MATH 176
Homework 6
Nov 16, 2016

Collaborators:

Homework: Reid 2.3, 2.11, and Portfolio Problem

(Reid 2.6) Let $C = Z(f) \subseteq \mathbb{A}^2$ and let $p = (a, b) \in C$; assume $\dfrac{\partial f}{\partial x}(p) \neq 0$. Prove that the line

$$L = Z\left(\frac{\partial f}{\partial x}(p)(x - a) + \frac{\partial f}{\partial y}(p)(y - b)\right)$$

is the tangent line to C at p, that is, the unique line L of $\mathbb{A}^2$ for which $f|_L$ has a multiple root at p. (This is worked out in detail in (6.1).)

(Reid 2.11) Consider the curve $C = Z(z - x^3) \subset \mathbb{A}^2$. C is the image of the bijective map

$$\varphi : \mathbb{A}^1_k \mapsto C, \quad \varphi(t) = (t, t^3),$$

so it inherits a group law from the additive group structure on k. Prove that this is the unique group law on C such that $(0, 0)$ is the neutral element and

$$P + Q + R = 0 \Leftrightarrow P, Q, R \text{ are collinear },$$

for $P, Q, R \in C$.
Hint: You might find useful the identity

$$\det \begin{pmatrix} 1 & a & a^3 \\ 1 & b & b^3 \\ 1 & c & c^3 \end{pmatrix} = (a - b)(b - c)(c - a)(a + b + c).$$

In projective terms, C is the curve $y^2z = x^3$, our old friend with a cusp at the origin and an inflection point $(0, 1, 0)$, and the point of the question is that the usual construction gives a group law on the complement of the singular point.

Portfolio Problem *Following Dragos Oprea.*

1. Consider two points $P = (x_1 : y_1 : 1)$ and $Q = (x_2 : y_2 : 1)$ on the elliptic curve

$$y^2z = x(x-z)(x-\lambda z) \subset \mathbb{P}^2_{\mathbb{C}}.$$

   Prove that the sum

$$P + Q = \begin{cases} (0:1:0) & \text{if } x_1 = x_2 \text{ but } y_1 \neq y_2 \\ (x_3 : y_3 : 1) & \text{if } x_1 \neq x_2, \end{cases}$$

   where

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 + 1 + \lambda - x_1 - x_2$$
$$y_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right) x_3 + \left(\frac{x_1y_2 - y_1x_2}{x_1 - x_2}\right).$$

   What are the corresponding formulas if $P = Q$?

   Hint: First let $y = mx + b$ be the line passing through P and Q. Find m and b in terms of x_1, y_1, x_2, y_2. Then substitute in the equation of the elliptic curve. Note if you know two of the roots of a cubic polynomial, the third one can be determined from one of the coefficients.

2. Show that if $\lambda \in \mathbb{Q}$, then the set of points on the elliptic curve with rational coordinates form an abelian group. You only need to check that if P and Q have rational coordinates, so do $-P$ and $P + Q$.

   Remark: The abelian group of rational points on the elliptic curve is typically denoted $\overline{E}_\lambda(\mathbb{Q})$. The Mordell-Weil theorem states that this abelian group is finitely generated.