LECTURE 3
MATH 256A

LECTURES BY: PROFESSOR MARK HAIMAN
NOTES BY: JACKSON VAN DYKE

1. Projective space

The general definition of an n-dimensional projective space $\mathbb{P}^n$ is the collection of lines through 0 in k^{n+1}. For example, $\mathbb{P}^1$ consists of the lines through the origin in the plane, so this is clearly somehow one dimensional, since it is determined by the slope. Then $\mathbb{P}^2$ consists of the lines through the origin in k^3, which is somehow 2-dimensional.

Example 1. For $n = 1$, any line $l = k(x, y)$ is the k-span of the vector $(x, y) \neq (0, 0)$. Note that for any $c \neq 0$, $c(x, y)$ will represent the same line, so we use the notation $(x : y)$ for this equivalence class.

If we fix the first coordinate to be nonzero, we can nicely parametrize it as

$$\mathcal{U}_x = \{(x : y) \mid x \neq 0\} = \{(1 : y/x = t)\} \simeq k^1 .$$

Of course this doesn't cover everything, since $(0, 1)$ should certainly be allowed. To do this, we alternatively insist that $y \neq 0$ to get

$$\mathcal{U}_y = \{(x, y) \mid y \neq 0\} = \{(s = x/y : 1)\} \simeq k^1$$

Now we want good behavior in the intersection of these two, $\mathcal{U}_x \cap \mathcal{U}_y$, which looks like $t \neq 0$ in $\mathcal{U}_x$ and $s \neq 0$ in $\mathcal{U}_y$. Then since $st = 1$, we take $V(st - 1) \subseteq k^2$ and get $V(st - 1) \cong \mathcal{U}_x \cap \mathcal{U}_y$.

Example 2. $\mathbb{P}^2$ consists of the equivalence classes, under scalar multiplication, of 3-vectors. We will use the same notation $\mathbb{P}^2 \{(w : x : y)\}$. Now to get local coordinates, we can play the same game as before.

$$\mathcal{U}_w = \{w \neq 0\} = \{(1 : u = x/w : v = y/w)\} \cong k^2$$

and then we get $\mathcal{U}_x \cong k^2$ with coordinates w/x and y/x, and $\mathcal{U}_y \cong k^2$ with coordinates x/y, and w/y.

Now $\mathcal{U}_w \cap \mathcal{U}_x$ is $u \neq 0$ in $\mathcal{U}_w$, and has coordinates u, v, u^{-1}, which are of course x/w, y/w, and w/x. We can also think of this in terms of the $\mathcal{U}_x$ coordinates w/x and y/x, but on this open set, they should be expressible in terms of u, v, u^{-1}. And indeed, $w/x = u^{-1}$, and $y/x = v/u$.

This can be viewed as the $\mathcal{U}_w$ plane along with a line $L_\infty = \mathbb{P}^1$ at infinity.

Now consider a line in the affine plane given by $V(au + bv + c)$ where a, b are not both 0. On $\mathcal{U}_w$, this means $ax/w + by/w + c = 0$. This can be written $ax + by + cw = 0$, and then to get this in coordinates on $\mathcal{U}_x$ (resp. $\mathcal{U}_y$) we just divide through by x (resp. y) since this is homogeneous of degree 1 in x, y, and

Date: August 27, 2018.

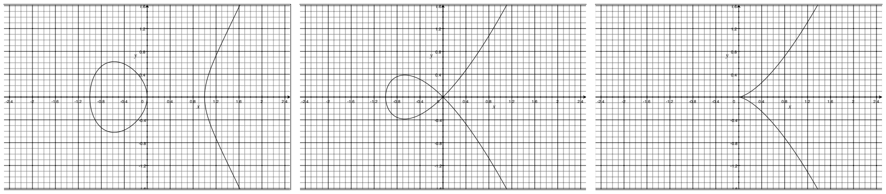

FIGURE 1. (Left) The plane curve $V\left(y^2 - x^3 + x\right)$ illustrating the generic case. (Middle) The case of a nodal curve illustrated by the curve $V\left(y^2 - x^3 - x^2\right)$ and (right) a cusp singularity.

w. Notice that this line is really the $\mathbb{P}^1$ given by the lines on k^2 of the form $ax + by + cw = 0$. At every point in $L \cap L_\infty$ must have $w = 0$, which is only the case at the point $(b : -a)$, so this intersection consists only of this point. Note that there are no parallel lines in the projective plane. Every two distinct lines meet at unique points.

Now we consider curves in the projective plane. The simplest example beyond lines is quadratic curves. Let's consider the parabola $v = u^2$ and the hyperbola $uv = 1$. These can be written as varieties $V\left(y - u^2\right)$ and $V\left(uv - 1\right)$. The equation for the parabola can be rewritten as

$$V\left(y/w - (x/w)^2\right) \qquad \rightsquigarrow \qquad V\left(yw - x^2\right)$$

which is a homogeneous equation of degree 2. Then for $w = 1$, we have that this is just $V\left(y - x^2\right)$. We can always do this to any polynomial by multiplying sufficiently many powers of w. For $x = 1$, the equation on $\mathcal{U}_x$ is just $V\left(yw - 1\right)$, so the parabola looks like a hyperbola. On $\mathcal{U}_y$, we get $V\left(w - x^2\right)$, so it again looks like a parabola. If we intersect this with the line at infinity, in homogeneous coordinates this is just insisting that $w = 0$, so we get $V\left(w, x^2\right)$ which is just the equation $(0 : 0 : 1)$. The fact that we get $x^2 = 0$ instead of just $x = 0$ is a reflection of the fact that this is somehow tangent to the line at infinity. The reason we saw it as a parabola two ways and a hyperbola one way, is that from any point of view, two of w, x, y become the axes, and the third becomes the line at infinity. The distinction between hyperbolas and parabolas is the way the curve meets the line at infinity. If it is tangent at one point, then it is a parabola in these coordinates, and if it intersects the line at infinity in two places, it is a parabola in these coordinates.

2. Elliptic curves

We will return to this when we have developed a bit more theory, but this is a huge part of algebraic geometry, so we consider some examples now. Consider a plane curve

$$C = V\left(y^2 - (x-a)(x-b)(x-c)\right) \ .$$

We will really be interested in $\overline{C}$ in projective space. WLOG we can consider $y^2 = x(x+1)(x-c)$. If $x > c$, there will be two real y values, between 0 and c, there will be no real solutions, between 0 and 1 we will have double real solutions again as in fig. 1.

One thing that happens is that there are degenerate cases. If c goes to 0, we get a nodal curve, and when all three parameters go to 0, we get a cusp singularity as in fig. 1.

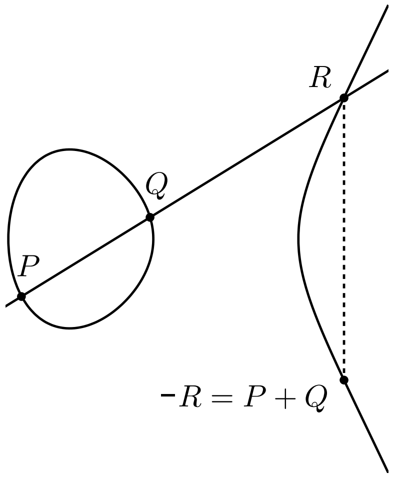

Figure 2. The straight line drawn to find R from P and Q such that $P + Q + R = 0$.

If we consider the closure of the generic case in projective space, then we get $y^2w - (x - aw)(x - bw)(x - cw)$. Now if we let $w = 0$ to see where this meets the line at infinity, we get $V\left(w, x^3\right)$.

As it turns out we can put a group structure on the points of an elliptic curve. The group law is defined as follows. Take any 2 points P and Q on the curve, now draw a line as in fig. 2 and then find the third point of intersection[1] R and then $P + Q + R = 0$ gives the identity point at infinity. Then the inverse of the point $R = (x, y)$ is $-R = (x, -y)$.

[1] We know there are three since this is an elliptic curve.