PLANE ALGEBRAIC CURVES

ANDREW DING

Abstract. We go over some of the basics of plane algebraic curves, which are planar curves described as the set of solutions of a polynomial in two variables. We study many basic notions, such as projective space, parametrization, and the intersection of two curves. We end with the group law on the cubic and search for torsion points.

Contents

1. Introduction

Solving systems of polynomial equations in several variables is of interest in algebraic geometry. It is a generalization of both solving for roots of polynomials (algebra) and solving systems of linear equations (linear algebra). The main insight of algebraic geometry is to view solutions to a system of polynomial equations geometrically. For example, the set of solutions to a polynomial equation in two variables forms an algebraic curve. We can study the topological and geometrical properties of such a curve. In addition, geometric pictures provide valuable insight in solving problems in algebraic geometry.

Unlike topology, which focuses on continuous functions, and differential geometry, which focuses on smooth functions, the main focus in algebraic geometry are polynomial functions. The main advantage of this fact is that a majority of results work over an arbitrary field. Occasionally, an algebraically closed field is needed.

Date: 08/26/2012.

Another advantage of polynomials is a sense of finiteness. For example, a polynomial over one variable has finitely many roots, and S_d, the space of all homogeneous polynomials of degree d, is a finite-dimensional vector space.

Some curves can be parametrized, which allows us to completely understand these curves. Notably, parametrizing a curve over any field gives all rational solutions, which is of interest in number theory.

Another object of study is algebraic subsets in projective space. In the projective plane, every pair of distinct lines intersect at exactly one point. In the affine plane, two distinct lines generally intersect at one point, with the exception of parallel lines, which are a special case. Projective geometry eliminates this special case, and allows the statement of Bezout's Theorem, which fully describes the number of intersection of two algebraic curves. In addition, there is a handful of theorems that are stated in the context of projective space, such as the Cayley-Bacharach Theorem and Pascal's Theorem.

Given certain conditions, Bezout's Theorem states that a line and a cubic will intersect at three points. Given this fact and that two points determine a line, if the cubic is 'nice enough', then we can define a group over the set of points on the cubic. These types of cubics are called elliptic curves. The theory of elliptic curves is extremely rich and remains an active area of research.

2. Parametrization of a Conic

Let's start with an example that hopefully both gives motivation to study algebraic geometry and demonstrates the interplay between algebra and geometry.

Example 2.1. Find all integer solutions to the equation $X^2 + Y^2 = Z^2$.

Proof. At first, this seems like a purely algebraic question. In addition, we can find several solutions, such as $(1, 0, 1)$ and $(3, 4, 5)$, but it may seem daunting to find all solutions.

We can start by narrowing our search to all primitive integer solutions, that is, solutions such that $\gcd(X, Y, Z) = 1$, because all solutions come from a primitive one. For example, $(12, 16, 20)$ comes from $(3, 4, 5)$.

Substitute $x = X/Z, y = Y/Z$. We obtain $x^2 + y^2 = 1$. Since (X, Y, Z) is a primitive solution, we have a bijection from the rational points on the circle C to primitive integer solutions. For example, $(3, 4, 5)$ would correspond to $(\frac{3}{5}, \frac{4}{5})$.

To find all the rational points, we use a technique called projection. First of all, we need one rational point, so we will use $(-1, 0)$. Next, note that every line through $(-1, 0)$ (except one) intersects the circle through another point. Each of these lines has a different slope λ and hits the circle at different points P_λ. We have a bijection from $\mathbb{R}$ to $C\backslash(-1, 0)$. Simplifying, we obtain $P_\lambda = (\frac{2\lambda}{\lambda^2+1}, \frac{\lambda^2-1}{\lambda^2+1})$.

Note if $\lambda \in \mathbb{Q}$, then $P_\lambda \in \mathbb{Q}^2$. Conversely, if $P_\lambda \in \mathbb{Q}^2$, then by calculating the slope of the line through $(-1, 0)$ and P, we get $\lambda \in \mathbb{Q}$. This gives a bijection from $\mathbb{Q}$ to rational points on the circle.

We are almost done. Let $\lambda = \frac{m}{n} \in \mathbb{Q}$, where m, n are coprime. Substitute $\frac{m}{n}$ for λ. Clearing denominators, we get $X = 2mn, Y = m^2 - n^2, Z = m^2 + n^2$. If l, m are both odd, then divide X, Y, Z by 2. This gives us all primitive Pythagorean triples. □

We can make a few important observations.

(1) We were working with the equation $X^2 + Y^2 = Z^2$, which is a homogeneous equation. This process does not work for polynomials in general. Homogeneous polynomials are convenient for many reasons, one of which is highlighted in Section 3.
(2) We started projection with the rational point $(-1, 0)$. Projection does not help us find this first rational point. In fact, some conics will have no rational points, such as $2x^2 + y^2 = 5$. (To verify this, work with the polynomial $2X^2 + Y^2 = 5Z^2$ modulo 5).
(3) The vertical line through $(-1, 0)$ should be mentioned. It intersects the circle at $(-1, 0)$ with multiplicity 2, so the vertical line corresponds to the point $(-1, 0)$. We did not miss the associated primitive solution; by allowing $m = -1, n = 0$ in the last step, we get the point $(-1, 0, 1)$.
(4) The fact that we got a bijection from the set of rational points on the conic to the set of rational numbers is not a coincidence. In fact, this will hold for conics in general. This will be explained in more detail in Section 4.

3. Projective Space

We take a break from conics to develop the notion of projective space. It is often convenient to work in projective space when discussing the number of intersection points of two algebraic curves. For example, in the affine plane, two distinct lines intersect at one point, unless they are parallel. In the projective plane, any two distinct lines will always intersect at exactly one point. We will begin with the projective line and the projective plane.

Definition 3.1. Let k be a field, $O = (0, 0) \in k^2$. The *projective line* $\mathbb{P}^1_k$ is defined as the geometry with $\{\text{lines through } O \in k^2\}$ as the set of points.

Let us try to imagine what the projective line looks like. In the affine plane, a line is determined by a point on the line and its slope. Since all lines go through O, the only difference between two distinct lines is their slopes. Hence, we have the following injection:

$$\varphi : k \to \mathbb{P}^1_k, \varphi(\lambda) = \text{ line with slope } \lambda \text{ through } O.$$

However, this misses the vertical line through O. Let's say it has slope ∞. Adding it to the domain, we have:

$$\mathbb{P}^1_k \cong k \cup \{\infty\}.$$

Now, let us develop a system of coordinates to describe these points. Suppose we have a point $P \in \mathbb{P}^1_k$. The point P is an affine line l through $O \in k^2$. The line l must pass through another point, say (A, B). We give P the *homogeneous coordinates* $[A : B]$. If $\lambda \neq 0$, then $[\lambda A : \lambda B]$ represents P as well. This is analogous to the fact that, if $B \neq 0$, $\frac{A}{B}$ and $\frac{\lambda A}{\lambda B}$ represent the same number. In mathematical language,

$$\mathbb{P}^1_k = k^2 - \{(0, 0)\}/\sim,$$
$$\text{where } (a, b) \sim (c, d) \text{ if } c = \lambda a, d = \lambda b \text{ for some } \lambda \neq 0.$$

In other words, we define a point on the projective line as an equivalence class of points on the affine plane, where two points are related if they lie on the same veritable line through the origin.

The advantage of using homogeneous coordinates is that it describes projective points without the use of infinity, making them easier to use in algebraic manipulation. Homogeneous coordinates treat all points equally, which is also true for the original definition of the projective line.

Now we will move to a more interesting concept, the projective plane. As the projective line is an 'extension' of the affine line, the projective plane is also an 'extension' of the affine plane. The process is similar.

Definition 3.2. Let k be a field, $O = (0,0,0) \in k^3$. The *projective plane* $\mathbb{P}_k^2$ is defined as the geometry with $\{$lines through $O \in k^3\}$ as the set of points and $\{$planes through $O \in k^3\}$ as the set of lines.

Let us try to imagine what the projective plane looks like. Let $P \in \mathbb{P}_k^2$. Then P is a line l through $O \in k^3$. Let (A, B, C) be a nonzero point on l. There are two cases to consider.

If $C \neq 0$, then l intersects the plane $Z = 1$ in k^3 at the unique point $(\frac{A}{C}, \frac{B}{C}, 1)$. Make sure to understand why the choice of (A, B, C) does not matter. We conclude that if $C \neq 0$, then P corresponds to $(\frac{A}{C}, \frac{B}{C}) \in k^2$. If $C = 0$, then the entire line lies on the plane $Z = 0$. This case is just the projective line. In summary, we have:

$$\mathbb{P}_k^2 \cong k^2 \cup \mathbb{P}_k^1.$$

We will develop coordinates for points on the projective plane similarly. Suppose we have a point $P \in \mathbb{P}_k^2$. The point P is an affine line l through $O \in k^3$. The line l has to pass through another point, say (A, B, C). We give P the *homogeneous coordinates* $[A : B : C]$. If $\lambda \neq 0$, then $[\lambda A : \lambda B : \lambda C]$ represents P as well. In mathematical language,

$$\mathbb{P}_k^2 = k^3 - \{(0,0,0)\}/\sim,$$
$$\text{where } (a,b,c) \sim (d,e,f) \text{ if } d = \lambda a, e = \lambda b, f = \lambda c \text{ for some } \lambda \neq 0.$$

Lastly, let us compare the geometries of the affine plane and the projective plane. In the affine plane, we have two familiar axioms:

(1) Axiom 1: For every distinct pair of points P, Q, there exists a unique line l such that both P and Q lie on l.
(2) Axiom 2: For every line l and point P not on l, there exists a unique line m such that l is parallel to m.

Let us see which axioms hold in the projective plane.

Let $P, Q \in \mathbb{P}_k^2$ be two distinct points. Suppose projective points P, Q correspond to affine lines l, m, respectively. Since lines l, m intersect at O, there exists a unique plane (through O) that contains l, m. This affine plane corresponds to a projective line, hence, Axiom 1 is satisfied.

Let $l', m' \subseteq \mathbb{P}_k^2$ be two distinct lines. Suppose they correspond to affine planes P', Q', respectively. Since planes P', Q' intersect at O, they intersect at a line (through O). This line corresponds to a projective point, hence, *every* pair of lines intersect, so there is no notion of parallel lines and Axiom 2 is not satisfied.

In summary, the following two axioms hold in the projective plane.

(1) Axiom 1: For every distinct pair of points P, Q, there exists a unique line l such that both P and Q lie on l.
(2) Axiom 2': Every distinct pair of lines l, m intersect at a point.

4. Lines and Conics

The following treatment is taken from Miles Reid's *Algebraic Geometry* [1].

Definition 4.1. A *form* of degree d is a homogeneous polynomial of degree d.

Definition 4.2. A *line* $L \subseteq \mathbb{P}^2$ is the set given by $\{[X : Y : Z] : H(X, Y, Z) = 0\}$, where H is a linear form.

Definition 4.3. A *conic* $C \subseteq \mathbb{P}^2$ is the set given by $\{[X : Y : Z] : Q(X, Y, Z) = 0\}$, where Q is a quadratic form.

We must see if they are well-defined before continuing. If $\lambda \neq 0$, then $[X : Y : Z]$ and $[\lambda X, \lambda Y, \lambda Z]$ represent the same point in $\mathbb{P}^2$. Therefore, we must check that (X, Y, Z) is a solution to H if and only if $(\lambda X, \lambda Y, \lambda Z)$ is a solution, in other words,

$$H(X, Y, Z) = 0 \Leftrightarrow H(\lambda X, \lambda Y, \lambda Z) = 0. \tag{4.4}$$

Fortunately, $H(X) = aX + bY + cZ$, where $a, b, c \in k$, so the following holds:

$$H(\lambda X, \lambda Y, \lambda Z) = a(\lambda X) + b(\lambda Y) + c(\lambda Z) = \lambda(aX + bY + cZ) = \lambda H(X, Y, Z).$$

Since $\lambda \neq 0$, (4.4) is satisfied. Similarly, $Q(X, Y, Z) = aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2$, and we have the following:

$$Q(\lambda X, \lambda Y, \lambda Z) = \lambda^2 Q(X, Y, Z) = 0 \Leftrightarrow Q(X, Y, Z) = 0.$$

Again, $\lambda \neq 0$. Therefore, the concepts of line and conic are well-defined. In fact, the set of zeroes for a form of any degree is well-defined. The key property is homogeneity.

Conics may be either nondegenerate or degenerate. Degenerate conics are conics that can be expressed as a finite union of points and lines. They include (but are not limited to) pair of lines ($XY = 0$), or a 'double line' ($X^2 = 0$). We will often work with nondegenerate conics.

Definition 4.5. Define $S_2 = \{\text{quadratic forms}\} \subseteq k[X, Y, Z]$.

Note that any element $Q \in S_2$ can be written in the form $aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2$ where $a, b, c, d, e, f \in k$. Therefore, S_2 is a vector space over k of dimension 6.

Let $P_0 = [X_0 : Y_0 : Z_0] \in \mathbb{P}^2_k$. Define $S_2(P_0) = \{Q \in S_2 : Q(X_0, Y_0, Z_0) = 0\}$. So we have the following necessary condition.

$$F(X_0, Y_0, Z_0) = aX_0^2 + bX_0Y_0 + \cdots + fZ_0^2 = 0.$$

If P_0 is fixed, then this is a linear equation in the variables (a, b, c, d, e, f). This constraint gives us $\dim(S_2(P_0)) = 5$.

Let $P_1, \ldots, P_n \in \mathbb{P}^2_k$. Similarly, define

Definition 4.6. $S_2(P_0, \ldots, P_n) = \{Q \in S_2 : Q(P_i) = 0\}$ for $i = 1, \ldots, n$.

We have n linear equations in the variables (a, b, c, d, e, f). We have proved the following proposition.

Proposition 4.7. *dim*$(S_2(P_1, \ldots, P_n)) \geq 6 - n$.

Now let us take a step back and prove an important result about forms of degree d in U, V and the projective line.

Let $F(U,V) \in k[U,V]$ be a form of degree d. Then F can be expressed in the following manner.

$$F(U,V) = a_dU^d + a_{d-1}U^{d-1}V + \cdots + a_1UV^{d-1} + a_0V^d, \text{ where } a_i \in k \text{ for } i = 1, \ldots, d.$$

Using the substitution $u = U/V$ and dividing through by V^d, we get an association between the homogeneous $F(U,V)$ and the inhomogeneous $f(u)$.

$$f(u) = a_du^d + \cdots + a_0, \text{ where } a_i \in k \text{ for } i = 1, \ldots, d.$$

Polynomials in one variable are much more familiar to us. Let $c \in k$.

$$f(c) = 0 \Leftrightarrow (u-c)|f(u) \Leftrightarrow (U - cV)|F(U,V) \Leftrightarrow F(c,1) = 0.$$

$$F(1,0) = 0 \Leftrightarrow V|F(U,V) \Leftrightarrow a_d = 0 \Leftrightarrow \deg(f(u)) < d.$$

Now we define the *multiplicity* of a root of F as follows.

(1) The multiplicity of the corresponding c in f or
(2) if [1:0] is a root, then its multiplicity is $d - \deg(f)$.

Proposition 4.8. *Let $F(U,V)$ be a form of degree d in U, V. Then F has at most d roots, counting multiplicities, on $\mathbb{P}^1_k$, with equality if k is algebraically closed.*

Proof. Let m_∞ be the multiplicity of the point $[1 : 0]$. Then F and its roots are associated with the inhomogeneous $f(u)$ over one variable and its roots. The polynomial f has degree $d - m_\infty$ and hence has at most that many roots, with equality if k is algebraically closed. Therefore, F has a total of at most d roots, counting multiplicities. □

Now we can prove Bezout's Theorem for small cases, in particular, when one of the curves is a line or nondegenerate conic.

Theorem 4.9. *Bezout's Theorem (small cases). Let $L \subseteq \mathbb{P}^2_k$ be a line (respectively, $C \subseteq \mathbb{P}^2_k$ be a nondegenerate conic), and $D \subseteq \mathbb{P}^2_k$ a curve defined by*

$$D = \{[X : Y : Z] \in \mathbb{P}^2_k : G_d(X,Y,Z)\}, \text{ where } G_d \text{ is a form of degree } d.$$

Assume that $L \nsubseteq D$ ($C \nsubseteq D$). Then

$$|\{L \cap D\}| \leq d \quad (|\{C \cap D\}| \leq 2d)$$

Equality holds if we count multiplicities and k is algebraically closed.

Proof. The key to the proof is to parametrize the line (conic) and then use the previous proposition.

L is represented by $H = 0$, where H is a linear form on X, Y, Z. We wish to parametrize L. We can do this in the following way:

$$X = a(U,V), Y = b(U,V), Z = c(U,V), \text{ where } a, b, c \text{ are linear forms.}$$

Since any nondegenerate conic is parametrically equivalent to $XZ = Y^2$, which can be parametrized by $X = U^2, Y = UV, Z = V^2$, we have

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = M \begin{pmatrix} U^2 \\ UV \\ V^2 \end{pmatrix} \text{ where } M \text{ is a nonsingular 3x3 matrix.}$$

Therefore, we have

$$X = a(U,V), Y = b(U,V), Z = c(U,V), \text{ where } a, b, c \text{ are quadratic forms.}$$

To find the intersection points of L and D (respectively, C and D), we want to find $(U, V) \in \mathbb{P}^1_k$ such that

$$F(U, V) = G_d(a(U, V), b(U, V), c(U, V)) = 0.$$

F is a form of degree d (respectively, $2d$), so by the previous proposition, there are at most d ($2d$) roots, with equality if we count multiplicities and k is algebraically closed. □

Remark 4.10.
(1) We can use this theorem to show that we can parametrize any nondegenerate conic $C \subseteq \mathbb{P}^2_k$. Let $P \in C$, L be a line through P. We have $L \nsubseteq C$ because C is nondegenerate. By Bezout's Theorem, L must intersect C at two points, one of which is P. The set of lines through $P \in \mathbb{P}^2_k$ is just the projective line, so we have a bijection between C and the projective line. If $k' \subseteq k$ is a subfield and there exists a k'-point, then we can find all points on C with coordinates in k' by setting P to be a k'-point and using projection in a similar manner to Example 2.1.
(2) Bezout's Theorem actually states that the number of intersection points between curves of degree m and n is mn, given that we work in an algebraically closed field, count multiplicities, and work in projective space. An additional condition is that the two curves do not 'share components'. For example, a degenerate conic can be either a line pair or a 'double line'. The intersection of a degenerate conic and one of its line components can be infinite, so that case must be eliminated. The theorem in full generality requires different reasoning than the proof above.

Corollary 4.11. *If* $|\{L \cap D\}| > d \quad (|\{C \cap D\}| > 2d)$, *then* $L \subseteq D$ $(C \subseteq D)$.

Corollary 4.12. *Let* $P_1, \ldots, P_5$ *be distinct points such that no four are collinear. There exists at most one conic passing through* $P_1, \ldots, P_5$

Proof. We will use contradiction. Suppose that C_1, C_2 are two conics with $C_1 \neq C_2$ and $\{P_1, \ldots, P_5\} \subseteq C_1 \cap C_2$.

(1) Case 1: C_1 or C_2 is non-degenerate. Assume WLOG that C_1 is nondegenerate. Then C_1 is projectively equivalent to the curve

$$C_1 = \{(U^2, UV, V^2) : (U, V) \in \mathbb{P}^k_1\}.F$$

By the previous corollary, $C_1 \subseteq C_2$. Let Q_2 be the equation of C_2, this implies $Q_2(U^2, UV, V^2) = 0$. By a calculation (see Lemma 6.3 for justification), $(XZ - Y^2)|Q_2$. Since both are quadratics, Q_2 is a scalar multiple of $XZ - Y^2$, but this implies $C_1 = C_2$, a contradiction.

(2) Case 2: C_1 and C_2 are degenerate. After some casework, both conics must be line pairs. If all four lines are distinct, then each line of C_1 intersects C_2 twice, making a total of four intersection points. Therefore, they must share a line. We have

$$C_1 = L_0 \cup L_1, C_2 = L_0 \cup L_2,$$

$$C_1 \cap C_2 = L_0 \cup (L_1 \cap L_2).$$

Since L_1, L_2 are distinct, they intersect at one point. Then the other four points of intersection lie on L_0, a contradiction.

□

Corollary 4.13. *If $n \leq 5$ and no four points are collinear, then*

$$dim(S_2(P_1, \ldots, P_n)) = 6 - n.$$

Proof. We already proved that $\dim(S_2(P_1, \ldots, P_n)) \geq 6-n$. The intuition is that if the points are general enough, equality holds. If $n = 5$, then the previous corollary implies that $\dim(S_2(P_1, \ldots, P_n)) \leq 1$ and we are done. If $n \leq 5$, then we add points $P_{n+1}, \ldots, P_5$, while keeping the condition that no four points are collinear. Each additional point imposes at most one linear condition, we have

$$1 = \dim(S_2(P_1, \ldots, P_5)) \geq \dim(S_2(P_1, \ldots, P_n)) - (5 - n)$$

$$\Rightarrow 6 - n \geq \dim(S_2(P_1, \ldots, P_n)).$$

Since we have already proved the other direction, we are done. □

This shows that five general points determine a conic. For conics, general means that no four points are collinear. If three points are collinear, we get a line pair.

5. Parametrization of Singular Cubics

Definition 5.1. A *cubic* $C \subseteq \mathbb{P}^2$ is the set given by $\{[X : Y : Z] : F(X, Y, Z) = 0\}$, where F is a cubic form.

Again, there are nondegenerate and degenerate cubics. Degenerate cubics are cubics that can be expressed as a finite union of points, lines, and conics. They include (but are not limited to) line triplets ($XY(X + Y) = 0$), 'triple lines' ($X^3 = 0$), and unions of a line and a conic ($Z(X^2 + Y^2) = 0$).

We will consider cubics of the following form.

$$y^2 = x^3 + ax + b, \text{ where } a, b \in k$$

We will not prove it, but there are three types of nondegenerate cubics: nodal cubics, cuspidal cubics, and elliptic curves. In fact, we can parametrize the first two types of cubics.

Example 5.2. Parametrize the *nodal cubic* $y^2 = x^3 + x^2$.

By the same method as the conic, we substitute the equation for a generic line through $(0, 0)$, $y = \lambda x$, into the equation of the cubic and solve for x. We obtain the following.

$$x^3 + (-\lambda^2 + 1)x^2 = 0.$$

Counting multiplicity, the solutions are $x = 0, 0, \lambda^2 - 1$. So the points of intersection are $(0, 0), (0, 0), (\lambda^2 - 1, \lambda^3 - \lambda^2)$. Therefore, to parametrize the curve, we send λ to $(\lambda^2 - 1, \lambda^3 - \lambda^2)$.

Example 5.3. Parametrize the *cuspidal cubic* $y^2 = x^3$.

By the same method as the conic, we substitute the equation for a generic line through $(0, 0)$, $y = \lambda x$, into the equation of the cubic and solve for x. We obtain the following.

$$x^3 + (-\lambda^2)x^2 = 0$$

Counting multiplicity, the solutions are $x = 0, 0, \lambda^2$. So the points of intersection are $(0, 0), (0, 0), (\lambda^2, \lambda^3)$. Therefore, to parametrize the curve, we send λ to (λ^2, λ^3).

We can make a few important observations. The reason this parametrization is possible over an arbitrary field is because we have to solve the equations $x^3 + (-\lambda^2 + 1)x^2 = 0$ and $x^3 + (-\lambda^2)x^2 = 0$, which can be completely factored. The line intersects the cubic in at most two points because $(0, 0)$ is an intersection point of multiplicity two. (This can be seen in the x^2 factor that appears in the two equations above.) So any line through $(0, 0)$ intersects the cubic at one other point. Lastly, unlike the conic, we cannot choose an arbitrary rational point; as mentioned above, most lines intersect the cubic at three distinct points over an algebraically closed field. For example, over $\mathbb{C}$, the line through $(-1, 0)$ with slope 1 intersects $y^2 = x^3 + x^2$ thrice and the line through $(1, 1)$ with slope 2 intersects $y^2 = x^3$ thrice. In fact, all above intersections are $\mathbb{R}$-points.

Take the curve $y^2 = x^3$. Let's look at the cubic in the projective plane instead of the affine plane. This corresponds to the homogeneous polynomial $Y^2Z = X^3$. To find where this curve intersects the line at infinity, we plug in $Z = 0$ and get that $X^3 = 0$. So $[0 : 1 : 0]$ is in the cubic as well as the familiar affine part. So every vertical line intersects the cubic at three points: $[X : Y : Z], [X : -Y : Z], [0 : 1 : 0]$, which was promised by Bezout's Theorem. We have a similar result with $y^2 = x^3 + x^2$. Note that our intuition in $\mathbb{R}$ fails us here; it is necessary that the field is algebraically closed to get exactly three points of intersection.

6. Cayley-Bacharach Theorem

The Cayley-Bacharach Theorem states that, given certain conditions, if two cubics intersect in exactly nine points, then any cubic that passes through any eight of the points must pass through the ninth. This will be an essential step in proving Pascal's Theorem and associativity of the group law on the cubic.

The following treatment is taken from Miles Reid's *Algebraic Geometry* [1].

Definition 6.1. Define $S_d = \{\text{forms of degree d}\} \subseteq k[X, Y, Z]$.

Recall that a form is just a homogeneous polynomial.

Note that any element $F \in S_d$ can be written in the form $\sum a_{i,j,k}X^iY^jZ^k$ where $a_{i,j,k} \in k$ and the sum is taken over all nonnegative i, j, k with $i + j + k = d$. Therefore, S_d is a vector space over k. Using combinatorics, $\dim(S_d) = \binom{d+2}{2}$. For now, we will consider 0 a homogeneous polynomial of degree d for any d.

Definition 6.2. Let $P_1, \ldots, P_n \in \mathbb{P}^2_k$. Define

$$S_d(P_1, \ldots, P_n) = \{F \in S_d : F(P_i) = 0 \text{ for } i = 1, \ldots, n\}.$$

In a similar manner to the conic case, each P_i imposes a linear condition on S_d, so $\dim(S_d) \geq \binom{d+2}{2} - n$.

Lemma 6.3. *Suppose k is an infinite field and $F \in S_d$.*

1. *Let $L \subseteq \mathbb{P}^2_k$ be a line, and H be the equation of L. If $F(P) = 0$ for all P on L, then F is divisible by H in $k[X, Y, Z]$. In other words, $F = HF'$, where $F' \in S_{d-1}$.*
2. *Let $C \subseteq \mathbb{P}^2_k$ be a nondegenerate conic, and Q be the equation of C. If $F(P) = 0$ for all P on C, then F is divisible by Q in $k[X, Y, Z]$. In other words, $F = QF'$, where $F' \in S_{d-2}$.*

Proof. (1) By change of coordinates, we can assume $H = X$. There exists a unique expression $F = HF'_{d-1} + G(Y, Z)$ because we can move all the terms

with X in the first part and we are left with an expression in Y, Z. We have the following.

$$F \equiv 0 \text{ on L } \Leftrightarrow G \equiv 0 \text{ on L } \Leftrightarrow G(Y, Z) = 0.$$

The last step holds because if $G \neq 0$, then it has at most d zeroes on $\mathbb{P}^1_k$, but since k is infinite, so is $\mathbb{P}^1_k$.

(2) By change of coordinates, we can assume $Q = XZ - Y^2$. There exists a unique expression $F = QF'_{d-2} + A(X, Z) + Y \cdot B(X, Z)$ because we can substitute $Q - XZ$ for Y^2 and we are left with terms of degree less than or equal to one in Y. Parametrize C by $X = U^2, Y = UV, Z = V^2$. We have the following.

$$F \equiv 0 \text{ on C } \Leftrightarrow A(U^2, V^2) + UV \cdot B(U^2, V^2) \Leftrightarrow$$

$$A(U^2, V^2) + UV \cdot B(U^2, V^2) = 0 \in k[U, V] \Leftrightarrow A(X, Z) = 0 = B(X, Z).$$

The last step holds because $A(U^2, V^2)$ only contains terms where exponents of both U and V are even, while $UV \cdot B(U^2, V^2)$ only contains terms where neither exponent is even.

□

Corollary 6.4. *Let $P_1, \ldots, P_n \in \mathbb{P}^2_k$. Fix d. Consider $S_d(P_1, \ldots, P_n)$.*

(1) Let $L \subseteq \mathbb{P}^2_k$ be the line given by $H = 0$. If $P_1, \ldots, P_a \in L, P_{a+1}, \ldots, P_n \notin L$ with $a > d$, then we have

$$S_d(P_1, \ldots, P_n) = H \cdot S_{d-1}(P_{a+1}, \ldots, P_n).$$

(2) Let $C \subseteq \mathbb{P}^2_k$ be the nondegenerate conic given by $Q = 0$. If $P_1, \ldots, P_a \in L, P_{a+1}, \ldots, P_n \notin L$ with $a > 2d$, then we have

$$S_d(P_1, \ldots, P_n) = Q \cdot S_{d-2}(P_{a+1}, \ldots, P_n).$$

Proof. We start with the line case. Suppose F is homogeneous of degree d and that D is the curve given by $F = 0$. If D intersects L at $P_1, \ldots, P_a$ where $a > d$, then by Bezout's Theorem, L must be a component of D, that is, $L \subseteq D$. By the previous lemma, we have $F = H \cdot F'$, where $F' \in S_{d-1}$. Since $P_{a+1}, \ldots, P_n \notin L$, we have $F' \in S_{d-1}(P_{a+1}, \ldots, P_n)$. The conic case follows similarly. □

Proposition 6.5. *Let k be an infinite field, $P_1, \ldots, P_8 \in \mathbb{P}^2_k$ be eight distinct points. If no four of the points are collinear and no seven of the points are conconic, then*

$$dim(S_3(P_1, \ldots, P_8)) = 2.$$

Proof. We know that

$$\dim(S_3(P_1, \ldots, P_8)) \geq \binom{3+2}{2} - 8 = 10 - 8 = 2,$$

so it is sufficient to show $\dim(S_3(P_1, \ldots, P_8)) \leq 2$.

(1) Case 1: No three of the points are collinear and no six of the points are conconic. This is the general case. Suppose for contradiction that $S_3(P_1, \ldots, P_8) \geq 3$. Let P_9, P_{10} be two points on the line $L = P_1P_2$. We have

$$\dim(S_3(P_1, \ldots, P_{10})) \geq \dim(S_3(P_1, \ldots, P_8)) - 2 \geq 3 - 2 \geq 1.$$

This implies that there exists nonzero $F \in S_3(P_1, \ldots, P_{10})$. By the previous corollary, $F = H \cdot Q$ where $Q \in S_2(P_3, \ldots, P_8)$. Now we have a contradiction: If Q is nondegenerate, then there exist seven conconic points, and if Q is a line pair or double line, then there exist three collinear points.

(2) Case 2: $P_1, P_2, P_3 \in L$ are collinear. Let L be the line given by the equation $H = 0$. Let P_9 be another point on L. By the previous corollary,

$$S_3(P_1, \ldots, P_9) = H \cdot S_2(P_4, \ldots, P_8).$$

Since no four of $P_4, \ldots, P_8$ are collinear, we have

$$\dim(S_2(P_4, \ldots, P_8)) = 1,$$

because five distinct points, no four of which are collinear, determine a conic. Therefore, $\dim(S_3(P_1, \ldots, P_9)) = 1$, so $\dim(S_3(P_1, \ldots, P_8)) \leq 2$.

(3) Case 3: $P_1, \ldots, P_6 \in C$ are conconic. Let C be the nondegenerate conic given by the equation $Q = 0$. Let P_9 be another point on C. By the previous corollary,

$$S_3(P_1, \ldots, P_9) = Q \cdot S_1(P_7, P_8).$$

Since two distinct points determine a line, we have

$$\dim(S_1(P_7, P_8)) = 1.$$

Therefore, $\dim(S_3(P_1, \ldots, P_9)) = 1$, so $\dim(S_3(P_1, \ldots, P_8)) \leq 2$.

□

Corollary 6.6. *The Cayley-Bacharach Theorem: Let C_1, C_2 be two cubic curves that intersect at exactly nine points, that is, $C_1 \cap C_2 = \{P_1, \ldots, P_9\}$. Then any cubic C through $P_1, \ldots, P_8$ also passes through P_9.*

Proof. If any four points of $P_1, \ldots, P_8$ were collinear, then by Bezout's Theorem, both C_1 and C_2 must contain the entire line, which is infinite since k is infinite, which is a contradiction to $|C_1 \cap C_2| = 9$. Similarly, no seven points are conconic. Therefore, the assumptions of the previous proposition are satisfied, so

$$\dim(S_3(P_1, \ldots, P_8)) = 2.$$

In other words, C_1, C_2 form a basis for $S_3(P_1, \ldots, P_8)$, which means if C is a cubic given by $G = 0$, then $G = \lambda F_1 + \mu F_2$, where F_1, F_2 are the equations for C_1, C_2, respectively. Since F_1, F_2 vanish at P_9, so does G. □

Note that we never required the cubics in question to be nondegenerate. In fact, it will often be useful to define a cubic as a line triplet when applying the Cayley-Bacharach Theorem.

Now we will use this result to prove Pascal's Theorem.

Suppose $ABCDEF$ forms a hexagon in $\mathbb{P}^2$. Extend opposite sides until they intersect. Explicitly, define

(1) P as the intersection of FA and CD,
(2) Q as the intersection of AB and DE,
(3) R as the intersection of BC and EF.

Theorem 6.7. *If the nine points and the six lines are all distinct, then*

$$ABCDEF \text{ conconic} \Leftrightarrow PQR \text{ collinear.}$$

Proof. Define the following two triples of lines:

$$L_1 = PFA, L_2 = QDE, L_3 = RBC,$$
$$M_1 = PCD, M_2 = QAB, M_3 = REF.$$

Define the two cubics:

$$C_1 = L_1 + L_2 + L_3,$$
$$C_2 = M_1 + M_2 + M_3.$$

We now have

$$C_1 \cap C_2 = \{A, B, C, D, E, F, P, Q, R\}.$$

Suppose P, Q, R collinear. Let $L = PQR$ and K be the unique conic passing through A, B, C, D, E (four points collinear would contradict the hexagon). Then $L + K$ is a cubic passing through A, B, C, D, E, P, Q, R, by the Cayley-Bacharach Theorem, it must pass through F as well. By our assumptions, $F \notin L$, so $F \in K$.

Conversely, suppose A, B, C, D, E, F conconic. Let $K = ABCDEF$ and L be the line through P, Q. Then $L + K$ is a cubic passing through A, B, C, D, E, F, P, Q, by the Cayley-Bacharach Theorem, it must pass through R as well. By our assumptions, $R \notin K$ (otherwise K is a line pair, which contradicts distinctness), so $R \in L$. □

7. Group Law on a Cubic

Recall that both of our examples of the nodal and cuspidal cubics had a singularity at $(0, 0)$. It turns out that there is a third type of cubic, called an elliptic curve. One of its defining characteristics is that it has no nonsingular points, so that our method of using projection will fail for elliptic curves. We will not prove this, but it is impossible to parametrize an elliptic curve.

Let $k \subseteq \mathbb{C}$ be a subfield. Suppose we have a cubic form $F \in k[X, Y, Z]$ that defines a curve $C \subseteq \mathbb{P}^2_k$, the set of all points where $F = 0$. Assume that

(1) F is irreducible.
(2) For every point P in C, there exists a unique line L such that L is a repeated zero of $F|_L$.

The first condition eliminates degenerate cases, and the second condition asks for a unique tangent line L.

Now we can begin constructing the group on the points of the cubic. First, we pick an arbitrary point O in C. We will define addition below.

(1) For any point $P \in C$, define $\overline{P}$ as the third point of intersection of the line OP and the cubic C.
(2) For any points $P, Q \in C$, define R as the third point of intersection of the line PQ and the cubic C, and define $P + Q = \overline{R}$.

Theorem 7.1. *This construction defines an abelian group law on C, with O as the identity.*

Proof. We have four parts.

(1) Addition is well-defined:
    If $P \neq Q$, then the line PQ is unique by properties of the projective plane. If $P = Q$, then we use the unique tangent line by (2). By Bezout's Theorem, we are guaranteed a unique third point of intersection in the

algebraic closure of k. However, since the two points have k-coordinates and the cubic has coefficients in k, the third point must also be a k-point.

(2) Identity:

We claim that O is the identity. For any point P, OP intersects C at $\overline{P}$. $O\overline{P}$ intersects C at P, so $O + P = P$. Similarly, $P + O = P$.

(3) Inverses:

Let A' be the intersection of $\overline{O}A$ and C. We claim that $A' = -A$. AA' intersects C at $\overline{O}$, and $O\overline{O}$ intersects C at O (substitute O=P in (1)).

(4) Commutativity:

This follows directly from the fact that there exists a unique line between any two distinct points (and that every element commutes with itself).

(5) Associativity

Let $A, B, C \in C$. Here, we are concerned with 'general points', that is, A, B, C, R, S, Q, T, etc. are all distinct.

We need to draw four lines to define $(A + B) + C = \overline{S}$.

$$L_1 = ABR, L_2 = RO\overline{R}, L_3 = \overline{R}CS, L_4 = SO\overline{S}.$$

We need four additional lines to define $A + (B + C) = \overline{T}$.

$$M_1 = BCQ, M_2 = QO\overline{Q}, M_3 = A\overline{Q}T, M_4 = TO\overline{T}.$$

We want to show that $\overline{S} = \overline{T}$. It is enough to show $S = T$. We will use the Cayley-Bacharach Theorem. Construct the following degenerate cubics:

$$D_1 = L_1 + M_2 + L_3, D_2 = M_1 + L_2 + M_3.$$

Counting intersection points gives us

$$C \cap D_1 = \{A, B, C, O, Q, \overline{Q}, R, \overline{R}, S\},$$
$$C \cap D_2 = \{A, B, C, O, Q, \overline{Q}, R, \overline{R}, T\}.$$

Assuming that $A, B, C, O, Q, \overline{Q}, R, \overline{R}, S$ are distinct, D_2 is a cubic passing through the first eight points of $C \cap D_1$, so it passes through S. This is only possible if $S = T$.

For points that are not general, we can extend the proof 'by continuity'. If $k \subseteq \mathbb{C}$, then what we would do is show that $A+B$ is a continuous function on A, B and that the set of A, B, C such that the nine points used in the construction of $(A+B)+C$ are, in some sense, dense. For details, see pages 35-36 in Reid's Undergraduate Algebraic Geometry [1].

□

Note that the conditions required for the group law do not mention singularities. In fact, we can modify the nodal and cuspidal cubics to allow a group law by removing the singularity.

For example, recall the cuspidal cubic $y^2 = x^3$, parametrized by $\lambda \mapsto (\lambda^2, \lambda^3)$. In the projective plane, $Y^2Z = X^3$ is parametrized by

$$[U : V] \mapsto' [(U/V)^2 : (U/V)^3 : 1]' = [U^2V : U^3 : V^3].$$

The preimage of the singularity $[0 : 0 : 1]$ is $[0 : 1]$. If we remove that point from the domain (the projective line), we get the affine line. It turns out that the group law on the modified cuspidal cubic is $(k, +)$.

Similarly, for the nodal cubic, $Y^2Z = X^3 + X^2Z$ is parametrized by

$$[U : V] \mapsto [V(U^2 - V^2 : U(U^2 - V^2 : V^3].$$

The preimage of the singularity $[0 : 0 : 1]$ is $[1 : 1]$ and $[-1 : 1]$. If we remove those two points from the domain, we get the affine line minus a point. It turns out that the group law on the modified cuspidal cubic is $(k^\times, \cdot)$.

8. Weierstrass Form

By projective transformations, all elliptic curves in $\mathbb{P}^2_k$ can be written in the form $Y^2 = X^3 + AXZ^2 + BZ^3$, where k is either $\mathbb{R}$ or $\mathbb{C}$. Where does this curve intersect the line at infinity L $(Z = 0)$? By substituting $Z = 0$, we get $X^3 = 0$, so $X = 0$. Therefore, it meets $Z = 0$ at the point $P = [0 : 1 : 0]$. Since this is a triple zero, by the uniqueness of the tangent line, L is the tangent line of P. Now let's construct the group law on C and choose $O = [0 : 1 : 0]$ as the identity.

Since P is a triple zero of $F|_L$, by Bezout's Theorem, it does not intersect C elsewhere. So we can think of the curve C as $P \cup C_0$ where C_0 is the affine curve $\{(x, y) : y^2 = x^3 + ax + b\}$.

The lines through O are L and the projective lines $X = \lambda Z$ (affinely, $x = \lambda$). These lines intersect C at $(\lambda, \pm\sqrt{\lambda^3 + a\lambda + b})$ and $[0 : 1 : 0]$. Therefore, for any point $P = (x, y)$, $\overline{P} = (x, -y)$.

We have the interesting property that $\overline{O} = O$ (We have $\overline{O} = -O$ in any group law, and $O = -O$ for any group). Since $-P$ is defined to be the third point of $\overline{O}P$ and C, this simplifies to $-P = \overline{P}$ (because $O = \overline{O}$).

From these three observations, we can conclude the following theorem.

Theorem 8.1. *Given a cubic C in the Weierstrass form, we can define an abelian group law on C with $O = [0 : 1 : 0]$ as the identity element, inverses are given by $(x, y) \mapsto (x, -y)$, and*

$$P + Q + R = O \iff P, Q, R \text{ collinear.}$$

9. Torsion Points

Since elliptic curves cannot be parametrized, we cannot determine the group that the group law forms as easily as we did for the modified nodal and cuspidal cubics. The theory of elliptic curves turns out to be a very interesting and deep subject. It has many applications in other fields of mathematics, such as number theory. In fact, elliptic curves were used in Andrew Wiles's proof of Fermat's Last Theorem. The remainder of the paper will be used as a basic introduction to analyzing elliptic curves.

All calculations will be done in Weierstrass form.

Definition 9.1. A *n-torsion point* is a point whose order divides n.

Before we get to the torsion points, we will do a quick exercise: finding the coordinates of $P+P$ given the coordinates of P. Define $x(P)$ to be the x-coordinate of a point P.

Let $y^2 = x^3 + ax + b$ be an elliptic curve, $P = (x_0, y_0)$. We want to find $x(P+P)$. Recall that if $P = (x, y)$, then $-P = (x, -y)$, so

$$x(2P) = x(-2P) = x(\overline{2P})$$

Therefore, we need to find the x-coordinate of the third point of intersection of the tangent line at P and C. Let L be the tangent line. The equation of L is

$$y - y_0 = \frac{3x_0^2 + a}{2y_0}(x - x_0)$$

After substitution,

$$\left(\frac{3x_0^2 + a}{2y_0}(x - x_0) + y_0\right)^2 = x^3 + ax + b$$

If the reader wishes to go through the simplification, then he should keep in mind that x_0 is a root of multiplicity 2. The reader should obtain

$$x(2P) = \frac{x_0^4 - 2ax_0 - 8bx_0 + a^2}{4x_0^3 + 4ax_0 + 4b}.$$

Note that this formula fails when x_0 is a root of $x^3 + ax + b$. In this case, it turns out that the tangent line is vertical.

9.1. **2-Torsion Points.** We want to solve

$$2P = O, \text{ where } P \neq O.$$

This is equivalent to $-P = P$. If $P = (x, y)$, then $-P = (x, -y)$. Therefore, a 2-torsion point must have $y = -y$, or $y = 0$. To find these types of points, we need to solve

$$x^3 + ax + b = 0.$$

Over $\mathbb{C}$, this equation will always have 3 roots. Suppose we are in $\mathbb{C}$, call the roots $\alpha_1, \alpha_2, \alpha_3$. The 2-torsion points form the following group:

$$\{O, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0)\}.$$

Since every element has order dividing 2, this group is $(\mathbb{Z}/2\mathbb{Z})^2$.

9.2. **3-Torsion Points.** We want to solve

$$3P = 0, \text{ where } P \neq O.$$

This is equivalent to $-P = 2P$. Let $P = (x_0, y_0)$. Recall the duplication formula

$$x(2P) = \frac{x_0^4 - 2ax_0^2 - 8bx_0 + a^2}{4x_0^3 + 4ax_0 + 4b}.$$

There is no need to worry about the denominator equalling zero. If $4x_0^3 + 4ax_0 + 4b = 0$, then x_0 is a 2-torsion point. To find 3-torsion points, we need to solve

$$3x_0^4 + 6ax_0^2 + 12bx_0 - a^2 = 0.$$

Over $\mathbb{C}$, this equation will always have 4 roots. It turns out that this is a separable polynomial, so all roots are distinct. Unlike the 2-torsion case, plugging these four roots will give 8 points on the curve. Last time, all roots gave the y-coordinate 0, but this time, all y-coordinates are nonzero (see note on denominator above), so we get a positive and a negative y-value for each x-value.

Including O, the 3-torsion points form a group of order 9. Since every element has order dividing 3 and it is commutative, this group is $(\mathbb{Z}/3\mathbb{Z})^2$.

9.3. **More on Torsion Points.** We can extend this process for n-torsion points. Note that if an elliptic curve is defined over k, that is, its coefficients are in k, then the n-torsion points are all in $\overline{k}$ because they are solutions to polynomials defined over k. Adjoining the coordinates of n-torsion points to k gives interesting field extensions. The Galois group acts on n-torsion points and gives a Galois representation $\mathrm{Gal}(\overline{k}/k) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Acknowledgments. I would like to thank Peter May for organizing the REU and for correcting mistakes, and my mentor Daniel Le for explaining essential concepts on algebraic geometry (sometimes multiple times), and for always promptly proofreading this paper. The help was definitely appreciated.

References

[1] Miles Reid. Undergraduate Algebraic Geometry Cambridge University Press 1988