Peize Liu
St. Peter's College
University of Oxford

Problem Sheet 2

B3.3: Algebraic Curves

8 February, 2021

Question 1

Let C be the projective curve with equation

$$x^2 + y^2 = z^2$$

Show that the projective line through the points [0,1,1] and $[t,0,1]$ meets C in the two points [0,1,1] and $\left[2t, t^2-1, t^2+1\right]$.

Show that there is a bijection between the projective line $y = 0$ and C given by:

$$[t,0,1] \mapsto \left[2t, t^2-1, t^2+1\right]$$
$$[1,0,0] \mapsto [0,1,1]$$

Proof. Let $A = [0:1:1]$ and $B = [t:0:1]$. Note that $A \in C$. The projective line AB is

$$\left\{[\mu t : \lambda : \lambda + \mu] : \ \lambda \neq 0 \text{ or } \mu \neq 0\right\}$$

Suppose that $P \in AB \cap C$. Then:

$$\mu^2 t^2 + \lambda^2 = (\lambda + \mu)^2 \implies \mu^2(t^2-1) - 2\lambda\mu = 0$$

If $\mu = 0$, then we can take $\lambda = 1$. Hence $P = A = [0:1:1]$. If $\mu \neq 0$, then $\mu(t^2-1) = 2\lambda$. We can take $\mu = 2$ and $\lambda = t^2 - 1$. Then

$$P = (t^2-1)[0:1:1] + 2[t:0:1] = [2t : t^2-1 : t^2+1]$$

The projective line $\{y = 0\}$ is parametrised by

$$\{[t:0:1] : \ t \in F\} \cup \{[1:0:0]\}$$

Let $\alpha : \{y = 0\} \to C$ given by $[t:0:1] \mapsto [2t : t^2-1 : t^2+1]$, $[1:0:0] \mapsto [0:1:1]$. To show that α is bijective. We need to construct its inverse. For $Y \in C$ with $Y \neq A$, AY is a projective line so it intersects $\{y = 0\}$ at a unique point X.

If $X = [1:0:0]$, then $AY = \{[\lambda : \mu : \mu] : \ \lambda \neq 0 \text{ or } \mu \neq 0\}$. If $P \in AY \cap C$, then $\lambda^2 + \mu^2 = \mu^2$, which implies that $\lambda = 0$. Then $P = A$, contradicting that $AY \cap C$ contains at least two points. Hence $X = [t:0:1]$ for some $t \in F$. From the discussion above we see that $Y = [2t : t^2-1 : t^2+1] = \alpha(X)$.

Now we have defined α^{-1} on $C \setminus \{A\}$. For A we simply let $\alpha^{-1}(A) = [1:0:0]$. Therefore α^{-1} is the inverse of α. α is bijective. □

Question 2

Show that a homogeneous polynomial in two variables x, y may be factored into linear polynomials over $\mathbb{C}$.

Proof. Suppose that $P(x, y)$ is a homogeneous polynomial of degree n. Then there exists $a_0, \ldots, a_n \in \mathbb{C}$ such that

$$P(x, y) = \sum_{i=0}^{n} a_i x^i y^{n-i}$$

Let m be the largest integer such that $a_m \neq 0$. Let $Q(x) = \sum_{i=0}^{n} a_i x^i$. By the fundamental theorem of algebra, Q factorises into linear factors: $Q(x) = a_m \prod_{i=1}^{m} (x - \lambda_i)$. For $y \neq 0$, we have

$$P(x, y) = y^n \sum_{i=0}^{m} a_i \left(\frac{x}{y}\right)^i = y^n Q(x/y) = a_m y^n \prod_{i=1}^{m} \left(\frac{x}{y} - \lambda_i\right) = a_m y^{n-m} \prod_{i=1}^{m} (x - \lambda_i y)$$

If $m < n$, then both sides of the equation is zero when $y = 0$; if $m = n$, then

$$P(x, 0) = a_n x^n = a_m y^{n-m} \prod_{i=1}^{m} (x - \lambda_i y)\Bigg|_{y=0}$$

We deduce that for any $x, y \in \mathbb{C}$,

$$P(x,y) = a_m y^{n-m} \prod_{i=1}^{m} (x - \lambda_i y)$$

Since $\mathbb{C}$ is an infinite field, the equation also holds in $\mathbb{C}[x,y]$. Hence we have factorised $P(x,y)$ into linear polynomials over $\mathbb{C}$. □

Question 3

This question deals with how to define tangent lines at singular points. Let C be a curve in $\mathbb{C}^2$ defined by $Q(x,y) = 0 : x, y \in \mathbb{C}$. Define the multiplicity m of C at a point $(a,b) \in C$ to be the smallest positive integer m such that some m-th partial derivative of Q at (a,b) is nonzero (so (a,b) is a singularity of C iff $m > 1$) Consider the polynomial

$$\sum_{i+j=m} \frac{\partial^m Q}{\partial x^i \partial y^j}(a,b) \frac{(x-a)^i (y-b)^j}{i!j!}$$

As in question 2, we can factorise this as a product of m linear polynomials of the form

$$\alpha(x-a) + \beta(y-b)$$

The lines defined by the vanishing of these linear polynomials are called the m tangent lines to C at (a,b).

(i) Show that if $m = 1$ this definition agrees with the definition given in lectures for the tangent line at a nonsingular point.

(ii) Find the multiplicities and tangent lines of the singularities for the nodal cubic $y^2 = x^3 + x^2$ and the cuspidal cubic $y^2 = x^3$.

Proof. (i) When $m = 1$, we have

$$\sum_{i+j=m} \frac{\partial^m Q}{\partial x^i \partial y^j}(a,b) \frac{(x-a)^i (y-b)^j}{i!j!} = \frac{\partial Q}{\partial x}(a,b)(x-a) + \frac{\partial Q}{\partial y}(a,b)(y-b) = 0$$

We extend Q to a curve in $\mathbb{CP}^2$ by considering $P(x,y,z) := z^d Q(x/z, y/z)$ for sufficiently large $d \in \mathbb{N}$. Then we have

$$\frac{\partial P}{\partial x}(x,y,z) = z^{d-1} \frac{\partial Q}{\partial x}\left(\frac{x}{z}, \frac{y}{z}\right), \qquad \frac{\partial P}{\partial y}(x,y,z) = z^{d-1} \frac{\partial Q}{\partial y}\left(\frac{x}{z}, \frac{y}{z}\right)$$

$$\frac{\partial P}{\partial z}(x,y,z) = d z^{d-1} Q\left(\frac{x}{z}, \frac{y}{z}\right) - z^{d-2}\left(x \frac{\partial Q}{\partial x}\left(\frac{x}{z}, \frac{y}{z}\right) + y \frac{\partial Q}{\partial y}\left(\frac{x}{z}, \frac{y}{z}\right)\right)$$

We embed $\mathbb{C}^2$ into $\mathbb{CP}^2$ via $(x,y) \mapsto [x:y:1]$. Observe that

$$\frac{\partial P}{\partial x}(a,b,1) = \frac{\partial Q}{\partial x}(a,b), \qquad \frac{\partial P}{\partial y}(a,b,1) = \frac{\partial Q}{\partial y}(a,b), \qquad \frac{\partial P}{\partial z}(a,b,1) = dQ(a,b) - \left(a\frac{\partial Q}{\partial x}(a,b) + b\frac{\partial Q}{\partial y}(a,b)\right)$$

Since $[a:b:1] \in C$, we have $Q(a,b) = 0$. Now the equation

$$\frac{\partial Q}{\partial x}(a,b)(x-a) + \frac{\partial Q}{\partial y}(a,b)(y-b) = 0$$

is equivalent to

$$x\frac{\partial P}{\partial x}(a,b,1) + y\frac{\partial P}{\partial y}(a,b,1) + \frac{\partial P}{\partial z}(a,b,1) = 0$$

which is the definition of the tangent line at a non-singular point of a projective curve.

(ii) Firse we identify the singular points.

For $Q_1(x,y) = y^2 - x^3 - x^2$, a singular point is where

$$y^2 = x^3 + x^2, \qquad \frac{\partial Q_1}{\partial x} = -3x^2 - 2x = 0, \qquad \frac{\partial Q_1}{\partial y} = 2y = 0$$

Then Q_1 has a singular point at $(0,0)$. The point $(0,0)$ has multiplicity $m=2$, because

$$\frac{\partial^2 Q_1}{\partial x^2}(0,0) = -2 \neq 0$$

The tangent lines of Q_1 at $(0,0)$ are determined by

$$0 = \frac{1}{2}\frac{\partial^2 Q_1}{\partial x^2}(0,0)x^2 + \frac{\partial^2 Q_1}{\partial x \partial y}(0,0)xy + \frac{1}{2}\frac{\partial^2 Q_1}{\partial y^2}(0,0)y^2 = -x^2 + y^2 = (y-x)(y+x)$$

Hence the tangent lines are $x = y$ and $x = -y$.

For $Q_2(x,y) = y^2 - x^3$, a singular point is where

$$y^2 = x^3, \qquad \frac{\partial Q_2}{\partial x} = -3x^2 = 0, \qquad \frac{\partial Q_2}{\partial y} = 2y = 0$$

Then Q_2 has a singular point at $(0,0)$. The point $(0,0)$ has multiplicity $m=2$, because

$$\frac{\partial^2 Q_2}{\partial y^2}(0,0) = 2 \neq 0$$

The tangent lines of Q_2 at $(0,0)$ are determined by

$$0 = \frac{1}{2}\frac{\partial^2 Q_1}{\partial x^2}(0,0)x^2 + \frac{\partial^2 Q_1}{\partial x \partial y}(0,0)xy + \frac{1}{2}\frac{\partial^2 Q_1}{\partial y^2}(0,0)y^2 = y^2$$

Hence the tangent line is $y = 0$ (with a repeated factor of 2). □

Question 4

Show that if $\alpha_1, \dots, \alpha_r$ are distinct, then the affine curve

$$y^2 = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_r)$$

is nonsingular. What can you say about the associated projective curve?

Proof. Let $p(x) := \prod_{i=1}^{r}(x-\alpha_i)$. Suppose that $(a,b) \in F^2$ is a singular point on the affine curve $y^2 = p(x)$. Then

$$b^2 = p(a), \qquad 2b = 0, \qquad p'(a) = 0$$

which implies that $p(a) = p'(a) = 0$. Hence a is a repeated root of the polynomial p. But we know that the roots of p are distinct, which is a contradiction.

Now we embed F^2 into $F\mathbb{P}^2$ via $(x,y) \mapsto [x:y:1]$.

- For $r > 2$, the extension of $y^2 = p(x)$ on $F\mathbb{P}^2$ is given by

$$P(x,y,z) = z^r\left(\left(\frac{y}{z}\right)^2 - p\left(\frac{x}{z}\right)\right) = z^{r-2}y^2 - \prod_{i=1}^{r}(x-\alpha_i z) = 0$$

  We observe that $z = 0$ implies that $x = 0$. Therefore the curve passes through $[0:1:0]$. At this point, we have

$$\frac{\partial P}{\partial x} = -\left(\prod_{i=1}^{r}(x-\alpha_i z)\right)\sum_{i=1}^{r}\frac{1}{x-\alpha_i z} = 0, \quad \frac{\partial P}{\partial y} = 2z^{r-2}y = 0, \quad \frac{\partial P}{\partial z} = (r-2)z^{r-3}y^2 + \left(\prod_{i=1}^{r}(x-\alpha_i z)\right)\sum_{i=1}^{r}\frac{\alpha_i}{x-\alpha_i z} = (r-2)z^{r-3}y^2$$

  If $r = 3$, then $\frac{\partial P}{\partial z} \neq 0$. $[0:1:0]$ is not a singularity. The projective curve is non-singular. If $r > 3$, then $\frac{\partial P}{\partial z} = 0$. $[0:1:0]$ is a singularity. The projective curve is singular.

- For $r = 2$, the extension of $y^2 = p(x)$ on $F\mathbb{P}^2$ is given by

$$P(x,y,z) = y^2 - (x-\alpha_1 z)(x-\alpha_2 z) = 0$$

$z = 0$ implies that $y^2 = x^2$. Therefore the curve passes through $[1:1:0]$ and $[1:-1:0]$.

At these points, we observe that

$$\frac{\partial P}{\partial x} = -(x - \alpha_1 z) - (x - \alpha_2 z) = -2x \neq 0$$

Hence $[1:1:0]$ and $[1:-1:0]$ are not singularities. The projective curve is non-singular.

- For $r = 1$, the extension of $y^2 = p(x)$ on $F\mathbb{P}^2$ is given by

$$P(x, y, z) = y^2 - z(x - \alpha_1 z)$$

$z = 0$ implies that $y = 0$. Therefore the curve passes through $[1:0:0]$.

At this point, we have

$$\frac{\partial P}{\partial x} = -z = 0, \qquad \frac{\partial P}{\partial y} = 2y = 0, \qquad \frac{\partial P}{\partial z} = -x + 2\alpha_1 z = -1 \neq 0$$

Hence $[1:0:0]$ is not a singularity. The projective curve is non-singular. □

Question 5

(i) Show that the affine curve $y^2 = x^3 + x$ in $\mathbb{C}^2$ is nonsingular.

(ii) Now consider this curve over the finite field $\mathbb{Z}_p$ where p is a prime. That is, we consider the curve in $(\mathbb{Z}_p)^2$ with equation $y^2 = x^3 + x$. For which p is this nonsingular?

Proof. (i) $x^3 + x = x(x + \mathrm{i})(x - \mathrm{i})$ has no repeated roots. By the discussion in Question 4, we know that the affine curve $y^2 = x^3 + x$ in $\mathbb{C}^2$ is non-singular.

(ii) Since $x^3 + x = x(x^2 + 1)$, and $x^2 + 1 \neq 0$ in any $\mathbb{Z}_p$, we know that $y^2 = x^3 + x$ is non-singular if $x^2 + 1$ has no repeated roots in $\mathbb{Z}_p$. If $\alpha \in \mathbb{Z}_p$ is a root of $x^2 + 1$, then $x^2 + 1 = (x - \alpha)(x + \alpha)$. We see that $\alpha = -\alpha$ if and only if $p = 2$. We deduce that for $p > 2$, $y^2 = x^3 + x$ is non-singular in $\mathbb{Z}_p^2$.

For $p = 2$, $y^2 = x^3 + x = x(x-1)^2$. Let $P(x, y) = y^2 - x(x-1)^2$. We find that

$$P(1,0) = 0, \qquad \frac{\partial P}{\partial x}(1,0) = 0, \qquad \frac{\partial P}{\partial y}(1,0) = 0$$

Hence $(1,0)$ is a singularity of $y^2 = x(x-1)^2$. The curve is singular in $\mathbb{Z}_p^2$. □