MATH 115, SUMMER 2012
LECTURE 29

JAMES MCIVOR

- last time we define the projective plane - like $\mathbb{R}^2$ but with "points at infinity", one for each slope we can use to approach infinity.

- points in $\mathbb{P}^2$ are given by $[x : y : z]$, where x, y, z are not all zero, and

$$[x : y : z] = [\lambda x : \lambda y : \lambda z]$$

for all $\lambda \neq 0$.

- we also defined curves in the projective plane - they are defined by setting a *homogeneous* polynomial equal to zero. The polynomial could have rational or real coefficients, depending on our purposes.

- we can study how these curves look by setting first $x = 1$, and seeing how it looks in the yz-plane; then $y = 1$ and seeing how it looks in the xz plane; and finally $z = 1$ and looking in the xy plane.

- we need to identify certain "problems" that can occur with projective curves (these can also occur with regular plane curves in $\mathbb{R}^2$)

Definition 1. Let $P = [a : b : c]$ be a point on a projective plane curve C defined by $F(x, y, z) = 0$, where F is a homogeneous polynomial. We call P a **singular point** of C if

$$\frac{\partial F}{\partial x}(a, b, c) = \frac{\partial F}{\partial y}(a, b, c) = \frac{\partial F}{\partial z}(a, b, c) = 0$$

If C has no singular points, we say C is **nonsingular**.

Geometrically, a singular point is a problem because it is unclear what the tangent line is at that point. The main examples are points where the curve crosses itself (two tangent lines at one point), or something like a "sharp corner" / cusp.

Definition 2. A projective plane curve C defined by $F(x, y, z) = 0$ is called **reducible** if the polynomial factors into polynomials of positive degree. If C is not reducible, it's called **irreducible**.

If F factors as $F = GH$, where G and H are nonconstant homogeneous polynomials, then the curves defined by $G = 0$ and $H = 0$ are called **components** of C.

The point about factoring into positive degree polynomials is that we can always factor out a degree 0 polynomial - that's just a constant.

Example 0.1. The cubic curve C given by $F(x, y, z) = x^3 - x^2z - xy^2 - xz^2 + y^2z + z^3 = 0$ is reducible, because F factors as

$$F(x, y, z) = (x - z)(x^2 - y^2 - z^2)$$

Thus C has two components: the line $x = z$ and the conic $x^2 = y^2 + z^2$.

C is a singular curve: we can compute this directly or observe that the two components intersect at points of the form $[x : 0 : x]$. By the property of homogeneous

coordinates, there is in fact just one point of this form, which we may as well write as $[1:0:1]$.

Exercise: Use the product rule for derivatives to prove that points lying on both components simultaneously must be singular points. Conclude that the curve above is singular.

For a computationally easier example, let C be the conic $x^2 - yz$. Then we have

$$\frac{\partial F}{\partial x} = 2x$$
$$\frac{\partial F}{\partial y} = z$$
$$\frac{\partial F}{\partial z} = y,$$

and these all vanish only at $[0:0:0]$, which is not a point of the projective plane.

1. (De-)Homogenization

We have seen that projective plane curves are described by homogeneous polynomials. Regular plane curves (in $\mathbb{R}^2$), which are usually called **affine** plane curves to distinguish from the projective ones, are described by any polynomial.

But since $\mathbb{R}^2$ is a subset of $\mathbb{P}^2$ (it's $\mathbb{P}^2$ without the points at infinity), it's natural to ask: given an affine plane curve, is there a way to extend it to a projective plane curve.

There is, and it's accomplished by a process called homogenization, which makes a non-homogeneous polynomial into a homogeneous one.

Rather than give a formal definition,we just do an example:

Examples 1.1. (1) Consider the affine plane curve $f(x,y) = y - x^2 = 0$. It's a parabola. The **homogenization** of f is obtained by multiplying each term by some power of z in order to ensure that every term has the same degree. Since f has degree two, we must multiply the term y by z to give it degree two. The x^2 term is untouched. Thus the homogenization of f is $F(x,y,z) = yz - x^2$.

In this example, the affine curve is just a parabola. By homogenizing, we extend this curve to a curve in $\mathbb{P}^2$. Which points at infinity did we add? In homogeneous coordinates, the points of $\mathbb{R}^2 \subset \mathbb{P}^2$ are those $[x:y:z]$ with $z \neq 0$. The points at infinity are those where $z = 0$. So to see what the points at infinity on our new projective curve are, we just set $z = 0$ in the homogenized equation, giving $x^2 = 0$. Thus the points at infinity on the projective curve are $[0:y:0]$, but again using properties of homogeneous coordinates, there's only one such point, which we may as well write as $[0:1:0]$. If we think of the set of points at infinity as being a copy of $\mathbb{P}^1$, then this point corresponds to the point $\infty = [0:1] \in \mathbb{P}^1$.

You could have guessed this geometrically, actually. The points at infinity correspond to the slopes with which you approach infinity - one point for every real number slope, and one point for slope infinity (i.e., a vertical line). Since, as we move out along the parabola, the slop of the parabola approaches infinity, it makes sense that the parabola meets the line at infinity at the point corresponding to slope infinity.

(2) The homogenization of $f(x,y) = x^3 + xy + 2x^2y^2$ is $F(x,y,z) = x^3z + xyz^3 + 2x^2y^2$.
(3) One can also dehomogenize a polynomial $F(x,y,z)$ which is already homogeneous by setting one of the three variables equal to 1. This is exactly what we did when we looked at the image of a projective curve in each of the three subsets U_0, U_1, U_2

2. Elliptic Curves

- we studied in some detail the question of rational points on conics - degree 2 curves. Now we turn our attention to cubics - degree 3 curves. These are some of the most interesting objects in all of mathematics, especially in number theory!

Definition 3. An elliptic curve is a nonsingular irreducible degree 3 projective plane curve.

Example 2.1.
Many of the elliptic curves of interest are defined by polynomials of the form

$$F(x,y,z) = y^2z - ax^3z - bx^2z - cxz^2 - dz^3$$

We more commonly write these in their dehomogenized forms, namely $f(x,y) = y^2 - ax^3 - bx^2 - cx - d$. We can express this more succinctly by the equation

$$y^2 = q(x),$$

where q is a cubic polynomial in x. Then it is not hard to check that F is nonsingular if and only if q has no repeated roots.

For instance, the equation

$$y^2 = x(x-1)(x-\lambda),$$

where $\lambda \neq 0, 1$ is probably the most common equation for an elliptic curve

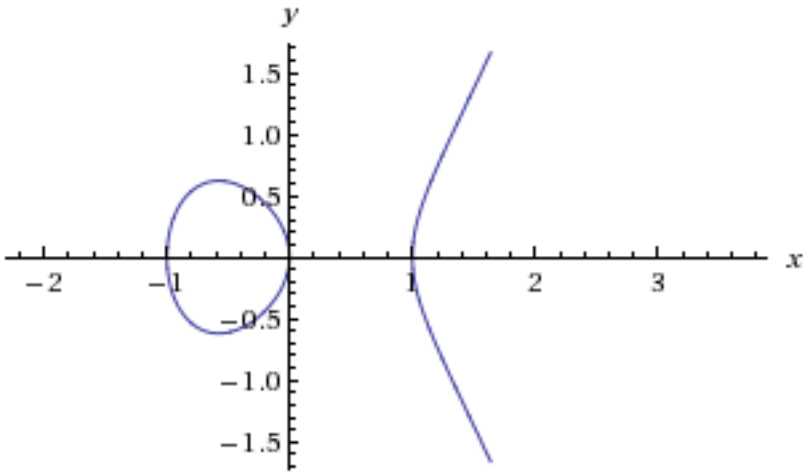

Figure 1. The Elliptic Curve $y^2 = x(x-1)(x+1)$

3. Group Law on an Elliptic Curve

We are of course interested in the question of finding rational points on an elliptic curve. Following our geometric approach to finding rational points on conics, we would like to connect various rational points by lines with rational slopes. This leads to an incredible discovery: the set of points (real or rational) on an elliptic curve has the structure of a group! So we can study the rational points by asking what sort of group this is for each different elliptic curve.

For completeness, we recall the definition of a group:

Definition 4. A **group** is a set G equipped with a binary operation $+\colon G\times G \to G$ which is associative, has an identity element 0, and for which every element has an inverse.

The main examples of groups are $\mathbb{Z}$ and $\mathbb{Z}/m$. We called these rings before, and used addition *and* multiplication on them. If you ignore the multiplication, and only allow yourself to add, then they're just groups.

If, in addition, our group law satisfies the condition $g+h = h+g$ for all $g, h \in G$, then we say G is an **abelian group**. The examples above are both abelian groups. For an example of a group that is not abelian, take G to be the set of invertible $n \times n$ real matrices, where $+$ is to be interpreted as multiplication of matrices.

Let us now fix an elliptic curve $E \subset \mathbb{P}^2$ and construct an operation $+$ on E.

First of all we will need the identity element O for our group. For this we pick any point we like on E and call it O. Next, given two points P and Q on E, not necessarily distinct, then the line through L intersects E at exactly one other point (which could be P or Q again, if the line is tangent to one of these points).

Exercise: Prove this. Why can't a line just pass through two points on the curve without intersecting in a third point?

The reason is that this amounts to solving a cubic polynomial. Such things will always have three complex roots (possibly repeated), but the number of real roots must be on or three, since purely complex roots come in pairs $a \pm bi$. Since we know there are two real roots (coming from our two points P and Q), there must be three real roots, giving a third real point on the line and E.

Notice also that for this it is essential that we work in $\mathbb{P}^2$, not $\mathbb{R}^2$ - the third point of intersection may well be a point at infinity.

- Draw an example showing that this fails in $\mathbb{R}^2$. Extend the $\mathbb{R}^2$ picture by embedding it in $\mathbb{P}^2$ and finding the missing third intersection.

Let us now call this third intersection point PQ. Now consider the line between O and PQ. It, too, intersects E in a unique third point (which could be O or PQ again). We call this third point $P+Q$, although it could also be written as $O(PQ)$, meaning the third point of intersection of E and the line between O and PQ.

- **Draw some examples**

- note what happens if the line joining P and Q is tangent to E at either P or Q.