Math. Ann. 214, 35—47 (1975)

Which Abelian Surfaces are Products of Elliptic Curves?

Frans Oort

In general an abelian surface is not the product of two elliptic curves, e.g. it may even be not isogenous with a product of elliptic curves, cf. [3], p. 93; [9], Remark (4.3); [4]; [13], last lines of p. 528. But even if the surface is isogenous with a product of elliptic curves, it need not be isomorphic with such a product. For example let E_1 and E_2 be two non-isogenous elliptic curves, and $N = \mathbf{Z}/q$ a subgroup scheme of $E_1 \times E_2$ not contained in either one of the factors; then $(E_1 \times E_2)/N$ is not isomorphic with the product of two elliptic curves. Another example is the following: let E be a supersingular elliptic curve over a field k of characteristic p, choose

$$(i, j) : \alpha_p \to E \times E$$

such that

$$\left(\alpha_p \xrightarrow[\sim]{i} {}_F E \xrightarrow[\sim]{j^{-1}} \alpha_p\right) = \frac{i}{j} \in k \cong \operatorname{End}_k(\alpha_p)$$

has the property

$$\frac{i}{j} \notin \mathbf{F}_{p^2} ;$$

here ${}_F E = \operatorname{Ker}(F : E \to E^{(p)})$; then $X = (E \times E)/(i, j)(\alpha_p)$ can be shown not to be isomorphic with a product of elliptic curves (X is a "Barsotti extension" of E/α_p by E, cf. [7], 15.7). In this note we show that this last example is the "only obstruction" for a supersingular abelian variety not to be isomorphic with a product of elliptic curves.

All fields in consideration will be of characteristic $p > 0$; for any such field we write α_p for the kernel of F on G_a, the additive linear group. We abbreviate abelian variety by AV, and supersingular by ss (i.e. $\hat{X} \sim (G_{1,1})^g$, cf. below, or cf. [9], Section 4).

I thank Mr. T. Shioda for asking a question concerning abelian surfaces in characteristic p, which induced me to prove the results of this note.

Notation 1 (cf. [9], 4.4). Let k be an algebraically closed field, X an AV (= abelian variety) over k,

$$a(X) := \dim_k \operatorname{Hom}(\alpha_p, X).$$

Theorem 2. *Let k be an algebraically closed field, X and AV over k, $\dim X = g$, and suppose*

$$a(X) = g ;$$

then there exist ss elliptic curves $E_1, \ldots, E_g$ over k and an isomorphism

$$X \cong E_1 \times \ldots \times E_g .$$

Remark 3. If $X \cong \Pi E_i$, with E_i ss, then $a(X) = \dim X$; hence for a ss AV this condition is necessary and sufficient for the AV to be isomorphic with a product of elliptic curves. In the example above $a(E \times E/(i, j)(\alpha_p)) = 1$ if $ij^{-1} \notin \mathbf{F}_{p^2}$.

First we note that the fact $a(X)=\dim(X)$ implies X is ss: let $\Sigma G_{n_i,m_i}$ be the isogeny type of the formal group $\hat{X}$ of X (notation of [5]); the fact

$$a(X) \leqq \Sigma_i \min(n_i, m_i)$$

(cf. [7], 15.8) has been proved by Poletti (cf. [10]); because $a(X)=g$, the group scheme μ_p cannot be embedded in X, thus $G_{1,0}$ is not contained in $\hat{X}$, and

$$\hat{X} \sim (G_{1,1})^h + \Sigma_j (G_{s_j,t_j} + G_{t_j,s_j})$$

with $1 \leqq s_j < t_j$ (cf. [5], Theorem 4.1); thus

$$a(X) \leqq h + \Sigma 2s_j, \qquad h + \Sigma(s_j + t_j) = g,$$

which proves $h=g$,

$$\hat{X} \sim (G_{1,1})^g,$$

i.e. X is ss.

By [9], Theorem (4.2) this implies X is isogenous over k with a product of ss elliptic curves; now we are going to show X in fact is isomorphic with such a product iff $a(X)=\dim X$.

Proof, first step. If $g=2$, and $a(X)=2$, then X is purely inseparably isogenous with a product of two elliptic curves. In fact by what is said above, there exist E_1, E_2 and an isogeny

$$\varphi : E_1 \times E_2 \to X.$$

Suppose q is a prime number, $q \neq p = \mathrm{char}(k)$, and suppose the kernel of φ contains a point of order q, i.e.

$$\boldsymbol{Z}/q = N \subset \mathrm{Ker}(\varphi).$$

If $N \subset E_1 \times 0$, then

$$(E_1 \times E_2 \to (E_1/N) \times E_2 \xrightarrow{\varphi'} X) = \varphi.$$

If $N \not\subset E_1 \times 0$, then we construct an isomorphism $i: E_3 \xrightarrow{\sim} E_2$, and a commutative diagram

$$\begin{tikzcd} N \arrow[r, hook] \arrow[dr, dashed] & E_1 \times E_2 \\ & E_3 \arrow[u, "{(u,i)}"'] \end{tikzcd};$$

in that case

$$\begin{pmatrix} id & u \\ 0 & i \end{pmatrix} : E_1 \times E_3 \xrightarrow{\sim} E_1 \times E_2,$$

and

$$(E_1 \times E_2 \cong E_1 \times E_3 \to E_1 \times (E_3/N) \xrightarrow{\varphi'} X) = \varphi.$$

Thus induction on the separable degree of φ then concludes the proof of the first step.

The construction of u can be done as follows. Because $q \neq p$, and $k = \bar{k}$,

$${}_qE_i := \mathrm{Ker}(q: E_i \to E_i) \cong (\boldsymbol{Z}/q) \times (\boldsymbol{Z}/q).$$

Because E_1 and E_2 are supersingular, and because $k=\bar{k}$,

$$H := \mathrm{Hom}_k(E_2, E_1) \cong \boldsymbol{Z}^4$$

(E_1 and E_2 are supersingular, hence isogenous over $\bar{k}$, and H is torsion free over $\mathrm{End}_k(E_1)$; note that $\mathrm{End}_k(E_i)$ is free of rank 4 over $\boldsymbol{Z}$; for references, cf. below). Suppose $h \in H$ has the property

$$({}_qE_2 \hookrightarrow E_2 \xrightarrow{h} E_1) = 0,$$

then $\mathrm{Ker}(h) \supset {}_qE_2$, thus $h \in q.\,H$. This shows that

$$\mathrm{Ker}\,(\varrho: H \to \mathrm{Hom}\,({}_qE_2, {}_qE_1)) = q \cdot H,$$

thus $\varrho(H) = H/q \cdot H = \boldsymbol{Z}^4/q \cdot \boldsymbol{Z}^4$, and because

$$\mathrm{Hom}\,({}_qE_2, {}_qE_1) \cong (\boldsymbol{Z}/q)^4,$$

this shows ϱ to be *surjective*. Let

$$v_i := (\boldsymbol{Z}/q = N \to E_1 \times E_2 \to E_i);$$

because v_2 is injective, we can construct a commutative diagram

$$\begin{tikzcd} \boldsymbol{Z}/q = N \arrow[r, "v_2"] \arrow[d, "v_1"'] & {}_qE_2 \cong (\boldsymbol{Z}/q) \times (\boldsymbol{Z}/q); \arrow[dl, dashed, "w"] \\ (\boldsymbol{Z}/q) \times (\boldsymbol{Z}/q) \cong {}_qE_1 & \end{tikzcd}$$

thus $E_3 = E_2$, $u \in H$ with $\varrho(u) = w$ has the desired property

$$N \subset (u, \mathrm{id})\,(E_3) \subset E_1 \times E_2,$$

which proves the first step by what is said above.

The next step in the proof will be the inseparable case with $g = 2$, it will be based on the same idea as the first step; beforehand we recall some facts we need:

Some Facts and Notations 4. As before we denote by k an algebraically closed field (of characteristic $p > 0$); by K_i we denote the field with p^i elements, $K_i = \boldsymbol{F}_{p^i}$. Note:

(4.1) *There exists a ss elliptic curve E defined over $K_1 = \boldsymbol{F}_p$ which has all its endomorphisms defined over K_2.* Take the case $\beta = 0$ of [13], Theorem (4.1.5): then $\pi = \pm\sqrt{-p}$, and E defined over K_1 with Weil number π has the property

$$\mathrm{End}_{K_2}(E) \cong \boldsymbol{Z}^4$$

($\cong$ as abelian groups).

All isogenies in consideration will be over $k = \bar{k}$, and we write E instead of $E \otimes k$ or $E \otimes K_i$.

(4.2) *Let E_1 be a ss elliptic curve; then there exist separable isogenies*

$$E \to E_1 \quad \text{and} \quad E_1 \to E.$$

In fact any two ss elliptic curves are isogenous over $\overline{\boldsymbol{F}_p}$ (cf. [13], p. 538), so we can choose an isogeny (with E as in 4.1)

$$d: E \to E_1;$$

suppose the inseparable degree of d equals p^j, then d can be factored

$$(E \xrightarrow{F^j} E^{(p^j)} \xrightarrow{d'} E_1) = d\,,$$

with d' separable; because E is defined over the prime field K_1, we know $E^{(p)} \cong E$, thus $E^{(p^j)} \cong E$ (isomorphisms even over K_1), thus $d': E \to E_1$ is a separable isogeny. The degree n of d' is not divisible by p (because E has no points of order p and d' is separable), thus d'' defined by

$$(E \xrightarrow{d'} E_1 \xrightarrow{d''} E) = n \cdot \mathrm{id}_E$$

is separable, which proves (4.2).
Let E_2 and E_1 be elliptic curves. We write

$$_FE_i := \mathrm{Ker}\,(F: E_i \to E_i^{(p)})$$

(thus $_FE_i \cong \alpha_p$ iff E_i is ss). We write $\mathrm{Hom} = \mathrm{Hom}_k$; the inclusions

$$_FE_i \hookrightarrow {}_pE_i \hookrightarrow E_i$$

define restriction homomorphisms:

$$\varrho: H := \mathrm{Hom}\,(E_2, E_1) \to H_p := \mathrm{Hom}\,({}_pE_2, {}_pE_1)$$

and

$$r: H_p \to H_F := \mathrm{Hom}\,({}_FE_2, {}_FE_1)\,.$$

Lemma 5. Suppose E_1 and E_2 are ss, and $k = \bar{k}$, then

$$r(\varrho(H)) = r(H_p)\,.$$

Proof. We choose E as in (4.1), and we take *separable* isogenies

$$x: E_2 \to E, \qquad y: E \to E_1\,;$$

composition with x and y yields a homomorphism

$$y?x: \mathrm{Hom}_k(E, E) \to H = \mathrm{Hom}_k(E_2, E_1)\,.$$

Thus we arrive at a commutative diagram

$$\begin{tikzcd}
A := \mathrm{Hom}_{K_2}(E, E) \arrow[r] \arrow[d, "\varrho"] & \mathrm{Hom}_k(E, E) \arrow[r, "y?x"] \arrow[d] & H \arrow[d, "\varrho"] \\
A_p := \mathrm{Hom}_{K_2}({}_pE, {}_pE) \arrow[r] \arrow[d, "r"] & \mathrm{Hom}_k({}_pE, {}_pE) \arrow[r] \arrow[d] & H_p \arrow[d, "r"] \\
A_F := \mathrm{Hom}_{K_2}({}_FE, {}_FE) \arrow[r, "a"] & \mathrm{Hom}_k({}_FE, {}_FE) \arrow[r, "b"] & H_F\,.
\end{tikzcd}$$

We note the following facts. The homomorphism a is injective (if $z \in {}_F A$, and $z \otimes k = a(z) = 0$, then $z = 0$). The homomorphism b is bijective (x and y are separable, hence

$$x|_F E_2 : {}_F E_2 \xrightarrow{\sim} {}_F E ,$$

and the same for $y|_F E$). By the choice of E, cf. (4.1), we know A is a free abelian group of rank 4. We claim

$$|r(\varrho(A))| = p^2$$

First note $\operatorname{Ker}(\varrho : A \to A_p) = p \cdot A$ (same arguments as used in the first step), thus

$$\varrho(A) = A/p \cdot A \cong (\mathbf{Z}/p)^4 .$$

Next note that

$$|A_p| = p^4 \quad \text{and} \quad r(A_p) = A_F ;$$

in fact, for ${}_pE$ we have an exact sequence

$$0 \to {}_F E \to {}_p E \to {}_p E/{}_F E \to 0 ,$$

thus an injection

$$\operatorname{Ker}(r : A_p \to A_F) \hookrightarrow \operatorname{Hom}_{K_2}(({}_pE/{}_FE), {}_FE) ;$$

because

$${}_pE/{}_FE \cong \alpha_p \cong {}_FE \quad \text{and} \quad \operatorname{Hom}_{K_2}(\alpha_p, \alpha_p) \cong K_2 ,$$

we conclude that the kernel of r has at most $|K_2| = p^2$ elements, A_p contains $\varrho(A)$, thus $r(A_p)$ has at least p^2 elements, and $r(A_p) \subset A_F \cong K_2$, thus

$$|A_p| = p^4 , \quad \varrho(A) = A_p , \quad r(\varrho(A)) = r(A_p) = A_F .$$

Thus the image $\operatorname{bar}\varrho(A)$ has p^2 elements. Clearly

$$\operatorname{bar}\varrho(A) \subset r\varrho(H) \subset r(H_p) ,$$

and now we show:

$$|r(H_p)| = p^2 .$$

This we prove with the help of Dieudonné modules (cf. [5], and [2], V.1.4). Consider the ring $\mathfrak{E} := W[F, V]$, where W is the ring of infinite Witt vectors over k, and F and V satisfy the well known relations; the Dieudonné modules of ${}_pE_2$ and ${}_pE_1$ are isomorphic with $M_2 := \mathfrak{E}/\mathfrak{E}(F - V, p)$, the Dieudonné modules of ${}_FE_2$ and ${}_FE_1$ are isomorphic with $M_1 := \mathfrak{E}/\mathfrak{E}(F - V, F)$, and

$$\begin{array}{ccc} H_p = \operatorname{Hom}_k({}_pE_2, {}_pE_1) & \cong & \operatorname{End}_{\mathfrak{E}}(M_2) \\ \Big\downarrow r & & \Big\downarrow r \\ H_F = \operatorname{Hom}_k({}_FE_2, {}_FE_1) & \cong & \operatorname{End}_{\mathfrak{E}}(M_1) ; \end{array}$$

denote by $e = 1 \bmod \mathfrak{E}(F - V, p)$, which is a generator for the $\mathfrak{E}$-module M_2. Any element of M_2 can be written uniquely in the form $(a + bF).e$, with $a, b \in k$. Suppose $f \in \operatorname{End}_{\mathfrak{E}}(M_2)$;

$$f(e) = (a + bF) \cdot e ;$$

then

$$0 = f((F - V) \cdot e) = (F - V)(a + bF) \cdot e = (a^p - a^{p^{-1}}) \,\mathrm{Fe} ,$$

thus $a^p = a^{p^{-1}}$, i.e. $a \in K_2$. Thus

$$H_p \cong \{(a,b) | a \in K_2, b \in k\},$$

and

$$r(H_p) \cong \{a | a \in K_2\};$$

this proves

$$|r(H_p)| = p^2.$$

By what is said before, this shows the equality stated in the lemma. Q.E.D

Remark. The notation H_p is slightly misleading: note that $A_p = A/p \cdot A$, and H_p contains $H/p \cdot H$, but $H_p \neq \varrho(H) = H/p \cdot H$.

Proof, second step. The case $g=2$. By the first step we may assume there exists an isogeny

$$\varphi : E_1 \times E_2 \to X$$

which is purely inseparable. If ${}_F\mathrm{Ker}(\varphi)$ equals ${}_FE_1 \times {}_FE_2$ we can factor

$$(E_1 \times E_2 \longrightarrow E_1^{(p)} \times E_2^{(p)} = E_1 \times E_2/{}_F\mathrm{Ker}(\varphi) \xrightarrow{\varphi'} X) = \varphi;$$

repeating this process we end at a situation where $\varphi : E_1 \times E_2 \to X$ has the property

$$N := {}_F\mathrm{ker}(\varphi) \cong \alpha_p.$$

If $N \subset E_1 \times 0 \subset E_1 \times E_2$, then

$$(E_1 \times E_2 \longrightarrow (E_1/N) \times E_2 \xrightarrow{\varphi'} X) = \varphi.$$

If $N \not\subset E_1 \times 0$, we claim there exist E_3 and $u : E_3 \longrightarrow E_1$, $i : E_3 \xrightarrow{\sim} E_2$ exactly as in the first step; if so we can factor

$$(E_1 \times E_2 \cong E_1 \times E_3 \longrightarrow E_1 \times (E_3/N) \xrightarrow{\varphi'} X) = \varphi,$$

and induction on the degree of φ' concludes the proof of the second step; thus it remains to construct $u : E_3 \to E_1$ as indicated.

If

$${}_F\mathrm{Ker}(\varphi) = N = \alpha_p \neq \mathrm{Ker}(\varphi),$$

then

$$L := \mathrm{Ker}(F^2 : \mathrm{Ker}(\varphi) \to \mathrm{Ker}(\varphi)^{(p^2)})$$

is a group scheme of rank p^2, and

$$u_2 := (L \to \mathrm{Ker}\,\varphi \to E_1 \times E_2 \to E_2)$$

is monomorphic because $N \hookrightarrow F_2$, and N is the only proper non-trivial subgroup scheme of L; thus in this case

$$L \xrightarrow[w_2]{\sim} {}_pE_2 \hookrightarrow E_2.$$

If

$$v_1 := (N \to {}_FE_1 \times {}_FE_2 \to {}_FE_1)$$

equals zero, we can choose $(u : E_2 = E_3 \to E_1) = 0$; if $v_1 \neq 0$, then v_1 is an isomorphism between N and ${}_FE_1$, and

$$u_1 := (L \to E_1 \times E_2 \to E_1)$$

defines an isomorphism

$$u_1|L = w_1 : L \xrightarrow{\sim} {}_pE_1 .$$

Thus

$$\begin{tikzcd}
{}_pE_2 \arrow[r, "w_2^{-1}"] & L \arrow[r, "w_1"] & {}_pE_1 \\
{}_FE_2 \arrow[r, "v_2^{-1}"] \arrow[u, hook] & N \arrow[r, "v_1"] \arrow[u, hook] & {}_FE_1 \arrow[u, hook]
\end{tikzcd} \qquad r(w_1 w_2^{-1}) = v_1 v_2^{-1},$$

and by Lemma 5 we conclude the existence of $u: E_2 \to E_1$ with $u|_FE_2 = v_1 v_2^{-1}$, i.e.

$$\begin{tikzcd}
N \arrow[r, "(u_1, u_2)"] \arrow[dr, dashed] & E_1 \times E_2 \\
& E_3 \cong E_2 . \arrow[u, "(u, i)"']
\end{tikzcd}$$

The last case to consider in this step is $N \not\subset E_1 \times 0$, thus $v_2 : N \xrightarrow{\sim} {}_FE_2$, and $N = \operatorname{Ker} \varphi$.

Consider the exact commutative diagram

$$\begin{tikzcd}
& & & 0 \arrow[d] & \\
& & E_1 \arrow[r, "\sim"] \arrow[d] & E_1 \arrow[d] & \\
0 \arrow[r] & N = \alpha_p \arrow[r] \arrow[d, equal] & E_1 \times E_2 \arrow[r, "\varphi"] \arrow[d] & X \arrow[r] \arrow[d, "\pi"] & 0 \\
0 \arrow[r] & N \arrow[r] & E_2 \arrow[r] \arrow[d] & E_2/N \arrow[r] \arrow[d] & 0 \\
& & 0 & 0 &
\end{tikzcd}$$

Because $a(X) = 2$, we know

$${}_FX \cong \alpha_p \times \alpha_p ,$$

thus we can choose

$$\alpha_p = L' \hookrightarrow {}_FX$$

so that

$$\pi|L' : L' \xrightarrow{\sim} {}_F(E_2/N) ;$$

we define

$$L := \varphi^{-1}(L') \subset E_1 \times E_2 .$$

We show ${}_FL \neq L$; in fact suppose we would have ${}_FL = L$, then $L = {}_F(E_1 \times E_2)$, because $L \subset E_1 \times E_2$ and rank $(L) = p^2$, thus $L \cap E_1 \neq 0$, thus $\varphi(L \cap E_1) \neq 0$ (because $\varphi|E_1$ is monomorphic); this contradicts $E_1 \cap \varphi L = E_1 \cap L' = 0$. Thus ${}_FL \neq L$, and we conclude N is the only non-trivial proper subgroup scheme of L; now we conclude as before: if

$$v_1 := (N \to {}_FE_1 \times {}_FE_2 \to {}_FE_1) = 0$$

we choose $u=0$; if $v_1 \neq 0$, then

$$w_1 := (L \to {}_pE_1 \times {}_pE_2 \to E_1)$$

is an isomorphism and we construct u as before. This concludes the proof of the second step.

From these proofs we conclude the following corollary:

Proposition 6. *Let E_1 and E_4 be elliptic curves fitting into an exact sequence*

$$0 \to E_1 \to X \to E_4 \to 0\,; \tag{$*$}$$

suppose $a(X)=2$; then this sequence splits.

Proof. By a result of Serre (cf. [11], 5.3, Lemma 7; [12], 7.4, Proposition 4) we know that every element of $\operatorname{Ext}(E_4, E_1)$ is a torsion element, thus there exists an integer m such that

$$m \cdot \mathrm{id} : E_4 \to E_4$$

splits the extension $(*)$:

$$\begin{tikzcd}
0 \arrow[r] & E_1 \arrow[r] & X \arrow[r] & E_4 \arrow[r] & 0 \\
0 \arrow[r] & E_1 \arrow[r] \arrow[u, equal] & Y \arrow[r] \arrow[u] & E_4 \arrow[r] \arrow[u, "m \cdot \mathrm{id}"'] \arrow[l, dashed, bend right] & 0 \\
 & & I \arrow[u] \arrow[r, phantom, ":="] & {}_mE_4 \arrow[u] &
\end{tikzcd}$$

We factor $m \cdot \mathrm{id}: E_4 \to E_4$ in the following way:

$$m \cdot \mathrm{id} = (E_4 = D_0 \to D_1 \to \cdots \to D_j \xrightarrow{f_j} D_{j+1} \to \cdots \to D_t = E_4)\,,$$

such that the degree of each f_j is a prime number (thus t equals twice the number of prime factors in m), and there exist some j_0 with f_j separable for $j \leqq j_0$ and f_{j_0} inseparable for $j > j_0$, i.e. $D_{j_0} = E_4/I_{\mathrm{sep}}$. Induction assumption: for $0 \leqq j < t$,

$$\begin{tikzcd}
(*) & 0 \arrow[r] & E_1 \arrow[r] & X \arrow[r] & E_4 \arrow[r] & 0 \\
(*_{j+1}) & 0 \arrow[r] & E_1 \arrow[r] \arrow[u, equal] & X_{j+1} \arrow[r] \arrow[u] & D_{j+1} \arrow[r] \arrow[u] & 0 \\
(*_j) & 0 \arrow[r] & E_1 \arrow[r] \arrow[u, equal] & X_j \arrow[r] \arrow[u] & D_j \arrow[r] \arrow[u] \arrow[l, dashed, bend right] & 0\,, \\
 & & & I_j \arrow[u] \arrow[r, phantom, ":="] & \operatorname{Ker}(f_j) \arrow[u] &
\end{tikzcd}$$

the extension $(*_j)$ splits; here $D_{j+1} \to E_4 = D_t$ is defined as the composite map of $f_{t-1}, \ldots, f_{j+1}$, and $(*_{j+1})$ and $(*_j)$ are defined by pulling back $(*)$. From this induction assumption we are going to deduce that the morphism $g_j: D_j \to X_j$ which splits $(*_j)$ can be chosen in such a way that

$$I_j \subset g_j(D_j)\,;$$

if that is proved

$$g_j(D_j)/I_j \subset X_{j+1} = X_j/I_j$$

is a section for $X_{j+1} \to D_{j+1} = D_j/\mathrm{Ker}(f_j)$ which establishes the induction step: $(*_{j+1})$ splits. In order to construct g_j we look at the proofs of the first and the second step. If $j \leqq j_0$, then $\mathrm{Ker}(f_j) \cong (\mathbf{Z}/q)$ for some prime number $q \neq p$; we can apply the first step with $D_j = E_2$, and construct

$$g_j(D_j) = E_3 \hookrightarrow E_1 \times E_2$$

containing $N = \mathrm{Ker}(f_j)$. If $j > j_0$ and $j < t-1$, then we choose

$${}_pD_j \cong L := \mathrm{Ker}\,(D_j \xrightarrow{f_j} D_{j+1} \xrightarrow{f_{j+1}} D_{j+2}),\ D_j = E_2$$

and proceed as in step two, arriving at $\mathrm{Ker}(f_j) \subset E_3 = : g_j(D_j)$. If $j > j_0$ and $j = t-1$, then $a(X) = 2$ ensures the existence of $L \cong {}_pD_{t-1}$ with $I_{t-1} \subset L \subset X_{t-1}$, and we conclude again as in step two. This establishes the induction step, and the proposition is proved.

Corollary 7. *Let $k = \bar{k}$, Let X be a ss abelian surface, with $a(X) = 1$; then X is an α_p-covering of a product of two elliptic curves, i.e. X/α_p is isomorphic with a product of two elliptic curves.*

Corollary 8. *Let E_1, E_4 be ss elliptic curves over $k = \bar{k}$. The homomorphism*

$$F: E_4^{(p^{-1})} \to E_4$$

induces the zero map

$$0 = F^*: \mathrm{Ext}\,(E_4, E_1) \to \mathrm{Ext}\, E_4^{(p^{-1})}, E_1)\,.$$

For any ss elliptic curve E_5,

$$\mathrm{Ext}\,(E_5, E_1) \cong k^+$$

Proof. We write $E_5 = E_4^{(p^{-1})}$. Because

$$\mathrm{Ext}\,(E_4, \alpha_p) \cong k^+$$

(cf. [7], II.14—2), we conclude

$$(D_{t-1} \to D_t = E_4) \cong (F: E_5 \to E_4)\,,$$

and the arguments of the previous proof apply, thus proving the splitting of $(*_{t-1})$; thus $F^* = 0$. If E_5 is given, we choose E_4 with $E_5 = E_4^{(p^{-1})}$, because $F^* = 0$, and because $\mathrm{Ext}\,(E_4, E_1) = 0$ (cf. [8]; [6], Theorem 2; here we use $k = \bar{k}$), the isomorphisms

$$\mathrm{Ext}\,(E_5, E_1) \xrightarrow{\sim} \mathrm{Ext}\,(\alpha_p, E_1) \cong k^+$$

results, which concludes the proof of the corollary.

Proof of Theorem 2, last step. If $g = 1 = \dim X$, then X is a ss elliptic curve. Suppose $g > 1$, and suppose the theorem to be proved in the case of AV of dimension equal to $g-1$. If $a(X) = g = \dim X$, then X is ss as we have proved above, there exist a ss elliptic curve E_1 and an inclusion $E_1 \subset X$ (there exist an isogeny $E'_1 \times \ldots \times E'_g \to X$, with all E'_i ss, and let E_1 be the image in X of one of these factors). The exact sequence

$$0 \to E_1 \to X \to Y \to 0$$

yields an exact sequence

$$0 \to {}_F E_1 \to {}_F X \to {}_F Y \to 0\,.$$

Because $a(X) = \dim(X) = g$, we know

$${}_F X \cong (\alpha_p)^g\,,$$

thus $a(Y) = g - 1 = \dim(Y)$. The induction hypothesis can be applied, i.e.

$$Y \cong E_2 \times \ldots \times E_g, \qquad \text{with } E_i \; ss\,.$$

Consider the diagram

$$\begin{tikzcd}
0 \arrow[r] & E_1 \arrow[r] \arrow[d, equal] & Z_i \arrow[r] \arrow[d, shift right] & E_i \arrow[rr] \arrow[d, shift right] & & 0 \\
0 \arrow[r] & E_1 \arrow[r] & X \arrow[r] \arrow[u, shift right] & E_2 \times \cdots \times E_g \arrow[rr] \arrow[u, shift right] & & 0
\end{tikzcd}$$

with exact rows, $2 \leqq i \leqq g$. It follows that $a(Z_i) = 2$ for all i, and by Proposition 6 this implies

$$0 = (Z_i) \in \operatorname{Ext}(E_i, E_1)\,;$$

under the isomorphism

$$\operatorname{Ext}(Y = E_2 \times \ldots \times E_g, E_1) \cong \bigoplus_{i=2}^{g} \operatorname{Ext}(E_i, E_1)$$

the extension Z corresponds with

$$(Z_2, \ldots, Z_g) = (0, \ldots, 0)$$

thus

$$X \cong E_1 \times Y \cong E_1 \times E_2 \times \ldots \times E_g\,,$$

and Theorem 2 is proved

Remark 9. Let K be a field of characteristic $p > 0$, and G a commutative K-group scheme; we write

$$a_K(G) = \dim_K \operatorname{Hom}(\alpha_p, G)\,;$$

let k be a field containing K; then

$$a_K(G) \leqq a_k(G \otimes k)\,;$$

equality holds if K is perfect. Equality holds if ${}_F G$ is unipotent, thus equality holds if $G = X$, an AV, and $a_K(G) = \dim(X)$. The equality does not hold e.g. if K is not perfect, $k = \bar{K}$, and G fits into a non-splitting exact sequence.

$$0 \to \mu_p \to G \to \alpha_p \to 0\,.$$

Remark 10. Let K be a field, $k \supset \bar{K}$, and X an AV over K. Then $a_K(X) = \dim(X)$ is equivalent with $a_k(X) = \dim(X)$, but these conditions are not sufficient to ensure X is isomorphic *over* K with a product of elliptic curves (i.e. $k = \bar{k}$ is essential in Theorem 2):

Example (10.1). There exists an abelian surface X over K_1 with $a(X) = 2$ and X *not isogenous over* K_1 with a product of two elliptic curves over K_1; take

$\pi = p^{\frac{1}{2}}$, this is the Weil number of an elementary abelian surface Z over $K_1 = \boldsymbol{F}_p$ (cf. [13], bottom of p. 528); if $a(Z) = 2$, take $X = Z$; if $a(Z) = 1$, then $\alpha_p \subset Z$ and $X := Z/\alpha_p$ is easily seen to have the property $a(X) = 2$.

Example (*10.2*). There exist an abelian surface X, two elliptic curves E_1 and E_2, an isogeny $E_1 \times E_2 \to X$, all defined over K_2, such that $a(X) = 2$, and X not *K_2-isomorphic* with a product of two elliptic curves over K_2. Choose a prime number p with $p \equiv 3 \pmod 4$, Let $\beta_1 = 0$, $\beta_2 = 2p$, and consider two elliptic curves E_1, respectively E_2 defined over $K_2 = \boldsymbol{F}_{p2}$ defined by the Weil numbers π_1, respectively π_2 which are zeros of $T_1^2 + p^2$, respectively $T_2^2 - 2p + p^2$ (cf. [13], Theorem 4.1, case (5), respectively (2)); the curves E_1, E_2 correspond to different K_2-isogeny classes; note that

$$(\pi_1 \bmod 2)^2 = 1 = (\pi_2 \bmod 2)^2,$$

thus both curves contain a point of order 2 rational over K_2; use these points to obtain an embedding

$$\boldsymbol{Z}/2 = N \hookrightarrow E_1 \times E_2, \quad N \not\subset E_1 \times 0, \quad N \not\subset 0 \times E_2,$$

and define

$$X := (E_1 \times E_2)/N;$$

suppose $X \cong E_3 \times E_4$ ($\cong$ over K_2); E_1 is K_2-isogenous with E_3 (or with E_4), in that case E_2 is not K_2-isogenous with E_3, thus $E_4 \cong X/E_1 = E_2/N$, and

$$(E_1 \times E_2 \to X)^{-1}(E_4)$$

contains an elliptic curve $E_5 \subset E_1 \times E_2$ with $E_5 \neq E_1 \times 0$ and $E_5 \neq 0 \times E_2$; thus E_5 is the graph of an isogeny between E_1 and E_2, contradiction, thus $X \not\cong E_3 \times E_4$. Note that $E_1 \times E_2 \to X$ is separable, thus $a(X) = a(E_1 \times E_2) = 2$, and the example is established.

Note that if X is K-isogenous with $E_1 \times E_2$, such that E_1 and E_2 are K-isogenous and all endomorphisms defined over K (i.e. $\mathrm{End}_K(E_1) \cong \boldsymbol{Z}^4$), and $a(X) = 2$, then X is K-isomorphic with a product of two elliptic curves: $X/E_3 \cong E_4$ with $E_1 \sim E_3$, $E_2 \sim E_4$, and $\Gamma := \mathrm{Gal}(k = \bar{K}/K)$ acts trivially on $\mathrm{Hom}_k(E_4, E_3)$, thus

$$H^1(\Gamma, \mathrm{Hom}_k(E_4, E_3)) = \mathrm{Hom}(\Gamma, \mathrm{Hom}(E_4, E_3)) = 0,$$

which proves (cf. [6], Proposition on p. 437), that $\mathrm{Ext}_K(E_3, E_4)$ is a subgroup of $\mathrm{Ext}_k(E_3 \otimes k, E_4 \otimes k)$; moreover the extension splits over k, thus it splits over K. However:

Example (*10.3*). Let $K = K_2$, and E a *ss* elliptic curve over K_2, such that

$$r\varrho : \mathrm{End}_K(E) \to \boldsymbol{F}_p \subset \mathrm{End}_K({}_F E) \cong K$$

(e.g. $p = 3$, $\beta = p$, $\pi^2 - 3\pi + 9 = 0$ corresponds to a curve E over $\boldsymbol{F}_9$ (cf. [13], Theorem 4.1.3), $\mathrm{End}_K(E)$ is contained in $\boldsymbol{Z}[\frac{1}{2}(1 + \sqrt{-3})]$, thus any $\alpha \in \mathrm{End}_K(E)$ operates on the tangent space of E at zero by multiplication by an element of $\boldsymbol{F}_p$). Choose two monomorphisms

$$i, j : \alpha_p \longrightarrow E, \frac{i}{j} = ({}_F E \xrightarrow{j^{-1}} \alpha_p \xrightarrow{i} {}_F E) =: x$$

with $x \notin \boldsymbol{F}_p$. Define

$$N := (i, j)(\alpha_p), \qquad X := (E_1 \times E_2)/N, \qquad E_1 = E = E_2 .$$

We claim: $a(X) = 2$, and X is not isomorphic over $K = K_2$ with a product of two elliptic curves. The fact $a(X) = 2$ follows fron $x \in K_2$ (e.g.: over $\bar{K}$ there exists $D \subset E_1 \times E_2$ containing N because $\varrho r(\mathrm{End}_K(E)) = K_2 \subset H_F$, cf. Lemma 5). Suppose

$$X \cong E_3 \times E_4 \qquad (\text{over } K_2).$$

Because $q: E_1 \times E_2 \to X$ is a non-trivial extension $E_1 \times E_2/N \cong X$, at least one of the extensions

$$0 \to \alpha_p \to \bar{q}^1(E_a) \to E_a \to 0 \qquad a = 3, 4$$

is non-split, thus $\bar{q}^1 E_3 = : D$ (or 3 replaced by 4) is an elliptic curve, containing N; the two projections $E_1 \times E_2 \to E_a$ yield homomorphisms

$$f, g: D \to E_1, E_2$$

which are non-zero and separable (because ${}_F D = N$, and $(N \to E_1 \times E_2 \to E) = i$ or $= j$); choose a natural number m, not divisable by p, so that a commutative diagram

$$\begin{tikzcd} E_2 \arrow[rr, "m"] \arrow[dr, "g'"'] & & E_2 \\ & D \arrow[ur, "g"'] & \end{tikzcd}$$

exists, and

$${}_F E \xrightarrow{m} {}_F E \xrightarrow{j^{-1}} N \xrightarrow{i} {}_F E$$

equals

$$(f g')|_F E : ({}_F E_2 \to {}_F D \to {}_F E_1) ;$$

because g' and f are defined over $K = K_2$, we conclude

$$m x = m \cdot \frac{i}{j} = f g'|_F E = r \varrho(f g') \in \boldsymbol{F}_p ,$$

a contradiction with $x \notin \boldsymbol{F}_p$, which shows that X is not isomorphic with a product of two elliptic curves over K_2.

References

1. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg **14**, 197—272 (1941)
2. Demazure, M., Gabriel, P.: Groupes algébriques, I. Amsterdam: North-Holl. Publ. Cy. 1970
3. Honda, T.: Isogeny classes of abelian varieties over finite fields. Journ. Math. Soc. Japan **20**, 83—95 (1968)
4. Lenstra, H. W. Jr., Oort, F.: Simple abelian varieties having a prescribed formal isogeny type. Journ. pure appl. algebra **4**, 47—53 (1974)
5. Manin, Yu. I.: The theory of commutative formal groups over fields of finite characteristic. Russ. Math. Surveys **18**, 1—80 (1963)
6. Milne, J. S.: The homological dimension of commutative group schemes over a perfect field. Journ. Algebra **16**, 436—441 (1970)

7. Oort, F.: Commutative group schemes. Lect. Notes Math. 15, Berlin-Heidelberg-New York: Springer 1966
8. Oort, F., Oda, T.: Higher extensions of abelian varieties. Nagoya Math. J. **31**, 81—88 (1968)
9. Oort, F.: Subvarieties of moduli spaces. Inventiones math. **24**, 95—119 (1974)
10. Poletti, M.: Differentiali esatti di prima specie su varietà abeliane. Ann. Scuola norm. sup. Pisa, Sci. fis. mat. **21**, 107—110 (1967)
11. Serre, J.-P.: Espaces fibrés algébriques. Sém. C. Chevalley **2**, exp. 1 (1958)
12. Serre, J.-P.: Groupes proalgébriques. Publ. Math. No. 7, IHES, 1960
13. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. sc. Ec. Norm. Sup. **2**, 521—560 (1969)

F. Oort
Mathematisch Instituut
Roetersstraat 15
Amsterdam, The Netherlands

(Received June 19, 1974)