Professor Joyce **B3.3 Algebraic Curves** **Hilary Term 2019**

Initial problem sheet. Solutions

1. Let $[2,1],[1,1],[3,4]$ be points in the projective line $\mathbb{CP}^1$. Find representative vectors v_1,v_2,v_3 for these points which satisfy $v_1+v_2+v_3=0$.

Solution. Each vector v_i is a multiple x_i of the given vectors. So $v_1+v_2+v_3 = 0$ gives

$$\begin{aligned} 2x_1 + x_2 + 3x_3 &= 0, \\ x_1 + x_2 + 4x_3 &= 0. \end{aligned}$$

Simple elimination gives $x_1 = x_3 = x, x_2 = -5x$, so that

$$v_1 = (2,1), \quad v_2 = (-5,-5), \quad v_3 = (3,4)$$

is a solution.

2. Explain why two photographs taken from the same point, but with the camera pointed in different directions, are related by a projective transformation.

A photograph shows four fence posts beside a straight road. On the photograph, the distances between successive fence posts are 4 inches, 3 inches and 2 inches. Is it possible that the fence posts are evenly spaced? Give reasons.

Solution. Think of the camera as a single point at the origin 0 in $\mathbb{R}^3$. Then points of the projective space $P(\mathbb{R}^3)$ correspond to lines – paths of light rays – in $\mathbb{R}^3$ passing through the camera. Taking a photograph maps such lines, i.e. points in $P(\mathbb{R}^3)$, to points in the photograph, which we think of as a subset of $\mathbb{R}^2$. So a photograph maps a portion of $P(\mathbb{R}^3)$ to a portion of $\mathbb{R}^2$, essentially by *inhomogeneous coordinates*.

Taking two photographs from the same point with the camera pointing in different directions corresponds to transforming between two different sets of inhomogeneous coordinates on $P(\mathbb{R}^3)$, or equivalently, to a projective transformation of $P(\mathbb{R}^3)$.

The edge of the road corresponds to a line $P(\mathbb{R}^2)$ in $P(\mathbb{R}^3)$. The photograph corresponds to a choice of inhomogeneous coordinates on $P(\mathbb{R}^2)$, identifying

$P(\mathbb{R}^2) = \mathbb{R} \cup \{\infty\}$. In these coordinates the fence posts appear at points 0, 4, 7, 9 in $\mathbb{R} \subset P(\mathbb{R}^2)$.

If they were regularly spaced, we could take a photograph in which the fence posts appeared at points 0, 1, 2, 3 in $\mathbb{R}$. So there should exist a projective transformation of $P(\mathbb{R}^2)$ taking points 0, 4, 7, 9 to points 0, 1, 2, 3, respectively. Using material on points in general position in Lecture 3, you can show this is impossible.

3. If a line with slope t intersects the circle $x^2 + y^2 = 1$ in the points $(-1, 0)$ and (x, y), show that x and y are both rational functions of t. (A rational function is one that can be written as the quotient of two polynomials.) By taking $t = p/q$ to be a rational number, construct the general solution of the equation $x^2 + y^2 = z^2$ for which x, y, z are coprime integers.

Solution. We have $x^2 + y^2 = 1$ and $y = t(x + 1)$, so

$$0 = x^2 + t^2(x + 1)^2 - 1 = (x + 1)\big(x - 1 + t^2(x + 1)\big).$$

Since $x \neq -1$, we have $x - 1 + t^2(x + 1) = 0$, so $x = (1 - t^2)/(1 + t^2)$, and thus $y = 2t/(1 + t^2)$.

When $t = p/q$ this gives $x = (q^2 - p^2)/(p^2 + q^2)$ and $y = 2pq/(p^2 + q^2)$, so

$$\left[\frac{q^2 - p^2}{p^2 + q^2}\right]^2 + \left[\frac{2pq}{p^2 + q^2}\right]^2 = 1,$$

and multiplying up gives

$$(q^2 - p^2)^2 + (2pq)^2 = (p^2 + q^2)^2.$$

Hence $x = q^2 - p^2$, $y = 2pq$, $z = p^2 + q^2$ are solutions to $x^2 + y^2 = z^2$ in integers. If p, q are coprime and not both odd then x, y, z are coprime; if p, q are both odd then we need to pass to $x = \frac{1}{2}(q^2 - p^2)$, $y = pq$, $z = \frac{1}{2}(p^2 + q^2)$ to get x, y, z coprime. Since $(x/z)^2 + (y/z)^2 = 1$, we must have $x/z = (1 - t^2)/(1 + t^2) = (q^2 - p^2)/(p^2 + q^2)$ and $y/z = 2t/(1 + t^2) = 2pq/(p^2 + q^2)$ for some $t = p/q$, so this gives all solutions.

4*. Suppose $p(t), q(t)$ and $r(t)$ are pairwise coprime, complex polynomials in t satisfying $p(t)^3 + q(t)^3 + r(t)^3 \equiv 0$. Let $\omega = e^{2\pi i/3}$, so that $\omega^3 = 1$. Then the equation $p(t)^3 + q(t)^3 + r(t)^3 = 0$ may be rewritten as

$$\big(p(t) + q(t)\big)\big(\omega\, p(t) + \omega^2 q(t)\big)\big(\omega^2 p(t) + \omega\, q(t)\big) = \big(-r(t)\big)^3. \qquad (1)$$

(i) Show that $p(t)+q(t)$, $\omega\, p(t)+\omega^2 q(t)$ and $\omega^2 p(t)+\omega\, q(t)$ are pairwise coprime.

(ii) Show that there exist pairwise coprime, complex polynomials $\alpha(t)$, $\beta(t)$ and $\gamma(t)$, such that $p(t)+q(t)\equiv\alpha(t)^3$, $\quad \omega\, p(t)+\omega^2 q(t)\equiv\beta(t)^3$, and $\omega^2 p(t)+\omega\, q(t)\equiv\gamma(t)^3$.

(iii) Deduce that $\alpha(t)^3+\beta(t)^3+\gamma(t)^3\equiv 0$.

[*Two polynomials are coprime if they have no nontrivial common factor.*]

Solution. **(i)** If some nontrivial factor $s(t)$ divides $p(t)+q(t)$ and $\omega\, p(t)+\omega^2 q(t)$ then $s(t)$ divides $p(t), q(t)$ as they are linear combinations of $p(t)+q(t)$ and $\omega\, p(t)+\omega^2 q(t)$, contradicting $p(t), q(t)$ coprime. So $p(t)+q(t)$ and $\omega\, p(t)+\omega^2 q(t)$ are coprime; similarly for the other two pairs.

(ii) Let $s(t)$ be an irreducible factor of $p(t)+q(t)$. Then $s(t)$ divides $(-r(t))^3$ by (1), so $s(t)$ divides $r(t)$ as $s(t)$ is irreducible, and thus $s(t)^3$ divides the l.h.s. of (1). But $s(t)$ does not divide $\omega\, p(t)+\omega^2 q(t)$ or $\omega^2 p(t)+\omega\, q(t)$ by (i). Hence $s(t)^3$ divides $p(t)+q(t)$.

In this way we see that every irreducible factor of $p(t)+q(t)$ occurs with multiplicity a multiple of 3, so $p(t)+q(t)$ is a cube, $p(t)+q(t)\equiv\alpha(t)^3$ for some polynomial $\alpha(t)$. Similarly for $\omega\, p(t)+\omega^2 q(t)$ and $\omega^2 p(t)+\omega\, q(t)$.

(iii) Now we have

$$\alpha(t)^3+\beta(t)^3+\gamma(t)^3\equiv\big(p(t)+q(t)\big)+\big(\omega\, p(t)+\omega^2 q(t)\big)+\big(\omega^2 p(t)+\omega\, q(t)\big)=0$$

since $1+\omega+\omega^2=0$.

5*. Using your answer to Question 4, prove that $p(t)$, $q(t)$ and $r(t)$ must be constant.

[*Hint: consider the degrees of* p, q, r *and* α, β, γ.]

Solution. Suppose we can find $p(t), q(t), r(t)$ not all constant in Question 4. Choose such p, q, r of minimal total degree. But then we can replace p, q, r by α, β, γ, which satisfy the same equation, are not all constant, and have smaller total degree (as $\deg\alpha=\frac{1}{3}\deg p$, and so on), a contradiction. Thus p, q, r are constant.

6*. Using Questions 4 and 5, show that there do not exist nonconstant rational functions $x(t)$, $y(t)$, such that $x(t)^3+y(t)^3+1\equiv 0$. How does this compare with Question 3?

Solution. If we could find such rational functions $x(t), y(t)$, say $x(t) = a(t)/b(t)$, $y(t) = c(t)/d(t)$ for $a(t), \ldots, d(t)$ polynomials with $c(t), d(t)$ not identically zero, then the polynomials $p(t) = a(t)d(t)$, $q(t) = b(t)c(t)$ and $r(t) = c(t)d(t)$ satisfy $p(t)^3 + q(t)^3 + r(t)^3 \equiv 0$. Hence $p(t), q(t), r(t)$ are constant, so $a(t), b(t), c(t), d(t)$ are constant, and $x(t), y(t)$ are constant.

Thus, from Question 3 we can parametrize the solutions of the equation $x^2 + y^2 = 1$ in $\mathbb{C}^2$ using rational functions, but from Questions 4-6 we cannot parametrize the solutions of the equation $x^3 + y^3 = 1$ in $\mathbb{C}^2$ using rational functions.

In terms of material later in the course, this is because the curve C defined by $x^2 + y^2 = z^2$ in $\mathbb{CP}^2$ has genus zero, so is a sphere $\mathcal{S}^2$, and is isomorphic to $\mathbb{CP}^1$ which is also a sphere $\mathcal{S}^2$. So we can find a map $\mathbb{CP}^1 \to C \subset \mathbb{CP}^2$ which parametrizes C using rational functions. But the curve C' defined by $x^3 + y^3 = z^3$ in $\mathbb{CP}^2$ has genus one, so is a torus T^2, and is not isomorphic to $\mathbb{CP}^1$. Thus we cannot parametrize C' by a map from $\mathbb{CP}^1$, that is, we cannot parametrize C' using rational functions.