Group Law for elliptic Curves

http://www.math.ku.dk/~verrill/grouplaw/
(Based on Cassels’ Lectures on Elliptic curves, Chapter 7)

1 Outline:

Introductory remarks
Construction of the group law
Case of finding 2A
need nonsingularity
example of 2 torsion point
Bezouts theorem (statement)
A cubic meets a line in 3 points
Note that $A + B$ is in $E(k)$, not just $E(\bar{k})$
We have abelian group:
the three easy properties
Associativity
Statement of a lemma needed
Proof of associativity, assuming the lemma and simple case of Bezout
Sketch proof of lemma

2 Introduction

The group law for an elliptic curve $E$ over some field $k$ is a map

$$E(k) \times E(k) \rightarrow E(k)$$

$$(A, B) \mapsto A + B$$

that gives $E(k)$ the structure of an abelian group.

This means that given any two points $P$ and $Q$ on $E(k)$ there is a way of “adding” them together to get a third point.

For $E$ over $\mathbb{Q}$ it will turn out that $E(\mathbb{Q})$ is a finitely generated abelian group, which means you can describe how to give all the points on $E(\mathbb{Q})$ by giving a finite list of points.

We will now describe
1) What is the group law.
2) Why does the construction work—i.e., that the construction is well defined, and that it gives $E(k)$ the structure of an abelian group.
3) If there’s any time: Examples
3 Definition of the group law

We will assume that our elliptic curve is given in Weierstrass form,

\[ E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \]

The group law is given by taking

1) The zero of the group is \( O = (0 : 1 : 0) \)

2) Given any two points \( A, B \in E(k) \), define \( A + B \) as in the following diagrams.

0. An elliptic curve, \( E \):

1. Take any two points \( A \) and \( B \) on \( E \).

2. Draw the line \( L_1 \) through \( A \) and \( B \).
   Let \( C \) be the third point on \( E \cap L_1 \).

3. Let \( L_2 \) be the vertical line through \( C \).
   Then \( A + B \) is the other (non infinite) point on \( E \cap L_2 \).
Does this definition make sense? Why does a line meet the elliptic curve in 3 points? And what do we do if $A = B$ and we want to find $2A$?

If $A = B$ the construction works like this:

For the construction of the point $2A$ to work we need that there is a tangent line, and this will be the case since the curve $E$ is non-singular. The tangent at $A$ is given by

$$\frac{dF}{dX}\bigg|_A X + \frac{dF}{dY}\bigg|_A Y + \frac{dF}{dZ}\bigg|_A Z = 0$$

Another example:

If $A = (0 : b : 1)$ then $2A = O$. 

$L_1 = L_2$
That a line meets a cubic in three points is a special case of Bezout’s Theorem:

**Theorem 3.1 (Bezout).** If $C$ and $D$ are curves given by homogeneous equations in $X,Y,Z$, of degrees $c$ and $d$, then, assuming $C$ and $D$ do not have an infinite number of points in common (which happens e.g., when $C = D$), then

$$\# \{ C \cap D \} \leq c.d.$$

If we work over an algebraically closed field, and intersection points are counted with “multiplicity”, we have an equality:

$$\sum_{P \in C \cap D} i(C, D; P) = c.d,$$

where $i(C, D; P)$ is the intersection multiplicity of $C$ and $D$ at $P$. (See below for a definition in a simple case. For more details: Fulton, Hartshorn, or Semple and Roth, (Algebraic curves, Chapter II, § 2, Theorem 3.))

**Special case of Bezout:** A cubic curve meets a line in three points:

Suppose the cubic curve is given by

$$F(X, Y, Z) = 0$$

where $F$ has degree 3. Suppose the line is given by

$$aX + bY + cZ = 0$$

One of $a, b$ or $c$ is non zero. Suppose $c \neq 0$, so points on the line are given by $Z = -(aX + bY)/c$. Then where the line and cubic intersect, we have

$$F(X, Y, -(aX + bY)/c) = 0.$$  

This is a homogeneous polynomial in two variables, so it looks like

$$\alpha_1 X^3 + \alpha_2 X^2 Y + \alpha_3 XY^2 + \alpha_4 Y^3 = 0.$$  

If $Y = 0$ is not a solution, then dividing by $Y^3$ we have

$$\alpha_1 \left( \frac{X}{Y} \right)^3 + \alpha_2 \left( \frac{X}{Y} \right)^2 + \alpha_3 \left( \frac{X}{Y} \right) + \alpha_4 = 0.$$  

By the fundamental theorem of algebra, over an algebraically closed field we can factor this polynomial as for example:

$$\left( \alpha_1 \left( \frac{X}{Y} \right) + b_1 \right) \left( \alpha_2 \left( \frac{X}{Y} \right) + b_2 \right) \left( \alpha_3 \left( \frac{X}{Y} \right) + b_3 \right) = 0.$$  

Multiplying back through by $Y^3$, we have

$$(a_1 X + b_1 Y) (a_2 X + b_2 Y) (a_3 X + b_3 Y) = 0.$$  

If $Y = 0$ is a solution, we’ll still be able to factor the original polynomial like this. So, there are three solutions, giving three points on the intersection of the line with the conic. The multiplicity of a root is the number of times the factor occurs in this factorization.
Example 3.2. For the curve

\[ E : Y^2Z = X^3 - X^2 \]

Take the line

\[ L : X = 0 \]

then substituting the equation for \( L \) into the equation for \( E \) we get

\[ Y^2Z = 0. \]

There are three factors of this cubic, \( Y, Y \) and \( Z \). If \( Y = 0 \), we get the point \((0 : 0 : 1)\). Since this factor has multiplicity two, the line \( L \) intersects \( E \) with multiplicity 2 at \((0 : 0 : 1)\). The third point of intersection is \( O = (0 : 1 : 0) \).

Reference: For a proof of Bezout's theorem see Fulton (Algebraic curves) or Hartshorn (Algebraic Geometry). Some special cases are given by Reid (undergraduate algebraic geometry). Semple and Roth give a classical viewpoint.

Note: For \( A, B \in E(k) \) we have \( A + B \in E(k) \). If a cubic has coefficients in \( k \) and two roots in \( k \), then the third root is in \( k \). This implies \( A + B \in E(k) \).

Note: If \( A, B, C \) on \( E \) are on a line, then \( A + B + C = O \).

Note: You can give explicit formulas for the coordinates of \( A + B \) in terms of the coordinates for \( A \) and \( B \).

4 We have an abelian group on \( E(k) \)

We need to check the following:

1) \( O + A = A \) for all \( A \in E(k) \). (easy)
2) For every point \( A = (a,b) \) there is an inverse \(-A\) given by \((a,-b)\). (easy)
3) \( A + B = B + A \). (easy)
4) The group law is associative. (hard!)

5 associativity

Lemma 5.1. If \( P_1, \ldots, P_8 \) are points in \( \mathbb{P}^2 \), no 4 on a line, and no 7 on a conic, then there is a 9th point \( Q \) such that an cubic through \( P_1, \ldots, P_8 \) also passes through \( Q \).

Proof of Associativity of the group law on an elliptic curve:

Assuming the lemma, and Bezout's theorem, we now give a proof of associativity. (For a complete proof see Hartshone, Chapter V, §4, corollary 4.5.)

We need to show that for \( A, B, C \) we have

\[ (A + B) + C = A + (B + C) \]

So it's enough to show that

\[ -(A + B + C) = -(A + (B + C)) \]
Consider the following lines:

\[ L_1 \text{ is the line through } A, B, - (A + B) \]
\[ L_2 \text{ is the line through } A + B, C, - ((A + B) + C) \]
\[ L_3 \text{ is the line through } B + C, O, - (B + C) \]
\[ N_1 \text{ is the line through } A + B, O, - (A + B) \]
\[ N_2 \text{ is the line through } B, C, - (B + C) \]
\[ N_3 \text{ is the line through } A, B + C, - (A + (B + C)) \]

We can draw a picture to represent all the above information, and we also label a point \( D \) where \( L_2 \) intersects \( N_3 \):

This picture should be taken as a reminder of which lines pass through which points, not as a remotely accurate drawing. Remember, our elliptic curve is in the background, also passing through these points:
(Again, this is not what an accurate picture would look like! Also note, we don’t know $E$ passes through $D$. This is what we want to show.)

We know that $-(A + B + C)$ lies on $L_2$, because this is how $L_2$ was defined.
And we know that $-(A + (B + C))$ lies on $N_3$, because this is how $N_3$ was defined.

But we’d like these points to be equal, i.e., they must both be equal to the point $D$ which is on $L_2 \cup N_3$.

Now we have two cubic curves,

$$(L_1 L_2 L_3 = 0) \quad \text{and} \quad (N_1 N_2 N_3 = 0)$$

We know by construction that these both pass through the eight points
$O, \ A, \ B, \ C,$
$A + B, \ B + C, \ -(A + B), \ -(B + C),$

By Bezout’s theorem we know that two cubics intersect in 9 points, and we call the 9th point $D$.

By the lemma (assuming conditions are satisfied so we can apply the lemma) we know that any other cubic through these 8 points also passes through $D$.

So, since $E$ is through these 8 points, it also passes through $D$.

So on $N_1 N_2 N_3 \cap E$ we have the points
$O, \ A, \ B, \ C,$
$A + B, \ B + C, \ -(A + B), \ -(B + C),$
$-(A + (B + C)), \ D$

But since there are only 9 points on a line intersect a cubic, two of these must be equal, but, by definition, $D$ is not equal to any of the first 8, so we have

$$D = -(A + (B + C)).$$

Similarly, by considering the 10 labeled points on $L_1 L_2 L_3 \cap E$, we will have $D = -((A + B) + C))$.

So, we have

$$-(A + (B + C)) = D = -((A + B) + C)),$$

and this completes the proof of associativity.

**filling in details**

1) The lemma does apply: No four of the points
$O, \ A, \ B, \ C,$
$A + B, \ B + C, \ -(A + B), \ -(B + C),$

can lie on a line, since if those four points are on $L$, then since they are also on $E$, we have that $\# \{L \cap E\} \geq 4$, which contradicts Bezout’s theorem. Also, no 7 can lie on a conic, since 7 are on a conic $C$, since they are also on $E$, so $\# \{C \cap E\} \geq 7$, which again contradicts Bezout’s theorem. (Conic has degree 2, cubic degree 3, and $2 \times 3 = 6$.)
2) Sketch proof of lemma:

We want to show that given points $P_1, \ldots, P_8$, no 4 on a line, no 7 on a conic, there is a 9th point $Q$ so that all cubics through $P_1, \ldots, P_9$ also pass through $Q$.

Any cubic curve is given by an equation of the form

$$f(X,Y,Z) = a_1X^3 + a_2X^2Y + a_3X^2Z + a_4XY^2 + a_5XZ^2 + a_6XY + a_7Y^3 + a_8Y^2Z + a_9YZ^2 + a_{10}Z^3 = 0$$

Given any cubics we can add them together to get a another, just by adding the coefficients; and we can also multiply by any element of $k$. So the cubic equations form a vector space of dimension 10, and any cubic corresponds to a point:

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}) \in k^{10}$$

To say a point lies on a cubic curve given by an equation $f(X,Y,Z)$ as above puts a linear condition on the coefficients $(a_i)$ for example, if we say that $(1,1,1)$ must lie on $f(X,Y,Z) = 0$, then we must have

$$f(1,1,1) = a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} = 0.$$

Or, if $(1,0,0)$ is on $(f(X,Y,Z) = 0)$, we must have

$$f(1,0,0) = a_1 = 0.$$

Generally, saying that a point is on the cubic puts a linear condition on the space of cubic. So, the space of all cubics is 10 dimensional. The space of cubics through a given point, for example, the space of cubics passing through $(1,0,0)$ is 9 dimensional. Each extra point we require to be on a set of cubics will reduce the dimension by 1, provided that the conditions are linearly independent. It turns out that to make the conditions imposed by 8 points linearly independent, we need that no 4 points are on a line, and no 7 on a conic. (Hartshone, page 400 proves this).

So, assuming that our points give linearly independent conditions, the space of cubics through $P_1, \ldots, P_8$ is $10 - 8 = 2$ dimensional.

So, this two dimensional vector space is spanned by 2 things, call them $F_1$ and $F_2$. That they span this space means that all the points $P_1, \ldots, P_8$ lie on both $(F_1 = 0)$ and $(F_2 = 0)$, and that for any other curve $(G = 0)$ through these points, that curve is in this subspace, and so can be expressed in terms of the basis, so for some $\mu, \nu$ we have

$$G = \mu F_1 + \nu F_2.$$

By Bezout’s theorem, $\#\{F_1 \cap F_2\} = 9$. So, there is another point $Q$ on $(F_1 = 0)$ and $(F_2 = 0)$, so we have $F_1(Q) = F_2(Q) = 0$. This means that

$$G(Q) = \mu F_1(Q) + \nu F_2(Q) = 0 + 0 = 0.$$

So $Q$ is also on $G = 0$.

So, there is a ninth point, $Q$ lying on all cubics through $P_1, \ldots, P_8$. 

8