Alexandra Koletsos

The Group Law On Elliptic Curves

Brief Historical Relevance

- elliptic curve cryptography
- Fermat's Last theorem - Andrew Wiles
- modular forms

Outline

- Referenced MIT lecture slides, J.S. Milne Elliptic Curves
- discuss elliptic curves
- discuss group theory
- proof outline of group law on elliptic curves

Elliptic curves

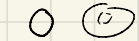
→ have a lot of structure

→ can have points with coordinates in any field: $\mathbb{F}_p$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

- Recall: A field is a set $\mathbb{F}$ with two binary operations on $\mathbb{F}$ called addition ($+$) and multiplication ($\cdot$), satisfying the field axioms.
  ↳ elliptic curves with coordinates in $\mathbb{F}_p$ are finite groups.

Def An elliptic curve is a smooth projective curve of genus 1 with a distinguished point. More precisely, an elliptic curve over a field K is a smooth projective curve of genus 1 (defined over K) with a distinguished (K-rational) point.

* intuitively, the genus is the number of "holes" of a surface



Def The projective plane over K is

$$\mathbb{P}^2(K) = \{(x,y,z) \in K^3 \mid (x,y,z) \neq (0,0,0)\}$$

(Projective n-space $\mathbb{P}^n(K)$, $n \in \mathbb{N}$ can be defined similarly)

where $(x,y,z) \sim (x',y',z')$ if and only if there exists a $c \neq 0$ in K such that $(x',y',z') = (cx, cy, cz)$.

Def The projective point $(x:y:z)$ is the equivalence class of (x,y,z)

Note: points of the form $(x:y:1)$ are called affine points. They form an affine (Euclidean) plane $\mathbb{A}^2(K)$ embedded in $\mathbb{P}^2(K)$.

Points of the form $(x:y:0)$ are called points at infinity. Consist of points $(x:1:0)$ and $(1:0:0)$ which form $L_\infty(K)$, $\mathbb{P}^1(K)$ embedded in $\mathbb{P}^2(K)$.

Def A nonconstant homogeneous polynomial $f \in K[x,y,z]$, assumed to have no repeated factors in $\bar{K}$, defines a projective plane curve C_f over K whose points in any field $k \supset K$ are the zeros of f in $\mathbb{P}^2(K)$. The K-rational points of C_f form the set

$$C_f(K) = \{(x:y:z) \in \mathbb{P}^2(K) \mid f(x,y,z) = 0\}$$

A point $P \in C_f(K)$ is singular if $\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}, \frac{\partial f}{\partial z}$ all vanish at P. C_f is smooth (nonsingular) if there are no singular points in $C_f(\bar{K})$.

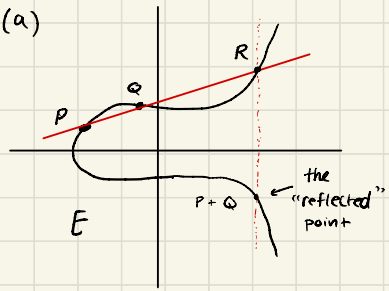
Def A Weierstrass elliptic curve is given by an equation of the form

$$\{y^2 = x^3 + Ax + B\}$$

for which the discriminant $\Delta = 4A^3 + 27B^2$ is nonzero
(non-singularity condition: the polynomial $x^3 + Ax + B$ has distinct roots)

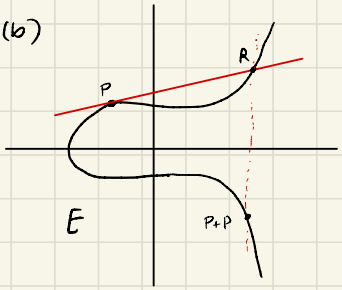
Now lets talk about adding points on an elliptic curve.

(a)



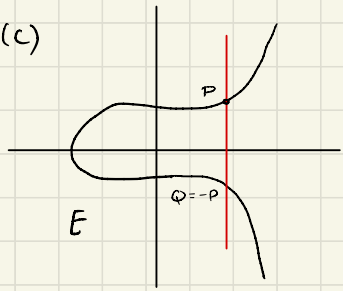
$P + Q + R = 0$.

(b)



$P + P + R = 0$.

(c)



$P + Q + O = O$

But there's no third point!

Three points on a line sum to O!

Bezout's Theorem Let C and D be projective plane curves over K of degrees m and n respectively having no common component. Then C and D intersect over $\bar{K}$ in exactly mn points counted with multiplicity.

For case C (with $z = 0$) we add an extra point at ∞!

Thus, we can express $\{y^2 = x^3 + Ax + B\} \subseteq \mathbb{C}^2$ as

$$\{y^2z = x^3 + axz^2 + bz^3\} \subseteq \mathbb{P}^2_{\mathbb{C}}$$

Because of this we are able to define a group operation on $E(K)$ for any elliptic curve E defined over a field K.

So let's get into group theory...

Def A group is a non-empty set G equipped with a binary operation $* : G \times G \to G$ satisfying the following axioms:

(i) Closure. if $a, b \in G$, then $a * b \in G$.

(ii) Associativity. $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.

(iii) **Identity** there exists an element $e \in G$ s.t. $a * e = e * a = a$ for all $a \in G$.

(iv) **Inverse** for each element $a \in G$, there exists an element $b \in G$ s.t. $a * b = e = b * a$.

Def A group G is said to be abelian (commutative) if $a * b = b * a$ for all $a, b \in G$.

Def A subgroup $H \subset G$ is **normal** in G if $gH = Hg$ for all $g \in G$. That is, a normal subgroup of a group G is one in which the right and left cosets are precisely the same.

Corollary: Let G be an abelian group. Every subgroup $H \subset G$ is a normal subgroup. Since $gh = hg$ for all $g \in G$ and $h \in H$, it will always be the case that $gH = Hg$.

Def If N is a normal subgroup of a group G, then the cosets of N in G form a group G/N under the operation $(aN)(bN) = abN$. This group is called the factor or quotient group of G and N.

Ex (i) $\mathbb{Z}$ is an abelian group under addition.

Ex (ii) $3\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$. The cosets of $3\mathbb{Z}$ in $\mathbb{Z}$ are:

$$0 + 3\mathbb{Z} = \{\ldots, -3, 0, 3, 6, \ldots\}$$
$$1 + 3\mathbb{Z} = \{\ldots, -2, 1, 4, 7, \ldots\}$$
$$2 + 3\mathbb{Z} = \{\ldots, -1, 2, 5, 8, \ldots\}$$

And $\mathbb{Z}/3\mathbb{Z}$ is given by the Cayley table

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

So now that we know some basic information about a group, let's prove that the points of an elliptic curve have a group structure.

Recall: (i) closure (ii) associativity (iii) identity (iv) inverse.

With addition defined as before, $E(K)$ becomes an abelian group.

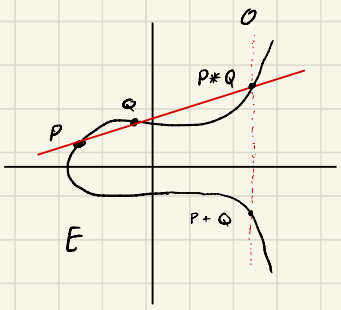
→ Closure is obvious since $P * Q = P + Q = -R$.

→ identity: the point $(0:1:0)$ at ∞ is the identity element 0.

→ inverse: the inverse of $P = (x:y:z)$ is the point $-P = (x:-y:z)$

→ Commutativity: $P + Q = Q + P$

→ Associativity: Not so obvious.



Many different ways to show associativity, but let's focus on the geometric proof.

<u>Prop</u> If two cubic curves in $\mathbb{P}^2$ intersect in exactly nine points, then every cubic curve passing through eight of the points also passes through the ninth.

Pf Consider $f(x,y,z) = a_1 x^3 + a_2 x^2 y + \dots + a_{10} z^3$

if C_F passes through $P = (x:y:z)$,

$$a_1 x^3 + a_2 x^2 y + \dots + a_{10} z^3 = 0.$$

Cubic forms having $P_1, \dots, P_8$ as zeros form a 2-Dimensional space, and so there exist 2 such forms F and G s.t. the remainder can be written

$$\lambda F + \mu G \quad , \lambda, \mu \in K.$$

F and G have a ninth zero in common, and every curve $\lambda F + \mu G = 0$ passes through it.

Let $\ell(P,Q) \subseteq \mathbb{P}^2$ pass through the points P, Q. Let $P, Q, R \in C(K)$ s.t.

$$S = (P+Q)R \quad , \quad T = P(Q+R)$$

$(P+Q)+R = O_S$ & $P+(Q+R) = O_T$. Let's show that $S = T$.

(O_S: point at ∞)

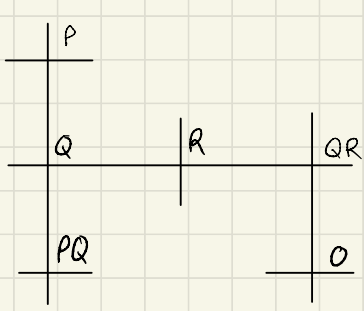
Consider the cubic curves $\ell(P,Q) \cdot \ell(R, P+Q) \cdot \ell(QR, O) = 0$,

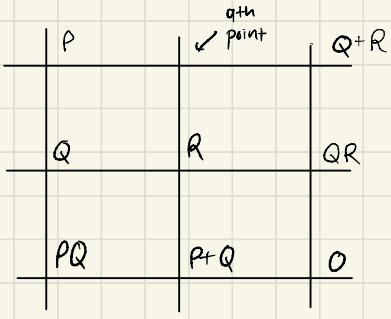
$\ell(P, Q+R) \cdot \ell(Q, R) \cdot \ell(PQ, O) = 0$,

both pass through $\longrightarrow$ $U := \ell(R, P+Q) \cap \ell(P, Q+R)$

We want to show these lines are distinct. i.e. $S = U = T$.

space of cubic curves through $P_1, \dots P_8$ has dim 1.





So every curve $\lambda F + \mu G = 0$ passes through it.