Algebraic Geometry

Zandi

November 4, 2013

THIS IS A DRAFT. Expect inaccuracte and incomplete information.

Introduction

Algebraic Geometry is a field of mathematics with roots as far back as at least the 19^{th} century, and with major advancement and applications in recent years. At its core, Algebraic Geometry is concerned with studying the sets of zeroes of a system of polynomials, in particular their algebraic structure. Though real polynomials are surely the first that come to mind, much of the power in Algebraic Geometry comes from the generalization to polynomials with coefficients in arbitrary fields.

The undergraduate mathematics student would hopefully find this paper accessible, but experience with algebra and geometry would help. A "Basics" section is included, but will not be exhaustive. As unhelpful as it seems, it's recommended to do independent research as necessary using Wikipedia, YouTube (videotaped lectures) and the referenced textbooks.

This paper draws heavily from "Undergraduate Algebraic Geometry" by Miles Reid, with the primary addition being annotated proofs. Where Reid's proofs left details to the reader, these details are mostly provided, although the proofs remain the same.

1 Basics

Here's where I'll put all the theorems and definitions that are simply necessary. I'll definitely talk about projective space here, and homogenous equations.

Definition 1.1. *Given a Field k, the* Projective Space of Degree n over k*, denoted* $\mathbb{P}^n_k$ *is the quotient* $(k^{n+1} \setminus \{\mathbf{0}\})/\sim$*, where* $\sim$ *is the equivalence relation defined as*

$$(x_0, ..., x_n) \sim (y_0, ..., y_n) \text{ if } \exists \lambda \in k \text{ s.t. } \lambda \neq 0, (x_0, ..., x_n) = (\lambda y_0, ..., \lambda y_n)$$

Given this, points in projective space are often denoted $P = [x_0 : ... : x_n]$*, with the colons and brackets indicating this is an equivalence class. So then,* $[y_0 : ... : y_n] = P = [x_0 : ... : x_n]$ *if* $(y_0, ..., y_n) \sim (x_0, ..., x_n)$.

The definition is abstract to purposely highlight the fact that, given a field k we can create a projective space. Effectively, the projective space is the set of all lines in k^n through the origin. This is also why the projective space has one fewer dimension than its corresponding vector space.

So, the "points" in projective space are lines in the corresponding vector space. Another interesting feature of projective space is that parallel lines intersect at a "point at infinity". This can be thought of as making partitions of lines in the projective space pased on parallelism, as if we were defining an equivalence relation. Now, each equivalence class is assigned a unique "point at infinity" that each line in the equivalence class intersects. Thus, if two lines are parallel, they intersect at some point at infinity. Likewise, if two lines aren't parallel, they'll have their own points at infinity, but they won't be the same, thus they will only have the usual intersection normally expected of non-parallel lines.

This may seem very strange, but can be illustrated with a stereographic projection. Suppose we're in $\mathbb{R}^3$, and picture two things: the plane $z = 1$ and a sphere of radius 1 centered at the origin. Now, we can map any point p on $z = 1$ to a unique point on the upper hemisphere of our sphere; simply note that the line passing through p and the origin $(0, 0, 0)$ intersects the specified hemisphere precisely once at some point q. Knowing this, we can see that lines on our plane $z = 1$ are mapped to great circles on our sphere. In the case of two parallel lines, they will never intersect in $z = 1$, but the great circles they're mapped to will intersect on the equator of the hemisphere.

Definition 1.2. *A function $f(x)$ is* Homogenous of Degree n *if, for some constant λ, we have $f(\lambda x) = \lambda^n f(x)$. If f is a homogenous polynomial of degree n, it is known as a* form of degree n.

Homogenous functions are particularly useful when considering their sets of zeroes in projective space. If f is homogenous of degree n, and some point $x = (x_0, ..., x_n)$ is a zero of f, then $f(\lambda x) = \lambda^n f(x) = \lambda^n 0 = 0$. Thus, we can say that, if f is homogenous, then we can indeed have zeroes of f in $\mathbb{P}^n_k$, assuming k is algebraically closed.

2 Conic Sections

Use conic sections to illustrate some basics here and provide necessary theorems/tools for elliptic curve section. Will draw heavily from the book

3 Bezout's Theorem

Bezout's theorem will be important later, but we probably won't be able to fully prove it here. However, the book does prove the limited cases that we'll most rely on.

Theorem 3.1. Bezout's Theorem*:*

If C and D are plane curves of degree m and n (respectively) then $C \cap D$ contains precisely mn points, provided:

$$\text{The field we're working over is algebraically closed} \tag{i}$$
$$\text{Points of intersection are counted with multiplicity} \tag{ii}$$
$$\text{We work in } \mathbb{P}^2_k \text{ to account for points at infinity} \tag{iii}$$

Instead of proving the general theorem, we'll only cover a special case of particular importance to us; intersections involving lines and conics.

Theorem 3.2. *Let $L \subset \mathbb{P}^2_k$ be a line (respectively, $C \subset \mathbb{P}^2_K$ a non-degenerate conic) and $D \subset \mathbb{P}^2_k$ a curve defined by $D : (G_d(X, Y, Z) = 0)$ where G is a form of degree d in the 3 variables X, Y, Z. Also, assume that $L \not\subset D$ (resp. $C \not\subset D$). Then*

$$|L \cap D| \leq d$$

and respectively

$$|C \cap D| \leq 2d$$

And in fact, once accounting for multiplicity, points at infinity, and if k is algebraically closed, we have equality.

4 Elliptic Curves

One of the more interesting sections. Definitely need to cover proving the given construction on the non-singuler elliptic curve creates a group. Should also cover how in practice for crypto the identity is chosen as the point at infinity, allowing for much cheaper computation.

Current strategy is to develop this section, then determine dependencies for understanding, and stuff those in the earlier sections.

Definition 4.1. Group Law on a Plane Cubic: *Suppose $k \subset \mathbb{C}$ is a subfield of $\mathbb{C}$, and $F \in k[X, Y, Z]$ is a cubic form defining a non-empty plane curve $\mathfrak{C} : (F = 0) \subset \mathbb{P}^2_k$. Additionally, assume that F satisfies the following:*

$$F \text{ is irreducible, so } \mathfrak{C} \text{ won't contain a line or conic} \tag{a}$$
$$\forall P \in \mathfrak{C},\ \exists! \text{ line } L \subset \mathbb{P}^2_k \text{ s.t. } P \text{ is a repeated zero of } F|_L \tag{b}$$

Now, fix any point $O \in \mathfrak{C}$ and make the following construction:

for $A \in \mathfrak{C}$, let $\bar{A}$ be the third point of intersection of $\mathfrak{C}$ with $\overleftrightarrow{OA}$ (i)

for $A, B \in \mathfrak{C}$ let R be the third point of intersection of $\mathfrak{C}$ with $\overleftrightarrow{AB}$ and define $A + B = \bar{R}$ (ii)

Geometrically, the uniqueness in (b) says that $\mathfrak{C}$ should be non-singular, and we can see that this line L is in fact the tangent line to $\mathfrak{C}$ at P. Likewise, (a) prevents somewhat degenerate cases.

As you may have noticed, we've defined an operation on points of this cubic curve $\mathfrak{C}$, so naturally we're curious what sort of structure then arises. It turns out that this actually defines an Abelian Group on $\mathfrak{C}$, as we will now prove.

Theorem 4.1. *The above construction (Definition 4.1) defines an Abelian Group $(\mathfrak{C}, +)$ with O as the identity element.*

Proof. Well, to prove this is an abelian group, we have a few conditions we must satisfy:

1. Well-definedness of the operation and inverses
2. Existence of an identity element
3. Existence of unique inverses
4. Commutativity
5. Associativity

Well-Definedness:
Let $P, Q \in \mathfrak{C}$. Then, we have two simple cases:

case 1: $P \neq Q$. Then $\exists! L \subset \mathbb{P}_k^2$ such that $L = \overleftrightarrow{PQ}$.

case 2: $P = Q$. Then, part (b) of the definition gives that $\exists! L \subset \mathbb{P}_k^2$ such that P is a repeated root of $F|_L$.

Note, however, that in both cases $F|_L$ is a cubic form in 2 variables. So, as $F|_L$ is a 3rd degree form, it has precisely 3 roots, 2 of which are the k-valued points P and Q. Well, $P \in \mathbb{P}_k^2$, $Q \in \mathbb{P}_k^2$, so $F|_L$ is the product of 3 linear terms from $k[X, Y, Z]$. Thus, the third root of $F|_L$ is certainly defined, and must also be from $\mathbb{P}_k^2$, and of course from $\mathfrak{C}$.

So, given any two points on $\mathfrak{C}$, the line they determine intersects $\mathfrak{C}$ at some third point. Thus our construction, which relies on such a third point existing, is well defined. That is, Given any $A \in \mathfrak{C}$, $\bar{A}$ is a unique element of $\mathfrak{C}$, and given any $A, B \in \mathfrak{C}$, $A + B$ is a unique point of $\mathfrak{C}$.

Commutativity:
Well, need to show that $A+B=B+A$. Miles Reid chooses to "leave this to the reader", and likewise we won't elaborate on this. Simply note that $\overleftrightarrow{AB}=\overleftrightarrow{BA}$, so they share the same 3rd point of intersection with $\mathfrak{C}$.

Identity:
Let $A\in\mathfrak{C}$ be some arbitrary point of $\mathfrak{C}$, and consider $O+A$. Well, by our construction, we first find the third point of intersection of $\overleftrightarrow{OA}$ with $\mathfrak{C}$, which by (i) is $\bar{A}$. From here, to find $O+A$ we must now find the third point of intersection of $\overleftrightarrow{O\bar{A}}$ with $\mathfrak{C}$. However, note that $O,\ A,\ \bar{A}$ are all collinear. Thus, this third point of intersection of $\overleftrightarrow{O\bar{A}}$ with $\mathfrak{C}$ is A. Hence, $O+A=A,\ \forall A\in\mathfrak{C}$.

Inverses:
Let L be the line tanget to $\mathfrak{C}$ at O. That is, L is the unique line s.t. $F|_L$ has O as a repeated zero. Now, let $\bar{O}$ be the 3rd root of $F|_L$. Now, given any point $A\in\mathfrak{C}$, we can see that the third point of intersection of $\overleftrightarrow{A\bar{O}}$ with $\mathfrak{C}$ is the inverse of A.

Call this third point of intersection A'. Now, consider $A+A'$. By definition, $A,\ A',\ \bar{O}$ are all collinear, so the third point of intersection of $\overleftrightarrow{AA'}$ with $\mathfrak{C}$ is $\bar{O}$. Now, by how we defined $\bar{O}$, we know that the third point of intersection of $\mathfrak{C}$ with $\overleftrightarrow{O\bar{O}}$ is O, as O is a repeated root of this line. Thus, $A+A'=O$, so in the future we'll refer to such an A' as A^{-1}.

Finally, note that as A^{-1} was picked as the third point of intersection of $\mathfrak{C}$ with $\overleftrightarrow{A\bar{O}}$, it is well-defined.

Associativity:
Associativity is by far the most difficult part of this proof. We'll first prove Associativity for one case, and then reduce the general case to this special case.

Suppose that $A,B,C\in\mathfrak{C}$. We want to show that $(A+B)+C=A+(B+C)$. Well, in the construction of $(A+B)+C$ we use the 4 lines

$$L_1:\overleftrightarrow{AB\bar{R}},\ L_2:\overleftrightarrow{RO\bar{R}},\ L_3:\overleftrightarrow{C\bar{R}S},\ L_4:\overleftrightarrow{S\bar{O}S}$$

Likewise, the construction of $A+(B+C)$ involves

$$M_1:\overleftrightarrow{B\bar{C}Q},\ M_2:\overleftrightarrow{Q\bar{O}Q},\ M_3:\overleftrightarrow{A\bar{Q}S'},\ M_4:\overleftrightarrow{S'\bar{O}S'}$$

Clearly, $(A+B)+C=A+(B+C)\iff\bar{S}=\bar{S}'\iff S=S'$. We'll prove $S=S'$ by inspecting the two cubics

$$D_1=L_1+M_2+L_3 \text{ and } D_2=M_1+L_2+M_3$$

TODO: *clearly* define what this "+" operation on curves is. are we taking the product of their defining polynomials? I suspect so, but this definition raises

other concerns on the applicability of other theorems, such as "if two cubics intersect 8 of 9 common points they both intersect the 9th". study this later...

Thus, by construction we have

$$\mathfrak{C} \cap D_1 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$$

and

$$\mathfrak{C} \cap D_2 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S'\}$$

Now, assuming all 9 points of $\mathfrak{C} \cap D_1$ are distinct, then $\mathfrak{C}$ and D_1 satisfy the conditions of proposition 2.7 (TODO: add prop. 2.7 from book to earlier sections), so D_2 must pass through the 9th point S, which is only possible if $S' = S$. Hence, $\bar{S} = \bar{S}'$ and, so long as our construction involves 9 distinct points, $+$ is Associative.

Now, to extend to the more general case of points $A, B, C \in \mathfrak{C}$ which don't necessarily involve only distinct points in the construction of $(A + B) + C$ or $A + (B + C)$. We'll make use of some concepts from calculus here.

First, some useful lemmas:

Lemma 4.1. *$+$ is a continuous function. Thus, as the composition of continuous functions, both*

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

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

are continuous

Lemma 4.2. *$\forall A, B, C \in \mathfrak{C}, \exists A', B', C' \in \mathfrak{C}$ arbitrarily near A, B, C such that the 9 points $\{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$ are distinct.*

Specifically, there exist sequences $(A_n), (B_n), (C_n)$ s.t.

$$A_n \to A,\ B_n \to B,\ C_n \to C \text{ as } n \to \infty.$$

Thus, $\forall n \in \mathbb{N}$ the previous limited proof of associativity gives that

$$(A_n + B_n) + C_n = A_n + (B_n + C_n) \qquad (*)$$

Now, by the continuity in Lemma 4.1, we have the following limits using the sequences from Lemma 4.2:

$$\lim_{n\to\infty} (A_n + B_n) + C_n = (A + B) + C$$

$$\lim_{n\to\infty} A_n + (B_n + C_n) = A + (B + C)$$

But, by the above noted equality (*) gained from Lemma 4.2, we know that

$$\lim_{n\to\infty} (A_n + B_n) + C_n = \lim_{n\to\infty} A_n + (B_n + C_n)$$

Thus, by uniqueness of limits

$$(A + B) + C = A + (B + C)$$

More specifically, we can see from Lemma 4.2 that the set of such points (A, B, C) where the 9 involved points of the construction are distinct is in fact dense in $\mathfrak{C} \times \mathfrak{C} \times \mathfrak{C}$. Thus, as the two functions from Lemma 4.1 agree on this dense set, they agree everywhere on $\mathfrak{C} \times \mathfrak{C} \times \mathfrak{C}$, giving us Associativity $\forall A, B, C \in \mathfrak{C}$.

Therefore, $(\mathfrak{C}, +)$ is an Abelian Group. □

It should be noted that the fact the curve is cubic is quite important. This allows us to have precisely 3 points of intersection when intersecting our curve with a line, letting us define a relatively natural operation based on this. On the contrary, a quartic curve would have 4 points of intersection with a line, and an increasing number of points if we were to consider intersections with conics and cubics, so it's even less clear how we would define an operation here to get a group. Likewise, intersections of a line with another line are so trivial it's hard to imagine such an interesting structure arising.

Also note curves of the form $y^2 = x^3 + ax + b$ fulfill the requirements of our theorem, and are symmetric about the x-axis. In practice, the identity O is taken to be the ideal point at infinity (since we are really in $\mathbb{P}^2_k \subset \mathbb{P}^2_{\mathbb{C}}$), allowing for all vertical lines to intersect O. As our curve tends towards infinity, it also intersects O, so everything is still well-defined. The benefit of this approach is that calculating inverses is trivial: $A = (x, y) \implies A^{-1} = (x, -y)$. Once we pair this with a field k with desirable number-theoretic properties, we enter the realm of cryptography using elliptic curves, and travel far outside the scope of this short paper.

5 Regular Polyhedra??

If we even get here, this should be a neat topic to talk about for a bit to offset the earlier material.