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 $\ell$-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
2. The generic fiber of simple group schemes
3. Filtrations by simple group schemes
4. Application to abelian varieties
References

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 $\ell$ be a rational prime such that none of the primes in $S$ divides $\ell$.

Definition 1.1. Let $\mathcal{C}$ be a subcategory of the category of finite flat commutative group schemes over $O_S$ of $\ell$-power order, such that $\mathcal{C}$ 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 $\mathcal{C}$ might or might not satisfy. These conditions involve simple group schemes in $\mathcal{C}$, i.e., group schemes that have no non-trivial closed flat subgroup schemes.

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

Condition (2): Let $F$ be the compositum of all $K(E)$, where $E$ runs over all simple étale group schemes $E$ in $\mathcal{C}$. 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 $\ell^n$-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 $A[\ell^n]$ is an object in $\mathcal{C}$ for all $n \in \mathbb{N}$. If Conditions (1) and (2) hold for the category $\mathcal{C}$, then $A[\ell]$ 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 $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{17})$ with good reduction everywhere.

In the rest of the article we continue as follows. First we indicate how one finds simple group schemes in $\mathcal{C}$. Then we discuss filtrations and extensions of group schemes in $\mathcal{C}$ 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 $\mathcal{C}$ that contains $A[\ell^n]$ for all $n$

(2) Find the simple objects in the category $\mathcal{C}$ by using the generic fiber of objects in $\mathcal{C}$ annihilated by $\ell$ and the discriminant bounds of Odlyzko to classify the generic fibers of simple objects in $\mathcal{C}$, 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 $\mathcal{C}$ 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 $\text{char}(K) = 0$, $J_K$ is an étale group scheme. Therefore, the group scheme $J_K$ is just an abelian group $J(K)$ together with the Galois action $\rho_J : G_K \to \text{Aut}(J(K))$. We denote by $K(J)$ the field extension obtained by adjoining the $\overline{K}$-points of $J$ to $K$. The representation $\rho_J$ 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 $\mathcal{C}$ is to classify its simple objects up to isomorphism. Every simple object is annihilated by $\ell$: if not, the Zariski closure of the $\ell$-torsion points in the generic fiber would form a non-trivial closed flat subgroup scheme. Since by assumption $\mathcal{C}$ is closed under taking subquotients, this subgroup scheme would again be in $\mathcal{C}$.

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

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

Proof. Suppose $\rho_J$ 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
The generic fiber of a simple object $J$ in $\mathcal{C}$ is a simple $F_\ell[\text{Gal}(\mathcal{O}_S/L)]$-module. Since simple objects are killed by $\ell$, such a generic fiber is also a simple $F_\ell[\text{Gal}(\mathcal{O}_S/L)]$-module. Therefore we classify all simple $F_\ell[\text{Gal}(\mathcal{O}_S/L)]$-modules. If we can find a relatively large normal $\ell$-subgroup $H$ in $\text{Gal}(\mathcal{O}_S/L)$, it is easier to classify irreducible submodules: the representation $\rho_J$ factors not only through $\text{Gal}(\mathcal{O}_S/L)$, but also through the quotient of $\text{Gal}(\mathcal{O}_S/L)$ by $H$. This is an immediate consequence of:

**Lemma 2.2.** Let $J$ be a simple object in $\mathcal{C}$. Then $\text{Gal}(\mathcal{O}_S/L)$ contains no non-trivial normal $\ell$-subgroup.

**Proof.** The representation $\rho_J$ factors through $\text{Gal}(\mathcal{O}_S/L)$. Let $H$ be a non-trivial normal $\ell$-subgroup of $\text{Gal}(\mathcal{O}_S/L)$. Then $H$ must act faithfully as an $\ell$-group on the $\ell$-group $J$, but this is impossible. There are non-trivial fixed points of $J$ under this action and they form a closed flat subgroup scheme of $J$, which must equal $J$ since $J$ is simple. $\square$

Finally, once simple $F_\ell[\text{Gal}(\mathcal{O}_S/L)]$-modules have been found, the question remains if they extend to finite flat commutative group schemes over $\mathcal{O}_S$. 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 $\mathcal{C}$ 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 $\mathcal{C}$ that admits the simple group scheme $A$. Suppose that for each simple $B$ with $B \not\cong A$ occurring in the filtration of $J$, the group $\text{Ext}^1_{\mathcal{C}}(A, B)$ is trivial. Then $A$ is a closed flat subgroup scheme of $J$.

**Proof.** Consider the short exact sequence

$$0 \rightarrow J' \rightarrow J \rightarrow J/J' = F_2 \rightarrow 0,$$

where $J'$ is simple. If $J' \cong A$ there is nothing to prove, so assume $A \not\cong J'$. 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:

$$0 \rightarrow A \rightarrow J/J' = F_2 \rightarrow F_3 \rightarrow 0.$$
The pull-back of $A$ by $J$ over $F_2$, using (1), gives the short exact sequence

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

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 $\mathcal{C}$ that admits a simple group scheme $A$. If for each simple $B$ with $B \not\simeq A$ occurring in the filtration of $J$, the group $\text{Ext}^1_{\mathcal{C}}(A, B)$ 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 $\mathcal{C}$, then for any $J$ in $\mathcal{C}$ we have an exact sequence

$$0 \rightarrow J' \rightarrow J \rightarrow J'' \rightarrow 0$$

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

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

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 $\text{Frat}(G)$ of $G$ is equal to $[G, G]G^p$. The group $G/\text{Frat}(G)$ 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

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$$

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. \qed

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

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

$$0 \rightarrow J'_F \rightarrow J_F \rightarrow \mathbb{Z}/\ell \mathbb{Z} \rightarrow 0.$$

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

We note that $\Lambda/[\Lambda, \Lambda]$ is an abelian $\ell$-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 $\Lambda$ is cyclic. We conclude that $F(J_F)$ is contained in $R$, which is exactly what we wanted to prove. \qed

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 $\mathcal{C}$. Then for any $J$ in $\mathcal{C}$ having $n$ simple étale group schemes and $m$ simple group schemes of multiplicative type in its filtration, the following inequalities hold:

$$|J_q(F_q)| \geq \ell^n \quad \text{and} \quad |J^*_q(F_q)| \geq \ell^m.$$

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

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 1.3 says that the number of $\ell$-torsion points of $A$ in the fiber at $q$ is at least $\ell^k$. Hence $A[\ell^n]$ has at least $\ell^{kn}$ points in the fiber at $q$. This is in contradiction with the fact that $A(F_q)$ is finite for $n$ sufficiently large. Let $A^{\text{dual}}$ be the dual abelian variety of $A$. For each $n$, the group scheme $A^{\text{dual}}[\ell^n]$ is the Cartier dual of $A[\ell^n]$. If $A[\ell]$ has subquotients of multiplicative type, then $A^{\text{dual}}[\ell]$ has étale subquotients which is impossible by the same argument given above but now applied to the abelian variety $A^{\text{dual}}$. \qed

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 $\mathbb{Q}(\sqrt{13})$ with good reduction everywhere.

Proof. We follow the steps mentioned in the introduction:

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

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

$$Q(\sqrt{13}) \subset \mathcal{C} \subset \mathbb{Q}(i, \sqrt{\eta}) \subset T_{\mathcal{E}}.$$

The extension $T_{\mathcal{E}}/\mathbb{Q}(i, \sqrt{\eta})$ is unramified outside 2 and is solvable. However, the smallest non-trivial abelian extension unramified outside 2 of $\mathbb{Q}(i, \sqrt{\eta})$ is a subfield of the ray class field of conductor $\pi_2^6$, where $\pi_2$ is the unique prime above 2 in $\mathbb{Q}(i, \sqrt{\eta})$. This subfield violates the root discriminant bound on $T_{\mathcal{E}}$. It follows that $T_{\mathcal{E}} = \mathbb{Q}(i, \sqrt{\eta})$. By Lemma 2.2 this implies that every simple object in $\mathcal{C}$ has rank 2.

(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 $\mathbb{Q}(\sqrt{13})$ with good reduction everywhere is an object in $\mathcal{C}$, and this 2-torsion subgroup scheme must be filtered by copies of $\mu_2$ or $\mathbb{Z}/2\mathbb{Z}$. This, however, contradicts Theorem 1.2.

As another example, we show that:

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

Proof. We follow the steps mentioned in the introduction:

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

(2) We find the maximal 2-torsion extension $T_{\mathcal{E}}/\mathbb{Q}(\sqrt{17})$ of $\mathcal{C}$. We leave it as an exercise to show that the extension $T_{\mathcal{E}}/\mathbb{Q}(\sqrt{17})$ 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: $\mu_2$, $\mathbb{Z}/2\mathbb{Z}$, $G_{\pi}$, and $G_{\bar{\pi}}$, where we refer to [TO70] for the meaning of $G_{\pi}$ and $G_{\bar{\pi}}$.

(3) The only simple étale group scheme is $\mathbb{Z}/2\mathbb{Z}$ and we immediately verify Condition (2) for our category $\mathcal{C}$. However, Condition (1) fails because $\text{Ext}^1_O(\mu_2, \mathbb{Z}/2\mathbb{Z})$ is non-trivial due to the splitting of the prime 2 in $\mathbb{Q}(\sqrt{17})/\mathbb{Q}$: 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 $G_π^*$’s. Using this, for any abelian variety $A$ over $\mathbb{Q}(\sqrt{17})$ with good reduction everywhere one deduces that the rank of $A[2^n]$ (which is an object in $\mathcal{C}$) 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 $\mathbb{Q}(\sqrt{D})$ 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 $\mathbb{Z}$. *Invent. Math.*, 81(3):515–538, 1985.

[Hallo59] 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 $(p, \ldots, p)$. *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.