcal{Y} \to \operatorname{Spec} \mathcal{O}_{S,s}$

of finite presentation, first spread out $\mathcal{Y}$ to $\mathcal{Y}' \to \operatorname{Spec} R$ and α to $\alpha'\colon Y_{R[\frac{1}{\pi}]} \xrightarrow{\sim} \mathcal{Y}'_{R[\frac{1}{\pi}]}$ for some R as above using limit considerations of [Ols06, proof of Prop. 2.2]. As in (a), α' gives a descent datum with respect to $V \bigsqcup \operatorname{Spec} R \to S$ which is effective [LMB00, 1.6.4], thus yielding a desired X. Full faithfulness follows from analogous limit arguments using étale (or Zariski) descent for morphisms of sheaves on $S_{\text{Ét}}$ and [LMB00, 4.18 (i)].

Before dealing with henselizations and completions we make a preliminary reduction concentrating on the case of $\mathcal{O}^h_{S,s}$ and $K^h_{S,s}$ (that of $\widehat{\mathcal{O}}_{S,s}$ and $\widehat{K}_{S,s}$ is completely analogous). In the categories described below morphisms are tuples of morphisms which are compatible with the isomorphisms that are specified as part of the data of an object.

Let $\mathscr{C}$ be the target category of F, and $\mathscr{C}^h$ its analogue in the case of henselizations. We proved that F is an equivalence when restricted to the subcategories of (a) and (b), so it remains to show that

$$G\colon \mathscr{C} \to \mathscr{C}^h, \qquad (Y, \mathcal{Y}, \alpha\colon Y_K \xrightarrow{\sim} \mathcal{Y}_K) \mapsto \left(Y, \mathcal{Y}_{\mathcal{O}^h_{S,s}}, \alpha_{K^h_{S,s}}\colon Y_{K^h_{S,s}} \xrightarrow{\sim} (\mathcal{Y}_{\mathcal{O}^h_{S,s}})_{K^h_{S,s}}\right)$$

is too. Let $\mathscr{D}$ be the category of $\mathcal{O}_{S,s}$-algebraic spaces and $\mathscr{D}^h$ the category of triples

$$(Z, \mathcal{Z}, \beta\colon Z_{K^h_{S,s}} \xrightarrow{\sim} \mathcal{Z}_{K^h_{S,s}})$$

consisting of a K-algebraic space, an $\mathcal{O}^h_{S,s}$-algebraic space, and an isomorphism as indicated. Let $\mathscr{D}\widehat{\ }$ be the analogous category of triples with $\mathcal{O}^h_{S,s}$ and $K^h_{S,s}$ replaced by $\widehat{\mathcal{O}}_{S,s}$ and $\widehat{K}_{S,s}$. Let $B\colon \mathscr{D} \to \mathscr{D}^h$ be the base change functor and $\mathscr{E}$ the category of triples

$$(Y, (Z, \mathcal{Z}, \beta) \in \mathscr{D}^h, \gamma\colon Y_K \xrightarrow{\sim} Z)$$

with Y a V-algebraic space. The diagram of functors

$$\begin{array}{ccc}
\mathscr{C} & \xrightarrow{G} & \mathscr{C}^h \\
& {\scriptstyle (\mathrm{id},B,\mathrm{id})}\searrow & \downarrow{\scriptstyle H} \\
& & \mathscr{E},
\end{array}
\qquad
\begin{array}{ccc}
(Y, \mathcal{Y}, \alpha) & \xrightarrow{\quad G \quad} & (Y, \mathcal{Y}_{\mathcal{O}^h_{S,s}}, \alpha_{K^h_{S,s}}) \\
\downarrow{\scriptstyle (\mathrm{id},B,\mathrm{id})} & & \downarrow{\scriptstyle H} \\
(Y, (\mathcal{Y}_K, \mathcal{Y}_{\mathcal{O}^h_{S,s}}, \mathrm{id}), \alpha) & \cong & (Y, (Y_K, \mathcal{Y}_{\mathcal{O}^h_{S,s}}, \alpha_{K^h_{S,s}}), \mathrm{id}),
\end{array}
\qquad
\begin{array}{c}
(Y, \mathcal{Z}, \alpha^h) \\
\downarrow{\scriptstyle H} \\
(Y, (Y_K, \mathcal{Z}, \alpha^h), \mathrm{id}).
\end{array}$$

is commutative up to a natural isomorphism given by the α's. Moreover, H is an equivalence, because the functor $(Y, (Z, \mathcal{Z}, \beta), \gamma) \mapsto (Y, \mathcal{Z}, \beta \circ \gamma_{K^h_{S,s}})$ is inverse to H. Thus, the restriction of G to appropriate subcategories as in (a) and (b) is an equivalence if and only if $(\mathrm{id}, B, \mathrm{id})$ is, which is the case if the restriction of B is an equivalence. It remains to prove

Claim 4.1.1. Let $B\colon \mathscr{D} \to \mathscr{D}^h$ be the base change functor.

(a) When restricted to the full subcategory of $\mathcal{O}_{S,s}$-schemes, B is an equivalence onto the full subcategory of triples of schemes that admit a quasi-affine open covering. The analogous conclusion holds with $\mathcal{O}^h_{S,s}$, $K^h_{S,s}$, and $\mathscr{D}^h$ replaced by $\widehat{\mathcal{O}}_{S,s}$, $\widehat{K}_{S,s}$, and $\mathscr{D}\widehat{\ }$.

(b) When restricted to the full subcategory of $\mathcal{O}_{S,s}$-algebraic spaces of finite presentation, B is an equivalence onto the full subcategory of triples involving only algebraic spaces of finite presentation.

To complete the proof of Lemma 4.1, we prove Claim 4.1.1:

(a) See [BLR90, §6.2 Prop. D.4 (b)].

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

Remarks.

4.2. As is immediate from fpqc descent, if $\mathcal{P}$ is a property of morphisms of schemes (resp., algebraic spaces) that is stable under base change and is fpqc local on the base, then analogues of (a) (resp., (b)) hold after restricting further to subcategories involving only schemes (resp., algebraic spaces) possessing $\mathcal{P}$.

4.3. The functor F commutes with fiber products since those in the target category are formed componentwise. This continues to hold after restricting to the subcategories of (a)[5] and (b), and also further to subcategories of schemes or algebraic spaces possessing $\mathcal{P}$ as in 4.2 if $\mathcal{P}$ is in addition stable under composition. In particular, we obtain

Corollary 4.4. *In the notation of Lemma 4.1, the functor*

$$\mathcal{G} \mapsto (\mathcal{G}_V, \mathcal{G}_{\mathcal{O}_{S,s_1}}, \dots, \mathcal{G}_{\mathcal{O}_{S,s_n}}, \alpha_i\colon (\mathcal{G}_V)_{K_{S,s_i}} \xrightarrow{\sim} (\mathcal{G}_{\mathcal{O}_{S,s_i}})_{K_{S,s_i}} \text{ for } 1 \leqslant i \leqslant n) \tag{4.4.1}$$

is an equivalence of categories from the category of S-quasi-affine S-group schemes to the category of tuples consisting of a V-quasi-affine V-group scheme, a quasi-affine $\mathcal{O}_{S,s_i}$-group scheme for each i, and isomorphisms $\alpha_1, \dots, \alpha_n$ 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 $\widehat{K}_{S,s_i}$. If $\mathcal{P}$ is a property of morphisms of schemes stable under base change and composition and fpqc local on the base, the same conclusions hold after restricting to subcategories involving only quasi-affine (over their bases) group schemes possessing $\mathcal{P}$.

5. Models of finite group schemes over global bases

Let S be a connected Dedekind scheme, K its function field, and G a finite commutative K-group scheme. We study separated quasi-finite flat S-group schemes $\mathcal{G}$ equipped with an isomorphism $G \xrightarrow{\sim} \mathcal{G}_K$. Propositions 2.10 and A.11 show that such a $\mathcal{G}$ is commutative and allow to assume, as we do for the rest of the section, that $\#G = p^m$ for some prime p, in which case $\mathcal{G}$ is killed by p^m. If S is the spectrum of the ring of integers of a finite extension of $\mathbb{Q}_p$, finite flat $\mathcal{G}$ are the subject of a vast body of literature starting with [TO70] and [Ray74]. The goal of the present section is to use Corollary 4.4 to transfer some of the known results over local bases to those over global ones. Since we cannot prove much otherwise, we assume that $\operatorname{char} K \neq p$.

[5]For (a), a quasi-affine open covering of the fiber product tuple $T_1 \times_{T_2} T_3$ is given by the fiber products of the opens in coverings of T_1, T_2, and T_3 and is indexed by $J_1 \times J_2 \times J_3$, where J_i indexes a covering of T_i.

5.1. *S*-**models.** Let $V := S[\frac{1}{p}]$ be the open subscheme of S obtained by inverting p; the points $s_1, \ldots, s_n$ of $S - V$ have residue characteristic p. A commutative quasi-finite S-group scheme $\mathcal{G}$ with $\mathcal{G}_K$ of p-power order is an *S-model* (of its generic fiber) if $\mathcal{G}_V \to V$ is a Néron model and each $\mathcal{G}_{\mathcal{O}_{S,s_i}} \to \operatorname{Spec} \mathcal{O}_{S,s_i}$ is finite flat. An S-model is separated and flat because these properties are fpqc local; it is also S-affine due to [SGA $3_{\text{I new}}$, XXV, 4.1] (applied to the homomorphism towards the zero group). A morphism of S-models is a morphism of S-group schemes. A commutative finite flat S-group scheme of p-power order is an S-model due to Propositions 2.4 and A.9; allowing $\mathcal{G}_V \to V$ to be Néron instead of finite flat amounts to allowing ramification away from p, cf. Proposition 2.15.

Proposition 5.2. *Let $\mathcal{G}$ and $\mathcal{H}$ be S-models.*

(a) A morphism of S-models $\mathcal{G} \to \mathcal{H}$ is determined by its generic fiber.

(b) A sheaf of abelian groups $\mathcal{E}$ on S_{fppf} that is an extension of S-models $0 \to \mathcal{H} \to \mathcal{E} \to \mathcal{G} \to 0$ is represented by an S-model.

Proof.

(a) This is a special case of Proposition 2.10 (e).

(b) By Proposition A.8, $\mathcal{E}$ is represented by a quasi-finite S-group scheme which is finite flat over each $\mathcal{O}_{S,s_i}$. Since $\mathcal{E}_K$ is of p-power order, $\mathcal{E}$ is an S-model by Proposition 2.5. □

5.3. *S*-**models of a fixed** G. These are S-models $\mathcal{G} \to S$ equipped with a K-group scheme isomorphism $\alpha\colon G \xrightarrow{\sim} \mathcal{G}_K$; their morphisms are required to be compatible with the α's. Let $\mathscr{M}(G,S)$ be the resulting category of S-models of G; by Proposition 5.2 (a), the objects of $\mathscr{M}(G,S)$ have no nontrivial automorphisms. By Proposition 2.15 (a), $\mathscr{M}(G,V)$ is the terminal category. Note that $\mathscr{M}(G,\mathcal{O}_{S,s_i})$, $\mathscr{M}(G_{K^h_{S,s_i}},\mathcal{O}^h_{S,s_i})$, and $\mathscr{M}(G_{\hat{K}_{S,s_i}},\hat{\mathcal{O}}_{S,s_i})$ are simply the categories of finite flat models of the base changed G, where $K^h_{S,s_i} := \operatorname{Frac}\mathcal{O}^h_{S,s_i}$ and $\hat{K}_{S,s_i} := \operatorname{Frac}\hat{\mathcal{O}}_{S,s_i}$.

Theorem 5.4. *The base change functors*

$$\mathscr{M}(G,S) \to \mathscr{M}(G,\mathcal{O}_{S,s_1}) \times \cdots \times \mathscr{M}(G,\mathcal{O}_{S,s_n}),$$
$$\mathscr{M}(G,S) \to \mathscr{M}(G_{K^h_{S,s_1}},\mathcal{O}^h_{S,s_1}) \times \cdots \times \mathscr{M}(G_{K^h_{S,s_n}},\mathcal{O}^h_{S,s_n}),$$
$$\mathscr{M}(G,S) \to \mathscr{M}(G_{\hat{K}_{S,s_1}},\hat{\mathcal{O}}_{S,s_1}) \times \cdots \times \mathscr{M}(G_{\hat{K}_{S,s_n}},\hat{\mathcal{O}}_{S,s_n})$$

are equivalences of categories.

Proof. This follows from Corollary 4.4 by restricting the functors there to appropriate subcategories; the cases of henselizations and completions being analogous, we explicate that of localizations. Restrict (4.4.1) to the full subcategories of group schemes that are finite flat over each $\mathcal{O}_{S,s_i}$ and are Néron models over V with K-fiber isomorphic to G. At this point, making the latter isomorphism part of the data of an object identifies the source category with $\mathscr{M}(G,S)$ and the target category with $\mathscr{M}(G,\mathcal{O}_{S,s_1}) \times \cdots \times \mathscr{M}(G,\mathcal{O}_{S,s_n})$ (both up to equivalences). □

Remark 5.5. Theorem 5.4 continues to hold after relaxing the definition of an S-model by requiring it to be separated quasi-finite flat over each $\mathcal{O}_{S,s_i}$ (and Néron over V). Indeed, such an S-model is affine [SGA $3_{\text{I new}}$, XXV, 4.1], so Corollary 4.4 still applies.[6]

[6]Reliance on loc. cit. here and in §5.1 is superficial: Corollary 4.4 holds with "affine" replaced by "quasi-affine" throughout, whereas a separated quasi-finite S-scheme is quasi-affine [EGA IV_3, 8.11.2].

5.6. Integrally closed subdomains R of a number field K. Necessarily, R is the ring of Σ-integers $\mathcal{O}_{K,\Sigma}$ for a possibly infinite set Σ of finite places of K, namely, the places appearing in prime factorizations of denominators of elements of R. The Dedekind scheme $\operatorname{Spec} R$ has function field K; its nongeneric points correspond to finite places v of K not in Σ. The nonempty open subschemes of $\operatorname{Spec} \mathcal{O}_K$ are the $\operatorname{Spec} \mathcal{O}_{K,\Sigma}$ as above with finite Σ.

Proposition 5.7. *Suppose that K is a number field and $S = \operatorname{Spec} \mathcal{O}_{K,\Sigma}$ for an integrally closed subdomain $\mathcal{O}_{K,\Sigma} \subset K$ (as in §5.6). Fix a finite commutative K-group scheme G of p-power order (equivalently, a $\operatorname{Gal}(\overline{K}/K)$-representation $G(\overline{K})$ on a finite p-primary abelian group).*

(a) A tuple consisting of a finite flat $\mathcal{O}_v$-model of G_{K_v} for each $v \notin \Sigma$ above p arises from a unique $\mathcal{O}_{K,\Sigma}$-model of G. Up to isomorphism there are only finitely many $\mathcal{O}_{K,\Sigma}$-models of G.

(b) A finite flat $\mathcal{O}_{K,\Sigma}$-model of G exists if and only if $G(\overline{K})$ is unramified outside of $\Sigma \cup \{v \mid p\}$ and a finite flat $\mathcal{O}_v$-model of G_{K_v} exists for each $v \notin \Sigma$ above p. In this case every $\mathcal{O}_{K,\Sigma}$-model of G is finite flat.

(c) If each $v \notin \Sigma$ above p has absolute ramification index $< p-1$, then up to isomorphism there is at most one $\mathcal{O}_{K,\Sigma}$-model of G.

(d) For $\mathcal{O}_{K,\Sigma}$-models $\mathcal{G}_1$ and $\mathcal{G}_2$ of G, a tuple consisting of a morphism $(\mathcal{G}_1)_{\mathcal{O}_v} \to (\mathcal{G}_2)_{\mathcal{O}_v}$ of $\mathcal{O}_v$-models of G_{K_v} for each $v \notin \Sigma$ above p arises from a unique morphism $\mathcal{G}_1 \to \mathcal{G}_2$ of $\mathcal{O}_{K,\Sigma}$-models of G, in which case we write $\mathcal{G}_1 \geqslant \mathcal{G}_2$. There is at most one morphism $\mathcal{G}_1 \to \mathcal{G}_2$, so $\geqslant$ defines a partial order on the set of isomorphism classes of $\mathcal{O}_{K,\Sigma}$-models of G.

(e) Two $\mathcal{O}_{K,\Sigma}$-models $\mathcal{G}_1$ and $\mathcal{G}_2$ of G have the supremum and the infimum with respect to $\geqslant$.

(f) If an $\mathcal{O}_{K,\Sigma}$-model of G exists, then the set of isomorphism classes of $\mathcal{O}_{K,\Sigma}$-models of G has the unique maximum $\mathcal{G}^+$ and the unique minimum $\mathcal{G}^-$ with respect to $\geqslant$.

Proof. Combine Theorem 5.4 with

(a) Finiteness of the set of isomorphism classes of objects of $\mathscr{M}(G_{K_v}, \mathcal{O}_v)$ [Maz70, top of p. 221];

(b) Proposition 2.15 (b);

(c) The corresponding local result [Ray74, Thm. 3.3.3];

(d) Proposition 5.2 (a);

(e) The corresponding local result [Ray74, Prop. 2.2.2];

(f) The corresponding local result [Ray74, Cor. 2.2.3]. □

Remark 5.8. In the case of finite flat models of order p, Proposition 5.7 (a) is [TO70, Lemma 4].

Proposition 5.9 (Theorem 1.1 (b)). *Let L/K be an extension of number fields, $\phi\colon A \to B$ a K-isogeny between abelian varieties, $S := \operatorname{Spec} \mathcal{O}_L$, and $\mathcal{A}^L[\phi]$ 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 $p \mid \deg \phi$, where $e_p := \max_{v|p} e_v$ and e_v is the absolute ramification index of v.

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. The p-primary decomposition of $\mathcal{A}^L[\phi]$ from Proposition A.11 induces the K-rational p-primary decomposition of the generic fiber, so by Proposition 2.10 (a) and Corollary 3.8, the factors of the former are $\mathcal{A}^L[\psi]$ for K-isogenies ψ of prime power degree, reducing to the case $\deg\phi = p^n$.

By Corollaries 3.8 and 3.9, $\mathcal{A}^L[\phi]_{S[\frac{1}{p}]}$ is the Néron model of the finite étale $A[\phi]_L$, whereas $\mathcal{A}^L[\phi]_{\mathcal{O}_w}$ is finite flat for every place w of L above p. In conclusion, $\mathcal{A}^L[\phi]$ is an S-model of $A[\phi]_L$, and, due to Proposition 5.7 (c), the claim follows if $L = K$. Thus, $\mathcal{A}^K[\phi]$ is determined, and it remains to apply Proposition 5.7 (a): indeed, an abelian scheme is a Néron model (compare Proposition 2.4), so in general $\mathcal{A}^L[\phi]_{\mathcal{O}_w} = (\mathcal{A}^K[\phi]_{\mathcal{O}_v})_{\mathcal{O}_w}$ where v is the place of K below w. □

Remarks.

5.10. For a global field K of positive characteristic prime to $\deg\phi$, the analogue of Proposition 5.9 is a special case of Corollary 3.9.

5.11. Dropping (ii) but keeping (i) (or assuming instead of (i) and (ii) that A has semiabelian 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 $v \mid \deg\phi$ (in the semiabelian reduction case one has to use Remark 5.5 instead of Proposition 5.7 (a)).

Although (ii) excludes the $2 \mid \deg\phi$ cases, Remark 5.11 can sometimes overcome this:

Example 5.12. 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 $A[2]_{K_v}$ has at most one K_v-subgroup of order 2 for every such v. We show that under this assumption the conclusion of Proposition 5.9 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 5.11 reduces to proving that $\mathcal{A}^K[2]_{\mathcal{O}_v}$ is determined by $A[2]_{K_v}$ for each $v \mid 2$; one of the key assumptions is the unramifiedness of $K_v/\mathbb{Q}_2$. We analyze the ordinary and supersingular reduction cases separately; this is permissible since the 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], $A[2]_{K_v^{\mathrm{nr}}}$ is irreducible and also an $\mathbb{F}_4$-vector space scheme of dimension 1. By [Ray74, 3.3.2 3°], $\mathcal{A}[2]_{\mathcal{O}_v^{\mathrm{nr}}}$ is its unique finite flat $\mathcal{O}_v^{\mathrm{nr}}$-model. By schematic density (cf. Proposition 2.10 (e)) and limit considerations, the descent datum on $\mathcal{A}^K[2]_{\mathcal{O}_v^{\mathrm{nr}}}$ with respect to $\mathcal{O}_v^{\mathrm{nr}}/\mathcal{O}_v$ is uniquely determined by its restriction to the generic fiber, which in turn is determined by $A[2]_{K_v}$. Fpqc descent along $\mathcal{O}_v^{\mathrm{nr}}/\mathcal{O}_v$ 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, compare Example 6.14).

In the remainder of the section we collect several other results about S-models which, due to Corollary 4.4, are consequences of their local counterparts. Unlike in Proposition 5.7, we no longer fix G.

Proposition 5.13. *Suppose that K is a number field and $S = \operatorname{Spec}\mathcal{O}_{K,\Sigma}$ for an integrally closed subdomain $\mathcal{O}_{K,\Sigma} \subset K$ (as in §5.6).*

(a) Every automorphism of G extends to an automorphism of its maximal and minimal $\mathcal{O}_{K,\Sigma}$-models $\mathcal{G}^+$ and $\mathcal{G}^-$ (cf. Proposition 5.7 (f)).

If $e_v < p-1$ for every $v \notin \Sigma$ above p, then

(b) For $\mathcal{O}_{K,\Sigma}$-models $\mathcal{G}$ and $\mathcal{H}$, every homomorphism $\mathcal{G}_K \to \mathcal{H}_K$ extends uniquely to $\mathcal{G} \to \mathcal{H}$;

(c) For $\mathcal{O}_{K,\Sigma}$-models $\mathcal{G}$ and $\mathcal{H}$, the map $\mathrm{Ext}^1_{\mathcal{O}_{K,\Sigma}}(\mathcal{G},\mathcal{H}) \to \mathrm{Ext}^1_K(\mathcal{G}_K,\mathcal{H}_K)$ (extensions of sheaves of abelian groups on the fppf site) is injective;

(d) The kernel of a morphism of $\mathcal{O}_{K,\Sigma}$-models is again a $\mathcal{O}_{K,\Sigma}$-model;

(e) Finite flat $\mathcal{O}_{K,\Sigma}$-models form an abelian subcategory of the category of abelian sheaves on S_{fppf} that is equivalent by the exact generic fiber functor to the category of finite discrete p-primary $\mathrm{Gal}(\overline{K}/K)$-modules that are unramified outside $\Sigma \cup \{v \mid p\}$ and flat at all $v \notin \Sigma$ above p (i.e., whose restrictions to $\mathrm{Gal}(\overline{K_v}/K_v)$ admit finite flat $\mathcal{O}_v$-models for all $v \notin \Sigma$).

Proof.

(a) Use Corollary 4.4 to replace morphisms of $\mathcal{O}_{K,\Sigma}$-models by morphisms of tuples as in (4.4.1), and then use the Néron property to identify V-morphisms of the first entry with their generic fibers. It remains to prove the corresponding well-known local result, as can be done by considering Hopf algebras.

(b) After reasoning as in (a), apply the corresponding local result [Ray74, 3.3.6 1°].

(c) Combine (b) and Proposition 5.2 (b).

(d) Combine Proposition 2.15 (c) and the corresponding local result [Ray74, 3.3.6 1°].

(e) The full faithfulness and essential surjectivity follow from (b), Proposition 2.15 (b) and Proposition 5.7 (a). For the abelian subcategory claim, existence of products, kernels, and cokernels within the subcategory follows from (d), Proposition 2.15 (d), and [Ray74, 3.3.6 1°]. The generic fiber functor is exact because it is compatible with short exact sequences. □

5.14. $\mathbb{F}$-vector space schemes. Fix a characteristic p finite field $\mathbb{F}$. A group scheme G is an *$\mathbb{F}$-vector space scheme* if its functor of points factors through the category of $\mathbb{F}$-vector spaces (in particular, G is commutative). An S-model of G that has an $\mathbb{F}$-vector space scheme structure extending that of G is an *$\mathbb{F}$-vector space S-model of G*. Classification of finite locally free $\mathbb{F}$-vector space schemes of rank $\#\mathbb{F}$ over certain bases is the subject of [Ray74]. Due to the restriction [Ray74, p. 245 (★)], typically this classification does not apply over global bases. We use Corollary 4.4 to transfer some of the local results to the global setting.

Proposition 5.15. *Suppose that K is a number field and $S = \mathrm{Spec}\,\mathcal{O}_{K,\Sigma}$ for an integrally closed subdomain $\mathcal{O}_{K,\Sigma} \subset K$ (as in §5.6). Fix a finite $\mathbb{F}$-vector space K-scheme G.*

(a) If the maximal and minimal $\mathcal{O}_{K,\Sigma}$-models $\mathcal{G}^+$ and $\mathcal{G}^-$ of G exist (cf. Proposition 5.7 (f)), they are $\mathbb{F}$-vector space $\mathcal{O}_{K,\Sigma}$-models of G.

(b) If $\#G = \#\mathbb{F}$ and for every $v \notin \Sigma$ above p, either $e_v < p-1$, or $e_v = p-1$ and the $\mathrm{Gal}(\overline{K}_v/K_v)$-representation $G(\overline{K}_v)$ is simple, then the $\mathbb{F}$-vector space scheme structure of G extends to every $\mathcal{O}_{K,\Sigma}$-model.

Proof.

(a) Apply Proposition 5.13 (a) to the automorphisms of G given by the elements of $\mathbb{F}^\times$.

(b) To extend the automorphisms of G given by the elements of $\mathbb{F}^\times$ to an $\mathcal{O}_{K,\Sigma}$-model of G, argue as in the proof of Proposition 5.13 (a) and apply [Ray74, 3.3.2 2° et 3°]. □

5.16. Kisin's moduli. Suppose that K is a number field. Fix a continuous $\mathrm{Gal}(\overline{K}/K)$-representation on a finite dimensional $\mathbb{F}$-vector space V, which identifies with an étale $\mathbb{F}$-vector space K-scheme. For a place v of K above p, Kisin constructed [Kis09, 2.1.13] a projective $\mathbb{F}$-scheme $\mathscr{GR}_{V_{K_v},0}$ whose $\mathbb{F}'$-points are in bijection with isomorphism classes of $\mathbb{F}'$-vector space $\mathcal{O}_v$-models of the extension of scalars $(V_{K_v})_{\mathbb{F}'}$ for every finite extension $\mathbb{F}'/\mathbb{F}$ (this alone need not determine $\mathscr{GR}_{V_{K_v},0}$).

Proposition 5.17. *Suppose that K is a number field and $S = \operatorname{Spec}\mathcal{O}_{K,\Sigma}$ for an integrally closed subdomain $\mathcal{O}_{K,\Sigma} \subset K$ (as in §5.6). Fix a finite $\mathbb{F}$-vector space K-scheme V and set*

$$\mathscr{K}_V := \prod_{\substack{v\notin\Sigma\\ v|p}} \mathscr{GR}_{V_{K_v},0}.$$

For every finite extension $\mathbb{F}'/\mathbb{F}$, the $\mathbb{F}'$-points of the projective $\mathbb{F}$-scheme $\mathscr{K}_V$ are in bijection with isomorphism classes of $\mathbb{F}'$-vector space $\mathcal{O}_{K,\Sigma}$-models of the extension of scalars $V_{\mathbb{F}'}$.

Proof. An $\mathbb{F}'$-vector space $\mathcal{O}_{K,\Sigma}$-model of $V_{\mathbb{F}'}$ is an $\mathcal{O}_{K,\Sigma}$-model of $V_{\mathbb{F}'}$ to which the automorphisms of $V_{\mathbb{F}'}$ given by the elements of $\mathbb{F}'^{\times}$ extend. Due to Corollary 4.4 and the Néron property, it is equivalent to require this for the base changed $\mathcal{O}_v$-models for every $v \notin \Sigma$ above p. Thus, the third equivalence of Theorem 5.4 for $G = V_{\mathbb{F}'}$ and $S = \operatorname{Spec}\mathcal{O}_{K,\Sigma}$ restricts to that between categories involving only $\mathbb{F}'$-vector space models. □

Remark 5.18. Proposition 5.17 and the Weil conjectures prove the existence of algebraic integers $\alpha_1, \ldots, \alpha_a$ and $\beta_1, \ldots, \beta_b$ such that for every n and a degree n extension $\mathbb{F}'/\mathbb{F}$, the number of isomorphism classes of $\mathbb{F}'$-vector space $\mathcal{O}_{K,\Sigma}$-models of $V_{\mathbb{F}'}$ is $\alpha_1^n + \cdots + \alpha_a^n - \beta_1^n - \ldots - \beta_b^n$.

5.19. p-divisible S-models. Returning to general S, a *p-divisible S-model of height h* is a sequence $\mathcal{G} = (\mathcal{G}[p^n], i_n)_{n\geqslant 0}$ of S-models $\mathcal{G}[p^n]$ for which $\#\mathcal{G}[p^n]_K = p^{nh}$ and

$$0 \to \mathcal{G}[p^n] \xrightarrow{i_n} \mathcal{G}[p^{n+1}] \xrightarrow{p^n} \mathcal{G}[p^{n+1}] \tag{5.19.1}$$

is exact for every n. A morphism $\mathcal{G} \to \mathcal{H}$ of p-divisible S-models (of possibly distinct heights) is a compatible with the i_n's sequence of morphisms $\mathcal{G}[p^n] \to \mathcal{H}[p^n]$ of S-models; thus,

$$\operatorname{Hom}(\mathcal{G}, \mathcal{H}) = \varprojlim \operatorname{Hom}(\mathcal{G}[p^n], \mathcal{H}[p^n]).$$

Evidently, $\mathcal{G}_{\mathcal{O}_{S,s_i}}$, $\mathcal{G}_{\mathcal{O}^h_{S,s_i}}$, $\mathcal{G}_{\hat{\mathcal{O}}_{S,s_i}}$, and $\mathcal{G}_K$ are p-divisible groups of height h over respective bases. Since $\operatorname{char} K \neq p$, the continuous $\mathrm{Gal}(\overline{K}/K)$-representation $\mathcal{G}(\overline{K}) := \varprojlim \mathcal{G}[p^n](\overline{K})$ on a finite free $\mathbb{Z}_p$-module of rank h determines the étale $\mathcal{G}_K$. The category of p-divisible S-models contains that of p-divisible groups over S as the full subcategory of $\mathcal{G}$ with all $\mathcal{G}[p^n]$ finite; much like in §5.1, the difference between the two categories stems from the possible ramification of $\mathcal{G}(\overline{K})$ away from p for an arbitrary p-divisible S-model $\mathcal{G}$.

Tate's full faithfulness theorem for p-divisible groups continues to hold for p-divisible S-models:

Proposition 5.20. *The generic fiber functor from the category of p-divisible S-models to that of p-divisible groups over K is fully faithful, i.e., for p-divisible S-models $\mathcal{G}$ and $\mathcal{H}$, every $\mathbb{Z}_p$-linear homomorphism $\mathcal{G}(\overline{K}) \to \mathcal{H}(\overline{K})$ of $\mathrm{Gal}(\overline{K}/K)$-representations is induced from a unique morphism $\mathcal{G} \to \mathcal{H}$. In particular, a p-divisible S-model is determined by its generic fiber.*

Proof. Due to Corollary 4.4 and the Néron property, giving a morphism $\mathcal{G} \to \mathcal{H}$ amounts to giving $\mathcal{G}(\overline{K}) \to \mathcal{H}(\overline{K})$ (i.e., a morphism of the generic fiber p-divisible groups) together with its extensions to morphisms $\mathcal{G}_{\mathcal{O}_{S,s_i}} \to \mathcal{H}_{\mathcal{O}_{S,s_i}}$. The latter exist and are unique due to [Tat67, Thm. 4]. □

Raynaud's criterion for existence of a p-divisible model continues to hold, too:

Proposition 5.21. *For a p-divisible group $G = (G[p^n], i_n)_{n\geq 0}$ over K, the following are equivalent:*

(a) G has a p-divisible S-model;

(a′) Each $G[p^n]$ has an S-model;

(b) G extends to a p-divisible group over every $\mathcal{O}_{S,s_i}$;

(b′) Each $G[p^n]$ has a finite flat model over every $\mathcal{O}_{S,s_i}$.

The same conclusion holds if in (b) and (b′) one replaces G, $G[p^n]$, and $\mathcal{O}_{S,s_i}$ by $G_{K^h_{S,s_i}}$, $G[p^n]_{K^h_{S,s_i}}$, and $\mathcal{O}^h_{S,s_i}$ or by $G_{\widehat{K}_{S,s_i}}$, $G[p^n]_{\widehat{K}_{S,s_i}}$, and $\widehat{\mathcal{O}}_{S,s_i}$.

Proof. We treat the case of localizations; those of henselizations and completions are similar.

By [Ray74, 2.3.1], (b)⇔(b′), whereas (a)⇒(a′)⇒(b′) are evident. We prove the remaining (b)⇒(a). By Theorem 5.4, the layers of the extensions over $\mathcal{O}_{S,s_i}$ give rise to S-models $\mathcal{G}[p^n]$ of $G[p^n]$, whereas Corollary 4.4 and the Néron property furnish extensions

$$i_n\colon \mathcal{G}[p^n] \to \mathcal{G}[p^{n+1}] \quad \text{of} \quad i_n\colon G[p^n] \to G[p^{n+1}].$$

The remaining exactness of (5.19.1) can be checked fpqc locally and hence follows from Proposition 2.15 (c) and the definition of a p-divisible group over $\mathcal{O}_{S,s_i}$. □

6. Closed subgroups of Néron models

Let S be a connected Dedekind scheme and K its function field. The main result of this section, Theorem 6.1, yields an obstruction for an S-group scheme $\mathcal{G}$ to occur as a closed subgroup of a Néron (lft) model over S. The obstruction is trivial for finite flat $\mathcal{G}$, and we investigate the possibility of commutative such $\mathcal{G}$ always occurring as closed subgroups of Néron models in the discussion following Question 6.5.

Theorem 6.1. *For an S-group scheme $\mathcal{G}$, the map*

$$H^1_{\text{fppf}}(S, \mathcal{G}) \to H^1_{\text{fppf}}(K, \mathcal{G}_K) \tag{6.1.1}$$

(cf. §A.4) is injective if there is a closed immersion $\mathcal{G} \hookrightarrow \mathcal{X}$ of S-group schemes with either

(a) $\mathcal{X}$ a Néron lft model, or

(b) $\mathcal{X}$ commutative satisfying

(i) $\mathcal{X} \to S$ is separated and locally of finite presentation,

(ii) $\mathcal{X}(S) \to \mathcal{X}(K)$ is surjective, and

(iii) $H^1_{\text{fppf}}(S, \mathcal{X}) \to H^1_{\text{fppf}}(K, \mathcal{X}_K)$ is injective.

Proof. In both cases, by replacing $\mathcal{G}$ with the schematic image of its generic fiber and invoking Proposition 2.11, we may and do assume that $\mathcal{G}$ is flat.

(a) In terms of descent data with respect to a trivializing fppf $S' \to S$, an fppf $\mathcal{G}$-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 fppf $\mathcal{X}$-torsor $\mathcal{T}^{\mathcal{X}}$; by descent, there is a $\mathcal{G}$-equivariant closed immersion $\mathcal{T} \subset \mathcal{T}^{\mathcal{X}}$.

For generically isomorphic fppf $\mathcal{G}$-torsors $\mathcal{T}_1$ and $\mathcal{T}_2$, take a common trivializing $S' \to S$. For the injectivity of (6.1.1), we seek a $\mathcal{G}$-torsor isomorphism $\alpha\colon \mathcal{T}_1 \xrightarrow{\sim} \mathcal{T}_2$. In terms of descent data, an isomorphism $\alpha_K\colon (\mathcal{T}_1)_K \xrightarrow{\sim} (\mathcal{T}_2)_K$ of right $\mathcal{G}_K$-torsors is induced by left multiplication by a certain $h \in \mathcal{G}(S'_K)$; its 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 2.19, β_K extends to an $\mathcal{X}$-torsor isomorphism $\beta\colon \mathcal{T}_1^{\mathcal{X}} \xrightarrow{\sim} \mathcal{T}_2^{\mathcal{X}}$. Due to flatness of $\mathcal{T}_i \to S$, the schematic image of $(\mathcal{T}_i)_K \to \mathcal{T}_i^{\mathcal{X}}$ is $\mathcal{T}_i$ [SP, Lemma 089E]. Thus, β restricts to a desired $\alpha\colon \mathcal{T}_1 \xrightarrow{\sim} \mathcal{T}_2$ by Lemma 2.8.

(b) By Proposition A.13 (d), $\mathcal{Q} := \mathcal{X}/\mathcal{G}$ is a commutative separated S-group algebraic space. By Proposition 2.10 (e), q is injective in

$$\begin{array}{ccccccc}
\mathcal{X}(S) & \longrightarrow & \mathcal{Q}(S) & \longrightarrow & H^1_{\mathrm{fppf}}(S,\mathcal{G}) & \longrightarrow & H^1_{\mathrm{fppf}}(S,\mathcal{X}) \\
\downarrow & & \downarrow q & & \downarrow & & \downarrow \\
\mathcal{X}(K) & \longrightarrow & \mathcal{Q}(K) & \longrightarrow & H^1_{\mathrm{fppf}}(K,\mathcal{G}_K) & \longrightarrow & H^1_{\mathrm{fppf}}(K,\mathcal{X}_K),
\end{array}$$

and it remains to apply the four lemma. □

Since a closed subalgebraic space of a scheme is a scheme, Proposition 2.18 and the proof of Theorem 6.1 (a) reprove a special case of [Ana73, 4.D]:

Corollary 6.2. *Every torsor under a closed subgroup scheme of a Néron model over S is representable by a scheme.*

Theorem 6.1 gives no obstruction for proper $\mathcal{G}$:

Proposition 6.3. *For a proper flat S-group scheme $\mathcal{G}$,*

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

(cf. §A.4) is injective.

Proof. For an fppf $\mathcal{G}$-torsor $\mathcal{T}$, let ${}^{\mathcal{T}}\mathcal{G} := \mathcal{A}ut_{\mathcal{G}}\mathcal{T}$ (the fppf sheaf of $\mathcal{G}$-automorphisms of $\mathcal{T}$) be the corresponding *inner twist* of $\mathcal{G}$ (compare [Gir71, III.1.4.8]). Since ${}^{\mathcal{T}}\mathcal{G}$ is fppf locally isomorphic to $\mathcal{G}$, it is a proper flat S-group scheme [SP, Lemma 04SK], [Ana73, 4.B]. By [Gir71, III.2.6.3, V.1.5.1.2], there is a commutative diagram

$$\begin{array}{ccc}
H^1_{\mathrm{fppf}}(S,\mathcal{G}) & \xrightarrow{\sim} & H^1_{\mathrm{fppf}}(S,{}^{\mathcal{T}}\mathcal{G}) \\
\downarrow & & \downarrow \\
H^1_{\mathrm{fppf}}(K,\mathcal{G}_K) & \xrightarrow{\sim} & H^1_{\mathrm{fppf}}(K,{}^{\mathcal{T}}\mathcal{G}_K)
\end{array}$$

in which the horizontal "subtraction of the class of $\mathcal{T}$" (resp., $\mathcal{T}_K$) isomorphisms map the class of $\mathcal{T}$ (resp., $\mathcal{T}_K$) to the class of the trivial torsor. Replacing $\mathcal{G}$ by ${}^{\mathcal{T}}\mathcal{G}$ and a generically isomorphic to $\mathcal{T}$ fppf $\mathcal{G}$-torsor $\mathcal{T}'$ by the corresponding ${}^{\mathcal{T}}\mathcal{G}$-torsor, it remains to argue that a generically trivial $\mathcal{G}$-torsor $\mathcal{T}$ is trivial. We fix such a $\mathcal{T}$, which is a scheme [Ana73, 4.D].

Fix a $p \in \mathcal{T}(K)$ with the intention of lifting it to a $P \in \mathcal{T}(S)$. Since $\mathcal{T}$ inherits properness from $\mathcal{G}$, the valuative criterion extends p to $p_s \in \mathcal{T}(\mathcal{O}_{S,s})$ for every $s \in S$. Each p_s spreads out to a neighborhood U_s of s, compatibly on intersections $U_s \cap U_{s'}$ by Proposition 2.10 (e), and glueing gives a desired P. □

Remark 6.4. Proposition 6.3 applies to finite flat S-group schemes $\mathcal{G}$. Its conclusion also holds for the commutative S-models of §5.1: letting $\mathcal{T}$ be a generically trivial torsor under an S-model $\mathcal{G}$, a $P \in \mathcal{T}(K)$ extends to an $S[\frac{1}{p}]$-point due to Proposition 2.19 and also to an $\mathcal{O}_{S,s_i}$-point for each s_i due to properness of $\mathcal{T}_{\mathcal{O}_{S,s_i}}$; hence, Lemma 1.1 (a) extends P to an S-point trivializing $\mathcal{T}$. In conclusion, Theorem 6.1 furnishes no obstruction regarding Questions 6.5 and 6.5′:

Question 6.5. *For a number field K, is every commutative finite flat $\mathcal{O}_K$-group scheme a closed subgroup of a Néron model of an abelian variety?*

Question 6.5′. *For a prime p and a number field K, is every $\mathcal{O}_K$-model (cf. §5.1) a closed subgroup of a Néron model of an abelian variety?*

Remarks.

6.6. By Proposition A.11, Question 6.5′ generalizes Question 6.5.

6.7. The answers are negative if one insists on abelian schemes (which are Néron models, cf. Proposition 2.4): the only abelian scheme over $\mathbb{Z}$ is the trivial one [Fon85, p. 517 Corollaire], [Abr87, Thm. 5].

6.8. Over local rings embeddings of finite flat group schemes into abelian schemes are possible due to a theorem of Raynaud [BBM82, 3.1.1] (and [Mat89, 7.10]).

In the remainder of the section we discuss variants of these questions, settling the $K = \mathbb{Q}$ case:

Proposition 6.9. *Fix a prime $p \neq \operatorname{char} K$. If S has at most one point s of residue characteristic p, then every S-model $\mathcal{G}$ (cf. §5.1) is a closed subgroup of the Néron model $\mathcal{A}$ of an abelian variety $A = \mathcal{A}_K$ having good reduction at s (if s exists).*

Proof. If no such s exists, then $\mathcal{G}$ is a Néron model itself. Take a closed immersion $\mathcal{G}_K \hookrightarrow A$ into an abelian variety over K (construct it over a finite separable extension trivializing $\mathcal{G}$ and take restriction of scalars [CGP10, A.5.1, A.5.5, A.5.7, A.5.9], [BLR90, §7.6 Prop. 5 (f), (h)]). Letting $\mathcal{A} \to S$ be the Néron model of A and $\mathcal{H}$ the schematic image of $\mathcal{G}_K \to \mathcal{A}$, Propositions 2.10 and A.9 with Corollary 2.14 give the desired $\mathcal{G} \cong \mathcal{H}$.

If s exists, then [BBM82, 3.1.1] gives a closed immersion $i\colon \mathcal{G}_{\mathcal{O}_{S,s}} \hookrightarrow \mathcal{A}_{\mathcal{O}_{S,s}}$ of $\mathcal{O}_{S,s}$-group schemes into an abelian scheme, which by Proposition 2.4 is the Néron model of $A := (\mathcal{A}_{\mathcal{O}_{S,s}})_K$. Letting $\mathcal{A} \to S$ be the Néron model of A, Proposition 2.3 (a) justifies the notation, whereas i spreads out [EGA IV$_3$, 8.8.2 (i) et 8.10.5 (iv)] to a closed immersion $\mathcal{G}_U \hookrightarrow \mathcal{A}_U$ of U-group schemes for some open $U \subset S$ containing s. As in the first paragraph, the unique $\mathcal{G}_{S-\{s\}} \to \mathcal{A}_{S-\{s\}}$ extending $\mathcal{G}_K \hookrightarrow \mathcal{A}_K$ is a closed immersion and similarly over $U \cap (S - \{s\})$, so a desired closed immersion $\mathcal{G} \to \mathcal{A}$ results by glueing. □

Remarks.

6.10. For a prime $p \neq \operatorname{char} K$, let $S_{(p)}$ be the semilocal Dedekind scheme obtained from S by localizing away from p. The proof above continues to answer Question 6.5′ affirmatively as long as $\mathcal{G}_{S_{(p)}} \to S_{(p)}$ is a closed subgroup of the Néron model of an abelian variety.

6.11. The answer to Question 6.5 is negative if $\mathcal{G}$ is allowed to be separated quasi-finite flat. For instance, an open subgroup $\mathcal{G}$ of a finite étale $\mathcal{O}_K$-group scheme $\mathcal{N}$ with $\mathcal{G}_K = \mathcal{N}_K$ but $\mathcal{G} \neq \mathcal{N}$ cannot be a closed subgroup of a Néron model due to Proposition 2.4 and Corollary 2.14. To construct such $\mathcal{G}$, take $\mathcal{N} = \underline{\mathbb{Z}/p\mathbb{Z}}_{\mathcal{O}_K}$ and remove the closed subscheme complementary to the identity section in some nongeneric fiber.

6.12. For an S-flat closed subgroup $\mathcal{G}$ of a Néron model $\mathcal{X}$ and a smooth S-scheme T, due to Proposition 2.10 (c), $\mathcal{G}(T)$ identifies with the set of S-morphisms $T \to \mathcal{X}$ whose generic fiber factors through $\mathcal{G}_K$. In particular, $\mathcal{G}(T) \to \mathcal{G}_K(T_K)$ is bijective due to the Néron property of $\mathcal{X}$. Failure of this bijectivity obstructs realizing $\mathcal{G}$ as a closed subgroup of a Néron model. In Remark 6.11 this is witnessed with $T = \mathcal{N}$.

Question 6.13. *For local S, which commutative separated quasi-finite flat S-group schemes are closed subgroups of a Néron model?*

Example 6.14. We construct a commutative separated quasi-finite flat group scheme $\mathcal{G}$ over $S := \operatorname{Spec} \mathbb{Z}_p$ for which, due to Theorem 6.1, failure of the injectivity of $H^1_{\mathrm{fppf}}(S, \mathcal{G}) \to H^1_{\mathrm{fppf}}(K, \mathcal{G}_K)$ obstructs being a closed subgroup of a Néron model. Due to Corollary 2.14, we seek non-étale $\mathcal{G}$.

Since $1 \neq \mathbb{Z}_p^\times / \mathbb{Z}_p^{\times p} \cong H^1_{\mathrm{fppf}}(S, \mu_p) \cong \operatorname{Ext}^1_S(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ (extensions in the category of sheaves of $\mathbb{Z}/p\mathbb{Z}$-modules on S_{fppf}), there is a nonsplit extension

$$0 \to \mu_p \to \mathcal{H} \to \underline{\mathbb{Z}/p\mathbb{Z}}_S \to 0. \tag{6.14.1}$$

By Proposition A.8, $\mathcal{H}$ is represented by a finite flat S-group scheme. Let $U \subset \underline{\mathbb{Z}/p\mathbb{Z}}_S$ be the open subgroup obtained by removing the closed subscheme of the special fiber complementary to the identity section, set $\mathcal{G} := \mathcal{H} \times_{\underline{\mathbb{Z}/p\mathbb{Z}}_S} U$, and observe the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mu_p & \longrightarrow & \mathcal{G} & \longrightarrow & U & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mu_p & \longrightarrow & \mathcal{H} & \longrightarrow & \underline{\mathbb{Z}/p\mathbb{Z}}_S & \longrightarrow & 0. \end{array}$$

By construction, $\mathcal{G}$ is an open subgroup of $\mathcal{H}$, so it is separated quasi-finite flat (but not étale because it admits a nontrivial homomorphism from μ_p). It remains to argue that $H^1_{\mathrm{fppf}}(S, \mathcal{G}) \xrightarrow{a} H^1_{\mathrm{fppf}}(K, \mathcal{G}_K)$ is not injective. Since $\mathcal{H} \to S$ is proper and (6.14.1) is nonsplit, $\mathcal{H}(K) = \mathcal{H}(S) = \mu_p(S) = 0$. Therefore, since $\mathcal{H}/\mathcal{G} \cong \underline{\mathbb{Z}/p\mathbb{Z}}_S/U$, the injectivity of a would entail that of

$$(\underline{\mathbb{Z}/p\mathbb{Z}}_S/U)(S) \xrightarrow{b} (\underline{\mathbb{Z}/p\mathbb{Z}}_S/U)(K) = 0,$$

which fails because $(\underline{\mathbb{Z}/p\mathbb{Z}}_S/U)(S)$ contains $(\underline{\mathbb{Z}/p\mathbb{Z}}_S)(S) \cong \mathbb{Z}/p\mathbb{Z}$.

7. Selmer type descriptions of sets of torsors

The main result of this section is Theorem 7.2, which forms the basis of our approach to fppf cohomological interpretation of Selmer groups by describing certain sets of torsors by local conditions. In Proposition 7.5 it leads to a short reproof of a result of Mazur that gives étale (or fppf) cohomological interpretation of Shafarevich–Tate groups.

Lemma 7.1. *Let R be a discrete valuation ring, R^h its henselization, and set $K := \operatorname{Frac} R$ and $K^h := \operatorname{Frac} R^h$. For a flat R-group algebraic space $\mathcal{G}$ of finite presentation, if the horizontal arrows in*

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

(cf. §A.4) are injective, 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 quasi-affine.

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 Claim 4.1.1 (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

$$\mathcal{G} \times_R \mathcal{T} \to \mathcal{T} \times_R \mathcal{T}, \quad (g,t) \mapsto (gt,t) \tag{7.1.1}$$

is an isomorphism, because it is so over R^h. In the similar proof for $\widehat{R}$ and $\widehat{K}$, to apply Claim 4.1.1 one appeals to Proposition A.7. □

Let S be a connected Dedekind scheme and K its function field. As in §4, to clarify analogies in Theorem 7.2, we set $K_{S,s} := \operatorname{Frac} \mathcal{O}_{S,s}$ for a nongeneric $s \in S$.

Theorem 7.2. *For a flat S-group algebraic space $\mathcal{G}$ of finite presentation, if the horizontal arrows in (the products are indexed by the nongeneric $s \in S$)*

$$\begin{array}{ccc} H^1_{\mathrm{fppf}}(S,\mathcal{G}) & \hookrightarrow & H^1_{\mathrm{fppf}}(K,\mathcal{G}_K) \\ \downarrow & & \downarrow \\ \prod_s H^1_{\mathrm{fppf}}(\mathcal{O}_{S,s},\mathcal{G}_{\mathcal{O}_{S,s}}) & \hookrightarrow & \prod_s H^1_{\mathrm{fppf}}(K_{S,s},\mathcal{G}_{K_{S,s}}) \end{array} \tag{7.2.1}$$

(cf. §A.4) are injective and so is

$$H^1_{\mathrm{fppf}}(V,\mathcal{G}_V) \to H^1_{\mathrm{fppf}}(K,\mathcal{G}_K) \tag{7.2.2}$$

for every open $V \subset S$, then (7.2.1) is Cartesian. The same conclusion holds 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 $\mathcal{G}$ is a quasi-affine S-group scheme), if in addition the bottom horizontal arrow in (7.2.1) stays injective 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 $\widehat{K}_{S,s}$).

Proof. By Lemma 7.1, assuming injectivity of the bottom horizontal arrow, 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 (7.2.1) 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 $\mathcal{T}$. Since $\mathcal{T}_K \to \operatorname{Spec} K$ inherits finite presentation from $\mathcal{G}_K$, by [Ols06, Prop. 2.2 and its proof] and [LMB00, 4.18 (i)], for some nonempty open $U \subset S$, 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 (7.1.1) over U is bijective. Consequently, $\mathcal{T}_U$ is a $\mathcal{G}_U$-torsor.

To increase U by extending $\mathcal{T}_U$ over some $s \in S - U$, use limit arguments as above to 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. Since (7.2.2) is injective with $V = U \cap W$, 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 $U = S$. □

Corollary 7.3. *Let $\phi\colon A \to B$ be a K-isogeny between abelian varieties, and $\mathcal{A}[\phi]$ the kernel of the induced S-homomorphism between the Néron models. The square*

$$\begin{array}{ccc} H^1_{\mathrm{fppf}}(S, \mathcal{A}[\phi]) & \hookrightarrow & H^1_{\mathrm{fppf}}(K, A[\phi]) \\ \downarrow & & \downarrow \\ \prod_s H^1_{\mathrm{fppf}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}[\phi]_{\widehat{\mathcal{O}}_{S,s}}) & \hookrightarrow & \prod_s H^1_{\mathrm{fppf}}(\widehat{K}_{S,s}, \mathcal{A}[\phi]_{\widehat{K}_{S,s}}) \end{array}$$

is Cartesian (the products are indexed by the nongeneric $s \in S$).

Proof. Theorem 7.2 applies due to Proposition 2.3, Theorem 6.1, and Proposition 3.3. □

Remark 7.4. Due to Remark 6.4, another possible choice for $\mathcal{G}$ in Theorem 7.2 is a finite flat S-group scheme or an S-model.

We now use Theorem 7.2 to give an alternative proof of the results of [Maz72, Appendix].

Proposition 7.5. *Suppose that S has a finite residue field at every nongeneric point. Fix an abelian variety $A \to \operatorname{Spec} K$, its Néron model $\mathcal{A} \to S$, and set*

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

where the product is indexed by the nongeneric $s \in S$.

(a) Let c_s be the local Tamagawa factor of A at s (i.e., c_s is the number of connected components of $\mathcal{A}_s$ possessing a rational point). Then

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

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

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

(d) If S is the spectrum of the ring of integers of a number field or a proper smooth curve over a finite field and $Ш(A) := \operatorname{Ker}(H^1(K, A) \to \prod_v H^1(K_v, A))$ (the product is indexed by the places of K) is the Shafarevich–Tate group of A, then $Ш(A) \subset Ш(\mathcal{A})$ and

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

where $\pi_0(A(K_v))$ is the group of connected components of the compact real Lie group $A(K_v)$.

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

Proof. Smoothness of $\mathcal{A} \to S$ permits the interchangeable use of étale and fppf cohomology groups, cf. Proposition A.2 (a).

(a) Indeed, it will be proved in Lemma 8.6 that $\#H^1_{\text{ét}}(\widehat{\mathcal{O}}_{S,s}, \mathcal{A}_{\widehat{\mathcal{O}}_{S,s}}) = c_s$.

(b) Combine the cohomology sequence of the sequence from Proposition 3.2 with Lemma 8.6.

(c) Indeed, Theorem 7.2 and Corollary 2.20 give the Cartesian diagram

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

Working with henselizations suffices thanks to the injectivity of

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

for which we refer to [BLR90, §3.6 Cor. 10] (see also Proposition 2.18), and the bijectivity of

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

which follows from Proposition A.2 (b).

(d) Since $H^1(K_v, A) \cong \pi_0(A(K_v))$ and $\#\pi_0(A(K_v)) \leqslant 2^{\dim A}$ for real v (compare [GH81, 1.1 (3) and 1.3]), the claim follows from (c).

(e) Combine (a) and (d). □

8. Images of local Kummer homomorphisms as flat cohomology groups

8.1. The image of the Kummer map. For a field k and a k-isogeny $\phi\colon A \to B$ of abelian varieties, Proposition 3.10 (a) yields the exact sequence

$$0 \to A[\phi] \to A \xrightarrow{\phi} B \to 0 \tag{8.1.1}$$

in the fppf topos of k. Its cohomology sequence gives the *Kummer map* $B(k) \xrightarrow{\kappa_\phi} H^1_{\text{fppf}}(k, A[\phi])$ with image $B(k)/\phi A(k) \cong \operatorname{Im}\kappa_\phi \subset H^1_{\text{fppf}}(k, A[\phi])$.

If $\operatorname{char} k \nmid \deg\phi$ and $\psi\colon B \to A$ is the isogeny with $\ker\psi = \phi(A[\deg\phi])$, then $\frac{1}{\deg\phi}\operatorname{Lie}\psi$ is the inverse of $\operatorname{Lie}\phi$, proving étaleness of ϕ [BLR90, §2.2 Cor. 10], [SGA $3_{\text{I new}}$, IV_{B} 1.3]. In this case, ϕ is an étale surjection, (8.1.1) is exact already in the big étale topos, $A[\phi] \to \operatorname{Spec} k$ is finite étale, and

$$H^1_{\text{fppf}}(k, A[\phi]) \overset{A.2}{\cong} H^1_{\text{ét}}(k, A[\phi]) \overset{\text{§1.17}}{\cong} H^1(k, A[\phi]),$$

which restrict to identifications of the images of Kummer maps.

In this section we compare $\operatorname{Im}\kappa_\phi$ with other natural subgroups of $H^1_{\text{fppf}}(k, A[\phi])$ for k as in

8.2. The setup. For the rest of the section, let $S = \operatorname{Spec}\mathfrak{o}$ for a Henselian discrete valuation ring $\mathfrak{o}$, let $k = \operatorname{Frac}\mathfrak{o}$, let $\mathbb{F}$ be the residue field of $\mathfrak{o}$, let $i\colon \operatorname{Spec}\mathbb{F} \to \operatorname{Spec}\mathfrak{o}$ 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, and let Φ_A and Φ_B be the étale $\mathbb{F}$-group schemes of connected components of $\mathcal{A}_s$ and $\mathcal{B}_s$; write ϕ for $\phi_s\colon \mathcal{A}_s \to \mathcal{B}_s$ and also for the induced $\Phi_A \to \Phi_B$. We use various open subgroups of $\mathcal{A}$ and $\mathcal{B}$ constructed in §3.1.

8.3. The three subgroups of interest. The first one is $\operatorname{Im}\kappa_\phi \subset H^1_{\text{fppf}}(k, A[\phi])$ from §8.1.

The second subgroup is the image of $H^1_{\text{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \xrightarrow{a} H^1_{\text{fppf}}(k, A[\phi])$. By Theorem 6.1, a is injective, and we identify $H^1_{\text{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \cong \operatorname{Im} a \subset H^1_{\text{fppf}}(k, A[\phi])$.

The third subgroup is defined if $\operatorname{char} k \nmid \deg \phi$ (so $A[\phi]$ is étale, cf. §8.1); it is the unramified subgroup

$$H^1_{\mathrm{nr}}(k, A[\phi]) := \operatorname{Ker}(H^1(k, A[\phi]) \to H^1(k^{sh}, A[\phi])) \subset H^1(k, A[\phi]), \tag{8.3.1}$$

where $k^{sh} := \operatorname{Frac} \mathfrak{o}^{sh}$. If $\mathfrak{o}$ is the ring of integers of a nonarchimedean local field k, then k^{sh} is its maximal unramified extension, and (8.3.1) recovers the usual unramified subgroup.

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 8.8 and 8.9.

Lemma 8.4. *If $\mathbb{F}$ is finite and $G \to \operatorname{Spec} \mathbb{F}$ is a commutative connected algebraic group, then $H^j(\mathbb{F}, G) = 0$ for $j \geqslant 1$.*

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 8.5. *If $\operatorname{Gal}(\overline{\mathbb{F}}/\mathbb{F}) \cong \widehat{\mathbb{Z}}$ and M is a finite discrete $\operatorname{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-module, then*

$$\#H^0(\mathbb{F}, M) = \#H^1(\mathbb{F}, M).$$

Proof. The maps in $H^1(\mathbb{F}, M) = \varinjlim_{[\mathbb{F}_n:\mathbb{F}]=n} H^1(\mathbb{F}_n/\mathbb{F}, M^{\operatorname{Gal}(\overline{\mathbb{F}}/\mathbb{F}_n)})$ are inflation injections, whereas $\#H^1(\mathbb{F}_n/\mathbb{F}, M^{\operatorname{Gal}(\overline{\mathbb{F}}/\mathbb{F}_n)}) = \#H^0(\mathbb{F}, M)$ [Ser79, VIII.§4 Prop. 8]. □

Lemma 8.6. *Suppose that $\mathbb{F}$ is finite. 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 the cohomology sequence of $0 \to \mathcal{A}^0_{\mathbb{F}} \to \mathcal{A}^\Gamma_{\mathbb{F}} \to \Gamma \to 0$, Proposition A.2 (b), and Lemmas 8.4 and 8.5. □

8.7. The local Tamagawa factors. These are $c_A := \#\Phi_A(\mathbb{F})$ and $c_B := \#\Phi_B(\mathbb{F})$, i.e., the numbers of rational components of the special fibers of the Néron models $\mathcal{A}$ and $\mathcal{B}$. If A and B have good reduction, i.e., $\mathcal{A}$ and $\mathcal{B}$ are abelian schemes, then $c_A = c_B = 1$. The sequences

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

of discrete $\operatorname{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-modules are exact, and hence

$$\frac{\#\Phi_A(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \leqslant \#\Phi_A[\phi](\mathbb{F}), \qquad \frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \leqslant \#\left(\frac{\Phi_B}{\phi(\Phi_A)}\right)(\mathbb{F}). \tag{8.7.1}$$

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 §8.3:

Proposition 8.8. *Suppose that $\mathbb{F}$ is finite and $\mathcal{A} \xrightarrow{\phi} \mathcal{B}$ is flat (the latter assumption holds if A has semiabelian reduction in case $\operatorname{char} \mathbb{F} \mid \deg \phi$, cf. Lemma 3.4).*

(a) Then

$$\#\left(\frac{H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])}{H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \cap \operatorname{Im} \kappa_\phi}\right) = \frac{\#\Phi_A(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \overset{(8.7.1)}{\leqslant} \#\Phi_A[\phi](\mathbb{F}),$$
$$\#\left(\frac{\operatorname{Im} \kappa_\phi}{H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \cap \operatorname{Im} \kappa_\phi}\right) = \frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})} \overset{(8.7.1)}{\leqslant} \#\left(\frac{\Phi_B}{\phi(\Phi_A)}\right)(\mathbb{F}).$$

(b) There is an injection

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

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

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

(e) 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) Let $H^1_{\mathrm{fppf}}(\phi)$ denote the map $H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A})\to H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{B}^{\phi(\Phi_A)})$ induced by ϕ. The short exact sequence $0\to\mathcal{A}[\phi]\to\mathcal{A}\xrightarrow{\phi}\mathcal{B}^{\phi(\Phi_A)}\to 0$ of Proposition 3.10 (a) together with A.12 (b) give the commutative diagram

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

where the injectivity of the vertical arrows follows from the Néron property and Theorem 6.1. By Lemma 8.6, $H^1_{\mathrm{fppf}}(\phi)$ 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

$$\#\operatorname{Ker}h=\frac{\#H^1(\mathbb{F},\Phi_A)}{\#H^1(\mathbb{F},\phi(\Phi_A))}\overset{8.5}{=}\frac{\#\Phi_A(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})},$$

the first claim follows. On the other hand,

$$\frac{\operatorname{Im}\kappa_\phi}{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])\cap\operatorname{Im}\kappa_\phi}\cong\frac{B(k)/\phi A(k)}{\mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})/\phi\mathcal{A}(\mathfrak{o})}\cong\frac{\mathcal{B}(\mathfrak{o})/\phi\mathcal{A}(\mathfrak{o})}{\mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})/\phi\mathcal{A}(\mathfrak{o})}\cong\frac{\mathcal{B}(\mathfrak{o})}{\mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})}.\tag{8.8.1}$$

Lemma 8.6 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 3.2 give the exact sequence (cf. also Proposition A.2 (a))

$$0\to\frac{\mathcal{B}(\mathfrak{o})}{\mathcal{B}^{\phi(\Phi_A)}(\mathfrak{o})}\to\left(\frac{\Phi_B}{\phi(\Phi_A)}\right)(\mathbb{F})\to H^1(\mathbb{F},\phi(\Phi_A))\to H^1(\mathbb{F},\Phi_B)\twoheadrightarrow H^1\left(\mathbb{F},\frac{\Phi_B}{\phi(\Phi_A)}\right),\tag{8.8.2}$$

where we have used the exactness of i_* for the étale topology to obtain the last term. Combining (8.8.1) and (8.8.2) yields the remaining

$$\#\left(\frac{\operatorname{Im}\kappa_\phi}{H^1_{\mathrm{fppf}}(\mathfrak{o},\mathcal{A}[\phi])\cap\operatorname{Im}\kappa_\phi}\right)=\frac{\#(\Phi_B/\phi(\Phi_A))(\mathbb{F})\cdot\#H^1(\mathbb{F},\Phi_B)}{\#H^1(\mathbb{F},\phi(\Phi_A))\cdot\#H^1(\mathbb{F},\Phi_B/\phi(\Phi_A))}\overset{8.5}{=}\frac{\#\Phi_B(\mathbb{F})}{\#(\phi(\Phi_A))(\mathbb{F})}.$$

(b) Combine (8.8.1) and (8.8.2).

(c) Let $\psi\colon B \to A$ be the isogeny with $\ker\psi = \phi(A[\deg\phi])$, so $\psi\circ\phi = \deg\phi$, and thus also $\phi\circ\psi = \deg\phi$. 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 $\Phi_B(\mathbb{F}) = (\phi(\Phi_A))(\mathbb{F})$.

(d) Considering ψ as in the proof of (c), $\Phi_A[\phi] \subset \Phi_A[\deg\phi]$, 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 $\#H^1(\mathbb{F}, \Phi_A[\phi]) = \#\Phi_A[\phi](\mathbb{F})$.

(e) Combine (c) and (d). □

We now compare the third subgroup $H^1_{\mathrm{nr}}(k, A[\phi]) \subset H^1(k, A[\phi])$ of §8.3 to $\operatorname{Im}\kappa_\phi$ and $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$:

Proposition 8.9. *Suppose that* $\operatorname{char} k \nmid \deg\phi$.

(a) The Néron model $\mathcal{G} \to \operatorname{Spec}\mathfrak{o}$ *of* $A[\phi] \to \operatorname{Spec} k$ *exists and is étale.*

(b) $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{G}) \to H^1(k, A[\phi])$ *is an isomorphism onto* $H^1_{\mathrm{nr}}(k, A[\phi])$.

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

(d) $H^1_{\mathrm{nr}}(k, A[\phi]) \subset \operatorname{Im}\kappa_\phi$, *if in addition*

(a) $\mathbb{F}$ *is finite,*

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

(c) $\deg\phi$ *is prime to* c_A *or, more generally (cf. Proposition 8.8 (d)),* $\#\Phi_A(\mathbb{F}) = \#(\phi(\Phi_A))(\mathbb{F})$.

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

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

(i) $\mathbb{F}$ *is finite,*

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

(iii) $\deg\phi$ *is prime to* $c_A c_B$ *or, more generally (cf. Proposition 8.8 (c)–(d)),*

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

Proof.

(a) By 8.1, if $\operatorname{char} k \nmid \deg\phi$, then $A[\phi] \to \operatorname{Spec} k$ is finite étale, so Proposition 2.15 applies.

(b) This is a special case of Proposition 2.21.

(c) Due to (b), it suffices to find an $\mathfrak{o}$-homomorphism $\mathcal{G} \to \mathcal{A}[\phi]$ inducing an isomorphism on generic fibers, which is provided by Theorem 2.13 (and §2.12).

(d) By Proposition 8.8 (a), $H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi]) \subset \operatorname{Im}\kappa_\phi$, so the conclusion results from (c).

(e) This follows from (b), because if $\operatorname{char}\mathbb{F} \nmid \deg\phi$, then $\mathcal{G} = \mathcal{A}[\phi]$ by Corollary 3.9.

(f) By Proposition 8.8 (a), $\operatorname{Im}\kappa_\phi = H^1_{\mathrm{fppf}}(\mathfrak{o}, \mathcal{A}[\phi])$, so the conclusion results from (e). □

9. Selmer groups as flat cohomology groups

Let K be a global field. 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. A nonarchimedean place v of K corresponds to a closed $s \in S$, rendering K_v, $\mathcal{O}_v$, and $\mathbb{F}_v$ synonymous to $\widehat{K}_{S,s}$, $\widehat{\mathcal{O}}_{S,s}$, and $k(s)$. This section is concerned with relations between Selmer groups and certain flat cohomology groups of S: we investigate Selmer groups of abelian varieties in §§9.7–9.10 and also those associated to an S-model in §§9.2–9.5.

9.1. Selmer structures. Fix a finite discrete $\operatorname{Gal}(\overline{K}/K)$-module M. 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, the unramified subgroup $H^1_{\mathrm{ur}}(K_v, M) \subset H^1(K_v, M)$ 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.

9.2. The Selmer structure of an S-model $\mathcal{G}$ with $\#\mathcal{G}_K = p^m$. It is given by the subgroups

$$\begin{aligned} H^1_{\mathrm{fppf}}(\mathcal{O}_v, \mathcal{G}_{\mathcal{O}_v}) \subset H^1_{\mathrm{fppf}}(K_v, \mathcal{G}_{K_v}) &\overset{\S 1.17}{\cong} H^1(K_v, \mathcal{G}_{K_v}), && \text{if } v \nmid \infty, \text{ and} \\ H^1(K_v, \mathcal{G}_{K_v}) \subset H^1(K_v, \mathcal{G}_{K_v}), & && \text{if } v \mid \infty, \end{aligned} \tag{9.2.1}$$

which is a legitimate choice by Remark 6.4 and Proposition 2.21 (implicitly, $p \neq \operatorname{char} K$). By Theorem 7.2 and Remark 7.4, the resulting Selmer group is nothing else but $H^1_{\mathrm{fppf}}(S, \mathcal{G}) \subset H^1(K, \mathcal{G}_K)$, which is finite, being contained in the finite (cf. [Mil06, II.2.13 (a)]) $H^1_{\text{ét}}(S[\frac{1}{p}], \mathcal{G}_{S[\frac{1}{p}]}) \subset H^1(K, \mathcal{G}_K)$ (only the conditions away from p are imposed).

Example 9.3. If K is a number field and $\mathcal{G} = \underline{\mathbb{Z}/p^n\mathbb{Z}}_{\mathcal{O}_K}$, then (9.2.1) consists of the unramified subgroups for $v \nmid \infty$. The resulting Selmer subgroup of $H^1(K, \mathbb{Z}/p^n\mathbb{Z}) \cong \operatorname{Hom}_{\mathrm{cont}}(\operatorname{Gal}(\overline{K}/K), \mathbb{Z}/p^n\mathbb{Z})$ consists of the homomorphisms unramified at all the finite places. By the theory of the narrow Hilbert class field, it identifies with $\operatorname{Hom}(\operatorname{Pic}_+(\mathcal{O}_K), \mathbb{Z}/p^n\mathbb{Z})$, where $\operatorname{Pic}_+(\mathcal{O}_K)$ is the narrow class group of K. This is consistent with the description of $H^1_{\mathrm{fppf}}(\mathcal{O}_K, \mathbb{Z}/p^n\mathbb{Z}) \cong H^1_{\text{ét}}(\mathcal{O}_K, \mathbb{Z}/p^n\mathbb{Z})$ as $\operatorname{Hom}_{\mathrm{cont}}(\pi_1^{\text{ét}}(\mathcal{O}_K), \mathbb{Z}/p^n\mathbb{Z})$.

9.4. Morphisms of S-models and Selmer groups. The map $H^1(K, \mathcal{G}_K) \to H^1(K, \mathcal{H}_K)$ induced by a morphism $\mathcal{G} \xrightarrow{f} \mathcal{H}$ of S-models respects the Selmer subgroups: $H^1_{\mathrm{fppf}}(S, \mathcal{G}) \subset H^1(K, \mathcal{G}_K)$ maps into $H^1_{\mathrm{fppf}}(S, \mathcal{H}) \subset H^1(K, \mathcal{H}_K)$. In particular, if $\mathcal{G}$ and $\mathcal{H}$ are S-models of a fixed G as in §5.3, then f induces the inclusion $H^1_{\mathrm{fppf}}(S, \mathcal{G}) \subset H^1_{\mathrm{fppf}}(S, \mathcal{H})$ inside $H^1(K, G)$. Motivated by the local analogue (admitting a positive answer [Maz70]), one may ask whether an S-model is determined by its Selmer group, i.e., whether the functor

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

is fully faithful. The answer is negative:

Example 9.5. For a prime p, let $K = \mathbb{Q}(\zeta_{p^n})$ for some $n \geqslant 1$ excluding the $(p, n) = (2, 1)$ case and consider S-models of $G = \underline{\mathbb{Z}/p\mathbb{Z}}_K$. Letting v be the place above p, by the Oort–Tate classification [TO70, pp. 14–16 Remarks 1 and 5] and [Tat97, 4.4.1 (c)], there are $p^{n-1} + 1$ nonisomorphic finite flat $\mathcal{O}_v$-models of G_{K_v} which correspond to factorizations $(1 - \zeta_{p^n})^{(p-1)i} \cdot \frac{p}{(1-\zeta_{p^n})^{(p-1)i}} = p$ for $0 \leqslant i \leqslant p^{n-1}$ and are linearly ordered, i.e., each maps to the next one. Proposition 5.7 (a) and (d) therefore give $p^{n-1} + 1$ nonisomorphic linearly ordered S-models of G. If p is regular, i.e., p does not divide the class number of K (e.g., $p = 2$ [Was97, 10.5]), then the Selmer groups of these

S-models are subgroups of the $\left(\frac{p^{n-1}(p-1)}{2}+1\right)$-dimensional $H^1_{\text{ét}}(S[\frac{1}{p}],\mu_p)\cong\mathbb{Z}[\zeta_{p^n},\frac{1}{p}]^\times/\mathbb{Z}[\zeta_{p^n},\frac{1}{p}]^{\times p}$ (only the conditions away from p are imposed). Due to dimension reasons, for $p=2$ and $n\geqslant 3$ this space cannot have a flag of $p^{n-1}+1$ distinct subspaces, forcing some Selmer groups to coincide. We do not know, however, if distinct S-models of $\underline{\mathbb{Z}/p\mathbb{Z}}_K$ can have coinciding Selmer groups for odd p. Their defining local subgroups at v have been worked out by Mazur and Roberts [MR69, 9.3], [Rob73, Thm. 1].

9.6. The setup. 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. Denote the local Tamagawa factors by $c_{A,v}:=\#\Phi_{A,v}(\mathbb{F}_v)$ and $c_{B,v}:=\#\Phi_{B,v}(\mathbb{F}_v)$.

9.7. Two sets of subgroups (compare §8.3). The first one is the images $\operatorname{Im}\kappa_{\phi,v}\subset H^1_{\text{fppf}}(K_v,A[\phi])$ of the local Kummer homomorphisms (cf. §8.1) for all places v of K; its Selmer group, defined as in §9.1, is the *ϕ-Selmer group* $\operatorname{Sel}_\phi A\subset H^1_{\text{fppf}}(K,A[\phi])$.

The second one is

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

and has the corresponding Selmer group $H^1_{\text{fppf}}(S,\mathcal{A}[\phi])\subset H^1_{\text{fppf}}(K,A[\phi])$ by Corollary 7.3.

If $\operatorname{char}K\nmid\deg\phi$, these are two Selmer structures on $A[\phi]$ by Proposition 8.9 (f).

Proposition 9.8. *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 3.4).*

(a) Taking intersections inside $H^1_{\text{fppf}}(K,A[\phi])$, one has

$$\#\left(\frac{\operatorname{Sel}_\phi A}{H^1_{\text{fppf}}(S,\mathcal{A}[\phi])\cap\operatorname{Sel}_\phi A}\right)\leqslant\prod_{v\nmid\infty}\#\left(\frac{\Phi_{B,v}}{\phi_v(\Phi_{A,v})}\right)(\mathbb{F}_v),$$

$$\#\left(\frac{H^1_{\text{fppf}}(S,\mathcal{A}[\phi])}{H^1_{\text{fppf}}(S,\mathcal{A}[\phi])\cap\operatorname{Sel}_\phi A}\right)\leqslant\prod_{v\nmid\infty}\#\Phi_{A,v}[\phi_v](\mathbb{F}_v)\cdot\prod_{v\ real}\#\left(\frac{H^1(K_v,A[\phi])}{\operatorname{Im}\kappa_{\phi,v}}\right).$$

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

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

(d) 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 $H^1_{\text{fppf}}(S,\mathcal{A}[\phi])=\operatorname{Sel}_\phi A$ inside $H^1_{\text{fppf}}(K,A[\phi])$.

Proof. By §9.7, setting $H^1_{\text{fppf}}(\mathcal{O}_v,\mathcal{A}[\phi]_{\mathcal{O}_v}):=H^1(K_v,A[\phi])$ for $v\mid\infty$, there are injections

$$\begin{aligned} \frac{\operatorname{Sel}_\phi A}{H^1_{\text{fppf}}(S,\mathcal{A}[\phi])\cap\operatorname{Sel}_\phi A}&\hookrightarrow\prod_{v\nmid\infty}\frac{\operatorname{Im}\kappa_{\phi,v}}{H^1_{\text{fppf}}(\mathcal{O}_v,\mathcal{A}[\phi]_{\mathcal{O}_v})\cap\operatorname{Im}\kappa_{\phi,v}},\\ \frac{H^1_{\text{fppf}}(S,\mathcal{A}[\phi])}{H^1_{\text{fppf}}(S,\mathcal{A}[\phi])\cap\operatorname{Sel}_\phi A}&\hookrightarrow\prod_{v}\frac{H^1_{\text{fppf}}(\mathcal{O}_v,\mathcal{A}[\phi]_{\mathcal{O}_v})}{H^1_{\text{fppf}}(\mathcal{O}_v,\mathcal{A}[\phi]_{\mathcal{O}_v})\cap\operatorname{Im}\kappa_{\phi,v}}. \end{aligned}\tag{9.8.1}$$

This together with Proposition 8.8 (a), (c), (d), and (e) give the claim, since under the assumptions of (c) and (d) the factors of (9.8.1) 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.

9.9. As in Proposition 8.9 (d) and (f), the assumptions on $c_{A,v}$ and $c_{B,v}$ in Proposition 9.8 (b), (c), and (d) (and hence also in Theorems 1.1 (ii) and 1.11 (iii)) can be weakened to

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

9.10. In practice, it is useful not to restrict Proposition 9.8 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 9.8 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.

Let S be a scheme. For convenience of the reader we recall several general facts from algebraic geometry used in the main body of the text, which mostly concern S-group algebraic spaces and their torsors.

Lemma A.1. *Let $\mathcal{O}$ be a Henselian local ring, $\mathfrak{a} \subset \mathcal{O}$ an ideal, and X a smooth $\mathcal{O}$-algebraic space. If X is not a scheme, assume that it is quasi-separated. Then the natural map $X(\mathcal{O}) \to X(\mathcal{O}/\mathfrak{a})$ is surjective.*

Proof. We include a proof for the lack of reference. Assume that $\mathfrak{a} \neq \mathcal{O}$, let o be the closed point of $\operatorname{Spec}\mathcal{O}$ (or of $\operatorname{Spec}\mathcal{O}/\mathfrak{a}$), and fix a $b \in X(\mathcal{O}/\mathfrak{a})$ with the intention of lifting it to a $B \in X(\mathcal{O})$.

If X is a scheme, the local structure theorem for smooth morphisms [BLR90, §2.2 Prop. 11] applied at $b(o)$ allows us to assume that $X \to \operatorname{Spec}\mathcal{O}$ factors through $X \xrightarrow{u} \mathbb{A}^n_{\mathcal{O}}$ with u étale and separated. Lift $u \circ b \in \mathbb{A}^n_{\mathcal{O}}(\mathcal{O}/\mathfrak{a})$ to a $c \in \mathbb{A}^n_{\mathcal{O}}(\mathcal{O})$ and hence reduce to X being étale and separated over $\mathcal{O}$, in which case [EGA IV$_4$, 18.5.11 (c) et 18.5.15] provides the unique section $B \in X(\mathcal{O})$ with $B(o) = b(o)$.

In general, by [LMB00, 6.3], $b|_o$ lifts to a $c \in U(o)$ with U a smooth X-scheme. By the surjectivity in the scheme case, $c \in (U \times_{X,b} \mathcal{O}/\mathfrak{a})(o)$ yields a lift $d \in U(\mathcal{O}/\mathfrak{a})$ of b. Since U is a smooth $\mathcal{O}$-scheme, d lifts to a $D \in U(\mathcal{O})$, whose image in $X(\mathcal{O})$ is a desired B. □

Proposition A.2. *Let $\mathcal{G}$ be a commutative smooth S-group algebraic space which is either quasi-separated or a scheme.*

(a) If $j\colon S_{\text{fppf}} \to S_{\text{ét}}$ is the canonical morphism of sites, then $\mathbf{R}^n j_*\mathcal{G} = 0$ for $n \geqslant 1$, and the natural maps $H^i_{\text{ét}}(S, j_*\mathcal{G}) \to H^i_{\text{fppf}}(S, \mathcal{G})$ are isomorphisms.

(b) If $S = \operatorname{Spec}\mathcal{O}$ for a Henselian local ring $\mathcal{O}$ with residue field k, then the δ-functorial cohomology pullback maps $H^i_{\text{fppf}}(\mathcal{O}, \mathcal{G}) \to H^i_{\text{fppf}}(k, \mathcal{G}_k)$ are isomorphisms for $i \geqslant 1$.

Proof. Invoke [Gro68, 11.1 et 11.7] with $U = \mathcal{G}$ (and use Lemma A.1 to check condition (L))—when (R) in loc. cit. is modified by assuming U to be representable by a smooth algebraic space containing the zero section, the proofs continue to work with the following caveats:

1. In 11.4, assume in addition that $X_0 \neq \varnothing$;
2. On p. 175, $\underline{C}^i(U)$ is a smooth X-algebraic space by [SP, Proposition 05YF and Lemma 04AM];
3. On p. 177, the desired quasi-coherence of N is argued as follows: let $a\colon X_0 \to U$ be the zero section; by [SP, Lemma 061C and Remark 061D], in the notation of loc. cit., $\mathcal{H}om_{\mathcal{O}_{X_0}}(a^*\Omega_{U/X}, \mathcal{C}_{X_0/X}) \cong N$, so the conclusion follows from [SP, Lemmas 05ZF and 03M1];
4. To obtain 11.7 2°) and 3°), assume in addition that (L) and (R) hold for every Henselian (but not necessarily strictly Henselian) local X-scheme $\overline{X}$. □

Remark A.3. As is clear from the proof of Lemma A.1, if $\mathcal{G}$ is étale (and either quasi-separated or a scheme), then the conclusion of Proposition A.2 (b) also holds for $i = 0$.

A.4. H^1 and torsors. Let $\mathcal{G}$ be an S-group algebraic space. For commutative $\mathcal{G}$, the elements of the cohomology groups $H^1_{\text{fppf}}(S, \mathcal{G})$ (resp., $H^1_{\text{ét}}(S, \mathcal{G})$) can be put in bijection with fppf (resp., étale) torsors $\mathcal{T}$ under $\mathcal{G}$, under which the trivial torsor corresponds to the identity element, and the cohomology pullbacks for $i = 1$ identify with base change of torsors: $\mathcal{T} \mapsto \mathcal{T} \times_S S'$ (cf. [Gir71, III.3.5.4, III.2.4.2, III.2.4.5 et V.1.5.3]). Thus, for possibly noncommutative $\mathcal{G}$, one writes $H^1_{\text{fppf}}(S, \mathcal{G})$ (resp., $H^1_{\text{ét}}(S, \mathcal{G})$) for the set of isomorphism classes of fppf (resp., étale) right torsors under $\mathcal{G}$ and understands that $H^1_{\text{fppf}}(S, \mathcal{G})$ (resp., $H^1_{\text{ét}}(S, \mathcal{G})$) is functorial in S by base change.

Proposition A.5. *Every fppf torsor $\mathcal{T}$ under an S-group algebraic space $\mathcal{G}$ is representable by an S-algebraic space.*

Proof. Being an S-algebraic space is fppf local [SP, Lemma 04SK]. □

Proposition A.6. *Every fppf torsor $\mathcal{T}$ under a smooth S-group algebraic space $\mathcal{G}$ trivializes over an étale cover of S. In particular, for smooth $\mathcal{G}$, the natural map $H^1_{\text{ét}}(S, \mathcal{G}) \to H^1_{\text{fppf}}(S, \mathcal{G})$ is bijective.*

Proof. By Proposition A.5 and [SP, Lemmas 0429 and 041Q], $\mathcal{T}$ is a smooth surjective S-algebraic space. It trivializes over an étale cover of $\mathcal{T}$ by a scheme U. Since the smooth $U \to S$ has a section étale locally [EGA IV_4, 17.16.3 (ii)], we conclude. □

Proposition A.7. *Every fppf torsor under a quasi-affine* [EGA II, 5.1.1] *S-group scheme $\mathcal{G}$ is representable by a quasi-affine scheme.*

Proof. By [SP, Lemma 0247] and [EGA IV_2, 2.7.1 (xiv)], representability and quasi-affineness of an fppf sheaf $\mathcal{T} \xrightarrow{f} S$ can be checked fppf locally on S. □

Proposition A.8. *Let $1 \to \mathcal{H} \to \mathcal{E} \to \mathcal{G} \to 1$ be an exact sequence of sheaves of groups on S_{fppf} with $\mathcal{G}$ representable by an S-scheme and $\mathcal{H}$ representable by an S-algebraic space.*

(a) $\mathcal{E}$ is representable by an S-algebraic space.

(b) For a property $\mathcal{P}$ of morphisms of S-algebraic spaces that is stable under base change and is fppf local on the base, if $\mathcal{H} \to S$ has $\mathcal{P}$, then so does $\mathcal{E} \to \mathcal{G}$. If, in addition, $\mathcal{P}$ is stable under composition and $\mathcal{H} \to S$ and $\mathcal{G} \to S$ both have $\mathcal{P}$, then so does $\mathcal{E} \to S$.

(c) If $\mathcal{H} \to S$ is quasi-affine, then so is $\mathcal{E} \to \mathcal{G}$ and $\mathcal{E}$ is representable by an S-scheme.

Proof.

(a) Indeed, $\mathcal{E} \to \mathcal{G}$ is an fppf torsor under $\mathcal{H}_{\mathcal{G}}$, so the claim is a special case of Proposition A.5.

(b) Immediate from the proof of (a).

(c) Quasi-affine morphisms are representable [SP, Lemma 03WM], hence the claim by (b). □

Proposition A.9. *A quasi-finite fppf S-group scheme $\mathcal{G}$ whose fibers have orders that are prime to the residue characteristic is étale.*

Proof. This is [TO70, p. 17, Lemma 5] if $\mathcal{G}$ is finite. In general, the proof is the same: [EGA IV_4, 17.6.2 a) $\Leftrightarrow$ c'')] reduces to S being the spectrum of an algebraically closed field, in which case $\mathcal{G}$ is finite. One then uses the connected-étale sequence. □

Lemma A.10. *For a scheme S, let X, Y be S-schemes with $Y(S) \neq \varnothing$. If $X \times_S Y \xrightarrow{a} S$ is quasi-compact, locally of finite type, of finite type, separated, or flat, then so is $X \xrightarrow{b} S$.*

Proof. Working locally on S, in all cases we can assume that S is affine: $S = \operatorname{Spec} C$. Hence, since X is a continuous image of $X \times_S Y$, it is quasi-compact if so is $X \times_S Y$.

A section c of $X \times_S Y \to X$ exists by the $Y(S) \neq \varnothing$ assumption and is locally of finite type [EGA I, 6.6.6 (v)]. Hence $a \circ c = b$ is locally of finite type if so is a.

The finite type case follows by combining the quasi-compact and locally of finite type ones.

Since the diagonal morphism of the monomorphism c is an isomorphism, c is separated, hence so is $a \circ c = b$ if a is.

Flatness can be checked on stalks, reducing further to a local C and affine $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$. Since $Y(S) \neq \varnothing$, the C-module A is a direct summand of $A \otimes_C B$, yielding the claim. □

Proposition A.11 ([BC09, 7.4.2]). *Let S be a scheme and $\mathcal{G}$ a commutative S-group scheme. If $n, m \in \mathbb{Z}_{\geqslant 1}$ are relatively prime and nm kills $\mathcal{G}$, then $\mathcal{G} \cong \mathcal{G}[n] \times_S \mathcal{G}[m]$. If $\mathcal{G}$ is finite, quasi-finite, separated, or flat, then so are $\mathcal{G}[n]$ and $\mathcal{G}[m]$. In particular, a commutative separated quasi-finite flat S-group scheme $\mathcal{G}$ killed by an $N \in \mathbb{Z}_{\geqslant 1}$ decomposes as a product of commutative separated quasi-finite flat S-group schemes killed by prime power divisors of N; the factors are finite flat if so is $\mathcal{G}$.*

Proof. Checking on sections of represented fppf sheaves, $0 \to \mathcal{G}[n] \to \mathcal{G} \xrightarrow{n} \mathcal{G}[m] \to 0$ is split exact, giving the first claim. If $\mathcal{G}$ is finite, then so is its closed subscheme $\mathcal{G}[n]$; thus, if $\mathcal{G}$ is quasi-finite, then $\mathcal{G}[n]$ and $\mathcal{G}[m]$ have finite fibers, hence are quasi-finite by Lemma A.10. Similarly, $\mathcal{G}[n]$ and $\mathcal{G}[m]$ inherit separatedness or flatness from $\mathcal{G}$. □

A.12. Quotients by equivalence relations. Let R and X be sheaves on S_{fppf}. A monomorphism $R \xrightarrow{\delta} X \times_S X$ is an *equivalence relation* if $\delta(T)$ is the graph of an equivalence relation on $X(T)$ for each S-scheme T (cf. [Ray67, §3]). Form the fppf quotient sheaf $Y = X/R$. By loc. cit., the quotient is

(a) *Effective*, i.e., the canonical map $R \to X \times_Y X$ is an isomorphism;

(b) *Universal*, i.e., for an fppf sheaf morphism $Y' \to Y$, the quotient of $X \times_Y Y'$ by the base changed equivalence relation $R \times_Y Y'$ is Y'.

For us, the case of interest is when $\mathcal{H} \to \mathcal{G}$ is an immersion of S-group algebraic spaces, $X = \mathcal{G}$, $R = \mathcal{G} \times_S \mathcal{H}$, and $\delta\colon \mathcal{G} \times_S \mathcal{H} \to \mathcal{G} \times_S \mathcal{G}$ is $(g,h) \mapsto (g,gh)$; the resulting quotient is $\mathcal{G}/\mathcal{H}$.

Proposition A.13. *For an immersion $\mathcal{H} \xrightarrow{i} \mathcal{G}$ of S-group algebraic spaces, let $\mathcal{Q} := \mathcal{G}/\mathcal{H}$ be the fppf quotient sheaf. Assume that $\delta\colon \mathcal{G} \times_S \mathcal{H} \to \mathcal{G} \times_S \mathcal{G}$ given by $(g,h) \mapsto (g,gh)$ is quasi-compact.*

(a) If $\mathcal{H} \to S$ is fppf, then $\mathcal{Q}$ is a quasi-separated S-algebraic space.

(b) For a property $\mathcal{P}$ of morphisms of algebraic spaces that is stable under base change and is fppf local on the base, if $\mathcal{H} \to S$ has $\mathcal{P}$, then so does $\mathcal{G} \to \mathcal{Q}$.

(c) If $\mathcal{H} \to S$ is fppf (resp., smooth) and $\mathcal{P}$ is a property of morphisms of algebraic spaces that is fppf (resp., smooth) local on the source, then $\mathcal{Q} \to S$ has $\mathcal{P}$ if and only if $\mathcal{G} \to S$ does.

(d) If $\mathcal{H} \to S$ is fppf and i is a closed immersion, then $\mathcal{Q}$ is a separated S-algebraic space.

Proof. Note that δ is a base change of i, hence is quasi-compact whenever i is.

(a) Letting p_1, p_2 be the projections of $\mathcal{G} \times_S \mathcal{G}$, due to [LMB00, 10.4] it suffices to check that $p_1 \circ \delta$ and $p_2 \circ \delta$ are fppf, which is so because both are base changes of $\mathcal{H} \to S$.

(b) In the proof of [Ray67, Prop. 2] replace schemes by algebraic spaces and fpqc by fppf.

(c) Indeed, $\mathcal{G} \to \mathcal{Q}$ is fppf (resp., smooth) by (b) and [SP, Lemmas 041Q, 041W, 041T, and 0429].

(d) Since δ, being a base change of i, is a closed immersion, and the square

$$\begin{array}{ccc} \mathcal{G} \times_S \mathcal{H} & \xrightarrow{\delta} & \mathcal{G} \times_S \mathcal{G} \\ \downarrow & & \downarrow \\ \mathcal{Q} & \xrightarrow{\Delta} & \mathcal{Q} \times_S \mathcal{Q} \end{array}$$

is Cartesian by A.12 (a), due to [SP, Lemma 0420] it remains to note that $\mathcal{G} \to \mathcal{Q}$ is fppf. □

References

[Abr87] V. A. Abrashkin, *Galois modules of group schemes of period p over the ring of Witt vectors*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 4, 691–736, 910 (Russian); English transl., Math. USSR-Izv. **31** (1988), no. 1, 1–46. MR914857 (89a:14062)

[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, pp. 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)

[BBM82] Pierre Berthelot, Lawrence Breen, and William Messing, *Théorie de Dieudonné cristalline. II*, Lecture Notes in Mathematics, vol. 930, Springer-Verlag, Berlin, 1982 (French). MR667344 (85k:14023)

[BC09] Olivier Brinon and Brian Conrad, *CMI summer school notes on p-adic Hodge theory*. `http://math.stanford.edu/~conrad/papers/notes.pdf`, version of June 24, 2009.

[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)

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

[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)

[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 II] ———, *Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes*, Inst. Hautes Études Sci. Publ. Math. **8** (1961), 222 (French). MR0163909 (29 #1208)

[EGA III_1] ———, *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents. I*, Inst. Hautes Études Sci. Publ. Math. **11** (1961), 167. MR0217085 (36 #177c)

[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)

[Fon85] Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbf{Z}$, Invent. Math. **81** (1985), no. 3, 515–538, DOI 10.1007/BF01388584 (French). MR807070 (87g:11073)

[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)

[Gir71] Jean Giraud, *Cohomologie non abélienne*, Springer-Verlag, Berlin, 1971 (French). Die Grundlehren der mathematischen Wissenschaften, Band 179. MR0344253 (49 #8992)

[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, pp. 231–249 (French, with English and French summaries). MR3077171

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

[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)

[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)

[Kis09] Mark Kisin, *Moduli of finite flat group schemes, and modularity*, Ann. of Math. (2) **170** (2009), no. 3, 1085–1180, DOI 10.4007/annals.2009.170.1085. MR2600871 (2011g:11107)

[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)

[Mat89] Hideyuki Matsumura, *Commutative ring theory*, 2nd ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989. Translated from the Japanese by M. Reid. MR1011461 (90i:13001)

[Maz70] B. Mazur, *Finite flat structures*, Applications of Categorical Algebra (Proc. Sympos. Pure Math., Vol. XVII, New York, 1968), Amer. Math. Soc., Providence, R.I., 1970, pp. 219–225. MR0257182 (41 #1836)

[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)

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

[MR69] B. Mazur and L. Roberts, *Local Euler characteristics*, Invent. Math. **9** (1969/1970), 201–234. MR0258844 (41 #3490)

[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)

[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

[Ray67] M. Raynaud, *Passage au quotient par une relation d'équivalence plate*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 78–85 (French). MR0232781 (38 #1104)

[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)

[Rob73] Lawrence G. Roberts, *The flat cohomology of group schemes of rank P*, Amer. J. Math. **95** (1973), 688–702. MR0337972 (49 #2741)

[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)

[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)

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

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

[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)

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

[Tat67] J. T. Tate, $p-$*divisible groups.*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 158–183. MR0231827 (38 #155)

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

[Tat97] ———, *Finite flat group schemes*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 121–154. MR1638478

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

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR1421575 (97h:11130)

[Zar85] Yu. G. Zarhin, *A finiteness theorem for unpolarized abelian varieties over number fields with prescribed places of bad reduction*, Invent. Math. **79** (1985), no. 2, 309–321, DOI 10.1007/BF01388976. MR778130 (86d:14041)