ÉTALE SUBQUOTIENTS OF PRIME TORSION OF ABELIAN SCHEMES

HENDRIK VERHOEK

Abstract. Let A be an abelian variety over a number field K with good reduction outside a finite set of primes S. We show that if the ℓ-torsion subgroup schemes $A[\ell^n]$ lie in a certain category of group schemes, then $A[\ell^n]$ does not contain any subgroup schemes that are étale or are of multiplicative type.

Contents

1. Introduction 1
2. The generic fiber of simple group schemes 2
3. Filtrations by simple group schemes 3
4. Application to abelian varieties 4
References 7

1. Introduction

Let K be a number field with ring of integers O_K and let S be a finite set of primes in O_K. Denote by O_S the ring of S-integers of K. Let ℓ be a rational prime such that none of the primes in S divides ℓ.

Definition 1.1. Let $\mathscr{C}$ be a subcategory of the category of finite flat commutative group schemes over O_S of ℓ-power order, such that $\mathscr{C}$ is closed under taking products, subquotients and Cartier duality.

In addition, with an eye towards our main theorem stated below, we state the following two conditions that the category $\mathscr{C}$ might or might not satisfy. These conditions involve simple group schemes in $\mathscr{C}$, i.e., group schemes that have no non-trivial closed flat subgroup schemes.

Condition (1)**:** For all simple non-étale group schemes T in $\mathscr{C}$ and all simple étale group schemes E in $\mathscr{C}$, the group $\mathrm{Ext}^1_{\mathscr{C}}(T, E)$ is trivial.

Condition (2)**:** Let F be the compositum of all $K(E)$, where E runs over all simple étale group schemes E in $\mathscr{C}$. Then the extension F/K is finite and the maximal abelian extension R of F, that is unramified outside S and at most tamely ramified at primes over S, is a cyclic extension.

Let A be an abelian variety over K with good reduction outside S, let $\mathcal{A}$ denote its Néron model. Denote by $\mathcal{A}[\ell^n]$ the ℓ^n-torsion subgroup scheme of $\mathcal{A}$. The schemes $\mathcal{A}[\ell^n]$ are finite flat commutative group scheme over O_S. We prove:

Theorem 1.2. *Let A be an abelian variety such that $\mathcal{A}[\ell^n]$ is an object in $\mathscr{C}$ for all $n \in \mathbf{N}$. If Conditions* (1) *and* (2) *hold for the category $\mathscr{C}$, then $\mathcal{A}[\ell]$ does not have subquotients that are étale or of multiplicative type.*

As an application, we prove:

Corollary 1.3. *There do not exist abelian varieties over $\mathbf{Q}(\sqrt{13})$ and $\mathbf{Q}(\sqrt{17})$ with good reduction everywhere.*

In the rest of the article we continue as follows. First we indicate how one finds simple group schemes in $\mathscr{C}$. Then we discuss filtrations and extensions of group schemes in $\mathscr{C}$ and prove Theorem 1.2. The proof is divided into three steps, the same steps that can be found in [Fon85], [Sch03] and [Sch05] and that prove the non-existence or unique up to isogeny results of abelian varieties with good or semi-stable reduction at the primes in S.

(1) Define a category $\mathscr{C}$ that contains $\mathcal{A}[\ell^n]$ for all n
(2) Find the simple objects in the category $\mathscr{C}$ by using the generic fiber of objects in $\mathscr{C}$ annihilated by ℓ and the discriminant bounds of Odlyzko to classify the generic fibers of simple objects in $\mathscr{C}$, and subsequently use theorems of Oort-Tate and Raynaud to determine the simple objects up to isomorphism. Verify that Condition (2) holds.
(3) Calculate various extension groups of the objects in $\mathscr{C}$ and verify Condition (1). If both conditions hold, then apply Theorem 1.2.

2. The generic fiber of simple group schemes

The generic fiber of a finite flat commutative group scheme J over O_S is a group scheme over K, which we denote by J_K. Since $\mathrm{char}(K) = 0$, J_K is an étale group scheme. Therefore, the group scheme J_K is just an abelian group $J(\overline{K})$ together with the Galois action $\rho_J : G_K \longrightarrow \mathrm{Aut}(J(\overline{K}))$. We denote by $K(J)$ the field extension obtained by adjoining the $\overline{K}$-points of J to K. The representation ρ_J factors through a finite Galois extension $K(J)/K$. By considering the generic fiber J_K we obtain not only information about the group scheme J considered over K, but also as a scheme over O_S. It is even true that, under certain conditions (see [Ray74]), the generic fiber uniquely determines the group scheme J over O_S.

A first step to understand the category $\mathscr{C}$ is to classify its simple objects up to isomorphism. Every simple object is annihilated by ℓ: if not, the Zariski closure of the ℓ-torsion points in the generic fiber would form a non-trivial closed flat subgroup scheme. Since by assumption $\mathscr{C}$ is closed under taking subquotients, this subgroup scheme would again be in $\mathscr{C}$.

Define $T_{\mathscr{C}}$ to be the compositum of all fields $K(J)$, where the J are group schemes in $\mathscr{C}$ that are annihilated by ℓ. We call $T_{\mathscr{C}}$ the *maximal ℓ-torsion extension* of $\mathscr{C}$. This extension $T_{\mathscr{C}}$ need not be finite in general. The reason that we are interested in the maximal ℓ-torsion extension of $\mathscr{C}$ is that if $T_{\mathscr{C}}$ is finite, it enables us to find the simple objects in $\mathscr{C}$. Namely, the $\overline{K}$-points of every simple object generate an extension that is a subfield of the maximal ℓ-torsion extension of $\mathscr{C}$. As a side note we mention that to find $T_{\mathscr{C}}$ in practice, it is helpful that the category $\mathscr{C}$ is closed under taking products.

Lemma 2.1. *If J is a simple finite flat commutative group scheme over O_S, then the representation $\rho_J : G_K \to \mathrm{Aut}(J(\overline{K}))$ is irreducible.*

Proof. Suppose ρ_J admits a non-trivial G_K-stable subgroup V. Since the closure of the generic point of O_S is O_S (recall that O_S is a Dedekind ring), taking the Zariski closure of V gives a

non-trivial closed flat subgroup scheme of J. This closure is equal to J because J is simple. The generic fiber of the closure, which is equal to $J(\overline{K})$, is contained in V. □

The generic fiber of a simple object J in $\mathscr{C}$ is a simple $\mathbf{F}_\ell[\mathrm{Gal}(K(J)/K)]$-module. Since simple objects are killed by ℓ, such a generic fiber is also a simple $\mathbf{F}_\ell[\mathrm{Gal}(T_{\mathscr{C}}/K)]$-module. Therefore we classify all simple $\mathbf{F}_\ell[\mathrm{Gal}(T_{\mathscr{C}}/K)]$-modules. If we can find a relatively large normal ℓ-subgroup H in $\mathrm{Gal}(T_{\mathscr{C}}/K)$, it is easier to classify irreducible submodules: the representation ρ_J factors not only through $\mathrm{Gal}(L/K)$, but also through the quotient of $\mathrm{Gal}(L/K)$ by H. This is an immediate consequence of:

Lemma 2.2. *Let J be a simple object in $\mathscr{C}$. Then $\mathrm{Gal}(K(J)/K)$ contains no non-trivial normal ℓ-subgroup.*

Proof. The representation ρ_J factors through $\mathrm{Gal}(K(J)/K)$. Let H be a non-trivial normal ℓ-subgroup of $\mathrm{Gal}(K(\overline{J})/K)$. Then H must act faithfully as a ℓ-group on the ℓ-group $J(\overline{K})$, but this is impossible. There are non-trivial fixed points of $J(\overline{K})$ under this action and they form a closed flat subgroup scheme of J, which must equal J since J is simple. □

Finally, once simple $\mathbf{F}_\ell[\mathrm{Gal}(T_{\mathscr{C}}/K)]$-modules have been found, the question remains if they extend to finite flat commutative group schemes over O_S. This is addressed in the work of Raynaud [Ray74] and Oort-Tate [TO70].

3. Filtrations by simple group schemes

In this section we discuss filtrations of group schemes in $\mathscr{C}$ by simple subgroup schemes. These filtrations will be used to prove Theorem 1.2. Each finite flat commutative group scheme J contains a simple closed flat subgroup scheme J'. The same is true for J/J'. Continuing like this we obtain a filtration of J:

Definition 3.1. A *(left) filtration of a finite flat commutative group scheme* J is an ordered set $\{J_i\}_{i=1}^n$ such that

- J_1 is a simple closed flat subgroup scheme of $F_1 := J$
- for $1 < i < n$, let J_i be a simple closed flat subgroup scheme of $F_i := F_{i-1}/J_{i-1}$
- J_n is simple

We call n the length of the filtration.

We note that by using Cartier duality, we can get another (right) filtration. If A is a simple group scheme occurring in a filtration (or equivalently all filtrations) of J, we say that J *admits* A.

Lemma 3.2. *Let J be a group scheme in $\mathscr{C}$ that admits the simple group scheme A. Suppose that for each simple B with $B \not\simeq A$ occurring in the filtration of J, the group $\mathrm{Ext}^1_{\mathscr{C}}(A, B)$ is trivial. Then A is a closed flat subgroup scheme of J.*

Proof. Consider the short exact sequence

$$0 \longrightarrow J' \longrightarrow J \longrightarrow J/J' = F_2 \longrightarrow 0, \tag{1}$$

where J' is simple. If $J' \simeq A$ there is nothing to prove, so assume $A \not\simeq J'$. We proceed by induction on the length of the filtration of J. The statement of the lemma holds for length one and two. By induction we have the following exact sequence:

$$0 \longrightarrow A \longrightarrow J/J' = F_2 \longrightarrow F_3 \longrightarrow 0.$$

The pull-back of A by J over F_2, using (1), gives the short exact sequence

$$0 \longrightarrow J' \longrightarrow J \times_{F_2} A \longrightarrow A \longrightarrow 0.$$

The group scheme $J \times_{F_2} A$ is a closed flat subgroup scheme of J. By hypothesis, $J \times_{F_2} A \simeq A \times J'$. Hence A is a closed flat subgroup scheme of J. □

Corollary 3.3. *Let J be a finite flat commutative group scheme in the category $\mathscr{C}$ that admits a simple group scheme A. If for each simple B with $B \ncong A$ occurring in the filtration of J, the group $\mathrm{Ext}^1_{\mathscr{C}}(A, B)$ is trivial, then there exists a closed flat subgroup scheme J' of J admitting only copies of A and such that J/J' does not admit A.*

Proof. We proceed by induction on the length of the filtration of J. If the length of J is one, we are done. If the length is two, we are again done by hypothesis. Suppose the length of J is k and the statement holds if the length is at most $k-1$. By Lemma 3.2 we can write $0 \subset A \subset J$. By induction, there exists a closed flat subgroup scheme J'' of J/A such that $(J/A)/J''$ does not admit A and J'' only admits copies of A. Then $J' := J \times_{J/A} J''$ verifies the condition of the statement. □

The next proposition resembles the fact that for finite flat commutative group schemes over a local henselian ring, the quotient by the connected component is an étale group scheme. See for instance [CSS97, p. 138].

Proposition 3.4. *If Condition* (1) *holds for the category $\mathscr{C}$, then for any J in $\mathscr{C}$ we have an exact sequence*

$$0 \longrightarrow J' \longrightarrow J \longrightarrow J'' \longrightarrow 0$$

such that J'' is étale and J' does not admit an étale scheme.

Proof. Let J^* be the Cartier dual of J. It suffices to show that J^* contains a subgroup scheme M of multiplicative type such that J^*/M does not admit a simple group scheme of multiplicative type. We may suppose that J^* admits a simple group scheme of multiplicative type; if not, we are done. Then by Lemma 3.2, the group scheme J^* has a simple subgroup scheme of multiplicative type.

Next, suppose that J^* has a subgroup of multiplicative type M' such that J^*/M' admits a simple group scheme of multiplicative type; if not, we are done again. Then again by Lemma 3.2, the group scheme J^*/M' has a simple subgroup scheme of multiplicative type M''. Now $M'' \times_{J^*/M'} J^*$ is a closed flat subgroup scheme of J^* and sits inside the short exact sequence

$$0 \longrightarrow M' \longrightarrow J^* \times_{J^*/M'} M'' \longrightarrow M'' \longrightarrow 0.$$

Hence $M'' \times_{J^*/M'} J^*$ is an extension of two group schemes of multiplicative type and therefore itself of multiplicative type. Proceeding this way, we find a subgroup scheme of multiplicative type M such that J^*/M does not admit a simple group scheme of multiplicative type. □

4. Application to abelian varieties

In this section, we will prove Theorem 1.2. We first state two auxiliary lemmas:

Lemma 4.1. *Let p be a prime and G be a finite p-group such that $G/[G,G]$ is cyclic. Then G is cyclic.*

Proof. The Frattini subgroup $\mathrm{Frat}(G)$ of G is equal to $[G,G]G^p$. The group $G/\mathrm{Frat}(G)$ is by hypothesis a cyclic group of order p. Burnside's basis Theorem [Hal59, Theorem 12.2.1, p. 176] implies that G is cyclic. □

Lemma 4.2. *Let G be a group and A, B, C be finite G-modules such that A and C have trivial G-action and G acts faithfully on B. Let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be an exact sequence of G-modules. Let k denote the number of generators of C. Then $\#G$ divides $(\#A)^k$.

Proof. We leave the proof to the reader. □

Lemma 4.3. *Let R be the field as before in Condition (2). If Condition (2) holds for the category $\mathscr{C}$, then any étale object J in $\mathscr{C}$ becomes constant over R.*

Proof. Let J be any étale group scheme in $\mathscr{C}$. We claim that $\Lambda = \mathrm{Gal}(F(J_F)/F)$ is an ℓ-group. The proof proceeds by induction on the order of J. There exists an étale group scheme J' in $\mathscr{C}$ such that we have the following short exact sequence of group schemes over the field F:

$$0 \longrightarrow J'_F \longrightarrow J_F \longrightarrow \mathbf{Z}/\ell\mathbf{Z} \longrightarrow 0.$$

By induction, $\mathrm{Gal}(F(J'_F)/F)$ is an ℓ-group. Apply Lemma 4.2 to finish the induction and prove the claim.

We note that $\Lambda/[\Lambda,\Lambda]$ is an abelian ℓ-group and hence the fixed field of $[\Lambda,\Lambda]$ is at most tamely ramified at primes dividing the primes in S. This fixed field is contained in R, which by assumption is a cyclic extension of F. Hence also $\Lambda/[\Lambda,\Lambda]$ is cyclic and by Lemma 4.1 the group Λ is cyclic. We conclude that $F(J_F)$ is contained in R, which is exactly what we wanted to prove. □

For example, if the Hilbert class field of F is trivial and S contains only one prime that does not split in F/K, then R is a cyclic extension of F.

Proposition 4.4. *Let $q \notin S$ be a prime in O_K that is inert in R/K. Suppose that Conditions (1) and (2) hold for the category $\mathscr{C}$. Then for any J in $\mathscr{C}$ having n simple étale group schemes and m simple group schemes of multiplicative type in its filtration, the following inequalities hold:*

$$|J_q(\mathbf{F}_q)| \geq \ell^n \quad \textit{and} \quad |J_q^*(\mathbf{F}_q)| \geq \ell^m.$$

Proof. Let R as before. By Proposition 4.3 all étale objects in $\mathscr{C}$ become constant over R. Let E be the étale quotient of J as in Proposition 3.4. Let $\mathfrak{P}$ be a prime in O_R lying above q. The residue field $\mathbf{F}_\mathfrak{P}$ is equal to $\mathbf{F}_q$. Since E_R is constant, it follows that also $E_\mathfrak{P}$ is constant and hence that J_R has at least ℓ^n points in the fiber at $\mathfrak{P}$. The inequality $|J_q(\mathbf{F}_q)| \geq \ell^n$ follows. The second inequality follows by Cartier duality. □

We are now able to prove Theorem 1.2:

Proof. By contradiction, suppose that $A[\ell]$ contains k simple étale subquotients. Then for any prime q that is not in S and is inert in R/K, Proposition 4.4 says that the number of ℓ-torsion points of A in the fiber at q is at least ℓ^k. Hence $A[\ell^n]$ has at least ℓ^{kn} points in the fiber at q. This is in contradiction with the fact that $A(\mathbf{F}_q)$ is finite for n sufficiently large. Let A^{dual} be the dual abelian variety of A. For each n, the group scheme $A^{\mathrm{dual}}[\ell^n]$ is the Cartier dual of $A[\ell^n]$. If $A[\ell]$ has subquotients of multiplicative type, then $A^{\mathrm{dual}}[\ell]$ has étale subquotients which is impossible by the same argument given above but now applied to the abelian variety A^{dual}. □

We apply Theorem 1.2 together with the three steps described in the introduction to prove:

Theorem 4.5. *There are no non-zero abelian varieties over* $\mathbf{Q}(\sqrt{13})$ *with good reduction everywhere.*

Proof. We follow the steps mentioned in the introduction:

(1) We define $\mathscr{C}$ to be the category of finite flat commutative group schemes of 2-power order over $O = \mathbf{Z}[\frac{1+\sqrt{13}}{2}]$.

(2) By [Fon85] we know that the root discriminant δ of the extension $T_{\mathscr{C}}/\mathbf{Q}$ satisfies $\delta < 4\sqrt{13}$. By Odlyzko's tables this implies that $[T_{\mathscr{C}} : \mathbf{Q}] < 60$. Group schemes in $\mathscr{C}$ annihilated by 2 are isomorphic to $\mu_2, \mathbf{Z}/2\mathbf{Z}$ and the non-trivial extensions of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 described in [KM85, Section 8.7, p.251] using the units -1 and $\eta = \frac{3+\sqrt{13}}{2}$. Hence $T_{\mathscr{C}}$ contains i and the square root of η:

$$\mathbf{Q}(\sqrt{13}) \subset_4 \mathbf{Q}(i, \sqrt{\eta}) \subset_{\leq 7} T_{\mathscr{C}}.$$

The extension $T_{\mathscr{C}}/\mathbf{Q}(i, \sqrt{\eta})$ is unramified outside 2 and is solvable. However, the smallest non-trivial abelian extension unramified outside 2 of $\mathbf{Q}(i, \sqrt{\eta})$ is a subfield of the ray class field of conductor π_2^6, where π_2 is the unique prime above 2 in $\mathbf{Q}(i, \sqrt{\eta})$. This subfield violates the root discriminant bound on $T_{\mathscr{C}}$. It follows that $T_{\mathscr{C}} = \mathbf{Q}(i, \sqrt{\eta})$. By Lemma 2.2 this implies that every simple object in $\mathscr{C}$ has rank 2.

Since 2 is inert in $\mathbf{Q}(\sqrt{13})$, this implies by [TO70, Corollary, p.21] that the simple group schemes in $\mathscr{C}$ are μ_2 and $\mathbf{Z}/2\mathbf{Z}$. One now checks that Condition (2) is satisfied.

(3) For this category, Now we use Theorem [Sch03, Prop. 2.6] to verify that Condition (1) is satisfied.

The 2-torsion of a non-zero abelian variety over $\mathbf{Q}(\sqrt{13})$ with good reduction everywhere is an object in $\mathscr{C}$, and this 2-torsion subgroup scheme must be filtered by copies of μ_2 or $\mathbf{Z}/2\mathbf{Z}$. This, however, contradicts Theorem 1.2.

□

As another example, we show that:

Theorem 4.6. *There are no non-zero abelian varieties over* $\mathbf{Q}(\sqrt{17})$ *with good reduction everywhere.*

Proof. We follow the steps mentioned in the introduction:

(1) Let $\mathscr{C}$ be the category of finite flat commutative group schemes of 2-power order over $O = \mathbf{Z}[\frac{1+\sqrt{17}}{2}]$. We will see that the category $\mathscr{C}$ does not satisfy Condition (1) of Theorem 1.2.

(2) We find the maximal 2-torsion extension $T_{\mathscr{C}}/\mathbf{Q}(\sqrt{17})$ of $\mathscr{C}$. We leave it as an exercise to show that the extension $T_{\mathscr{C}}/\mathbf{Q}(\sqrt{17})$ is finite and has degree a power of 2. So we can apply Lemma 2.2. By factoring $2 = \pi\bar{\pi}$ in O we find the following simple group schemes: $\mu_2, \mathbf{Z}/2\mathbf{Z}, G_\pi$ and $G_{\bar{\pi}}$, where we refer to [TO70] for the meaning of G_π and $G_{\bar{\pi}}$.

(3) The only simple étale group scheme is $\mathbf{Z}/2\mathbf{Z}$ and we immediately verify Condition (2) for our category $\mathscr{C}$. However, Condition (1) fails because $\mathrm{Ext}^1_O(\mu_2, \mathbf{Z}/2\mathbf{Z})$ is non-trivial due to the splitting of the prime 2 in $\mathbf{Q}(\sqrt{17})/\mathbf{Q}$: A non-trivial extension is given by $G_\pi \times G_{\bar{\pi}}$.

Even though Condition (1) does not hold, it is true that all extensions of simple non-étale group schemes by simple étale group schemes are annihilated by 2: they are

products of G_π's and $G_{\bar{\pi}}$'s. Using this, for any abelian variety A over $\mathbf{Q}(\sqrt{17})$ with good reduction everywhere one deduces that the rank of $A[2^n]$ (which is an object in $\mathscr{C}$) cannot depend on n. Hence there are no such non-zero abelian varieties.

□

We end this article by asking for which square-free integers D do there exist abelian varieties over $\mathbf{Q}(\sqrt{D})$ with good reduction everywhere?

References

[CSS97] Gary Cornell, Joseph H. Silverman, and Glenn Stevens, editors. *Modular forms and Fermat's last theorem*. Springer-Verlag, New York, 1997. Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9–18, 1995.

[Fon85] Jean-Marc Fontaine. Il n'y a pas de variété abélienne sur **Z**. *Invent. Math.*, 81(3):515–538, 1985.

[Hal59] Jr. Marshall Hall. *The theory of groups*. The Macmillan Co., New York, N.Y., 1959.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[Ray74] Michel Raynaud. Schémas en groupes de type $(p, \dots, p)$. *Bull. Soc. Math. France*, 102:241–280, 1974.

[Sch03] René Schoof. Abelian varieties over cyclotomic fields with good reduction everywhere. *Math. Ann.*, 325(3):413–448, 2003.

[Sch05] René Schoof. Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only. *Compos. Math.*, 141(4):847–868, 2005.

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