HIGHER EXTENSIONS OF ABELIAN VARIETIES

FRANS OORT and TADAO ODA

In this paper we prove:

THEOREM: *Let k be an algebraically closed field of characteristic $p > 0$, and let X and Y be abelian varieties over k. Then the group $\mathrm{Ext}^2(X, Y) = 0$.*

The result was conjectured by Serre in a letter to the first named author. This case however was left open in [5] and in CGS, while the extension groups of elementary group schemes in all other cases are known over an algebraically closed field. The proof of the theorem we give is suggested by the use of 'Barsotti extensions': in [1], page 24, an extension is constructed of an elliptic curve C with Hasse invariant zero with itself (also compare CGS, 15.7) which has a special property, namely that its image under the map

$$i^*: \ \mathrm{Ext}^1(C, C') \longrightarrow \mathrm{Ext}^1(\alpha_p, C'), \quad C' = C \,/\, \alpha_p$$

is not zero. This suggests that (at least in this case) one should be able to prove $\mathrm{Ext}^2(C, C) = 0$. This idea can be realized even in the general case by translating the problem in terms of Dieudonné modules. So, up to some general considerations, the paper consists of a calculation concerning the non-commutative ring E (see below). We thank Peter Russell for interesting conversation on 'Barsotti extensions'.

First we recall some notions we are going to use. We fix an algebraically closed field k of characteristic $p > 0$ (in case of characteristic zero the result is known, cf. [6]). We denote by $\mathscr{N}_{il}$ the category of commutative finite group schemes over k which are local and unipotent (cf. CGS, I.2), and for any finite group scheme M over k we denote by M_{il} the largest summand of M contained in $\mathscr{N}_{il}$. A unipotent formal group will be an object of the category $\mathrm{Ind}(\mathscr{N}_{il})$ defined by a noetherian (complete, local) ring; the category of unipotent formal groups over k we denote by $\mathscr{F}$.

We write $W_\infty(k) = W$ for the ring of infinite Witt-vectors over k (cf. [7], II.5 and 6), and we denote by E the (non-commutative) power series ring $E = W[[F, V]]$ subject to the well-known relations $Fw = w^\sigma F$, $wV = Vw^\sigma$ and $FV = VF = p$ (cf. [3], [4], and CGS). For any algebraic group scheme G we denote by $\hat{G}_{ll}$ the unipotent formal group obtained as the inductive limit of all finite unipotent local group schemes contained in G:

$$\hat{G}_{ll} = \varinjlim (_{F^i}G)_{ll}$$

(where $_{F^i}G = \mathrm{Ker}\,(G \xrightarrow{F^i} \theta^i G)$). Let $I \in \mathscr{F}$ be the injective hull of $\alpha_p \in \mathscr{N}_{ll} \subset \mathscr{F}$. With any $F \in \mathscr{F}$ we can associate a left module over the ring $E = \underset{\mathscr{F}}{\mathrm{End}}\,(I, I)$ by writing

$$M(F) = \underset{\mathscr{F}}{\mathrm{Hom}}\,(F, I).$$

The Dieudonné-Gabriel classification of unipotent formal groups asserts that M is an anti-equivalence

$$M: \mathscr{F}^\circ \longrightarrow {}_E\mathscr{M}od$$

between the category $\mathscr{F}$ and the category of left Dieudonné modules over the ring E (cf. [3], [4]) (we remark that if H is the Dieudonné algebra which is the injective hull of the hyperalgebra of α_p, then H is the hyperalgebra of I, i.e. $I = \mathrm{Spf}\,(H^D)$).

Let X and X' be isogenuous abelian varieties, and Y and Y' idem. Then $\mathrm{Ext}^2(X, Y) = 0$ if and only if $\mathrm{Ext}^2(X', Y') = 0$: we can construct an isogeny $Y' \longrightarrow Y$ and an isogeny $X \xrightarrow{\varphi} X'$ (by a result of Weil, isogeny is an equivalence relation for abelian varieties), and we obtain (k being algebraically closed):

$$\mathrm{Ext}^2(X', Y') \longrightarrow \mathrm{Ext}^2(X', Y) \longrightarrow 0$$
$$\downarrow$$
$$\mathrm{Ext}^2(X, Y)$$
$$\downarrow$$
$$\mathrm{Ext}^2(\mathrm{Ker}\,\varphi, Y) = 0$$

(use CGS, 12.5 and 12.4), etc. Thus in order to prove the theorem for X' and Y' it suffices to prove the theorem for X and Y. If X' is an abelian

variety, its formal group $\hat{X}'$ is isogenuous to a direct sum of formal groups $G_{n,m}$, where $M(G_{n,m}) = E_{n,m} \overset{def}{=\!=\!=} E \,/\, E\,(V^n - F^m)$ (cf. [3], [4] page 35), with $n = 1$ and $m = 0$ (and $G_{1,0}$ is contained in the toroidal part part of $\hat{X}'$), or $n > 0$, $m > 0$ and $(n, m) = 1$ (and $G_{n,m} \in \hat{X}'_{ll}$). We can choose an abelian variety X isogenuous to X' such that $\hat{X}$ is isomorphic to that direct sum of formal groups (cf. CGS, page II. 15-5). Hence in order to prove the theorem we consider abelian varieties X and Y such that $\hat{X}$ and $\hat{Y}$ are isomorphic to direct sums of isosimple formal groups $G_{n,m}$.

Next we remark that $\mathrm{Ext}^2\,(X, Y)$ is a p-torsion group: we know it is a torsion group by a result of Serre (cf. CGS, 12.1); consider the exact sequence

$$0 \longrightarrow {}_nX \overset{i}{\longrightarrow} X \overset{n \cdot 1_X}{\longrightarrow} X \longrightarrow 0\,,$$

where n is a natural number, thus obtaining the exact sequence

$$\mathrm{Ext}^1\,(X, Y) \overset{i^*}{\longrightarrow} \mathrm{Ext}^1\,({}_nX, Y) \longrightarrow \mathrm{Ext}^2\,(X, Y) \overset{n}{\longrightarrow} \mathrm{Ext}^2\,(X, Y);$$

if $(p, n) = 1$, we know $\mathrm{Ext}^1\,({}_nX, Y) = 0$

Now consider the case $n = p$. In order to prove the theorem we have to show that i^* is a surjective map. We take a positive integer η (which will be fixed later), and we write $q = p^\eta$. Consider the exact commutative diagram

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & {}_qX & \overset{j}{\longrightarrow} & {}_{pq}X & \longrightarrow & {}_pX & \longrightarrow & 0 \\
 & & \Big\| & & \Big\downarrow & & \Big\downarrow{\scriptstyle i} & & \\
0 & \longrightarrow & {}_qX & \longrightarrow & X & \overset{q \cdot 1_X}{\longrightarrow} & X & \longrightarrow & 0
\end{array}
\qquad
\begin{array}{c}
\tau \in \mathrm{Ext}^1\,({}_pX, {}_qX)\,, \\[4pt]
\tau = i^*(\xi)\,, \\[4pt]
\xi \in \mathrm{Ext}^1\,(X, {}_qX)\,.
\end{array}
$$

Thus we obtain a commutative diagram

$$
\begin{array}{ccc}
\mathrm{Ext}^1\,(X, Y) & \overset{i^*}{\longrightarrow} & \mathrm{Ext}^1\,({}_pX, Y) \\[6pt]
\Big\uparrow{\scriptstyle d} & \nearrow & \\[6pt]
\mathrm{Hom}\,({}_qX, Y) & {\scriptstyle \delta} &
\end{array}
\qquad
\begin{array}{c}
d(\psi) = \psi_*(\xi)\,, \\[4pt]
\delta(\psi) = \psi_*(\tau)\,, \\[4pt]
\text{for}\quad \psi \in \mathrm{Hom}\,({}_qX, Y)\,.
\end{array}
$$

We are going to show that the number η can be choosen (X and Y being fixed) in such a way that δ (and hence i^*) is surjective (the image elements of d can be called 'Barsotti extensions'). First note that

$$\mathrm{Hom}\,((_qX)_{ll}, Y) \cong \mathrm{Hom}_{\mathscr{F}}((_qX)_{ll}, \hat{Y}_{ll}),$$

and that

$$\mathrm{Ext}^1\,(_pX, Y) = \mathrm{Ext}^1\,((_pX)_{ll}, Y) \cong \varinjlim \mathrm{Ext}^1\,((_pX)_{ll}, N),$$

the limit taken over all $N \subset Y$ such that $N \in \mathscr{N}_{ll}$ (cf. CGS, 7.4); moreover

$$\varinjlim \mathrm{Ext}^1\,((_pX)_{ll}, N) = \mathrm{Ext}^1_{\,\mathrm{Ind}\,(\mathscr{N}_{ll})}((_pX)_{ll}, \varinjlim N)$$

(cf. [3], page II–12, corollary 1), thus finally

$$\mathrm{Ext}^1\,(_pX, Y) \cong \mathrm{Ext}^1_{\mathscr{F}}((_pX)_{ll}, \hat{Y}_{ll}).$$

Consider the exact sequence

$$\mathrm{Hom}_{\mathscr{F}}((_qX)_{ll}, \hat{Y}) \xrightarrow{\ \delta\ } \mathrm{Ext}^1_{\mathscr{F}}((_pX)_{ll}, \hat{Y}_{ll}) \longrightarrow \mathrm{Ext}^1_{\mathscr{F}}((_{pq}X)_{ll}, \hat{Y}_{ll})$$
$$\xrightarrow{\ j^*\ } \mathrm{Ext}^1_{\mathscr{F}}((_qX)_{ll}, \hat{Y}_{ll});$$

it suffices to prove j^* to be injective. We have choosen X and Y in such a way that their formal groups are direct sums of isosimple formal groups. Hence $_{qp}X, _qX$ and Y can be written as *finite* direct sums; thus we are reduced to prove injectivity of a finite number of components of j^*, each of which is of the following type: $G_{n,m} \hookrightarrow \hat{Y}_{ll}, G_{j,i} \hookrightarrow \hat{X}_{ll}$,

$$\begin{array}{ccc}
\mathrm{Ext}^1_{\mathscr{F}}\,(_{p^{\eta+1}}(G_{j,i}),\ G_{n,m}) & \xrightarrow{\ j^*\ } & \mathrm{Ext}^1_{\mathscr{F}}\,(_{p^{\eta}}(G_{j,i}), G_{n,m}) \\[2pt]
\| & & \| \\[2pt]
\mathrm{Ext}^1_E(E_{n,m}, T_{\eta+1}) & \xrightarrow[M(j)_*]{} & \mathrm{Ext}^1_E(E_{n,m}, T_{\eta}),
\end{array}$$

where

$$E_{n,m} = E\,/\,E(V^n - F^m) \subset M(\hat{Y}_{ll}), \quad (n,m) = 1,$$
$$T_s = M(_{p^s}(G_{j,i})) = E\,/\,E(p^s, V^j - F^i) \subset M((_qX)_{ll}), \; s \geqq 1, \; (i,j) = 1,$$

while

$$0 \longrightarrow T_1 \longrightarrow T_{\eta+1} \xrightarrow{\ M(j)\ } T_{\eta} \longrightarrow 0$$

is the exact sequence corresponding to $\tau \in \mathrm{Ext}^1\,(_pX, _qX)$. Consider the projective resolution of the left E-module $E_{n,m}$:

$$0 \longleftarrow E_{n,m} \longleftarrow E \overset{\rho}{\longleftarrow} E \longleftarrow 0,$$

where $\rho(a) = a \cdot (V^n - F^m)$; we obtain a commutative, exact diagram of additive groups:

$$
\begin{array}{ccccc}
 & & 0 & & 0 \\
 & & \downarrow & & \downarrow \\
 & & T_1 & \longleftarrow & T_1 \\
 & & \downarrow {\scriptstyle p^\eta} & & \downarrow {\scriptstyle p^\eta} \\
0 \longleftarrow \mathrm{Ext}^1_E(E_{n,m}, T_{\eta+1}) & \longleftarrow & T_{\eta+1} & \overset{\lambda}{\longleftarrow} & T_{\eta+1} \\
\downarrow {\scriptstyle M(j)_*} & & \downarrow {\scriptstyle M(j)} & & \downarrow {\scriptstyle M(j)} \\
0 \longleftarrow \mathrm{Ext}^1_E(E_{n,m}, T_\eta) & \longleftarrow & T_\eta & \overset{\lambda}{\longleftarrow} & T_\eta
\end{array}
$$

where $\lambda(b) = (V^n - F^m) \cdot b$ (N.B. $\mathrm{Hom}_E(E, T_s)$ is isomorphic to T_s as an additive group, and right multiplication becomes left). Remark that injectivity of $M(j)_*$ is the same as:

$$Im(T_1 \longrightarrow T_{\eta+1}) \subset Im(\lambda\colon T_{\eta+1} \longrightarrow T_{\eta+1}),$$

which is the same as:

$$p^\eta E \subset p^{\eta+1} E + (V^n - F^m)E + E(V^j - F^i)$$

$(m, n, i$ and j are fixed). Since elements in E are power series in V and F with coefficients in W, every element of $p^\eta E$ is congruent to an element in E of the form

$$\sum_{r \geq 0} \{a_r\} p^\eta F^r + \sum_{s > 0} \{b_s\} p^\eta V^s$$

modulo $p^{\eta+1}E$; here we write $\{a\}$ for the infinite Witt vector with first component $a \in k$, and zero for the rest of its components.

Note that $\{a_r\} p^\eta F^r$ and $\{b_s\} p^\eta V^s$ converge in the topology of E for r and s becoming large. The set $p^{\eta+1}E + (V^n - F^m)E + E(V^j - F^i)$ is closed. Also note that this set is stable under right multiplication by F and by V. Hence to prove the theorem it suffices to show that an integer η can be chosen in such a way that

$$(*) \quad \{a\} p^\eta \in p^{\eta+1}E + (V^n - F^m)E + E(V^j - F^i)$$

for all $a \in k$. There are three cases:

(i) $\qquad \dfrac{m}{n} = \dfrac{i}{j}$, (ii) $\qquad \dfrac{m}{n} > \dfrac{i}{j}$, (iii) $\qquad \dfrac{m}{n} < \dfrac{i}{j}$.

Note that passing to the opposite ring of E case (iii) and case (ii) are interchanged. Thus it suffices to prove (∗) in the cases (i) and (ii).

In case (i), we have $m = i$ and $n = j$, since $(m, n) = 1 = (i, j)$. We choose $\eta = m$. For $a \in k$, there exists an element $b \in k$ such that

$$b^{p^{m+n}} - b = a,$$

k being algebraically closed. Then

$$\{a\}\, p^m = (\{b^{p^{m+n}}\} - \{b\})\, F^m V^m = -(V^n - F^m)\, \{b^{p^n}\}\, V^m + \{b\}\, V^m (V^n - F^m) ,$$

and we are done in the first case.

LEMMA: (1) *Let β be an integer, $0 \le \beta < \dfrac{\eta}{n}$, then*

$$p^\eta \in p^{\eta - \beta n}\, F^{\beta(m+n)} + (V^n - F^m)E .$$

(2) *Let γ, u be integers satisfying $0 \le \gamma(i + j) \le u$; then*

$$F^u \in p^{\gamma j} F^{u - \gamma(i+j)} + E(V^j - F^i) .$$

First we assume this lemma and we finish the proof of the theorem. Since $mj - ni > 0$, we can choose an integer β such that

$$\beta\left(\frac{mj - ni}{i + j}\right) \ge 1;$$

we take $\eta > \beta n$, and we choose for γ the largest integer satisfying

$$\gamma(i + j) \le \beta(m + n) .$$

Using the lemma we conclude:

$$\{a\}p^\eta \in p^{\eta - \beta n}\, F^{\beta(m+n)} \{a\} + (V^n - F^m)E \subset p^{\eta - \beta n + \gamma j}\, E$$
$$+ (V^n - F^m)E + E(V^j - F^i),$$

and we are done since the last inequality above implies

$$\eta - \beta n + \gamma j \ge \eta + \beta\left(\frac{mj - ni}{i + j}\right) \ge \eta + 1 .$$

Thus, granting the lemma, the theorem is proved.

Proof of the lemma: We prove (1) by induction on β (with m, n and η being

fixed). For $\beta = 0$ the formula is obviously true. The induction step is proved by:

$$p^{\eta - \beta n} F^{\beta(m+n)} = p^{\eta - (\beta + 1)n} \cdot V^n \cdot F^{\beta(m+n)+n} = p^{\eta - (\beta + 1)n} F^{(\beta + 1)(m+n)}$$

$$+ (V^n - F^m) F^{\beta(m+n)+n} \cdot p^{\eta - (\beta + 1)n}.$$

We prove (2) by induction on γ (i, j and u being fixed). For $\gamma = 0$ it is clear; the induction step runs as follows:

$$p^{\gamma j} F^{u - \gamma(i+j)} = p^{\gamma j} F^{u - (\gamma + 1)(i+j)} F^{i+j}$$

$$= p^{(\gamma + 1)j} F^{u - (\gamma + 1)(i+j)} - p^{\gamma j} F^{u - (\gamma + 1)(i+j)+j} (V^j - F^i),$$

and the lemma is proved.

REMARK: We note that the theorem is incorrect without the hypothesis k being algebraically closed. There may be non-trivial elements of $\mathrm{Ext}^2(X, Y)$ coming from the "toroidal parts", but also the unipotent parts may provide such elements. Choose a prime number p such that there exists an elliptic curve C of exceptional type defined over the prime field F_p; if $p \equiv 1 \pmod{12}$ this is possible, as was proved by Deuring, cf [2], page 201. We claim that for $X = C = Y$ we have $\mathrm{Ext}^2(X, Y) \neq 0$ (extensions now considered in the category of algebraic group schemes over the prime field). First remark that $\mathrm{Ext}^1(\alpha_p, Y) \neq 0$. Further notice that in this situation any element in the image of

$$\mathrm{Ext}^1(X, Y) \xrightarrow{i^*} \mathrm{Ext}^1(\alpha_p, Y)$$

comes from a Barsotti extension for some η. The similar reduction steps can be applied here. But E is commutative in this case, since we work over the prime field. Then it is easy to see that i^* is not surjective, hence $\mathrm{Ext}^2(X, Y) \neq 0$ in this case.

BIBLIOGRAPHY

[1] I. Barsotti, Abelian varieties over fields of positive characteristic. Rend. Circ. Palermo, Ser. II, **5** (1956), 1–25.

[2] M. Deuring, Die Typen der Multiplikatorenringe ellitischer Funktionenekörper. Abh. Math. Sem. Hamburg Univ. **14** (1941), 197–272.

[3] P. Gabriel, Sur les catégorie abéliennes localement noethériens et leurs applications aux algèbres étudiées par Dieudonné. Sem. J.–P. Serre, 1960.

[4] Yu. I. Manin, The theory of commutative formal groups over fields of finite characte-ristic. Russian Math. Surveys, **18** (1963), 1–80(=Uspehi mat. Nauk **18** (1963), 3–90).

CGS F. Oort, Commutative group schemes. Lecture N. Math. **15,** Springer Verlag, 1966.

[5] K.P. Russell, The theory of commutative algebraic groups. Thesis, University of Calif., Berkeley, 1966.

[6] J.-P. Serre, Groupes proalgébriques. Publ. Math. **7,** IHES, 1960.

[7] J.-P. Serre, *Corps locaux. Act. sc. ind. 1296, Hermann Paris, 1962.*

University of Amsterdam and Harvard University
Nagoya University and Harvard University