MATH CIRCLE - ELLIPTIC CURVES WEEK 4

SAM LICHTENSTEIN

This week we picked up where we left off regarding the use of so-called *homogeneous coordinates* on the *projective plane* instead of ordinary coordinates on the ordinary ("*affine*") plane. Recall that the projective plane can be thought of as the lines through the origin in three-dimensional space. Inside 3-space, we pick a plane $Z = 1$ which doesn't pass through the origin, and identify this with the usual affine plane. Each point of this plane corresponds to a unique line through the origin. On the other hand, *almost* any line through the origin passes through a point of this plane. However, we have a few extra lines, namely those *parallel* to the plane. If we specify a line through the origin by specifying a point $(X, Y, Z) \neq (0, 0, 0)$ on the plane, we get the *homogeneous coordinates* of that line $[X, Y, Z]$, which we regard as a **point** of the projective plane. The coordinates $[X, Y, Z]$ are defined up to multiplying all three by (the same) nonzero constant, since this just slides your point along the same line through the origin, so the same line is determined.

We saw that an ordinary equation in the plane, such as $y^2 = x^3 + x$, can because an equation for points of the projective plane in the following manner. Since the ordinary xy-plane corresponded to the points $(x, y, 1)$ in 3-space, the point (x, y) corresponds to the projective point $[x, y, 1]$ (remember, this is a line!). How do we get a point (x, y) from a projective point $[X, Y, Z]$? Well, to get an equivalent point (i.e. on the same line through $(0, 0, 0)$) which lies on the plane $Z = 1$ we can divide each coordinate by Z (assuming $Z \neq 0$):

$$[X, Y, Z] = [X/Z, Y/Z, 1].$$

So we should set $x = X/Z, y = Y/Z$ to be our *inhomogeneous* coordinates for the point $[X, Y, Z]$, provided that $Z \neq 0$. Let's plug these into the original equation $y^2 = x^3 + x$: we get

$$\frac{Y^2}{Z^2} = \frac{X^3}{Z^3} + \frac{X}{Z}.$$

Multiplying through by Z^3 to get back to a polynomial, we obtain

$$Y^2 Z = X^3 + XZ^2.$$

This is the *homogeneous equation* corresponding to the inhomogeneous equation $y^2 = x^3 + x$ we began with. Now we see why these coordinates and equations are called "homogeneous": every term of this equation has degree 3 as a polynomial in X, Y and Z; i.e. it is 'homogeneous of degree 3'.

Using this equation we were *finally* able to say precisely what we mean by "every line meets the cubic curve in three points" – where, remember, it was important to think about the curve over the *complex* numbers $\mathbb{C}$ rather than the real numbers $\mathbb{R}$ (so that we can take square roots of negative numbers, for example), and we were thinking about the curve with "extra points at infinity". These points at infinity correpond to points $[X, Y, 0]$ in the

projective plane which satisfy the inhomogeneous equation but do not lie in the ordinary plane $Z = 1$ which contained all the "usual" points of the curve. (Note that if Z takes any nonzero value, then we simply divide by Z to get $Z = 1$. So this is really everything.)

We considered a line such as $x = 3$ in the ordinary plane. Turning this into a homogeneous equation, we get $X = 3Z$. Plugging this into the homogeneous equation for our cubic curve, we got an polynomial $Y^2Z = 27Z^3 + 3Z^3 = 30Z^3$. This means that *either* $Z = 0$ or $y = \frac{Y}{Z} = \pm\sqrt{30}$. These correspond to the three *projective* points where the line $x = 3$ and the curve $y^2 = x^3 + x$ intersect: namely $[3, \pm\sqrt{30}, 1]$ and $[0, 1, 0]$. The last corresponds to the case when $Z = 0$, since in this case $X = 3Z = 0$, and there can only be one line through the origin in 3-space passing through a point $[0, Y, 0]$: the line which passes through $[0, 1, 0]$. Said differently, since X and Z are 0, Y can take any nonzero value, but we may as well divide by it (which gives the same projective point) to get $[0, 1, 0]$.

We ended class by observing that we can define a *rule* on a projective cubic curve using the fact that any line meets it in three places. Given points P and Q, we define $P \star Q$ to be the *third point of intersection* of the line $\overline{PQ}$ with the curve in question. Some thoughts we were left with: Does this rule have the properties of a nice operation like addition? Is there an identity? Inverses (i.e. negatives)? Is it commutative (i.e. $P \star Q = Q \star P$)? Is it associative (i.e. $P \star (Q \star R) = (P \star Q) \star R$)? We'll pick these threads up next time.