LECTURE 4, WEDNESDAY 18.02.04

FRANZ LEMMERMEYER

Today I will talk about affine and projective curves. Both will be important: the group law on conics works in the affine plane only, whereas for elliptic curves we need the projective plane to get a group law. In fancy language, conics are affine algebraic groups, and elliptic curves are projective algebraic groups, that is, examples of abelian varieties.

1. The Projective Plane

Let K be a field; define a relation $\sim$ on the set $K^{n+1} \setminus \{(0,\dots,0)\}$ by

$$(a_0, a_1, \dots, a_n) \sim (b_0, b_1, \dots b_n)$$

for $a_i, b_i \in K$ if there exists a $\lambda \in K^\times$ such that $b_i = \lambda a_i$ for $i = 0, 1, \dots, n$. This relation is easily seen to be an equivalence relation; denote the equivalence class of $(a_0, \dots, a_n)$ by $[a_0 : \cdots : a_n]$. The set of all equivalence classes is called the n-dimensional projective space over K and will be denoted by $\mathbb{P}^n K$.

In the following, we will mainly talk about the projective plane $\mathbb{P}^2 K$, but everything we say can easily be generalized. First let me explain why $\mathbb{P}^2 K$ is called a plane although its points are described by 3 coordinates. The reason is that the projective plane differs from the affine plane $\mathbb{A}^2 K = K \times K$ essentially by a line, therefore should have the same dimension. In fact, consider the map

$$\iota : \mathbb{A}^2 K \longrightarrow \mathbb{P}^2 K; (a, b) \longmapsto [a : b : 1].$$

It is easily seen to be injective, and the only points in the projective plane it misses are those whose third coordinate is 0, that is, the "line" $\{[x : 1 : 0]; x \in K\}$ and the point $[1 : 0 : 0]$.

2. Projective Closure of Lines

Using the embedding $\mathbb{A}^2 K \longrightarrow \mathbb{P}^2 K$ we can, of course, also embed algebraic curves. Consider the simplest example, that of a line $L : ax + by + c = 0$. Any point $P = (x, y)$ on L will get mapped to $\iota(P) = [x : y : 1] \in \mathbb{P}^1 K$. This point has different presentations; we can write it as $\iota(P) = [\lambda x : \lambda y : \lambda]$ for any $\lambda \in K^\times$. These coordinates all satisfy the equation $aX + bY + cZ = 0$: in fact,

$$a(\lambda x) + b(\lambda y) + c(\lambda) = \lambda(ax + by + c) = 0.$$

We call the set of all points $[X : Y : Z]$ in the projective plane satisfying $aX + bY + cZ = 0$ the projective closure of the line L and denote it by $L^\#$. The zero set of any equation $aX + bY + cZ = 0$ with $(a, b, c) \neq (0, 0, 0)$ is called a projective line.

Let us now investigate what the points at infinity on this line $L^\#$ are; all we have to do is put $Z = 0$ in the equation of the projective line: we get $ax + by = 0$. We cannot have $a = b = 0$, since $ax + by + c = 0$ was supposed to be a line. Now $ax + by = 0$ has the general solution $(x, y) = (\lambda b, -\lambda a)$ for $\lambda \in K$. Thus the only point at infinity on $L^\#$ is the point $[b : -a : 0]$.

Proposition 1. *The projective closure of an affine line has exactly one point at infinity.*

The "line" $\{[x:1:0]; x \in K\}$ that we were talking about before is a projective line: it is described as the set of projective solutions of $z = 0$ and is called the line at infinity. We have just seen that every affine line $L : ax+by+c = 0$ intersects the line at infinity in exactly one point $[b : -a : 0]$. Note that, if $b \neq 0$, then $m = -a/b$ is the slope of the line L, and $[1 : m : 0]$ is its point at infinity. Thus every affine line with slope m intersects the line at infinity at $[1 : m : 0]$. In particular, every pair of parallel lines has a point of intersection at infinity, and we have

Proposition 2. *Two distinct projective lines have exactly one point of intersection.*

This is of course the most special case of Bezout's theorem that you can imagine.

The notion of projective closure makes sense for arbitrary affine curves $\mathcal{C}$ given by $f(x, y) = 0$ for some $f \in K[x, y]$; the image of a point $P = (x, y) \in \mathcal{C}(K)$ in the projective plane, namely $\iota(P) = [x : y : 1]$, satisfies the equation $F(X, Y, Z) = 0$, where F is the homogenization of f defined by $F(X, Y, Z) = Z^{\deg f} f(\frac{X}{Z}, \frac{Y}{Z})$. Note that the degree of $x^a y^b$ is $a + b$.

3. Projective Closure of Conics

The projective closure of affine curves of degree > 1 might have more than one point at infinty. Consider the three types of conics over $K = \mathbb{R}$:

(1) the ellipse $x^2 + y^2 = 1$;
(2) the parabola $y^2 = x$;
(3) the hyperbola $x^2 - y^2 = 1$.

The projective closure of the circle is the zero set of $X^2+Y^2-Z^2 = 0$, its points at infinity satisfy $Z = 0$ and $X^2 + Y^2 = 0$; since $[0 : 0 : 0]$ is not part of $\mathbb{P}^2K$, the real circle does not have any points at infinity.

The points at infinity of the projective closure $\mathcal{C}^\# : YZ-X^2 = 0$ of the parabola satisfy $Z = 0$ and $X = 0$; there is only one such point, namely $[0 : 1 : 0]$, and this point is indeed a point at infinity on $\mathcal{C}^\#$.

Finally, the hyperbola has two points at infinity, namely $[1 : 1 : 0]$ and $[1 : -1 : 0]$. Note that these points coincide with the points at infinity of the lines $y = x$ and $y = -x$: these are exactly the asymptotes of the hyperbolas, and the asymptotes intersect the hyperbola at infinity.

We can use these facts to *define* that an affine conic defined over a finite field is an ellipse, a parabola or a hyperbola according as it has no, one, or two points at infinity.

4. Projective Closure of Weierstrass Cubics

Now consider a Weierstrass cubic

$$E : y^2 + a_1y + a_3xy = x^3 + a_2x^2 + a_4x + a_6.$$

The homogenization of the defining equation is

$$E^\# : Y^2Z + a_1YZ^2 + a_3XYZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Putting $Z = 0$ gives $X^3 = 0$, hence the only point at infinity on $E^\#$ is $[0 : 1 : 0]$. Thus every Weierstrass curve has a single point at infinity, and this point is K-rational (has coordinates in K) for any field K.