23MAC260 Problem Sheet 1: Solutions

Lectures 1–3

Last updated February 8, 2024

1. Recall that a field K is *algebraically closed* if every nonconstant polynomial $f \in K[x]$ has a root in K. Let K be an algebraically closed field, and let $F(X, Y, Z)$ be a nonconstant homogeneous polynomial with coefficients in K. Show that the set

$$V(F) = \left\{ [a, b, c] \in \mathbb{P}^2_K \mid F(a, b, c) = 0 \right\}$$

is infinite.

Solution: If F is proportional to a power of Z, say $F = kZ^d$ for some $k \in K$, then any point $[a, b, 0] \in \mathbb{P}^2_K$ is in $V(F)$. Since K is algebraically closed, it is infinite, so we get an infinite set of points in this case.

So now we can suppose F is not a power of Z, which means that one of the variables X and Y actually appears in F. Therefore the dehomogenisation $F_d(x, y)$ is a nonconstant polynomial in x and y. Let's write it as $f(x, y)$.

If $f(x, y)$ does not contain the variable x, we can view it as a nonconstant polynomial $\tilde{f}(y) \in K[y]$. This has a root, say y_0. Then for any $x \in K$ we have

$$\begin{aligned} 0 &= \tilde{f}(y_0) \\ &= f(x, y_0) \\ &= F(x, y_0, 1) \end{aligned}$$

For different values of x, the points $[x, y_0, 1] \in \mathbb{P}^2_K$ are different. So in this way, we get a different point of $V(F)$ for each $x \in K$, hence an infinite set of points.

So now we can assume that $f(x, y)$ does contain the variable x. For any $y_0 \in K$, we can substitute y_0 into $f(x, y)$ to get a polynomial in one variable as follows:

$$f_{y_0}(x) := f(x, y_0).$$

If $f_{y_0}(x)$ is nonconstant, then since K is algebraically closed, it has a root, say x_0. So in this case

$$\begin{aligned} 0 &= f_{y_0}(x_0) \\ &= f(x_0, y_0) \\ &= F(x_0, y_0, 1) \end{aligned}$$

For different values of y_0, the points $[x_0, y_0, 1] \in \mathbb{P}^2_K$ are different. So again, we get a different point of $V(F)$ for each $y_0 \in K$ such that f_{y_0} is nonconstant.

It remains to prove that there are infinitely many y_0 such that $f_{y_0}(x)$ is nonconstant. To see this, write out $f(x, y)$ in the form

$$f(x, y) = f_0(y) + f_1(y)x + \cdots + f_k(y)x^k.$$

We have assumed that $f(x, y)$ does contain the variable x, so at least one of the polynomials $f_1, \ldots, f_k$ is nonzero. Assume f_j say is nonzero, so it has only finitely many roots $y_1, \ldots, y_m$. Now

$$\begin{aligned} f_{y_0}(x) &= f(x, y_0) \\ &= f_0(y_0) + f_1(y_0)x + \cdots + f_k(y_0)x^k. \end{aligned}$$

So as long as one of the values $f_i(y_0)$ is nonzero, this polynomial is nonconstant. But we know that for example f_j has roots $y_1, \ldots, y_m$. So if y_0 is different from all of $y_1, \ldots, y_m$, then $f_j(y_0)$ is nonzero, and hence $f_{y_0}(x)$ is nonconstant. Since K is infinite, this leaves infinitely many choices for y_0 such that $f_{y_0}(x)$ is nonconstant.

2. Let p be a prime number. Show that the equation

$$X^3 + pY^3 + p^2Z^3 = 0 \tag{*}$$

has no solutions in $\mathbb{Q}^3 \setminus \{(0, 0, 0\}$.

Solution: Suppose that $(q, r, s) \in \mathbb{Q}^3 \setminus \{(0, 0, 0\}$ is a solution of the above equation. Since the equation is homogeneous, for any $a \in \mathbb{Q}$ we get another solution (aq, ar, as). In particular if we take $a = \frac{n}{m}$ where n is the lcm of the denominators of (q, r, s) and m is the gcd of the numerators, we get a solution

$$\left(\frac{nq}{m}, \frac{nr}{m}, \frac{ns}{m}\right)$$

in which all three elements are integers with no common factor. So we can assume that we have an integer solution (q, r, s) in which $\gcd(q, r, s) = 1$.

Equation (*) can be rearranged to the form

$$X^3 = -p\left(Y^3 + pZ^3\right)$$

so substituting our solution (q, r, s) we get

$$q^3 = -p\left(r^3 + ps^3\right)$$

Since the right-hand side is divisible by p, the left-hand side must be also. So p divides q^3, which implies that p divides q. So we can write $q = pq'$ for some other integer q'. Substituting back into (*) we get

$$p^3(q')^3 + pr^3 + p^2s^3 = 0$$

and dividing by p we get

$$r^3 + ps^3 + p^2(q')^2 = 0.$$

That means (r, s, q') is another integer solution of Equation (*). So we can apply the same argument to conclude that $r = pr'$ for some integer r', and apply it once again to get that $s = ps'$ for some integer s'.

So we have shown that all of q, r, s are divisible by p, contradicting our assumption that they have no common factor.

3. Let $f(x, y)$ be any polynomial in 2 variables. Show that $(f^h)_d = f$.

   Solution: Let

$$f = \sum_{i,j} \alpha_{ij} x^i y^j \qquad (\alpha_{i,j} \in K).$$

   Let n be the degree of f. Then

$$\begin{aligned} f^h &= \sum_{i,j} \alpha_{ij} X^i Y^j Z^{n-i-j} \quad \text{and} \\ (f^h)_d = f^h(X, Y, 1) &= \sum_{i,j} \alpha_{ij} x^i y^j 1^{n-i-j} \\ &= f. \end{aligned}$$

4. Let $F(X, Y, Z)$ be any homogeneous polynomial in 3 variables. Show that $(F_d)^h = F$ unless F is divisible by Z.

   Solution: Let F be homogeneous of degree n. Then

$$F = \sum_{i,j} \alpha_{ij} X^i Y^j Z^{n-i-j}$$

   So

$$F_d(x, y) = \sum_{i,j} \alpha_{ij} x^i y^j.$$

   If F_d has degree n then we get

$$\begin{aligned} (F_d)^h &= \sum_{i,j} \alpha_{ij} X^i Y^j Z^{n-i-j} \\ &= F. \end{aligned}$$

   If F_d has degree $< n$ it means that for every nonzero coefficient α_{ij} we have $i + j < n$, or equivalently $n - i - j > 0$. This means that F is divisible by Z.

5. Let C be an elliptic curve: that is, a curve in $\mathbb{P}^2$ defined by the equation

$$Y^2Z = G(X, Z) \tag{**}$$

where the dehomogenisation $G_d(x)$ has 3 distinct roots.

Show that C intersects the line at infinity $\{Z = 0\}$ in a unique point $[0, 1, 0]$.

Solution: Let

$$G(X, Z) = aX^3 + bX^2Z + cXZ^2 + dZ^3$$

so that

$$G_d(x) = ax^3 + bx^2 + cx + d.$$

Since G_d has 3 distinct roots we must have $a \neq 0$.

To find the intersection $C \cap \{Z = 0\}$ we set $Z = 0$ in Equation (**). Since all terms except for aX^3 are divisible by Z we get $aX^3 = 0$, which since $a \neq 0$ gives $X = 0$.

So any point of $C \cap \{Z = 0\}$ must have $X = Z = 0$, so it has the form $[0, \alpha, 0]$ for some nonzero α. Finally we can divide across by α without changing the point in $\mathbb{P}^2$, so we get a single point $[0, 1, 0]$.

6. Show that any line through the point $[0, 1, 0] \in \mathbb{P}^2$ is given by an equation of the form

$$aX + bZ = 0$$

for some complex numbers a, b, not both 0.

Solution: A line in $\mathbb{P}^2$ is given by a linear equation

$$aX + bY + cZ = 0$$

where a, b, c are not all zero. If a line L contains the point $[0, 1, 0]$, then substituting in we get

$$a \cdot 0 + b \cdot 1 + c \cdot 0 = 0$$

that is, $b = 0$. So the equation of L is of the form

$$aX + cZ = 0$$

with a, c not both zero.

Notice that if $a = 0$ we just get the line at infinity $\{Z = 0\}$. So a line through $[0, 1, 0]$ that intersects the affine plane must have an equation as above with $a \neq 0$.

7. Show that the curve C in $\mathbb{P}^2$ defined by the equation

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

is not an elliptic curve.

Solution: Here we have

$$\begin{aligned} G(X,Z) &= X^3 - 2X^2Z + XZ^2 \quad \text{hence} \\ G_d(x) &= x^3 - 2x^2 + x \\ &= x(x-1)^2. \end{aligned}$$

Since $G_d(x)$ has only 2 distinct roots, this is not an elliptic curve.

As a remark, this can be seen visually by graphing the curve: we find the curve crosses itself at the point $(1,0)$ (corresponding to the double root above), so the curve has a singular point. (That is not a rigourous proof, but it is good to keep such pictures in mind to understand the meaning of the condition in our definition.)

The following questions are optional and not examinable.

I. Let C be an ellipse given in the form

$$x^2 + \frac{y^2}{\alpha^2} = 1.$$

Show that the length $L(x_0)$ of the arc of C bounded by $x = -1$ and $x = x_0$ is given by

$$L(x_0) = \int_{-1}^{x_0} \frac{1 - \beta^2 x^2}{\sqrt{(1-x^2)(1-\beta^2x^2)}}\, dx$$

where $\beta = 1 - \alpha^2$.

II. (For students who have taken MAC142 *Introduction to Algebraic Geometry*) In this question, you will prove that every nonsingular plane cubic can be put in the form of Equation (3) in the Week 1 notes (at least over $\mathbb{C}$). So let C be a curve in $\mathbb{P}^2$ defined by the equation

$$F(X,Y,Z) = 0$$

where F is a homogeneous cubic.

(a) Prove that C has at least 1 inflection point; that is, a point where the tangent line to C meets C to order 3. You may use the fact that inflection points of C are exactly the common zeroes of F and its *Hessian determinant*

$$H(F) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}$$

(b) Choose an inflection point $p \in C$. Show that there is a projective transformation φ of $\mathbb{P}^2$ which maps the point p to the point $[0, 1, 0]$ and maps the tangent line of C at p to the line defined by $Z = 0$. Deduce that the curve $C' = \varphi(C)$ is defined by an equation $F'(X, Y, Z) = 0$ where F' has no terms in Y^3, XY^2, or X^2Y,

(c) Finally, "complete the square" in Y to eliminate the YZ^2 and XYZ terms in $F'(X, Y, Z)$. Divide across by the coefficient of Y^2Z (which must be nonzero!) to get an equation in the form of Equation (3) in the Week 1 notes.

I will not write down solutions to non-examinable questions like this, but if you are curious please feel free to come and ask me about them!