Introduction to Elliptic Curves

Adam Block

2017

1 Foundational Material

I begin by talking about some of the foundational material we need in order to discuss Elliptic Curves

1.1 Projective Geometry

Projective space over a field, k is the set of linear 1-dimensional subspaces (lines that go through 0) in an $n+1$ dimensional k-vector space that go through . It is given as the set

$$\{(x_0, ...x_n) \in k^{n+1} - (0, ..., 0)\}/k^\times$$

Where two points $(x_0, ..., x_n) \sim (x'_0, ..., x'_n)$ if and only if there is some $\lambda \in k^\times$ such that $x'_i = \lambda x_i$ for all $0 \leq i \leq n$. This can also be thought of as S^n with the antipodal points identified. We also have stereographic projection which associates k^n to $\mathbb{P}^n_k$ minus a point. This is where the terminology of adding a point at infinity comes from. Any two lines in projective space intersect exactly once. Note also that $\mathrm{P}(V)$ is a coordinate free way of writing projective space and this is clearly functorial. We write coordinates in projective space as $(x_0 : ... : x_n)$ as a way to emphasize that these are just equivalence classes modulo multiplication by a unit. This begs the question of how we define polynomials on projective coordinates because the evaluation is dependent on which representative of an equivalence class we choose. The solution is to use only homogenous polynomials, where a polynomial $P(x)$ is homogeneous of degree d if and only if for all $\lambda \in k^\times$, $P(\lambda x) = \lambda^d P(x)$. Thus, even if the output is not well defined, the zero sets of these polynomials are well defined, and this is what we care about. Any polynomial $f \in k[x_1, ..., x_n]$ can be homogenized into a polynomial in $k[x_0, x_1, ..., x_n]$ by considering the top degree term of degree d and for each monomial in f of degree j, multiply by a factor of x_0^{d-j}. One illustrative example is the equation

$$y^2 = x^3 + ax + b$$

Can be homogenized to become

$$y^2 z = x^3 + axz^2 + bz^3$$

Note that we can embed k^n into $\mathbb{P}^n$ by sending the coordinate $(x_1, .., x_n) \mapsto (x_1 : ... : x_n : 1)$. This relates to the above comment about adding a linear subspace to k^n to make it projective space. This space in the 2-dimensional case is the line at infinity $L_\infty = \{(x : y : 0) \in \mathbb{P}^2\}$.

1.2 Basic Geometry

For a seperable polynomial $f \in A = k[x, y]$ we define the set

$$C_f(k) = \{(x, y) \in k^2 | f(x, y) = 0\}$$

Note that for some $K \supset k$, we can consider $C_f(K)$ as well and in this case we have $C_f(k) \subset C_f(K)$. Such a curve is called irreducible if f is irreducible in A and geometrically irreducible if it remains such in the algebraic closure. For example, let $k = \mathbb{Q}$ and $K = \mathbb{R}$. Then if $f(x) = x^2 - 2$, it is irreducible over k but not K an extension so $C_f(k)$ is not geometrically irreducible. We can break f into irreducibles because A

is a UFD and so we can discuss the irreducible components of $C_f(k)$. We will be doing our analysis over perfect fields, so complicating factors involving seperability can be safely ignored. A singular point on some curve C is one in which both of the partial derivatives are 0. A point that is not singular is called regular. A curve with no singular points is called nonsingular. In the interest of foreshadowing, let us determine when the curve

$$y^2 = x^3 + ax + b$$

is singular. We must have

$$\begin{aligned} 2y &= 0 \\ 3x^2 + a &= 0 \\ y^2 &= x^3 + ax + b \end{aligned}$$

Assume that the characteristic of k is not 2 or 3. Then we have $y = 0$ and x is a common root of $x^3 + ax + b$ and its derivative. This exists if and only if $x^3 + ax + b$ has a multiple root. Thus we arrive at the result that the above is nonsingular if and only if $x^3 + ax + b$ has no multiple root.

1.3 Intersection Numbers and Bezout's Theorem

We wish to define the intersection number in an intuitive, canonical fashion. The following axioms are the result of our intuition. Let $f, g \in k[x, y]$ such that they have no common factor passing through the origin (this is to eliminate ambiguity). We wish for a map $I : k[x, y] \times k[x, y] \to \mathbb{N}$ that satisfies the below for

1. $I(x, y) = 1$
2. $I(f, g) = I(g, f)$
3. $I(f, gh) = I(f, g) + I(f, h)$
4. $I(f, g + hf) = I(f, g)$
5. $I(f, g) = 0$ if $g(0, 0) \neq 0$

As it turns out, these are sufficient to fully characterize such a function

Proposition 1. *There exists a unique function I that satisfies the above axioms.*

Proof. For existence, we merely provide the function

$$I(f, g) = \dim_k(k[x, y]/(f, g))_{(x,y)}$$

Note that $(k[x, y]/(f, g))_{(x,y)}$ is a finite dimensional vector space so this is well defined. It is easy to verify that the properties above hold for this function. To see 1 is a mere computation and 2 is trivial. To see that 3 holds, we compute again and 4 holds trivially from the definition of an ideal. Finally, 5 holds because if $g \notin (x, y)$ then it is a unit in the localization. To see uniqueness of the function, we appeal to the theory of resultants, which, if you are curious about, you can ask me after. ■

Note that the above proof does not depend on what field coefficients in f, g are considered in. For a point $P \in C_f \cap C_g$ we define the intersection number of the point, assuming there is no common irreducible component of f, g passing through P to be if $P = (a, b)$, then

$$I(P, C_f \cap C_g) = I(f(x + a, y + b), g(x + a, y + b)$$

A point is nonsingular on both curves and distinct tangent lines if and only if it has intersection number 1. The following theorem motivates the entire theory of Intersection Theory in algebraic geometry and is also very important for our purposes:

Theorem 2 (Bezout)**.** *If C, D are two projective plane curves over k sharing no irreducible component of degrees m, n then, counting with multiplicity, they intersect in mn points in the algebraic closure of k, i.e.,*

$$\sum_{P \in C \cap D} I(P, C \cap D) = mn$$

Proof. The most natural way to prove this is in a scheme theoretic setting as in Hartshorne's book, §5.1. If one does not wish to do this, then ask me after how it is done. ■

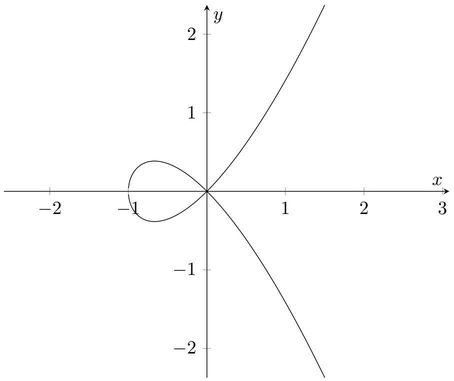
2 Elliptic Curves and the Group Law

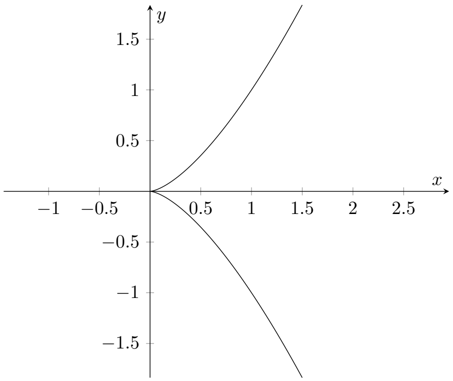
Part of what makes elliptic curves so important is that they have a group law on their points. First, though, we have to define an elliptic curve. We have

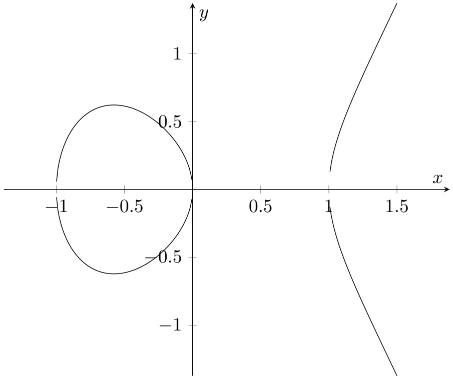
Definition 3. An elliptic curve can be defined in any of the following ways

1. A nonsingular projective plane curve of degree 3 E with a distinguished point O
2. A nonsingular projective plane curve of the form
$$Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_3X^2Z + a_4XZ^2 + a_5Z^3$$
3. A nonsingular projective plane curve of genus 1 with a distinguished point

Below are two examples of cubic curves that are not elliptic curves, the first being $y^2 = x^3 + x^2$ and the second being $y^2 = x^3$ and one example of an elliptic curve defined by $y^2 = x^3 - x$.







Note that the two are not elliptic because they are both singular, but that $x^3 - x = x(x^2-1) = x(x-1)(x+1)$ has no multiple root so does define an elliptic curve. If the characteristic of the field is neither 2 nor 3, then we can, by an affine transformation, transform the part of the curve on the affine open $z \neq 0$ to the form $y^2 = x^3 + ax + b$. Personally, I do not find the computations all that illuminating, but if for some reason you wish to see how it is done, I refer you to Silverman §3.1.

Now that we know what such a curve is, we can define a group law on it. There is a clear geometric interpretation of this law over $\mathbb{Q}$ if we restrict $\mathbb{P}^2_{\mathbb{Q}}$ to the affine open subset $z \neq 0$ and let the point at infinity $(0 : 1 : 0)$ be the distinguished point O. Note that by Bezout's theorem, a general line will intersect the curve E in three points. These three points are solutions to a cubic with coefficients in k. If two of the solutions lie in k then the third must as well by elementary Galois theory. Let PQ be the third point of intersection (if there is none in the affine plane, let $PQ = O$). Thus a naive choice for the group law is, if we have points $P, Q \in E$, then let $P + Q = PQ$. This is, however, not associative. Instead, we define $P + Q = O(PQ)$. If $P = Q$ then we use the tangent line instead of a secant. We need to show that this forms an abelian group. First of all, note that $OO = O$ and that $O(x, y) = (x, -y)$. Note also that the definition is symmetric in the P, Q because $PQ = QP$ so if it is a group then it is abelian. Moreover, $O(O(x, y)) = O(x, -y) = (x, y)$ so O is the additive identity. Also note that if P, Q are such that their y coordinates sum to 0, then $PQ = O$ so $Q = -P$. Thus it remains to check that this operation is associative. There are several ways of doing this. First, is we could compute exactly what this group law is and check it directly. This is boring and bad and we will not do this (although feel free to if you really want I guess...). The third way involves Riemann-Roch and I will discuss it a bit later if I have time. Here is the second way. We need a lemma:

Lemma 4 (Cayley-Bacharach)**.** *If two cubic curves in $\mathbb{P}^2$ intersect in 9 points, then any cubic passing through 8 of those points must pass through the 9^{th} as well.*

Proof. A homogeneous cubic is determined by 10 coefficients $a_1, .., a_{10}$. A solution $(x : y : z)$ to the cubic gives a linear relation on these a_i. Assuming that the P_i are linearly independent over k, 8 solutions reduces the 10 dimensional space to a 2 dimensional space, so there are two cubics $F, G \in k[X, Y, Z]_3$ such that all cubics passing through those 8 points are of the form $\alpha F + \beta G$. We have by Theorem 2 guarantees that there is some other common zero to F and G, and so any linear combination of F, G has this 0 as well and so we are done. If the solutions are not linearly independent, then it can be completed by doing casework on multiplicity. Alternatively, it is easier to prove from a scheme theoretic sense by doing some work with divisors. ■

We are now ready to prove that the group law is associative.

Proposition 5. *As defined above, the binary operation on points of an elliptic curve is associative.*

Proof. Let P, Q, R be points on the elliptic curve E with distinguished point O. Let $S = (P + Q)R$ and $T = P(Q + R)$. Then we have that $(P + Q) + R = OS$ and $P + (Q + R) = OT$. Thus we wish to show that $S = T$. Let $l(P, Q)$ denote the line passing through P and Q (if they are the same then it is the tangent line to E). Then consider

$$\begin{aligned} E &= 0 \\ l(P, Q) \cdot l(R, P + Q) \cdot l(QR, O) &= 0 \\ l(P, QR) \cdot l(Q, R) \cdot l(P, O) &= 0 \end{aligned}$$

Note that all three pass through the points $O, P, Q, R, PQ, QR, P+Q, Q+R$. The last two also pass through $l(P, Q + R) \cap l(P + Q, R) = U$ so if the lines are distinct then by Lemma 4 C passes through U as well and so we must have $S = U = T$. If the lines are not distinct, then we have to use more sophisticated machinery (intersection theory on surfaces). To do this we make use of the result

If C, C', C'' are cubic curves and $C \cdot C' = \sum_1^9 [P_i]$ with P_i nonsingular, then $C \cdot C'' = \sum_1^8 [P_i] + [Q]$ then $Q = P_9$. See Fulton's intersection theory or algebraic curves book for details. ■

2.1 Riemann-Roch and Divisors

I will get to this if I have time.

Fix a curve C. We define the divisor group, $\mathrm{Div}(C)$ to be the free abelian group on the points of C. For a polynomial, F, we define

$$\mathrm{Div}(F) = \sum_{P \in \{F=0\} \cap C} I(P, \{F=0\} \cap C)[P]$$

And so $\mathrm{Div}(FG) = \mathrm{Div}(F) + \mathrm{Div}(G)$ and $\mathrm{Div}(\frac{F}{G}) = \mathrm{Div}(F) - \mathrm{Div}(G)$. Now, given a divisor D, let

$$L(D) = \{\phi | \operatorname{Div}(\phi) + D \geq 0\} \cup \{0\}$$

Then $L(D)$ is a vector space and let $l(D) = \dim L(D)$. For any divisor $D = \sum n_P[P]$ we define $\deg D = \sum n_P$. We blackbox and introduce the concept of canonical divisor K. The genus, g of the curve is also black boxed, but is given to be in the case of nonsingular projective plane curves

$$g(C) = \frac{(\deg C - 1)(\deg C - 2)}{2}$$

Then we have

Theorem 6. *With all defined above, if C is a nonsingular curve, then*

$$l(D) - l(K - D) = \deg D + 1 - G$$

Proof. Easy with Serre Duality. ■

Now we define $\mathrm{Div}^0(C) \subset \mathrm{Div}(C)$ to be the subgroup of all degree 0 divisors on C and we define $P(C) \subset \mathrm{Div}^0(C)$ to be the subgroup of all principal divisors (a divisor D is principal if there is some rational F such that $D = \mathrm{Div}(F)$). Now we define Picard groups

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/P(C)$$
$$\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/P(C)$$

The Picard group can also be thought of as the group of invertible sheaves on C or equivalently, the group of line bundles on C. Now, we define a function $C \to \mathrm{Pic}^0(C)$

$$P \mapsto [P] - [O]$$

This map is bijective because C is not birational to $\mathbb{P}^1$ and surjective because if D has degree 0 then $D + [O]$ has degree 1 and so so there exists a unique up to scaling rational ϕ such that $\mathrm{Div}(\phi) + D + [O] \geq 0$ but this is of degree 1 so we must have some unique P such that $\mathrm{Div}(\phi) + D + [O] = [P]$. Thus, $D \sim [P] - [O]$.

Now this defines an abelian group structure on the points of C by letting $P + Q = R$ if and only if $[P] + [Q] \sim [R] + [O]$. A quick check shows that this agrees with the geometrically motivated group structure above, yielding another proof of associativity. (To see this agreement, let L_1, L_2 be the lines through P, Q and O, R respectively. Then we have that $L_1 \cap L_2 \ni S \in C$. Let $\phi = \frac{L_1}{L_2}$. Then we clearly have $\mathrm{Div}(\phi) = [P] + [Q] + [S] - [O] - [R] - [S] = [P] + [Q] - [O] - [S]$ and we are done.)