Elliptic Curves

Jihan Lee

December 13, 2023

1 Introduction

Elliptic curves are of great interest in many areas of mathematics, including from number theory and cryptography. In this exposition we present elliptic curves in an algebro-geometric manner, and in particular prove the associativity of the group operation.

2 Basic Definitions

Definition 1 (Group)**.** A group is a set G equipped with a binary operation $*\colon G \times G \to G$ (where $a*b$ denotes $*(a,b)$) that satisfies the following properties:

There exists an $e_G \in G$ such that $g * e_G = e_G * g = g$ for all $g \in G$.

$$a * (b * c) = (a * b) * c \text{ for all } a, b, c \in G.$$

For all $g \in G$, there is a g^{-1} such that $g * g^{-1} = g^{-1} * g = e_G$.

A group is said to be *abelian* if $*$ is commutative.

An element e_G is said to be an *identity element* of G, and g^{-1} is said to be an *inverse element* of g. When the context is clear, e_G and $*_G$ will be abbreviated to e and juxtaposition respectively.

A *free abelian group* F is a group with a basis S; that is, every element of F can be written uniquely as a sum of elements of S with coefficients in $\mathbb{Z}$, where the coefficient denotes the number of times the corresponding basis element appears in the sum. This is well defined because the group is abelian.

Definition 2 (Ring)**.** A ring is a set R equipped with an abelian group structure $+$ (ring addition) and an operation $*\colon R \times R \to R$ (ring multiplication) such that for all $a, b, c \in R$,

$$a * (b + c) = ab + ac,$$

$$a * (b * c) = (a * b) * c.$$

When $*$ is commutative, R is said to be a commutative ring. When there exists an identity for $*$ (some $1 \in R$ such that $1 * r = r * 1 = r$ for all $r \in R$), R is said to be unital. It is not required in general for the $*$ operation to be commutative, or have an identity. However, we assume all rings are commutative and unital.

Definition 3 (Ideal)**.** An ideal of a ring R is an additive subgroup that is closed under multiplication from all elements of R.

We say an ideal $\mathfrak{p}$ is prime if $p \in \mathfrak{p}$ and $p = ab$ implies one of $a, b \in \mathfrak{p}$.

Definition 4 (Localization)**.** Let $S = R - \mathfrak{p}$, the set of all elements of R not contained in a prime ideal $\mathfrak{P}$. We define the localization of R at $\mathfrak{p}$, $R_{\mathfrak{p}}$, to be the set $R \times \mathfrak{p}$ under the equivalence relation $(a, p) \sim (a', p')$ iff $(ap' - a'p)t = 0$ for some $t \in S$. This set inherits a well-defined ring structure from R.

If A is an integral domain, we define its field of fractions as $A \times \{A - 0\}$ under the relation $(a, b) \sim (a', b')$ iff $ab' - a'b = 0$. Again, this set inherits well-defined ring structure from A, and is a field.

Definition 5 (Quotient ring)**.** Given a ring R and an ideal I, we define R/I to be the set of cosets of R by I. This set inherits a well-defined ring structure from R.

Definition 6 (Field)**.** A field is a ring in which every nonzero element has a multiplicative inverse.

Definition 7 (Affine space)**.** Let k be a field. We define *affine n-space* over k $\mathbb{A}_k^n$ to be the set of all ordered n-tuples of elements of k. We call elements of $\mathbb{A}_k^n$ *points*, and write them as $P = (p_1, \ldots, p_n)$ with $p_i \in k$.

Definition 8 (Projective space)**.** Take a field k and an affine space A_k^{n+1}. We define the projective n-space $\mathbb{P}_k^n$ to be the set of equivalence classes of points in $\mathbb{A}_k^{n+1}$ given by the relation $(p_1, \ldots, p_{n+1}) \sim (q_1, \ldots, q_{n+1})$ iff $(p_1, \ldots, p_{n+1}) = (aq_1, \ldots, aq_{n+1})$ for some nonzero $a \in k$. We write elements of $\mathbb{P}$ as $P = [p_1 : \cdots : p_{n+1}]$.

3 Curves

We fix a field k and a projective space $\mathbb{P}_k^n$.

Definition 9 (Projective variety)**.** A projective variety is the set of $P = [p_1 : \cdots : p_{n+1}] \in \mathbb{P}_k^n$ such that $f(P) = f(p_1, \ldots, p_{n+1}) = 0$ for a homogeneous polynomial $f \in k[x_1, \ldots, x_{n+1}]$. We write the variety defined by f as $V(f)$.

This definition works because if $Q = kP$ and $f(P) = 0$, then $f(P) = k^d f(P) = f(kP) = f(Q)$, where d is the degree of f.

We say a curve is nonsingular if $\dfrac{\partial f}{\partial x} = \dfrac{\partial f}{\partial y} = \dfrac{\partial f}{\partial z} = 0$ at all points of $V(f)$.

The *dimension* of a variety V is the maximal integer d such that we may find a chain of varieties $\{V_0 \subset \cdots \subset V_d = V\}$ (the inclusions are strict).

We call a variety a curve if it is defined by a homogeneous polynomial in 3 variables.

Definition 10 (The ideal of a variety)**.** Given a variety V, we define the ideal of the variety $I(V)$ to be the set of all $f \in k[x_1 \ldots, x_{n+1}]$ with $f(P) = 0$ for all $P \in V$. It should be noted that when V is a single point, $I(V)$ is prime (in fact, it is maximal).

Definition 11 (Coordinate ring)**.** The coordinate ring $A(V)$ of a variety AV is the ring $k[x_1, \ldots, x_{n+1}]/I(V)$.

Definition 12 (Function field)**.** The function field of a variety V is the field of fractions of $A(V)$, and will be denoted $K(V)$.

Definition 13 (Elliptic curve)**.** An elliptic curve is a nonsingular projective curve of genus 1 with a distinguished point O.

Definition 14 (Rational map)**.** Let V, V' be varieties in $\mathbb{P}^n_k$. A *rational map* between V and V' is a function $\phi\colon V \to V'$ such that $\phi(P) = (f_1(P), \ldots, f_{n+1}(P))$ for polynomials f_i.

4 The Proof

We fix a(n algebraically closed) field k and a projective space P^n_k, and consider a nonsingular variety V.

Definition 15 (Divisor group)**.** We define the divisor group $\mathrm{Div}(V)$ of V as the free abelian group on the points of V.

The degree of an element of $\mathrm{Div}(V)$ is the sum of its coefficients. We define $\mathrm{Div}^0(V)$ to be the set of elements of $\mathrm{Div}(V)$ with degree 0.

We define $A(V)_P$ to be the localization of $A(V)$ at $I(P)$. We define a valuation ord_P on $A(V)_P$ to be the largest integer d such that $x \in A(P)^d$, and we define ord_P for elements $x = f/g \in K(V)$ by $\mathrm{ord}_P(x) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$.

We associate each $f \in K(V)$ to divisor by $\mathrm{Div}(f) = \sum_{P \in V} \mathrm{ord}_P(f(P))$. A divisor D is principal if there is a nonzero $f \in K(V)$ such that $\mathrm{div}(f) = D$. We note that every principal divisor has degree zero. We define $\mathrm{Pic}^0(V) = \mathrm{Div}^0(V)/\{\text{principal divisors of V}\}$.

Given a divisor D, define $\mathcal{L}(D)$ as the (finite-dimensional) vector space containing 0 and the nonzero functions in $f \in K(V)$ such that $\mathrm{div}(f) \geq -D$. Write $l(D)$ for the dimension of this space.

Given a nonzero differential on V, we can assign it a divisor, and every such divisor maps to the same element in Pic^0. Any divisor of this form will be denoted k_V.

Theorem 16 (The Riemann-Roch Theorem)**.** *Take a nonsingular curve V of genus g. Then $l(d) - l(k_V - D) = \deg(D) - g + 1$.*

Theorem 17. *Let E be an elliptic curve. Given a divisor D in $\mathrm{Div}^0(E)$, we can find a unique $P \in E$ with $D - (P + O)$ a principal divisor. Defining $\phi(D) = P$, ϕ is a bijection, thus induces a group law on E.*

Proof. By Riemann-Roch, $l(D+(O)) = 1$; taking an element f, $\mathrm{div}(f) \geq -D-O$ and $\deg(\div(f)) = 0$, so $\mathrm{div}(f) = -D - O + P$ for some P. Because E has genus 1, $\mathrm{div}(f) = P - Q$ implies $f \in \mathcal{L}(Q)$, and by Riemann-Roch $l(Q) = 1$, thus f is constant and $P = Q$.

Since $\phi(P-Q) = P$, ϕ is surjective. Since $\phi(D)-\phi(D')-(D-D')$ is a principal divisor, $D - D'$ is principal iff $\phi(D) = \phi(D')$, so ϕ is injective.

To have group operation agree with the geometric construction is seen to be equivalent to showing $(P +_E Q) - P - Q + O$ is principal.

Let L be the line through P, Q, and let R be the intersection of E and L. Letting L' be the line through R and O, the line $z = 0$ intersects E at O with mutiplicity 3, therefore $\mathrm{div}(f/Z) = P + Q + R - 3O$ and $\mathrm{div}(f'/Z) = R + (P +_E Q) - 2O$, so $(P +_E Q) - P - Q + O = \mathrm{div}(f/f')$. □