FROM CUBICS TO ELLIPTIC CURVES

MATH 556 – SPRING 2017

A Small Correction

We will follow the steps laid out in Section 1.3 [more precisely, pg. 17] from our text. We should start by observing that there is a small [fixable!] mistake in the text. Consider the [non-singular – check!] cubic:

$$C \ : \ xy^2 + x^2 + y^2 + 1 = 0,$$

or, in projective coordinates:

$$C \ : \ XY^2 + X^2Z + Y^2Z + Z^3 = 0,$$

So, note that C passes through $[1:0:0]$ and $[0:1:0]$. Moreover, the line tangent to the first point passes through the second: indeed, let $u \stackrel{\text{def}}{=} Y/X$ and $v \stackrel{\text{def}}{=} Z/X$. Then, in the affine plane $X \neq 0$, we have that our curve has equation:

$$u^2 + v + u^2v + v^3 = 0$$

and $[1:0:0]$ corresponds to $(0,0)$. Then we can see that the tangent line at $(0,0)$ is $v=0$, i.e., $Z=0$ [in which $[0:1:0]$ lays!].

So, C satisfies the conditions outlined in Section 1.3, but not the general formula given [in the first displayed equation of pg. 17], as it has a term in y^2.

But, this can be easily remediated: if we have an equation of the form:

$$xy^2 + fy^2 + (ax+b)y = cx^2 + dx + e,$$

then replacing $x+f$ by x [and y by y] we get the equation

$$xy^2 + (ax + (b-af))y = cx^2 + (d-2cf)x + (e + cf^2 - df).$$

[The map between them is $(x,y) \mapsto (x+f, y)$.]

So, we might need one extra step.

Date: February 15, 2017.

Example

Consider the curve and rational point

$$C \,:\, x^3 + y^3 = 2, \qquad \mathcal{O} = (1, 1). \tag{1}$$

In projective coordinates:

$$C \,:\, X^3 + Y^3 = 2Z^3, \qquad \mathcal{O} = [1 : 1 : 1].$$

The tangent line at $\mathcal{O}$ is $y = -x + 1$ [or $X + Y - Z = 0$]. The third point of intersection between this line and the cubic is $[1 : -1 : 0]$.

So, we need to map $[1 : 1 : 1] \mapsto [1 : 0 : 0]$ and $[1 : -1 : 0] \mapsto [0 : 1 : 0]$. By choosing to map $[0 : 0 : 1] \mapsto [0 : 0 : 1]$, we get a matrix transfomation given by a matrix that is the inverse of

$$M \stackrel{\text{def}}{=} \begin{bmatrix} 1 & 1 & 0 \\ 1 & -1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

Then, the equation becomes:

$$(X + Y)^3 + (X - Y)^3 = 2(X + Z)^3,$$

which simplifies to

$$XY^2 = X^2Z + XZ^2 + \frac{1}{3}Z^3, \tag{2}$$

or, in affine coordinates:

$$xy^2 = x^2 + x + \frac{1}{3}. \tag{3}$$

Note that the map between the curves is given by the matrix M^{-1}, but since are in projective coordinates, we can multiply M^1 by $\det(M)$ [or any other non-zero scalar] to avoid denominators. So, we get that the map between the curves is:

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \mapsto \det(M) \cdot M^{-1} \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} -1 & -1 & 0 \\ -1 & 1 & 0 \\ 1 & 1 & -2 \end{bmatrix} \cdot \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} -X - Y \\ -X + Y \\ X + Y - 2Z \end{bmatrix}.$$

Now, we multiply equation (3) by x, obtaining

$$(xy)^2 = x^3 + x^2 + \frac{1}{3}x$$

and make the change $(x, y) \mapsto (x, xy)$, giving a new equation:

$$y^2 = x^3 + x^2 + \frac{1}{3}x. \tag{4}$$

In projective coordinates, the map is $[X : Y : Z] \mapsto [X/Z : XY/Z^2 : 1]$, or better, $[X : Y : Z] \mapsto [XZ : XY : Z^2]$.

Let's see what happens with the points at infinity of the original curve, namely $[1 : 0 : 0]$ and $[0 : 1 : 0]$. [This is a bit tricky.] As we can see the map given above is not well defined at those points, as they yield $[0 : 0 : 0]$ [i.e., nonsense]. So, we need to modify them:

$$\begin{aligned} [X : Y : Z] \mapsto [XZ : XY : Z^2] &= [XYZ : XY^2 : YZ^2] && \text{[mult. by } Y\text{]} \\ &= [XYZ : X^2Z + XZ^2 + Z^3/3 : YZ^2] && \text{[by Eq. (2)]} \\ &= [XY : X^2 + XZ + Z^2/3 : YZ] && \text{[divide by } Z\text{]} \end{aligned}$$

So $[1 : 0 : 0] \mapsto [0 : 1 : 0]$. [This *had* to be the case, as the rational point has to go to $[0 : 1 : 0]$ in the end!]

Also,

$$\begin{aligned} [X : Y : Z] \mapsto [XZ : XY : Z^2] &= [XZ^2 : XYZ : Z^3] && \text{[mult. by } Z\text{]} \\ &= [XZ^2 : XYZ : 3XY^2 - 3X^2Z - 3XZ^2] && \text{[by Eq. (2)]} \\ &= [Z^2 : YZ : 3Y^2 - 3^2Z - 3Z^2] && \text{[divide by } X\text{]} \end{aligned}$$

So, $[0 : 1 : 0] \mapsto [0 : 0 : 3] = [0 : 0 : 1] = (0, 0)$ [in the xy-plane].

Note that if α_1, α_2 are the roots of $x^3 + x + 1/3$, then clearly $(\alpha_i, 0) \mapsto (\alpha_i, 0)$. But we also have $(0, 0)$ in the curve given by equation (4) and note that no *affine* point of the curve given by equation (3) can map to that one [as the map is $(x, y) \mapsto (x, xy)$ and there is no point with x-coordinate 0 in that curve], so it had to be one of the points at infinity that would map to it. Since we knew where the other point had to go, we knew already that $[0 : 1 : 0] \mapsto (0, 0)$.

If we want to go one step further, we can get rid of the term in x^2 in equation (4). The map is $(x, y) \mapsto (x + 1/3, y)$ and the new equation is

$$y^2 = x^3 - 1/27. \tag{5}$$

Finally if you want to have integral coefficients, we cab get it with the map $(x, y) \mapsto (3^2x, 3^3y)$ and new equation

$$y^2 = x^3 - 27. \tag{6}$$

Composing all these maps, we have that the map between the original curve (equation (1)) and the final (equation (6)) is

$$(x, y) \mapsto \left(\frac{6(x + y + 1)}{2 - x - y}, \frac{27(x^2 - y^2)}{(2 - x - y)^2} \right)$$

and the reverse maps is

$$(x, y) \mapsto \left(\frac{(x-3)^2 + 9y}{(x-3)^2 + 9(x-3)}, \frac{(x-3)^2 - 9y}{(x-3)^2 + 9(x-3)} \right).$$