MAT449
Algebraic Curves

by Brandon Papandrea

The following is based on lecture notes taken during the Winter 2026 offering of MAT449 - Algebraic Curves, at the University of Toronto. While there is no set textbook used, some recommended readings for the course include *Algebraic Curves* by Fulton, *Lectures on Riemann Surfaces* by Forston, *Equations over Finite Fields* by Schmidt. The notes are broken up in sections based on the week they were taught, and not necessarily broken up based on the textbook chapters. The intention is for these notes to be a polished version of my own lecture notes that allows me to revise and look over the material multiple times, and thus should not be considered a primary source for learning about this topic.

Contents

1

Week 1

Throughout this course, we will explore several different concepts that will, when combined, make up our theory of algebraic curves. Some of the concepts we will talk about will include:

- Projective Geometry
- Bézout's Theorem about intersections of curves in the plane.
- Riemann Surfaces, which are related to algebraic curves over $\mathbb{C}$. These will help motivate some ideas we will see much later on, such as differentials.
- Curves over finite fields, including elliptic curves, which are related to concepts in number theory.

1.1 A FIRST GLIMPSE AT PROJECTIVE GEOMETRY

1.1.1 THE PROJECTIVE PLANE IN 2 DIMENSIONS

Let $\mathbb{F}$ be any field. Then $\mathbb{F}^3$ is a 3D space. Notice that the 2D space $\mathbb{F}^2$ is contained within $\mathbb{F}^3$ as a slice of the 3D space. An explicit map may be constructed as

$$(x, y) \mapsto (x, y, 1)$$

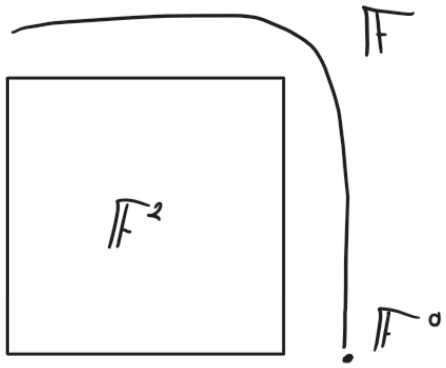
There is thus a projection of the 2D space into the 3D space.

Now, consider the set of all lines in $\mathbb{F}^3$ that pass through the origin. They all meet at the origin, and nowhere else. This means any point in $\mathbb{F}^3 \setminus \{0\}$ corresponds to a unique line in this space. If we scale this point, we stay on the line. Thus, if we quotient by the set of scalars, also known as $\mathbb{F}^*$, then we will get a set of points that correspond uniquely to a single line in the 3D space. This set,

$$(\mathbb{F}^3 \setminus \{0\})/\mathbb{F}^*$$

is known as the **Projective Plane**, and is denoted by $\mathbb{P}^2$. Going back to our $\mathbb{F}^2$ discussion, any $(x, y) \in \mathbb{F}^2$ can be thought of as the point $(x, y, 1) \in \mathbb{F}^3$. Taking the representative $[(x, y, 1)] \in \mathbb{P}^2$, we get that each point in $\mathbb{F}^2$ corresponds to a point in $\mathbb{P}^2$, and so $\mathbb{F}^2 \subset \mathbb{P}^2$. The set $\mathbb{P}^2 \setminus \mathbb{F}^2$ only contains the points of the form $[(x, y, 0)]$.

To visualize the projective plane, consider the below figure:



The square $\mathbb{F}^2$ is the **affine plane**, whilst the point $\mathbb{F}^0$ and the line $\mathbb{F}^1$ combine to become the **line at infinity**.

Let's use a finite field $\mathbb{F}_q$. The set $\mathbb{F}_q^3 \setminus \{0\}$ has $q^3 - 1$ points, while $\mathbb{F}_q^*$ has $q - 1$ points. Thus, the projective plane with repsect to $\mathbb{F}_q$ has

$$\frac{q^3 - 1}{q - 1} = q^2 + q + 1$$

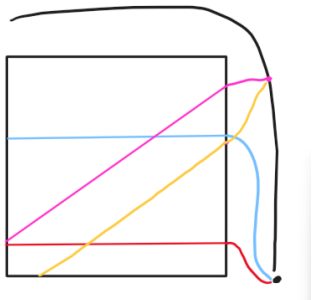
points. In particular, there are q^2 points of the form $(a, b, 1)$, q points of the form $(a, 1, 0)$, and 1 point of the form $(1, 0, 0)$.

The exponent should make clear that $\mathbb{P}^2$ is a 2D space. There is a nice correlation between the geometry in the projective plane and that of the underlying field. By construction, any point in $\mathbb{P}^2$ is a line in $\mathbb{F}^3$ passing through the origin. Similarly, any line in $\mathbb{P}^2$ is a plane in $\mathbb{F}^3$ that passes through the origin. For example, consider the plane $ax + by + cz = 0$ in $\mathbb{F}^3$. This corresponds to the line (a, b, c) in $\mathbb{P}^2$. The set of all lines in $\mathbb{P}^2$ is given by the set

$$(\mathbb{F}^3) \setminus \{0\}/\text{scaling}$$

This idea that connects lines and points is known as **line-point duality**, and is very important.

One thing to note about the projective plane is that every line, even parallel ones, intersect at some point. For lines that do not intersect in the affine plane, they intersect at the point on the line at infinity corresponding to their direction on the affine plane. This is shown below:



Another way to see the connection between lines and points is through a graph. Consider two sets of vertices, one for points in $\mathbb{P}^2$, and one for lines in the same space, where the underlying field is $\mathbb{F}_q$. An edge connects any point to any line that the point lies on. There are q^2+q+1 vertices in each set, and each vertex has degree $q-1$. This graph is bipartite, and is the largest bipartite graph with this number edges that does not contain a $K_{2,2}$ subgraph. This is because two lines cannot intersect at two distinct points.

1.1.2 THE PROJECTIVE PLANE IN N DIMENSIONS

We can generalize what we just did to n dimensions to get $\mathbb{P}^n$, which is defined to be

$$\mathbb{P}^n = (\mathbb{F}^{n+1} \setminus \{0\})/\mathbb{F}^*$$

Over a finite field $\mathbb{F}_q$, we get that

$$|\mathbb{P}^n| = q^n + q^{n-1} + \cdots + 1$$

where each q^k is a copy of $\mathbb{F}_q^k$. Instead of lines, we are now considering **hyperplanes**, which are codimension 1 subspaces of $\mathbb{F}^{n+1}$, that pass through the origin. Similar to before, a point in $\mathbb{P}^n$ corresponds to a hyperplane in $\mathbb{F}^{n+1}$, given by an equation

$$a_0x_0 + \cdots a_nx_n = 0$$

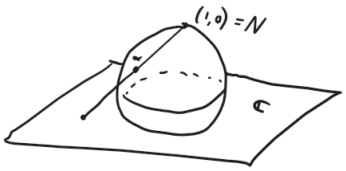
The space of all hyperplanes is also a $\mathbb{P}^n$. This gives us **hyperplane-point duality**.

1.1.3 THE RIEMANN SPHERE

There are some operations that allow us to take equations in the affine plane and convert them into equations in the projective space. Let's consider $\mathbb{P}^1$, where the underlying field is $\mathbb{C}$. This is the set of pairs $(a,b) \in \mathbb{C}^2 \setminus \{0\}$, modulo scaling. One can think of this space as the set

$$\mathbb{P}^1 = (\mathbb{C} \times \{1\}) \cup (1,0) \cong \mathbb{C} \cup \{\infty\}$$

This can be thought of as the complex numbers, with a single point, the point at infinity, lying above it. If we fold $\mathbb{C}$ onto this point at infinity, we get a sphere, called the **Riemann Sphere**:



To go from one to the other, we use **stereographic projection**. If we define the point at inifnity as the north pole N, we get a map which sends $S^2 \setminus N \to \mathbb{C}$, and $N \to (1,0)$.

1.2 ALGEBRAIC SETS

We now begin introducing some relevant concepts in algebraic geometry. We let $\mathbb{F}$ be an algebraically closed field, and consider $\mathbb{F}[x_1, \ldots, x_n]$, the field of polynomials in n variables with coefficients in $\mathbb{F}$.

We say that $S \subseteq \mathbb{F}^n$ is an **algebraic set** if there exists a set $U \subseteq \mathbb{F}[x_1, \ldots, x_n]$ such that we can write

$$S = \{x \in \mathbb{F}^n : f(x) = 0 \quad \forall f \in U\}$$

meaning S vanishes for every polynomial in U.

We should note some important facts:

1. The algebraic sets in $\mathbb{C}$ are $\mathbb{C}$, and all finite subsets.
2. Every finite subset of $\mathbb{C}^n$ is algebraic: For a point $(\alpha_1, \ldots, \alpha_n)$, take $U = \{x_1 - \alpha_1, \ldots, x_n - \alpha_n\}$.

Now, we want to pick U so that it is as large as possible. For an algebraic set S, the **ideal** of S is the set $I(S)$ of all polynomials that are equal to 0 on S. Recall by the Hilbert Basis Theorem that $\mathbb{F}[x_1, \ldots, x_n]$ is Noetherian, and thus $I(S)$ is always finitely generated. This means that there are polynomials $p_1, \ldots, p_k$ for which

$$I(S) = \{\sum_i A_i p_i : A_i \in \mathbb{F}[x_1, \ldots, x_n]\}$$

We can also go in the other direction. For any ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$, we can define the **vanishing set** $V(I)$ to be the set

$$\{x \in \mathbb{F}^n : P(x) = 0 \quad \forall P \in I\}$$

which is all values that map to 0 for every polynomial in I. This gives a nice duality: If S is algebraic, then $V(I(S)) = S$, and for an ideal J,

$$I(V(J)) = \sqrt{J} = \{P(x_1, \ldots, x_n) : P^m \in J \text{ for some } m\}$$

This idea that $I(V(J)) = \sqrt{J}$ is refered to as **Hilbert's Nullstellensatz**, or Hilbert's theorem of zeroes. It allows us to translate a problem about algebraic curves or surfaces into a question about algebra.

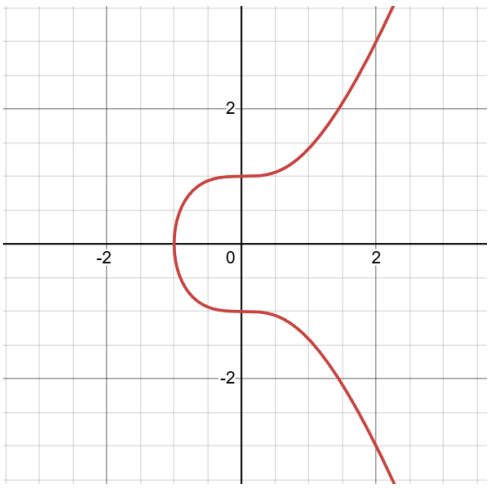
Given an algebraic set S, we can also form the ring

$$\mathbb{F}[x_1, \ldots, x_n]/I(S)$$

called the **coordinate ring of** S.

Let's consider an example to see everything in action. In $\mathbb{C}^2$, consider the curve

$$y^2 = x^3 + 1$$



which is the polynomial $y^2 - x^3 + 1$. We take $S = V(y^2 - x^3 - 1)$. The set

$$\{Q(x,y)\big|_S\} = \{f(x) + yg(x) : f, g \in \mathbb{C}[x]\}$$

is the coordinate ring of S with operations modulo $y^2 - x^3 + 1$, since all polynomials will be linear in y.

Notice that, in a small enough neighbourhood of $x = 0$, we can write $y = \sqrt{x^3 + 1}$, which equals the power series

$$1 + \frac{x^3}{2} + \cdots$$

or the negative of that power series. This corresponds to the fact that there are two points at which the line $x = 0$ and our curve intersect. To see this more explictely, we can notice that

$$\begin{aligned}\mathbb{C}[x,y]/(y^2 - x^3 - 1, x) &= \mathbb{C}[x,y]/(y^2 - 1) \\ &= \mathbb{C}[x,y]/(y-1) \oplus \mathbb{C}[x,y]/(y+1) \\ &\cong \mathbb{C}^2\end{aligned}$$

and because it is 2D, we get 2 solutions.

Note that this is not always something we can do. For example, near $x = 0$, the curve $y^2 = x^3 + x^2$ looks like the curve $y^2 = x^2$, which is a cross, giving us a singularity.

1.3 THE HILBERT BASIS THEOREM

The Hilbert Basis Theorem is a very important result in algebraic geometry.

Theorem 1.1 (Hilbert Basis Theorem)**.** *Given an algebraically closed field $\mathbb{F}$, $\mathbb{F}[x_1, \ldots, x_n]$ is Noetherian. In particular*

(i) All ideals in this ring are finitely generated.

(ii) Given an ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$, thre is a j_0 such that $I_j = I$ for all $j \geq j_0$.

Proving this amounts to proving the following lemma, as $\mathbb{F}$ is Noetherian:

Lemma 1.2. *If R is Noetherian, so too is $R[x]$.*

Proof. Let I be an ideal in $R[x]$, and let J be the set of leading coefficients of members of I. This is an ideal of R, so it is finitely generated by the leading coefficients of some finite number of polynomials in I, say

$$f_1, \ldots, f_n$$

Let d be the maximum degree of these n polynomials, and let J_k be the set of leading coefficients of members of I whose degree is at most k. Again, this is an ideal of R, so it too is finitely generated by some finite number of polynomials in I, say

$$f_1^{(k)}, \ldots, f_{n^{(k)}}^{(k)}$$

Now let I^* be the ideal of $R[x]$ genearted by all these polynomials: the set

$$\{f_i, f_j^{(k)} : i < n, j < n^{(k)}, k < d\}$$

Clearly $I^* \subseteq I$. We claim the reverse is true as well.

Suppose not. Then let $g \in I \setminus I^*$ be of minimal degree, with leading coefficient a. We have two cases:

1. Suppose that the degree of h is at least d. We know that $a \in J$, so we mau write it as linear combination of coefficients of f_i:

   $$a = \sum_i u_i a_i$$

   Now let

   $$h_0 = \sum_i u_i x^{(\deg(h) - \deg(f_i))} f_i$$

   This has the same leading term as h. Moreover, $h_0 \in I^*$, while h is not. So

   $$h - h_0 \in I \setminus I^*$$

   but the degree of $h - h_0$ is smaller than h, a contradiction.

2. Suppose that the degree of h is $k < d$. Then $a \in J_k$, and we can write

   $$a = \sum_i u_i a_i^{(k)}$$

   Then setting

   $$h_0 = \sum_i u_i x^{\deg(h) - \deg(f_i^{(k)})} f_i^{(k)}$$

   we get a similar contradiction.

Thus, $I = I^*$, so I is finitely generated, as desired. □

1.4 HILBERT'S NULLSTELLENSATZ

The result that, for an ideal J of $\mathbb{F}[x_1, \ldots, x_n]$ with $\mathcal{F}$ algebraically closed, $I(V(J)) = \sqrt{J}$, is an important result referred to as the **Nullstellensatz**, or "theorem of zeroes." To prove it, we are going to need to first prove a weaker result, and use that to prove the full claim.

1.4.1 THE WEAK NULLSTELLENSATZ

Theorem 1.3 (Weak Nullstellensatz)**.** *Suppose that we have some collection of polynomials $\mathbb{F}[x_1, \ldots, x_n]$, $P_1, \ldots, P_k$, that have no common zeroes in $\mathbb{F}^n$. Then there exists polynomials $A_1, \ldots, A_k$ such that*

$$\sum_i A_i P_i = 1$$

Another way of framing this theorem is as follows: Every maximal ideal of $\mathbb{F}[x_1, \ldots, x_n]$ is of the form $I_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ for some $a = (a_1, \ldots, a_n) \in \mathbb{F}^n$.

Proof. Let I be a maximal ideal of $\mathbb{F}[x_1, \ldots, x_n]$. Zariski's Lemma implies that $\mathbb{F}[x_1, \ldots, x_m]/I$ is a finite field extension of $\mathbb{F}$, and so by algebraic closure, it must be $\mathbb{F}$. It then follows that there is an $a = (a_1, \ldots, a_n) \in \mathbb{F}^n$ such that $x_i - a_i \in I$ for $i = 1, \ldots, n$. Writing

$$I_a = (x_1 - a_1, \ldots, x_n - a_n)$$

we get that $I \supset I_a$. I_a is also maximal, and so we conclude that $I = I_a$, as desired. □

Proof of Nullstellensatz. We use a proof called the Rabinowitsch trick.

Supposet that $f \in \mathbb{F}[x_1, \ldots, x_n]$ vanishes whenever all polynomials $f_1, \ldots, f_m$ vanish. It follows that, after introducing a new term x_0, the polynomials

$$f_1, \ldots, f_m, 1 - x_0 f$$

have no common zeroes. Weak Nullstellensatz then applies, and so there are polynomials $g_0, \ldots, g_m \in \mathbb{F}[x_0, \ldots, x_n]$ such that

$$1 = g_0(1 - x_0 f) + \sum_{i=1}^{m} g_i f_i$$

We can replace x_0 with the expression $1/f$, giving us

$$1 = \sum_{i=1}^{m} g_i(1/f(x_1, \ldots, x_n), x_1, \ldots, x_n) f_i(x_1, \ldots, x_n)$$

as an element of the field of fractions of $\mathbb{F}[x_1, \ldots, x_n]$. Notice that the only expresions in the denominators of the right hand side are f and powers of f, so for some r and polynomials $h_1, \ldots, h_m \in \mathbb{F}[x_1, \ldots, x_n]$,

$$1 = \frac{\sum_{i=1}^{m} h_i f_i}{f^r}$$

Thus,

$$f^r = \sum_{i=1}^{m} h_i f_i$$

so $f^r \in \langle f_1, \ldots, f_m \rangle$, as required. □