MATH3354 Assignment 4

August 22, 2019

Problem 1

Proof. We represent $\mathbb{P}^3$ in the coordinates $\mathbb{P}^3 = \{[W : X : Y : Z]\}$. The four open sets for our affine charts are then the intersections of the sets $U_0 = \{W \neq 0\}, U_1, U_2, U_3$ with Q, so we get the sets

$$\begin{aligned}
X_0 &= \{[W : X : Y : Z] : W \neq 0 \text{ and } XY - ZW = 0\}\\
X_1 &= \{[W : X : Y : Z] : X \neq 0 \text{ and } XY - ZW = 0\}\\
X_2 &= \{[W : X : Y : Z] : Y \neq 0 \text{ and } XY - ZW = 0\}\\
X_3 &= \{[W : X : Y : Z] : Z \neq 0 \text{ and } XY - ZW = 0\}
\end{aligned}$$

All of these are open in Q. We can now define the following maps to affine space:

$$\begin{aligned}
\phi_0([W : X : Y : Z]) &= (X/W, Y/W, Z/W)\\
\phi_1([W : X : Y : Z]) &= (W/X, Y/X, Z/X)\\
\phi_2([W : X : Y : Z]) &= (W/Y, X/Y, Z/Y)\\
\phi_3([W : X : Y : Z]) &= (W/Z, X/Z, Y/Z)
\end{aligned}$$

These are all continuous where they are defined since they are quotients of polynomials with nonzero denominator. They are also well-defined since each component function is homogeneous so the output value is independent of the representative element we choose from each scaling class in $\mathbb{P}^3$. Alternatively, these functions are continuous because they are restrictions of functions that we showed were continuous as an example in lectures. We also define

$$\begin{aligned} V_0 &= V(X_1X_2 - X_3) \subset \mathbb{A}^3 \\ V_1 &= V(X_2 - X_1X_3) \subset \mathbb{A}^3 \\ V_2 &= V(X_2 - X_1X_3) \subset \mathbb{A}^3 \\ V_3 &= V(X_2X_3 - X_1) \subset \mathbb{A}^3 \end{aligned}$$

where we are using different variables for (dehomogenised) polynomials over $\mathbb{A}^3$ to keep them notationally distinct. Each V_i is closed so is an affine variety. We claim that each $\phi_i : X_i \to V_i$ is a homeomorphism, and so the (X_i, V_i, ϕ_i) are affine charts for Q. We will prove this for ϕ_0, since the other three proofs are analogous.

First, ϕ_0 has the codomain we claim because if $[W : X : Y : Z] \in X_0$ then $XY - ZW = 0$, and so because $W \neq 0$ we may divide through to obtain $\frac{XY}{W^2} - \frac{Z}{W} = 0$. Then

$$\phi_0([W : X : Y : Z]) = (X/W, Y/W, Z/W)$$

and so $X_1X_2 - X_3 = (X/W) \cdot (Y/W) - (Z/W) = 0$. Hence we have that $\phi_0([W : X : Y : Z]) \in V_0$. Now, to show ϕ_0 has a continuous inverse, we construct an explicit inverse. Define

$$\begin{aligned} \psi_0 &: V_0 \to X_0 \\ (x, y, z) &\mapsto [1 : x : y : z] \end{aligned}$$

This map has the correct codomain since if $(x, y, z) \in V_0$ then from the defining polynomial of V_0, we have $xy - z = 0$. Hence $xy - z \cdot 1 = 0$ and so $[1 : x : y : z] \in X_0$. Also, ψ_0 is continuous since it is defined by polynomial functions in each coordinate. It remains to check that ψ_0, ϕ_0 are inverse. We have

$$\begin{aligned} (\psi_0 \circ \phi_0)([W : X : Y : Z]) &= \psi_0(X/W, Y/W, Z/W) \\ &= [1 : X/W : Y/W : Z/W] \\ &= [W : X : Y : Z] \\ (\phi_0 \circ \psi_0)(x, y, z) &= \phi_0([1 : x : y : z]) \\ &= (x/1, y/1, z/1) \\ &= (x, y, z) \end{aligned}$$

Thus ψ_0, ϕ_0 are inverse homeomorphisms. Hence (X_0, V_0, ϕ_0) is an affine chart. To check that ϕ_1, ϕ_2, ϕ_3 are also homeomorphisms, we note that they are all continuous since they consist of rational functions with nonzero denominator in each coordinate, and we can write down explicit inverses as follows.

$$\begin{aligned} \psi_1 : V_1 &\to X_1 \\ (w, y, z) &\mapsto [w : 1 : y : z] \\ \psi_2 : V_2 &\to X_2 \\ (w, x, z) &\mapsto [w : x : 1 : z] \\ \psi_3 : V_3 &\to X_3 \\ (w, x, y) &\mapsto [w : x : y : 1] \end{aligned}$$

Checking that these all compose to the identity correctly is a tedious computation much like the one above, so has been omitted. All of the ψ_i are continuous, so after checking that the appropriate compositions are the identity we may conclude that the (X_i, V_i, ϕ_i) are indeed affine charts for Q. It remains to check only that the affine charts are compatible on their intersection.

We will check only the transition function on $X_0 \cap X_3$. We consider the following diagram, with transition functions $\phi_{0,3}$ and $\phi_{3,0}$.

$$\begin{tikzcd} X_0 \cap X_3 \subset X_0 \arrow[r, "id_{X_0 \cap X_3}"] \arrow[d, "\phi_0"'] & X_0 \cap X_3 \subset X_3 \arrow[d, "\phi_3"] \\ \phi_0(X_0 \cap X_3) \arrow[r, dashed, "\phi_{0,3}"] & \phi_3(X_0 \cap X_3) \arrow[l, dashed, bend left, "\phi_{3,0}"] \end{tikzcd}$$

To find the transition functions, we perform a diagram chase. For $(a, b, c) \in \phi_0(X_0 \cap X_3)$, we have

$$\phi_{0,3}(a, b, c) = \phi_3(\phi_0^{-1}(a, b, c)) = \phi_3([1 : a : b : c]) = (1/c, a/c, b/c)$$

and since $(a, b, c) \in \phi_0(X_0 \cap X_3)$ must satisfy $c \neq 0$, this is well-defined and regular since it is a rational function with nonzero denominator in each coordinate.

For the other transition map, given $(a, b, c) \in \phi_3(X_0 \cap X_3)$, we have

$$\phi_{3,0}(a, b, c) = \phi_0(\phi_3^{-1}(a, b, c)) = \phi_0([a : b : c : 1]) = (b/a, c/a, 1/a)$$

This is well-defined and regular since $(a, b, c) \in \phi_3(X_0 \cap X_3)$ must satisfy $a \neq 0$, so $\phi_{3,0}$ is a rational function with nonzero denominator in each coordinate. Hence both transition maps are regular, as required. $\square$

Problem 2

In order to differentiate between the affine and projective closures of X, we use the following notation. Let

$$X_{\mathbb{P}^n} = \{[x : 1] \in \mathbb{P}^n : x \in X\}$$

where $X \subset \mathbb{A}^n$ is some set in affine space. Then we use $\overline{X_{\mathbb{P}^n}}$ to denote the projective closure of X, i.e. the smallest closed set in $\mathbb{P}^n$ that contains this embedding of X into $\mathbb{P}^n$. We first prove a general theorem about the projective closure which will make the given examples easier to compute.

Theorem. *For $X \subset A^n$, the projective closure of X is*

$$\overline{X_{\mathbb{P}^n}} = V(\{p^{hom} : p \in I(X)\}).$$

Remark. Here $I(X) \subset k[X_0, \ldots, X_{n-1}]$ is the usual ideal corresponding to a subset of affine space, and is not necessarily graded.

Proof. Let $F = V(\{p^{hom} : p \in I(X)\})$. We will first show that $\overline{X_{\mathbb{P}^n}} \subset F$. We observe that since F is closed, it is sufficient to prove that $X_{\mathbb{P}^n} \subset F$ because taking the closure is an inclusion-preserving operation and $\overline{F} = F$.

So, let $p \in I(X)$ and $\tilde{x} \in X_{\mathbb{P}^n}$ be chosen arbitrarily. Then $\tilde{x} = [x_0 : \ldots : x_n]$ with each $x_i \in k$. Also, by definition of $X_{\mathbb{P}^n}$ we know that $x_n \neq 0$ and $(x_0/x_n, \ldots, x_{n-1}/x_n) \in X$. Then

$$p^{hom}(\tilde{x}) = x_n^{deg(p)} p(x_0/x_n, \ldots, x_{n-1}/x_n) = x_n^{deg(p)} p(x) = 0$$

since $p \in I(X)$. Since $p \in I(X)$ was arbitrary, $\tilde{x} \in F$, and since $\tilde{x} \in X_{\mathbb{P}^n}$ was arbitrary, $X_{\mathbb{P}^n} \subset F$. Hence $\overline{X_{\mathbb{P}^n}} \subset F$ as we wanted.

For the other inclusion, we note that since $\overline{X_{\mathbb{P}^n}}$ is closed in $\mathbb{P}^n$, there exists a set $S \subset k[X_0, \ldots, X_n]$ of homogeneous polynomials with $\overline{X_{\mathbb{P}^n}} = V(S)$. Let $q \in S$, $\tilde{y} \in F$.

We claim that $q(\tilde{y}) = 0$. To prove this, define $p \in k[X_0, \ldots, X_{n-1}]$ by

$$p(x_0, \ldots, x_{n-1}) = q(x_0, \ldots, x_{n-1}, 1).$$

Then $p \in I(X)$. To show this, given $x \in X$, we have $[x : 1] \in X_{\mathbb{P}^n}$. Then

$$p(x) = q(x, 1) = 0$$

since $q \in S$ and $X_{\mathbb{P}^n} \subset V(S)$ so $q(X_{\mathbb{P}^n}) = 0$. Since $x \in X$ was arbitrary, $p \in I(X)$.

We next claim that

$$q = x_n^{deg(q)-deg(p)} p^{hom}.$$

To prove this, we observe that

$$\begin{aligned} p^{hom}(x_0, \ldots, x_n) &= x_n^{deg(p)} p(x_0/x_n, \ldots, x_{n-1}/x_n) \\ &= x_n^{deg(p)} q(x_0/x_n, \ldots, x_{n-1}/x_n). \end{aligned}$$

Then since q is homogeneous, $q(x_0, \ldots, x_n) = x_n^{deg(q)} q(x_0/x_n, \ldots, x_{n-1}/x_n)$. So, multiplying both sides of our first equality by $x_n^{deg(q)-deg(p)}$, we obtain

$$\begin{aligned} x_n^{deg(q)-deg(p)} p^{hom}(x_0, \ldots, x_n) &= x_n^{deg(q)-deg(p)+deg(p)} q(x_0/x_n, \ldots, x_{n-1}/x_n) \\ &= x_n^{deg(q)} q(x_0/x_n, \ldots, x_{n-1}/x_n) \\ &= q(x_0, \ldots, x_n) \end{aligned}$$

which is the equality we claimed. Finally, we have

$$q(\tilde{y}) = p^{hom}(\tilde{y}) \tilde{y}_n^{deg(q)-deg(p)} = 0$$

since $\tilde{y} \in F$ and $F \subset V(p^{hom})$. Since $q \in S$ was arbitrary, $\tilde{y} \in V(S) = \overline{X_{\mathbb{P}^n}}$. Then since $\tilde{y} \in F$ was arbitrary, $F \subset \overline{X_{\mathbb{P}^n}}$.

We thus have both set inclusions, and so $F = \overline{X_{\mathbb{P}^n}}$ as we wanted. □

(a) *Proof.* We are given $X = V(x^2 + y^2 - 1) \subset \mathbb{A}^2$. We have:

$$\begin{aligned} \overline{X_{\mathbb{P}^2}} &= V(\{p^{hom} : p \in I(X)\}) && \text{by the theorem} \\ &= V(\{p^{hom} : p \in I(V(x^2 + y^2 - 1))\}) && \text{by def. of } X \\ &= V(\{p^{hom} : p \in \sqrt{\langle x^2 + y^2 - 1 \rangle}\}) && \text{by Nullstellensatz} \\ &= V(\{p^{hom} : p \in \langle x^2 + y^2 - 1 \rangle\}) \end{aligned}$$

since $x^2 + y^2 - 1$ is irreducible, the ideal $\langle x^2 + y^2 - 1 \rangle$ is radical

$$\begin{aligned} &= V(\{(q \cdot (x^2 + y^2 - 1))^{hom} : q \in k[x, y]\}) && \text{by def. of an ideal} \\ &= V(\{q^{hom} \cdot (x^2 + y^2 - 1)^{hom} : q \in k[x, y]\}) && \text{see below} \\ &= V(\{q^{hom} \cdot (x^2 + y^2 - z^2) : q \in k[x, y]\}) \\ &= V(\{q^{hom} : q \in k[x, y]\}) \cup V(x^2 + y^2 - z^2) \end{aligned}$$

this is because $V(IJ) = V(I) \cup V(J)$

$$\begin{aligned} &= \emptyset \cup V(x^2 + y^2 - z^2) \\ &= V(x^2 + y^2 - z^2) \subset \mathbb{P}^2. \end{aligned}$$

We note that $f = x^2+y^2-1$ is irreducible by the generalised Eisenstein criterion, using $y-1$, since if we view f as a polynomial in x then the constant term is $(y-1)(y+1)$ which is divisible by $y-1$. In the above simplification, we used the fact that for $p, q \in k[X_0, \ldots, X_{n-1}]$ we have $(p \cdot q)^{hom} = p^{hom} q^{hom}$. A proof of this fact is given below. We have

$$\begin{aligned}
&(p \cdot q)^{hom}(X_0, \ldots, X_n) \\
=&x_n^{deg(pq)} \cdot (p \cdot q)(X_0/X_n, \ldots, X_{n-1}/X_n) \\
=&x_n^{deg(p)+deg(q)} \cdot p(X_0/X_n, \ldots, X_{n-1}/X_n) \cdot q(X_0/X_n, \ldots, X_{n-1}/X_n) \\
=&x_n^{deg(p)} \cdot p(X_0/X_n, \ldots, X_{n-1}/X_n) \cdot x_n^{deg(q)} \cdot q(X_0/X_n, \ldots, X_{n-1}/X_n) \\
=&p^{hom}(X_0, \ldots, X_n) \cdot q^{hom}(X_0, \ldots, X_n)
\end{aligned}$$

so we have the equality we claimed.

Now, to find the points at infinity in $\overline{X_{\mathbb{P}^2}}$, we solve for $[x : y : z] \in V(x^2 + y^2 - z^2)$ such that $z = 0$. We get $x^2 + y^2 = 0$, and so over an algebraically closed field k with $char(k) \neq 2$ we get

$$y = \pm\sqrt{-1}x.$$

The two square roots of -1 are distinct for $char(k) \neq 2$, so there are 2 points at infinity, namely

$$[1 : \sqrt{-1} : 0] \text{ and } [1 : -\sqrt{-1} : 0].$$

When $char(k) = 2$, the only square root of -1 is 1 so the only point at infinity is $[1 : 1 : 0]$. The projective closure of X is $V(x^2+y^2-z^2) \subset \mathbb{P}^2$, as calculated above. $\square$

(b) *Proof.* We are given $X = V(y - x^2, z - x^3)$. As above, we use the theorem to obtain an expression for $\overline{X_{\mathbb{P}^3}}$. We have

$$\begin{aligned}
\overline{X_{\mathbb{P}^3}} &= V(\{p^{hom} : p \in I(X)\}) && \text{by the theorem} \\
&= V(\{p^{hom} : p \in I(V(y - x^2, z - x^3))\}) && \text{by def. of } X \\
&= V(\{p^{hom} : p \in \sqrt{\langle y - x^2, z - x^3\rangle}\}) && \text{by the Nullstellensatz}
\end{aligned}$$

However, we cannot simplify any further because in this case it is not obvious that $\langle y - x^2, z - x^3\rangle$ is radical. Instead, we let T be the set of points at infinity contained in $\overline{X_{\mathbb{P}^3}}$.

We claim that $T = \{[0 : 0 : 1 : 0]\}$. We will prove this by two set inclusions.

First we will prove that $T \subset \{[0:0:1:0]\}$. Consider $y - x^2 \in I(X)$. We have

$$(y - x^2)^{hom} = yw - x^2$$

and so any point at infinity $a = [a_0 : a_1 : a_2 : 0] \in T$ must satisfy

$$0 = a_1 \cdot 0 - a_0^2 = a_0^2$$

and so $a_0^2 = 0$. Hence $a = [0 : a_1 : a_2 : 0]$. Now, we claim that the polynomial $y^3 - z^2 \in I(X)$. To see this, we note that every point $(x, y, z) \in X$ satisfies $y - x^2 = 0 = z - x^3$, and so $y = x^2$ and $z = x^3$. Hence $y^3 = x^6 = z^2$ and so $y^3 - z^2 = 0$. Since this polynomial relation is satisfied by every point in X, we have $y^3 - z^2 \in I(X)$. Hence $a \in \overline{X_{\mathbb{P}^3}}$ must be in the vanishing set of $(y^3 - z^2)^{hom} = y^3 - z^2 w$ and so we have $a_1^3 = 0$ and hence $a_1 = 0$. Therefore $a = [0:0:a_2:0] = [0:0:1:0]$ since $[0:0:0:0] \notin \mathbb{P}^3$ so we know $a_2 \neq 0$. Hence the only possible point at infinity in $\overline{X_{\mathbb{P}^3}}$ is $[0:0:1:0]$.

Next, to show that this point is actually in $\overline{X_{\mathbb{P}^3}}$, we define a function. Let $f : \mathbb{A}^1 \to \mathbb{P}^3$ be given by

$$f(t) = [t^2 : t : 1 : t^3].$$

overkill. Enough to know f is cont.

We claim that f is a homeomorphism to its image. To see this, we note that f is given by polynomial functions in each coordinate, so is continuous (and, in fact, regular). Also, f has a regular inverse given by $[a : b : c : d] \mapsto \frac{b}{c}$. This inverse is well-defined and continuous since every point in the image has third coordinate nonzero. So f is a homeomorphism, and a regular isomorphism.

We next observe that $f(\mathbb{A}^1 \setminus \{0\}) \subset X_{\mathbb{P}^3}$. To see this, we note that for $t \neq 0$, we have

$$f(t) = [t^2 : t : 1 : t^3] = \left[\frac{1}{t} : \frac{1}{t^2} : \frac{1}{t^3} : 1\right]$$

where we are scaling in each coordinate by the nonzero constant $\frac{1}{t^3}$. We see that $\left(\frac{1}{t}, \frac{1}{t^2}, \frac{1}{t^3}\right)$ satisfies $y - x^2 = 0$ and $z - x^3 = 0$. Hence the first three coordinates of $f(t)$ give a point in $V(y - x^2, z - x^3) = X$, and so by definition of $X_{\mathbb{P}^3}$ we have $f(t) \in X_{\mathbb{P}^3}$.

~~Finally, since f is a homeomorphism we have that $f(\overline{A}) = \overline{f(A)}$ for any set A contained in the domain of f. (This is a fairly straightforward topological result)~~. We consider $A = \mathbb{A}^1 \setminus \{0\}$. The set A is open, so it

This is not true! But for any continuous f, we have $f(\overline{A}) \subset \overline{f(A)}$. This is all we need here.

is dense, and hence $\overline{A} = \mathbb{A}^1$. So, $\overline{f(A)} = f(\overline{A}) = f(\mathbb{A}^1)$. Since $f(A) \subset X_{\mathbb{P}^3}$ and taking the closure is inclusion preserving, we have $\overline{f(A)} \subset \overline{X_{\mathbb{P}^3}}$. So, $f(\mathbb{A}^1) \subset \overline{X_{\mathbb{P}^3}}$. In particular, $f(0) = [0:0:1:0] \in f(\mathbb{A}^1)$ and so $[0:0:1:0] \in \overline{X_{\mathbb{P}^3}}$. This is the inclusion we wanted.

Hence the only point at infinity in $\overline{X_{\mathbb{P}^3}}$ is $[0:0:1:0]$, as we claimed.

We can now use this information to write out the closure $\overline{X_{\mathbb{P}^3}}$ more explicitly. We claim that

$$\overline{X_{\mathbb{P}^3}} = V(yw - x^2, zw^2 - x^3, y^3 - z^2w).$$

To see this, we first note that $\overline{X_{\mathbb{P}^3}} \subset V(yw - x^2, zw^2 - x^3, y^3 - z^2w)$ since these three polynomials are all homogenisations of polynomials in $I(X)$ — specifically, they are $(y - x^2)^{hom}$, $(z - x^3)^{hom}$ and $(y^3 - z^2)^{hom}$. The first two polynomials are in $I(X)$ by definition, and we proved that $y^3 - z^2 \in I(X)$ above. For the other set inclusion, we consider two cases. Suppose $a = [a_0 : a_1 : a_2 : a_3] \in V(yw - x^2, zw^2 - x^3, y^3 - z^2w)$ with $a_3 = 0$. Then a_0, a_1, a_2 must satisfy $a_0^2 = 0 = a_1^3$, so $a_0 = a_1 = 0$. Hence a is the point at infinity $[0:0:1:0]$, so is in $\overline{X_{\mathbb{P}^3}}$. Next consider the case $a_3 \neq 0$. Without loss of generality, we may scale to obtain $a = [a_0 : a_1 : a_2 : 1]$. Then a_0, a_1, a_2 must satisfy $y - x^2 = 0$ and $z - x^3 = 0$, so $(a_0, a_1, a_2) \in V(y - x^2, z - x^3) = X$. Hence $a \in X_{\mathbb{P}^3}$, and so $a \in \overline{X_{\mathbb{P}^3}}$.

We may thus conclude in either case that $a \in \overline{X_{\mathbb{P}^3}}$, and so $V((yw - x^2, zw^2 - x^3, y^3 - z^2w) \subset \overline{X_{\mathbb{P}^3}}$. Since we have both set inclusions, we have shown that

$$\overline{X_{\mathbb{P}^3}} = V(yw - x^2, zw^2 - x^3, y^3 - z^2w)$$

as we claimed. $\square$

Note that we have proved a specific case of a general result here. The reason the explicit presentation that we chose for $\overline{X_{\mathbb{P}^3}}$ works is that the points in $\overline{X_{\mathbb{P}^3}}$ are exactly the points in $X_{\mathbb{P}^3}$, plus some points at infinity. So, to find an expression for the closure it is sufficient to choose some elements of $I(X)$ such that the homogenised versions of these polynomials restrict the possible points at infinity to those in $\overline{X_{\mathbb{P}^3}}$. This is how the expression we used for the closure was motivated and constructed.

Problem 3

Proof. Let $X = \{p_1, p_2, p_3, p_4, p_5\}$ be our 5 distinct points, where each $p_i = [x_i : y_i : z_i]$ in projective coordinates. We define the following matrix using the coordinates of our 5 points.

$$M := \begin{bmatrix} x_1^2 & y_1^2 & z_1^2 & x_1y_1 & x_1z_1 & x_1z_1 \\ x_2^2 & y_2^2 & z_2^2 & x_2y_2 & x_2z_2 & x_2z_2 \\ x_3^2 & y_3^2 & z_3^2 & x_3y_3 & x_3z_3 & x_3z_3 \\ x_4^2 & y_4^2 & z_4^2 & x_4y_4 & x_4z_4 & x_4z_4 \\ x_5^2 & y_5^2 & z_5^2 & x_5y_5 & x_5z_5 & x_5z_5 \end{bmatrix}$$

Note that this is only well-defined up to scaling of each row, since these coordinates are projective. However, we will just fix x_1, x_2, x_3, x_4, x_5 so that we can think of this matrix as containing elements of k. We now consider the following equation, for $A, B, C, D, E, F \in k$.

$$M \cdot \begin{bmatrix} A \\ B \\ C \\ D \\ E \\ F \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Solutions to this equation in A, B, C, D, E, F are precisely homogeneous polynomials $G = Ax^2 + By^2 + Cz^2 + Dxy + Exz + Fyz$ such that $X \subset V(G)$. That is, the corresponding conic contains all 5 of our points. We wish to show that there exists a unique such conic. Since any conic in projective space has a unique polynomial equation up to scaling of the coefficients by a constant (since scaling a polynomial doesn't change its vanishing set), we wish to show that $ker(M)$ has dimension 1. Then $ker(M)$ contains a unique vector (A, B, C, D, E, F) up to scaling, and so there is a unique conic containing all 5 points.

We will show that $dim(ker(M)) = 1$ by showing that $rank(M) = 5$. Then by the rank-nullity theorem, since $M : k^6 \to k^5$, we have

$$dim(ker(M)) + rank(M) = 6$$

and so $dim(ker(M)) = 1$, as we wanted. We note first that M has 5 rows, so its rank is at most 5. To get the other inequality, we will prove that M is surjective by proving that it contains a basis for k^5 in its image. Let e_1, e_2, e_3, e_4, e_5 be the standard basis vectors in k^5, and let W_G denote the coefficient vector (A, B, C, D, E, F) of the homogeneous quadratic polynomial G. We notice that the ith component of the vector $M \cdot W_G$ will be 0 precisely when $p_i \in V(G)$ and will be nonzero otherwise. So, we know that

$$M \cdot W_G = re_i \iff \text{the conic } V(G) \text{ does not contain } p_i\text{, and does contain the other four of our points.}$$

Here $r \in k$ is some nonzero scalar. If $M \cdot W_G = re_i$ then we may simply scale the coefficients in W_G by $\frac{1}{\sqrt{r}}$ to get $M \cdot W_G = e_i$, so e_i is in the image of M. (This scaling will give us the output we want because M is linear, so it will have the result of scaling the output vector. Scaling only affects the nonzero components, so this will gives us precisely e_1.) Hence in order to prove M is surjective, we only need to construct some conic $V(G)$ such that $p_i \notin V(G)$ and the other four points are in $V(G)$. To do this, let $p_{j_1}, p_{j_2}, p_{j_3}, p_{j_4}$ be the four points that aren't p_i. Then p_{j_1}, p_{j_2} are distinct points in projective space, so they define a unique line. Denote this $L(p_{j_1}, p_{j_2})$. Similarly, let $L(p_{j_3}, p_{j_4})$ be the unique line containing p_{j_3}, p_{j_4}. Now, since no three of our original 5 points are colinear, $L(p_{j_3}, p_{j_4})$ and $L(p_{j_1}, p_{j_2})$ are distinct lines so they define a (degenerate) conic $V(G_i) = L(p_{j_1}, p_{j_2}) \cup L(p_{j_3}, p_{j_4})$. Then $V(G_i)$ contains $p_{j_1}, p_{j_2}, p_{j_3}, p_{j_4}$ by construction. Also, it doesn't contain p_i since every point in $V(G_i)$ is either colinear with p_{j_3}, p_{j_4} or colinear with p_{j_1}, p_{j_2}, but no three of our 5 original points were colinear. Hence $V(G_i)$ is the required conic for e_i, and so its coefficient vector W_{G_i} is such that $M \cdot W_{G_i} = e_i$ as we wanted. Therefore M is surjective, and so $rank(M) = 5$.

We may thus apply the rank nullity theorem to conclude that

$$dim(ker(M)) = 1.$$

Then the unique (up to scaling) non-zero vector in $ker(M)$ provides the coefficients for the homogeneous quadratic equation of the unique conic containing our 5 original points. $\square$

Problem 4

Proof. We note that if $s = 0$ then the conic $Q_{s:t} = V(tG)$. Since $[s : t] \in \mathbb{P}^1$, $t \neq 0$ and so this conic is non-degenerate because G is irreducible. Hence we may assume without loss of generality that $s \neq 0$, since we are only interested in finding all of the degenerate conics in the pencil. Since $s \neq 0$, we may take the representative coordinates with $s = 1$ from each set of projective coordinates $[s : t]$. The problem then becomes to prove that there are exactly 3 values for $t \in k$ such that $V(F + tG)$ is degenerate, for F, G irreducible homogeneous degree 2 polynomials in $k[X, Y, Z]$.

We first show that there are at most 3 such values of t. Let

$$F(X, Y, Z) = F_1X^2 + F_2Y^2 + F_3Z^2 + F_4XY + F_5XZ + F_6YZ$$

and

$$G(X, Y, Z) = G_1X^2 + G_2Y^2 + G_3Z^2 + G_4XY + G_5XZ + G_6YZ$$

be our two irreducible polynomials, with each $F_i, G_j \in k$. We know from the week 5 workshop that $V(F + tG)$ is degenerate iff its matrix of coefficients has zero as an eigenvalue, where the matrix of coefficients is given by

$$M_{coeff} = \begin{bmatrix} F_1 + tG_1 & \frac{F_4+tG_4}{2} & \frac{F_5+tG_5}{2} \\ \frac{F_4+tG_4}{2} & F_2 + tG_2 & \frac{F_6+tG_6}{2} \\ \frac{F_5+tG_5}{2} & \frac{F_6+tG_6}{2} & F_3 + tG_3 \end{bmatrix}.$$

Since this matrix of coefficients is symmetric, it is always diagonalisable. Hence it has zero as an eigenvalue iff its determinant is zero, since its determinant is the same as the determinant of its diagonalisation, which is just the product of the eigenvalues of M_{coeff}. Combining these two facts, we know that $V(F + tG)$ is degenerate iff $det(M_{coeff}) = 0$. Expanding $det(M_{coeff})$ as a polynomial in t, we obtain a degree 3 single-variable polynomial via the cofactor expansion. Hence this has at most three solutions in t, and so there are at most 3 values of $t \in k$ such that $V(F + tG)$ is degenerate.

To show that 3 such values of t exist, we first prove a useful lemma.

Lemma. *If a conic $V(H)$ has 3 colinear points then it is degenerate, and contains the line containing those three points.*

In lectures, we proved that if a conic contains 3 colinear points then it contains the entire line these points lie on. Hence $V(H)$ contains a linear component. Then H has a linear factor, and the remaining factor must also be linear. Hence H is reducible, so $V(H)$ is degenerate.

That concludes the proof of the lemma.

Now, to choose values of t which produce degenerate conics in the pencil, let $\{v_1, v_2, v_3, v_4\} = V(F) \cap V(G)$ be the four points of intersection of the two given non-degenerate conics. These points are distinct by assumption. Also, no three of them are colinear. To see this, we note that if three of them were colinear then $V(F)$ would contain 3 colinear points, and so by the lemma $V(F)$ would be degenerate so F would be reducible. This contradicts one of our assumptions, so in fact no three of the v_i can be colinear. Hence any pair v_i, v_j with $i \neq j$ defines a unique line (the line passing through both of these points), and the 6 lines thus defined are all distinct since if two such lines were equal, at least three of the v_i would be colinear. Using these 6 distinct lines, we next define 3 useful points. Let

$$\begin{aligned} a_1 &= L(v_1, v_2) \cap L(v_3, v_4) \\ a_2 &= L(v_1, v_3) \cap L(v_2, v_4) \\ a_3 &= L(v_1, v_4) \cap L(v_2, v_3) \end{aligned}$$

where $L(v_i, v_j)$ is the unique line passing through v_i, v_j. Each of these a_i is uniquely defined since any two distinct lines in projective space intersect in precisely one point. Next, set $t_i = \frac{-F(a_i)}{G(a_i)}$. This is well-defined since each a_i is colinear with a pair of other points in $V(G)$, so cannot be in $V(G)$ — if it were, $V(G)$ would contain 3 colinear points and would thus be degenerate, but $V(G)$ is non-degenerate because G is irreducible. Then

$$(F + t_iG)(a_i) = F(a_i) + \frac{-F(a_i)}{G(a_i)}G(a_i) = 0$$

and $(F + t_iG)(v_j) = F(v_j) + tG(v_j) = 0$ since $v_j \in V(F) \cap V(G)$. So, each $V(F + t_iG)$ contains a_i and also the four points in $V(F) \cap V(G)$, so it contains two sets of three colinear points. By the lemma, we thus have that each $V(F + t_iG)$ is degenerate.

Also, for $i = 1, 2, 3$ we obtain distinct conics, since $V(F + t_1G) = L(v_1, v_2) \cup L(v_3, v_4)$ is the union of the lines spanned by its two sets of three collinear points, and similarly for $V(F + t_2G)$ and $V(F + t_3G)$. Since these 6 lines are all distinct, the three conics are distinct and so we have found 3 degenerate conics in the pencil.

Hence there are exactly three degenerate conics in the pencil, given by

$$\begin{aligned} V(F + t_1G) &= L(v_1, v_2) \cup L(v_3, v_4) \\ V(F + t_2G) &= L(v_1, v_3) \cup L(v_2, v_4) \\ V(F + t_3G) &= L(v_1, v_4) \cup L(v_2, v_3) \end{aligned}$$

where v_1, v_2, v_3, v_4 are the intersection points of the non-degenerate conics $V(F)$ and $V(G)$. $\square$