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

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

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 $(f) + D + e \geqq 0$, 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 $L \,.\, C = P_1 + P_2 + P_3$ 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

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

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