Algebraic Geometry

Zandi

October 27, 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.

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* $\mathbb{P}_k^n$ *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 vector space k^n 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.

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.

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.

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.