§ 1. Elliptic curves and plane cubics

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.