MA434 Scribal Notes

Nathaniel Ferguson

February 28

1 Section 2.12

In this section, we seek to motivate a definition of inflection points. Consider a cubic C in ${\mathbb{P}^2}_{\mathbb{R}}$. We can write that cubic as:

$$C : Y^2Z = X^3 + aXZ^2 + bZ^3$$

Or, in affine form using $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$:

$$y^2 = x^3 + ax + b$$

Now, we wonder where this line meets the "line at infinity" of $L : (Z = 0)$. In normal form, we can solve for the other variables when $Z = 0$:

$$F = -Y^2Z + X^3 + aXZ + bZ^3$$

$$F = X^3$$

To find that there is a triple zero at $[0 : 1 : 0]$. If we instead divide by Y to produce our affine form, we see that:

$$z = x^3 + axz^2 + bz^2$$

And so our triple intersection looks like the graph of x^3 near $[0 : 1 : 0]$. This motivates the following definition:

1.1 Definition:

A point P on a curve C is an inflection point if there exists a line $L \subset {\mathbb{P}^2}_k$ such that $F|_L$ has a zero of multiplicity ≥ 3 at P.

It is worth noting we have that $L = T_PC$ by Section 2.8 and that the multiplicity $= 3$ by Bezout's theorem. Also, we can make the connection to inflection points defined by their derivative. If $y = f(x)$, then P is an inflection point if and only if $\frac{d^2}{dx^2}f(P) = 0$.

2 Section 2.13

Here, we will explore a nice simplification of the group law given in Section 2.8 when we choose our point $O = [0 : 1 : 0]$. We set out to find a general equation for lines through O:

$$aX + bY + cZ = 0$$

This defines a general line in $\mathbb{P}^2$. Now we observe that since the line goes through $[0 : 1 : 0]$, we must have $b = 0$. So:

$$aX + cZ = 0$$

If $a \neq 0$, then we have $X - \lambda Z = 0$ and so choosing $\lambda = \frac{X}{Z}$ we have, in affine form:

$$x = \lambda$$

Which is a vertical line in affine space. Otherwise, if $a = 0$, we have $z = 0$ which is the "line at infinity".

Since all lines through O are of this form, this greatly simplifies the group law. Recall that the inverse of a point A, denoted $\bar{A}$, is constructed by drawing a line through A and O and finding the third point of intersection. In our case, because every line through O is vertical, we simply draw a vertical line through A and its inverse is the other point on that vertical line.

Algebraically, we can think of our cubic as:

$$\{[0 : 1 : 0]\} \cup \{(x : y) | y^2 = x^3 + ax + b\}$$

Solving for y when $x = \lambda$ gives us:

$$y = \pm\sqrt{\lambda^3 + a\lambda + b}$$

Which means that the points that are on the same vertical line have coordinates (x, y) of:

$$(\lambda, \pm\sqrt{\lambda^3 + a\lambda + b})$$

Note that since O is an inflection point, $O = \bar{O}$. For other $P = (x, y)$, we have that $\bar{P} = (x, -y)$.

Now we may restate the group law as the following theorem:

2.1 Theorem:

Let C be a cubic in the normal form. Then there exists a unique group law on C with $O = [0 : 1 : 0]$ being the identity, with inverses given by $(x, y) \mapsto (x, -y)$, and for all $P, Q, R \in C$,

$$P + Q + R = O \Leftrightarrow P, Q, R \text{ are colinear.}$$

3 Exercises

Now we will examine two exercises and their solutions.

3.1 Exercise 2.4:

Let C : $(y^2 = x^3 + 4x)$ with the simplified group law. Show that the tangent line to C at $P = (2, 4)$ passes through $(0, 0)$, and deduce that P is a point of order 4 in the group law.

We begin finding the tangent line by considering:

$$f : 0 = -y^2 + x^3 + 4x$$

And we take the partial derivatives at P:

$$\frac{\partial f}{\partial x} = 3x^2 + 4|_{x=2} = 16$$

$$\frac{\partial f}{\partial y} = -2y|_{y=4} = -8$$

So, using the fact that the tangent line at point P is of the form:

$$\frac{\partial f}{\partial x}(P)(x-2) + \frac{\partial f}{\partial y}(P)(y-4) = 0$$

We are left with $16(x-2) - 8(y-4) = 0$, which simplifies to $y = 2x$ as our equation of the tangent line.

Now we deduce P is a point of order 4 in the group law. Since $P + P = P_2$, where $P_2 = (0, 0)$, and $P_2 + P_2 = P + P + P + P = 4P$, we have $4P = O$ by the simplified group law, which is what we wanted to show.

3.2 Exercise 2.5:

Let C : $(y^2 = x^3 + ax + b) \subset \mathbb{R}^2$ be nonsingular, find all points of order 2, and understand what group they form (there are two cases to consider).

We begin by noticing that all points of order 2 will have a vertical tangent in the simplified group law such that $P + P = O$. Now, considering:

$$f : x^3 + ax + b - y^2 = 0$$

We see that a vertical tangent occurs when:

$$\frac{\partial f}{\partial y}(P) = 0$$

Taking the partial derivative, we find that:

$$\frac{\partial f}{\partial y} = -2y$$

So we have a vertical tangent at $y = 0$, as we might hope. This means that the x coordinates of a vertical tangent will be roots of the cubic

$$x^3 + ax + b$$

In particular, when we have one real root, we have a one point of order 2, and when we have three real roots, we will have 3 points of order 2. When we have one point of order two in addition to our identity O, we have a abelian subgroup with two elements which must be isomorphic to $\mathbb{Z}_2$. On the other hand, when we have three roots and so four total points, we have an abelian subgroup where all the elements square to the identity. So it is isomorphic to $\mathbb{Z}_2 \otimes \mathbb{Z}_2$ in that case.