Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 19 (1973)

Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: AN ELEMENTARY PROOF THAT ELLIPTIC CURVES ARE ABELIAN VARIETIES

Autor: Olson, Loren D.

Kapitel: § 4. Uniqueness of the group law

DOI: https://doi.org/10.5169/seals-46291

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