AN ELEMENTARY PROOF THAT ELLIPTIC CURVES ARE ABELIAN VARIETIES

Autor(en): **Olson, Loren D.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **19 (1973)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-46291

AN ELEMENTARY PROOF THAT ELLIPTIC CURVES ARE ABELIAN VARIETIES

Loren D. OLSON

The basic purpose of this note is to give an elementary proof of the fact that an elliptic curve can be given the structure of an abelian variety. It is easy enough to give the rational points on such a curve an abelian group structure, but it is rather more difficult to show that the group structure so obtained actually arises from a morphism of schemes. Using properties of the Picard scheme, etc., this result follows almost immediately. However, such an approach presumes a fairly advanced knowledge of the modern machinery of algebraic geometry, and we would like to present here a more elementary proof of this fact. All the necessary material for the proof may be found in Fulton [1] and Mumford [3] together with the first chapter of Serre [4].

In addition to the proof mentioned above, we include some well-known results which allow us to outline the essential equivalence of the following three concepts:

(I) non-singular cubics in $\mathbf{P}^2$,
(II) elliptic curves, i.e. non-singular complete irreducible curves of genus 1, and
(III) 1-dimensional abelian varieties.

§ 1. ELLIPTIC CURVES AND PLANE CUBICS

Let k be an arbitrary field with algebraic closure $\bar{k}$. Throughout this paper, we shall assume that all varieties have a k-point, and that everything is defined over k. All curves are assumed to be non-singular, complete, and irreducible.

Let $g = g(X) = \dim_k H^1(X, \mathcal{O}_X)$ denote the genus of such a curve X.

Theorem 1. Let D be a divisor on X. Then $\deg(D) \geqq 2g + 1 \Rightarrow D$ is very ample, i.e. there is an embedding of X into $\mathbf{P}(L(D))$ where $L(D) = \{f \in k(X) \mid (f) + D \geqq 0\}$.

A proof of Theorem 1 may be found on page 28 of Serre [4].

Recall that:

(1) $\deg K = 2g - 2$ where K denotes the canonical divisor on X,
(2) the Riemann-Roch theorem, i.e. $l(D) = \deg D + 1 - g + l(K-D)$ where $l(D) = \dim_k L(D)$, and
(3) if X is a non-singular plane curve of degree n, then $g = (n-1)(n-2)/2$.

Def. X is an *elliptic curve* if $g = 1$.

Notice that if D is a divisor of degree n on a curve X, then $n < 0 \Rightarrow L(D) = 0 \Rightarrow l(D) = 0$. In particular, on an elliptic curve X, $n > 0 \Rightarrow \deg(K-D) = -n < 0 \Rightarrow l(K-D) = 0 \Rightarrow l(D) = n$ from (1) and (2) above.

Theorem 2 A non-singular complete curve C in $\mathbf{P}^2$ of degree 3 is an elliptic curve.

Proof:

$$(3) \Rightarrow g = (3-1)(3-2)/2 = 1.$$

Theorem 3 Every elliptic curve X is isomorphic to a non-singular complete irreducible curve C in $\mathbf{P}^2$ of degree 3.

Proof:

Let D be a divisor of degree 3 on X.

Theorem 1 implies that D is very ample, i.e. that we have an isomorphism from X to a non-singular complete irreducible curve C in $\mathbf{P}(L(D))$. Riemann-Roch $\Rightarrow l(D) = 3 \Rightarrow \mathbf{P}(L(D)) = \mathbf{P}^2$. Let $n = g(C)$. X an elliptic curve $\Rightarrow 1 = g(X) = g(C) = (n-1)(n-2)/2 \Rightarrow n = 3$.

Thus we have established the desired connection between (I) and (II).

§ 2. Algebraic and geometric group laws on an elliptic curve

Let X be an elliptic curve over k, and let $X(k)$ denote the set of k-points of X. We begin by defining a group law on $X(k)$ in a rather algebraic fashion. Let $\mathrm{Div}^0(X)$ be the group of divisors of degree 0 on X. Let $\sim$ denote linear equivalence, and let $\mathrm{Div}^0(X)/\sim$ be the quotient group. If $D \in \mathrm{Div}^0(X)$, let $\mathrm{Cl}(D)$ be its image in $\mathrm{Div}^0(X)/\sim$.

Recall that a divisor $D = \Sigma n_P P$ is called effective if $n_P \geqq 0$ for all P.

Lemma 4 Let D_1 and D_2 be effective divisors of degree 1 on X. Then

$$(4)\ D_1 = D_2 \Leftrightarrow D_1 \sim D_2.$$

Proof:

($\Rightarrow$) Obvious.

($\Leftarrow$) D_1 effective $\Rightarrow L(D_1)$ contains all the constant functions. $\deg(D_1) = 1 \Rightarrow l(D_1) = 1 \Rightarrow L(D_1)$ consists solely of the constant functions. Suppose now that $D_1 \sim D_2$. Then there exists $f \in k(X)$ such that $D_1 + (f) = D_2$. D_2 effective $\Rightarrow f \in L(D_1) \Rightarrow f$ constant $\Rightarrow D_1 = D_2$.

Fix a k-point e of X. Define a map Φ from $X(k)$ to $\mathrm{Div}^0(X)/\sim$ by $P \to \mathrm{Cl}(P-\mathrm{e})$.

Proposition 5 The map $\Phi : X(k) \to \mathrm{Div}^0(X)/\sim$ is a bijection.

Proof:

Claim Φ is injective. Let $P_1, P_2 \in X(k)$. $\Phi(P_1) = \Phi(P_2) \Leftrightarrow \mathrm{Cl}(P_1 - e) = \mathrm{Cl}(P_2 - \mathrm{e}) \Leftrightarrow P_1 - e \sim P_2 - e \Leftrightarrow P_1 \sim P_2 \Leftrightarrow P_1 = P_2$. So Φ is injective. Claim Φ is surjective. Let $\bar{D} \in \mathrm{Div}^0(X)/\sim$ with $D \in \mathrm{Div}^0(X)$ such that $\mathrm{Cl}(D) = \bar{D}$. $\deg(D+e) = 1 \Rightarrow l(D+e) = 1 \Rightarrow$ there exists $f \in L(D+e)$, $f \neq 0$, such that $(f) + D + e \geq 0$, i.e. $(f) + D + e = P$ for $P \in X(k)$. $\Phi(P) = \mathrm{Cl}(P-e) = \mathrm{Cl}((f)+D) = \mathrm{Cl}(D) = \bar{D}$. Therefore Φ is surjective, and hence bijective.

Thus $X(k)$ receives an abelian group structure via Φ, i.e. the sum of P_1 and P_2 is $\Phi^{-1}(\Phi(P_1) + \Phi(P_2)) = \Phi^{-1}(\mathrm{Cl}(P_1 - e) + \mathrm{Cl}(P_2 - e)) = \Phi^{-1}(\mathrm{Cl}(P_1 + P_2 - 2e)) =$ that point Q on X such that $Q \sim P_1 + P_2 - \mathrm{e}$. We therefore have a map $M : X(k) \times X(k) \to X(k)$ which we shall call the "algebraic" group law.

Now let us assume that C is a non-singular complete cubic in $\mathbf{P}^2$. We proceed to define a "geometric" group law on $C(k)$. If $P_1, P_2 \in C(k)$, there exists a unique line L such that the intersection cycle $L \cdot C = P_1 + P_2 + P_3$ for some $P_3 \in C(k)$. If $P_1 \neq P_2$, L is the unique line through P_1 and P_2. If $P_1 = P_2$, L is the unique tangent to C at P_1. P_3 is thus uniquely determined by P_1 and P_2 and we have defined a mapping $\varphi : C(k) \times C(k) \to C(k)$. Let e be a fixed k-point of C. By repeating the preceding procedure with the points $\varphi(P_1, P_2)$ and e, we will obtain a new point $P_1 + P_2$. Let $m : C(k) \times C(k)$ be the resulting map, i.e. m is the composition of (e, φ) and φ, $m = \varphi^{\circ}(e, \varphi)$. m is the "geometric" group law.

By using certain geometric properties of $\mathbf{P}^2$, it is possible to prove that m gives $C(k)$ an abelian group structure (cf. Fulton [1], p. 125). We choose instead to prove the following proposition.

Proposition 6 The "algebraic" group law on C coincides with the "geometric" group law on C, i.e. $m = M$.

Proof:

Let $P_1, P_2 \in C(k)$. Let $P_3 = \varphi(P_1, P_2)$. Then there exists a line L_1 such that $L_1 \,.\, C = P_1 + P_2 + P_3$. Let $P_4 = \varphi(e, P_3) = \varphi(e, \varphi(P_1, P_2)) = m(P_1, P_2)$. Then there exists a line L_2 such that $L_2 \,.\, C = e + P_3 + P_4$. Let $f = L_1/L_2$ and regard f as an element of $k(C)$. $(f) = P_1 + P_2 - e - P_4 \Rightarrow P_4 \sim P_1 + P_2 - e$, i.e. $P_4 = M(P_1, P_2)$. Therefore $m = M$.

§ 3. Elliptic curves and abelian varieties

The purpose of this section is to prove the equivalence of notions (II) and (III). Up to this point, we have a group law on the set of k-points of an elliptic curve, and we would like to know that this is induced by an abelian variety structure. We shall also prove that 1-dimensional abelian varieties are elliptic curves.

Definition Let k be a field. An *abelian variety* X is a complete non-singular variety defined over k together with k-morphisms

$$m : X \times X \to X$$
$$i : X \to X$$
$$e : \mathrm{Spec}(k) \to X$$

which satisfy the usual group axioms (cf. Mumford [2], p. 95).

To show that an elliptic curve can be given the structure of an abelian variety, it suffices to check that the map φ described in § 2 is a morphism. Recall that φ was defined on k-points as taking $(P_1, P_2) \in C(k) \times C(k)$ to the unique third point $P_3 \in C(k)$ such that $P_1 + P_2 + P_3 = L \,.\, C$ for some line L. It is quite easy to see that φ is a morphism on a certain affine open subset of $C \times C$. To be precise, we have the following lemma.

Lemma 7 φ defines a morphism from

$$\mathscr{S} = \mathrm{Spec}\left(k[X_1, Y_1, X_2, Y_2] / (f(X_1, Y_1), f(X_2, Y_2))(X_1 - X_2)\right)$$

to $\mathscr{T} = \mathrm{Spec}\left(k[X_3, Y_3] / f(X_3, Y_3)\right.$(where f is an affine equation for C.

Proof:

In any characteristic, C is isomorphic to a curve in $\mathbf{P}^2$ given by $F(X, Y, Z) = Y^2Z + a_1XYZ + a_2YZ^2 + X^3 + a_3X^2Z + a_4XZ^2 + a_5Z^3$ with $a_i \in k$. Assume C is in this form. Taking $Z = 0$ as the hyperplane at infinity, $Z \cap C = (0, 1, 0)$ which we take as the point e. The affine equation then becomes $f(X, Y) = Y^2 + a_1XY + a_2Y + X^3 + a_3X^2 + a_4X + a_5$.The k-points of $\mathscr{S}$ are points (P_1, P_2) such that $P_1, P_2 \in C(k) - \{e\}$ and such that if $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, then $x_1 \neq x_2$. The line L through P_1 and P_2 is given by $L = Y - \lambda X - \upsilon$ where $\lambda = (y_1 - y_2) / (x_1 - x_2)$ and $\upsilon = y_1 - \lambda x_1 = y_2 - \lambda x_2$. Letting $Y = \lambda X + \upsilon$ in $f(X, Y)$, we obtain a polynomial in X of degree 3. $P_1, P_2 \in C(k) \Rightarrow x_1$ and x_2 are roots of $f(X, \lambda X + \upsilon)$. The third root x_3 is thus an element of k, specifically $x_3 = < x_1 - x_2 - \lambda^2 - a_1\lambda - a_3$. Setting $y_3 = \lambda x_3 + \upsilon$, we obtain the third point $P_3 = (x_3, y_3)$ in the intersection cycle $L \,.\, C$, i.e. $P_3 = \varphi(P_1, P_2)$. [Note that we have just used an affine version of Lemma 8 below.] Thus the morphism φ is defined by the ring-homomorphism taking X_3 to $- X_1 - X_2\lambda^2 - a_1\lambda - a_3$ and Y_3 to $\lambda X_3 + \upsilon$.

Thus φ may be regarded as a rational map from $C \times C \to C$. The whole point is to prove that φ is defined on all of $C \times C$. Let φ' denote the morphism from $\mathscr{S}$ to C defined in Lemma 7. We proceed by taking the closure of the graph of φ' in $C \times C \times C$ and using this closed set to give us a morphism from $C \times C \to C$.

Let $\mathscr{P} = \mathbf{P}^2 \times \mathbf{P}^2 \times \mathbf{P}^2 \times \mathbf{P}^{2\check{}}$, where $P^{2\check{}}$ denotes the projective space consisting of all lines in $\mathbf{P}^2$ (we identify the line $a_1X + a_2Y + a_3Z$ with the point (a_1, a_2, a_3)). We want to define a certain subscheme of $\mathscr{P}$, namely the closed subscheme Γ whose k-points consist of all (P_1, P_2, P_3, L) such that the intersection cycle $L \,.\, C = P_1 + P_2 + P_3$. This should of course give us the graph of our sought-for φ after projection onto the first three factors.

Recall that the procedure for passing between a homogeneous polynomial G in two variables and an inhomogeneous polynomial G' in one variable implies that G can be written as a product of linear factors over $\bar{k}$ since G' can be written as a product of polynomials of degree 1 over $\bar{k}$. The resulting factorization is of course unique up to constant factors.

Lemma 8 (cf. Fulton [1], p. 82) Let F be a curve of degree n in $\mathbf{P}^2$ and let L be a line which is not a component of F. Then there exists a homogeneous form $G(M, N)$ in $k[M, N]$ of degree n such that the factors of

$G(M, N)$ correspond (with the same multiplicities) to the points in the intersection cycle $L \,.\, F$. To be precise: let $U = (u_1, u_2, u_3)$ and $V = (v_1, v_2, v_3)$ be two distinct k-points on the line L. We have an isomorphism $h : \mathbf{P}^1 \xrightarrow{\approx} L$ given by $(s, t) \to (su_1 + tv_1, su_2 + tv_2, su_3 + tv_3)$. Let $G(M, N) = F(Mu_1 + Nv_1, Mu_2 + Nv_2, Mu_3 + Nv_3)$. Moreover, let $H(M, N) = \prod_{i=1}^{n} (t_i M - s_i N)$ be a homogeneous form of degree n with $t_i, s_i \in \bar{k}$. Let $P_i = h(s_i, t_i) \in L(\bar{k})$. Then $L \,.\, F = P_1 + \ldots + P_n \Leftrightarrow H(M, N) = \lambda G(M, N)$ for $\lambda \in \bar{k}^*$.

Proof:

$G(M, N)$ factors over $\bar{k}$, and we can write $G(M, N) = \prod_{i=1}^{n} (\alpha_i M + \beta_i N)$ with $\alpha_i, \beta_i \in \bar{k}$. Let $P \in L(\bar{k})$ and let $(\alpha, \beta) = h^{-1}(P)$. The intersection number $I(P, F \cap L) = \operatorname{ord}_P^L(F) =$ the maximal $d \in \mathbf{Z}$ such that $(\beta M - \alpha N)^d \mid G(M, N)$. Bezout's theorem plus unique factorization finishes the proof.

Recall that we want to define a closed subscheme Γ of $\mathscr{P}$ whose k-points (P_1, P_2, P_3, L) are precisely such that $P_1 + P_2 + P_3 = L \,.\, C$. One way of defining a closed subscheme Γ is to give a set of homogeneous polynomials and take Γ as the closed subscheme defined by them. We then have to check the statement above concerning the k-points. Take $\mathscr{X} = (X_1, Y_1, Z_1, X_2, Y_2, Z_2, X_3, Y_3, Z_3, A_1, A_2, A_3)$ as a coordinate system for $\mathscr{P}$. The first thing we do is to write down three equations requiring that P_1, P_2, and P_3 all lie on the line L. The equations are

$$(E_1) \quad A_1X_1 + A_2Y_1 + A_3Z_1$$
$$(E_2) \quad A_1X_2 + A_2Y_2 + A_3Z_2$$
$$(E_3) \quad A_1X_3 + A_2Y_3 + A_3Z_3$$

Lemma 8 will now help us find the remaining equations. From now on, assume (P_1, P_2, P_3, L) satisfies E_1, E_2, and E_3. Let $L = (a_1, a_2, a_4)$, i.e. L is the line $a_1X + a_2Y + a_3Z$. At least one of a_1, a_2, a_3 is non-zero, say $a_1 \neq 0$ for the moment. Then $U = (a_2 + a_3, -a_1, -a_1)$ and $V = (a_2, -a_1, 0)$ are two distinct points on L.

From the homogeneous polynomial $G_1 = A_1 F(M(A_2 + A_3) + NA_2, -MA_1 - NA_1, -MA_1($ where F is the equation for C. Substituting (a_1, a_2, a_3) in G_1, we obtain the polynomial described in Lemma 8 for the two points U and V. Let $H_1 = A_1 \prod_{i=1}^{3} ((Z_i - Y_i)M + Z_iN)$. Evaluating

H_1 at (P_1, P_2, P_3, L) yields $a_1 \prod_{i=1}^{3} ((z_i - y_i)M + z_i N)$. Using the isomorphism h in Lemma 8, we find that $h(-z_i, z_i - y_i) = (-z_i(a_2 + a_3) + (z_i - y_i)a_2, -z_i(-a_1) + (z_i - y_i)(-a_1), -z_i(-a_1) + (z_i - y_i)(0)(= (-z_i a_3 - y_i a_2, y_i a_1, z_i a_1) = (x_i, y_i, z_i) = P_i$ since (P_1, P_2, P_3, L) is assumed to satisfy E_1, E_2, and E_3. Thus, by Lemma 8, $L \,.\, C = P_1 + P_2 + P_3 \Leftrightarrow G_1(P_1, P_2, P_3, L) = \lambda H(P_1, P_2, P_3, L)$ for some $\lambda \in \bar{k}^*$. But how can we write down this latter condition in terms of polynomials? Write

$$G_1 = \sum_{i=o}^{3} g_i M^i N^{3-i}$$

and

$$H_1 = \sum_{i=o}^{3} h_i M^i N^{3-i}$$

where $g_i, h_i \in k[\mathscr{X}]$

Let

$$D_{1ij} = \det \begin{pmatrix} g_i & g_j \\ h_i & h_j \end{pmatrix} = g_i h_j - g_j h_j$$

for $0 \leqslant i, j \leqslant 3$. To say that G_1 and H_1 differ by a non-zero constant $\lambda \in \bar{k}^*$ is precisely the same as requiring the D_{1ij}'s to be 0. So the case $a_1 \neq 0$ is taken care of. But clearly we can form the corresponding polynomials G_2, K_2, and the D_{2ij}'s for $a_2 \neq 0$ and G_3, H_3, D_{3ij}'s for $a_3 \neq 0$. We take Γ to be the closed subscheme of $\mathscr{P}$ defined by E_1, E_2, E_3 the E_{1ij}'s, the D_{2ij}'s, and the D_{3ij}'s. The k-points of Γ are precisely those (P_1, P_2, P_3, L) such that $L \,.\, C = P_1 + P_2 + P_3$.

Let $p_{123} : \mathscr{P} \to \mathbf{P}^2 \times \mathbf{P}^2 \times \mathbf{P}^2$ be projection on the first three factors. p_{123} is a closed map since $\mathbf{P}^{2\hat{}}$ is complete. Therefore $D = p_{123}(\Gamma)$ is closed in $\mathbf{P}^2 \times \mathbf{P}^2 \times \mathbf{P}^2$. $D \subseteq C \times C \times C \subseteq \mathbf{P}^2 \times \mathbf{P}^2 \times \mathbf{P}^2$ and D is closed in $C \times C \times C$. Consider $\Gamma_{\varphi'} \subseteq C \times C \times C$, where $\Gamma_{\varphi'}$ denotes the graph of φ'. Let E be its closure in $C \times C \times C$. We claim that $D = E$. D is closed and contains $\Gamma_{\varphi'}$, hence $D \supseteq E$. Consider the projection $p_{12} : D \to C \times C$ onto the first two factors. p_{12} is a bijection on closed points. $p_{12}(\Gamma_{\varphi'}) = \mathscr{S}$ is open in $C \times C$, so $\overline{p_{12}(\Gamma_{\varphi'})} = C \times C$ since $C \times C$ is irreducible. $p_{12}(E)$ is closed and $p_{12}(E) \supseteq p_{12}(\Gamma_{\varphi'})$. Therefore $p_{12}(E) = C \times C$. p_{12} is a bijection, so $D = E$. We claim moreover that p_{12} is an isomorphism from D to $C \times C$. We know that p_{12} restricted to $\Gamma_{\varphi'}$ is an isomorphism from $\Gamma_{\varphi'}$ onto $\mathscr{S}$ (cf. Mumford [3], p. 71). Thus p_{12} is a birational map from D to $C \times C$. By Zariski's Main Theorem (cf. Mumford [3], p. 413) we conclude that p_{12} is an isomorphism from

D onto $C \times C$. Let $p_3 : D \to C$ be projection onto the third factor. Let $\varphi : C \times C \to C$ be $p_3 \circ p_{12}^{-1}$. φ is a morphism. Define $m : C \times C \to C$ as the composition $C \times C \xrightarrow{(e,\varphi)} C \times C \xrightarrow{\varphi} C$. m is a morphism and on closed points it agrees with our old m. We have thus proved the following theorem.

Theorem 9 Every elliptic curve can be given the structure of an abelian variety.

We also want to sketch briefly how one goes about proving that a 1-dimensional abelian variety has genus 1.

Theorem 10 (cf. Mumford [2], p. 42) Let X be an abelian variety, and let Ω_0 be the dual space to the tangent space at e. Then there is a natural isomorphism $\Omega_0 \otimes_k \mathcal{O}_X \simeq \Omega_X^1$.

Corollary 11 Let X be a 1-dimensional abelian variety. Then X has genus 1, i.e. X is an elliptic curve.

Proof:

$\dim X = 1 \Rightarrow \Omega_0 \cong k \Rightarrow \Omega_X^1 \cong \mathcal{O}_X$ by Theorem 10. Setting $D = 0$ in the Riemann-Roch theorem gives $g = l(K) = \dim H^0(K) = \dim H^0(\Omega_X)$ $= \dim H^0(X, \mathcal{O}_X)$. X irreducible and complete $\Rightarrow \dim H^0(X, \mathcal{O}_X) = 1$ $\Rightarrow g = 1$.

Thus we have the desired connection between (II.) and (III.).

§ 4. Uniqueness of the group law

The various group laws which we have discussed, have all involved the choice of a k-point e as the identity element. It is natural to ask if this is the only way in which they can differ, and this is indeed the case.

Recall the following extremely useful lemma.

Lemma 12 *(Rigidity Lemma)* Let X be a complete variety, Y and Z any varieties, and let $f : X \times Z \to Z$ be a morphism such that for some $y_0 \in Y(k)$, $f(X \times \{y_0\})$ is a single point $z_0 \in Z(k)$. Then there is a morphism $g : Y \to Z$ such that if $p_2 : X \times Y \to Y$ is projection onto the second factor, then $f = g \circ p_2$.

For a proof, see Mumford [2], p. 43.

We state some immediate corollaries.

Corollary 13 Given the situation in Lemma 12, assume also that for some $x_0 \in X(k)$, $f(\{x_0\} \times Y)$ is the point z_0. Then $f(X \times Y) = \{z_0\}$.

Proof:

By the rigidity lemma, there exists $g : Y \to Z$ such that $f = g \circ p_2$. $f(x, y) = (g \circ p_2)(x, y) = g(y) = (g \circ p_2)(x_0, y) = f(x_0, y) = z_0$.

Corollary 14 If X and Y are abelian varieties and $f : X \to Y$ is any morphism, then there exists a homomorphism $h : X \to Y$ and a k-point $a \in Y(k)$ such that $f = T_a \circ h$ where T_a denotes translation by a.

Corollary 15 Let X and Y be abelian varieties. Then X and Y are isomorphic as abelian varieties $\Leftrightarrow$ X and Y are isomorphic as schemes.

Proof:

($\Rightarrow$.) obvious

($\Leftarrow$.) Let $f : X \to Y$ be an isomorphism of schemes. f can be written as $f = Y_a \circ h$ with $a \in Y(k)$ and h a homomorphism. T_a is an isomorphism of schemes with T_{Ua} as its inverse. Therefore $h = T_{Ua} \circ f$ is an isomorphism of schemes and hence of abelian varieties.

Corollary 16 Let X be a variety and suppose that (X, m) and (X, m') are two abelian variety structures on X with identity elements e and e' respectively. Then m and m' differ only by translation.

Proof:

Let $+$, $-$, and translation all denote operations with respect to m. Consider the morphism $(m-m') : X \times X \to X$. We have $(m-m')(X \times \{e'\}) = e' = (m-m')(\{e'\} \times X)$. By Corollary 13, $(m-m')(X \times Y) = e'$, i.e. $m = m' + e'$.

BIBLIOGRAPHY

[1] FULTON, William. *Algebraic Curves.* W. A. Benjamin, Inc., New York (1969).
[2] MUMFORD, David. *Abelian Varieties.* Oxford University Press, London (1970).
[3] —— *Introduction to Algebraic Geometry.* Mimeographed notes, Harvard University.
[4] SERRE, Jean-Pierre. *Groupes Algébriques et Corps de Classes.* Hermann, Paris (1959).

(Reçu le 22 janvier 1973)

Loren D. Olson
University of Oslo
Institute of Mathematics
Blindern Postboks 1053
Oslo 3, Norvège

vide-leer-empty