MA40188 ALGEBRAIC CURVES 2015/16 SEMESTER 1
BRIEF EXAM SOLUTIONS

Problem 1

(a) The ideal of X is $\mathbb{I}(X) = \{f \in \Bbbk[x_1, \cdots, x_n] \mid f(p) = 0 \ \forall\ p \in X\}$. The coordinate ring of X is $\Bbbk[X] = \Bbbk[x_1, \cdots, x_n]/\mathbb{I}(X)$. We say X is irreducible if it cannot be written as the union of two strictly smaller algebraic sets. If X is irreducible, then $\mathbb{I}(X)$ is a prime ideal. [bookwork, 4]

(b) One direction: If $X = \mathbb{V}(I)$, then by Nullstellensatz we have $\mathbb{I}(X) = \mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = I$ since I is a radical ideal. The other direction: Assume $I = \mathbb{I}(X)$. Write $X = \mathbb{V}(J)$ for some ideal $J \subseteq \Bbbk[x_1, \cdots, x_n]$. By Nullstellensatz, $\mathbb{V}(I) = \mathbb{V}(\mathbb{I}(X)) = \mathbb{V}(\mathbb{I}(\mathbb{V}(J))) = \mathbb{V}(\sqrt{J})$. Since $\sqrt{J} \supseteq J$, we have $\mathbb{V}(I) = \mathbb{V}(\sqrt{J}) \subseteq \mathbb{V}(J) = X$. For every point $p \in X$, since $I = \mathbb{I}(X)$, we have $f(p) = 0$ for every $f \in I$. It follows that $p \in \mathbb{V}(I)$ hence $X \subseteq \mathbb{V}(I)$. Then we conclude that $X = \mathbb{V}(I)$. [bookwork, 4]

(c) Consider the homomorphism $\varphi : \Bbbk[x_1, \cdots, x_n] \to \Bbbk$ defined by $\varphi(f) = f(a_1, \cdots, a_n)$. Every $a \in \Bbbk$ is the image of the constant polynomial a, hence φ is surjective and $\operatorname{im} \varphi = \Bbbk$. Every polynomial $f \in \Bbbk[x_1, \cdots, x_n]$ can be written in the form of $f = (x_1 - a_1)g_1 + \cdots + (x_n - a_n)g_n + r$ for some polynomials $g_1, \cdots, g_n$ and a constant $r \in \Bbbk$. This can be seen by replacing each x_i by $[(x_i - a_i) + a_i]$ throughout, expanding the square brackets while leaving the round brackets untouched, and gathering terms involving each round bracket $(x_i - a_i)$. Using this expression we have $\varphi(f) = r$. Therefore $f \in \ker \varphi \iff r = 0 \iff f \in I$. This shows that $\ker \varphi = I$. Using the fundamental isomorphism theorem, we have $\Bbbk[x_1, \cdots, x_n]/I \cong \Bbbk$, which is a field. Therefore I is a maximal ideal. [exercise sheet, 4]

(d) Define polynomial maps $\varphi : \mathbb{A}^1 \to C; \varphi(t) = (t, t^2, t^3)$ and $\psi : C \to \mathbb{A}^1; \psi(x, y, z) = x$. Notice that $(t, t^2, t^3) \in C$ since it satisfies the defining equations of C. For any $t \in \mathbb{A}^1$, $(\psi \circ \varphi)(t) = \psi(t, t^2, t^3) = t$. For any $(x, y, z) \in C$, $(\varphi \circ \psi)(x, y, z) = \varphi(x) = (x, x^2, x^3) = (x, y, z)$. Therefore $\mathbb{A}^1$ and C are isomorphic. [exercise sheet, 4]

(e) We need to show $y^2 - f(x)$ is irreducible. Assume $y^2 - f(x) = p(x, y)q(x, y)$, then the degrees of p and q with respect to y are 2 and 0, or 1 and 1. In the first case $y^2 - f(x) = (p_2(x)y^2 + p_1(x)y + p_0(x)) \cdot q_0(x)$, which implies $p_2(x)q_0(x) = 1$, hence $q = q_0$ is a constant. In the second case $y^2 - f(x) = (p_1(x)y + p_0(x)) \cdot (q_1(x)y + q_0(x))$, which implies $p_1(x)q_1(x) = 1$. Without loss of generality we assume $p_1(x) = q_1(x) = 1$. Then we have $p_0(x) + q_0(x) = 0$ and $p_0(x)q_0(x) = -f(x)$. It follows that $f(x) = p_0(x)^2$, which is impossible since $\deg f$ is odd. This proves $y^2 - f(x)$ is irreducible, hence the ideal $(y^2 - f(x))$ is a prime ideal, which implies $\mathbb{V}(y^2 - f(x))$ is an affine variety. [unseen, 4]

Problem 2

(a) The projective space $\mathbb{P}^n$ is the set of 1-dimension vector subspaces in $\mathbb{A}^{n+1}$. A standard affine chart $U_i = \{[a_0 : \cdots : a_n] \in \mathbb{P}^n \mid a_i \neq 0\}$. An ideal $I \subseteq \Bbbk[z_0, \cdots, z_n]$ is homogeneous if for every polynomial $f \in I$, all of its homogeneous components are in I. If I is homogeneous, the projective algebraic set $\mathbb{V}(I) = \{p \in \mathbb{P}^n \mid f(p) = 0 \text{ for every homogeneous polynomial } f \in I\}$. [bookwork, 4]

(b) $\mathbb{I}(X) = \{f \in \Bbbk[z_0, \cdots, z_n] \mid f(p) = 0$ for every choice of homogeneous coordinates of every point $p \in X\}$. To show it is homogeneous, let $f \in \mathbb{I}(X)$ and write $f = f_0 + f_1 + \cdots + f_m$ for the homogeneous decomposition of f. For each $p = [a_0 : \cdots : a_n] \in X$ and $\lambda \neq 0$, we have $0 = f(\lambda a_0, \cdots, \lambda a_n) = \sum_{i=0}^m f_i(\lambda a_0, \cdots, \lambda a_n) = \sum_{i=0}^m \lambda^i f_i(a_0, \cdots, a_n)$. Since every $\lambda \neq 0$ is a root, it must be a zero polynomial. It follows that $f_i(a_0, \cdots, a_n) = 0$ for every $0 \leqslant i \leqslant m$, so $f_i \in \mathbb{I}(X)$. [bookwork, 4]

(c) All components of φ are given by homogeneous polynomials of degree 2. φ is well-defined at $[x : y : z]$ if at least two coordinates are non-zero. $\varphi([x : y : z])$ is always a point in $\mathbb{P}^2$ if it is defined. So φ is a rational map. We show that φ is dominant. Consider the projective algebraic set $Z = \mathbb{V}(xyz) \subsetneq \mathbb{P}^2$. For every point $q = [a : b : c] \in \mathbb{P}^2 \backslash Z$, $q = [1/bc : 1/ca : 1/ab] = \varphi([1/a : 1/b : 1/c])$. So $\mathbb{P}^2 \backslash Z$ is in the image of φ, which implies that φ is dominant. [bookwork, 4]

(d) Define $\varphi : \mathbb{P}^1 \to C$ by $\varphi([u : v]) = [u^2 : uv : v^2]$ and $\psi : C \to \mathbb{P}^1$ by $\psi([x : y : z]) = [x : y]$ or $[y : z]$. We check φ is a morphism: all components of φ are homogeneous of degree 2; it is well-defined at every point $[u : v] \in \mathbb{P}^1$ since either u^2 or v^2 is non-zero; and the point $[u^2 : uv : v^2]$ satisfies the defining equation of C. We check ψ is a morphism: both expressions have homogeneous components of the same degree 1; for every point in C, at least one coordinate is non-zero hence at least one expression of ψ applies; when both expressions apply at $[x : y : z]$, all coordinates x, y and z are non-zero, hence $[x : y] = [\lambda x : \lambda y] = [y : z]$ for $\lambda = y/x = z/y$. It remains to check φ and ψ are mutually inverse to each other. For any $[u : v] \in \mathbb{P}^1$, depending on which expression of ψ is used, $(\psi \circ \varphi)([u : v]) = \psi([u^2 : uv : v^2]) = [u^2 : uv] = [u : v]$ or $(\psi \circ \varphi)([u : v]) = \psi([u^2 : uv : v^2]) = [uv : v^2] = [u : v]$. So $\psi \circ \varphi = \mathrm{id}_{\mathbb{P}^1}$. For any $[x : y : z] \in C$, $(\varphi \circ \psi)([x : y : z]) = \varphi([x : y]) = [x^2 : xy : y^2] = [x^2 : xy : xz] = [x : y : z]$ or $(\varphi \circ \psi)([x : y : z]) = \varphi([y : z]) = [y^2 : yz : z^2] = [xz : yz : z^2] = [x : y : z]$. So $\varphi \circ \psi = \mathrm{id}_C$. Therefore C is isomorphic to $\mathbb{P}^1$. [bookwork, 4]

(e) We claim $(x + y^2, y^2 + z^3, z^3 + x) = (x, y^2, z^3)$. It is clear that $x + y^2, y^2 + z^3, z^3 + x \in (x, y^2, z^3)$ hence "$\subseteq$" holds. We have $x = \frac{1}{2}(x + y^2) - \frac{1}{2}(y^2 + z^3) + \frac{1}{2}(z^3 + x) \in (x + y^2, y^2 + z^3, z^3 + x)$, similarly $y^2 = \frac{1}{2}(x + y^2) + \frac{1}{2}(y^2 + z^3) - \frac{1}{2}(z^3 + x) \in (x + y^2, y^2 + z^3, z^3 + x)$ and $z^3 = -\frac{1}{2}(x + y^2) + \frac{1}{2}(y^2 + z^3) + \frac{1}{2}(z^3 + x) \in (x + y^2, y^2 + z^3, z^3 + x)$. Therefore "$\supseteq$" holds. It follows that $I = (x, y^2, z^3)$ is generated by homogeneous polynomials, hence I is homogeneous. $\mathbb{V}(I) = \varnothing$ as $x = y = z = 0$ do not define a point in $\mathbb{P}^2$. [unseen, 4]

Problem 3

(a) The function field $\Bbbk(X) = \{f/g \mid f, g \in \Bbbk[z_0, \cdots, z_n]$ are homogeneous of the same degree and $g \notin \mathbb{I}(X)\} / \sim$, where $\sim$ is an equivalence relation defined by $f_1/g_1 \sim f_2/g_2 \iff f_1g_2 - f_2g_1 \in \mathbb{I}(X)$. An element in $\Bbbk(X)$ is called a rational function on X. The pullback of g along φ is $g \circ \varphi$. [bookwork, 4]

(b) Let $\overline{I}$ be the ideal in $\Bbbk[z_0, \cdots, z_n]$ generated by the set of homogeneous polynomials $\{z_0^{\deg f} f(1, \frac{z_1}{z_0}, \cdots, \frac{z_n}{z_0}) \mid \forall f \in \mathbb{I}(X)\}$, then the projective closure of X is $\overline{X} = \mathbb{V}(\overline{I}) \subseteq \mathbb{P}^n$. Points in the set $\{[z_0 : \cdots : z_n] \in \overline{X} \mid z_0 = 0\}$ are the points at infinity for X. Using z as the extra variable, the projective closure of the given affine hypersurface is $\mathbb{V}((x^2+y^2+z^2)^3 - x^2y^3z) \subseteq \mathbb{P}^2$. Setting $z = 0$, we get $(x^2+y^2)^3 = 0$, hence $y = \pm\sqrt{-1}x$. Therefore the points at infinity are $[x : y : z] = [1 : \pm\sqrt{-1} : 0]$. [bookwork, 4]

(c) The set of singular points in X is given by $X_{\text{sing}} = \mathbb{V}(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}) \subseteq X$. Suppose on the contrary that $X_{\text{sing}} = X$, then $\frac{\partial f}{\partial x_i} \in \mathbb{I}(X)$ for every i. Since f is an irreducible polynomial, (f) is a prime ideal hence $\mathbb{I}(X) = (f)$. Therefore for every i, we have $\frac{\partial f}{\partial x_i} = f \cdot g_i$ for some $g_i \in \Bbbk[x_1, \cdots, x_n]$. Assume f has degree d_i in x_i. If $d_i > 0$, then $\frac{\partial f}{\partial x_i}$ has degree $d_i - 1$ in x_i, while $f \cdot g_i$ has degree at least d_i in x_i. Contradiction. Therefore $d_i = 0$. In other words, x_i does not occur in f. Since this holds for every i, f must be a constant polynomial. Contradiction. [bookwork, 4]

(d) The singular points are defined by f and the two partial derivatives. We have $\frac{\partial f}{\partial x} = 6x(x^2+y^2)^2 - 8xy^2 = 2x \cdot (3(x^2+y^2)^2 - 4y^2)$ and $\frac{\partial f}{\partial y} = 6y(x^2+y^2)^2 \cdot 2y - 8x^2y = 2y \cdot (3(x^2+y^2)^2 - 4x^2)$. If $x = 0$ or $y = 0$, then $f = 0$ forces $x = y = 0$. The point $(0, 0)$ satisfies all equations hence is a singular point. If neither x nor y is 0, then we have $3(x^2+y^2)^2 = 4x^2 = 4y^2$, hence $3(x^2+x^2)^2 = 4x^2$ which implies $x^2 = \frac{1}{3} = y^2$. But this does not satisfy $f = 0$. Therefore the only singular point is $(0, 0)$. [exercise sheet, 4]

(e) The projective closure of X is given by $\overline{X} = \mathbb{V}(y^2z - (x^3 + axz^2 + bz^3)) \subseteq \mathbb{P}^2$. Setting $z = 0$, we find the point at infinity $[0 : 1 : 0]$. We claim it is always a non-singular point. The standard affine piece $\{[x : y : z] \in X \mid y \neq 0\}$ is given by $\mathbb{V}(g) \subseteq \mathbb{A}^2$ for $g = z - (x^3 + axz^2 + bz^3)$. The partial derivative $\frac{\partial g}{\partial z} = 1 - 2axz - 3bz^2 \neq 0$ at $x = z = 0$. It remains to consider the non-singularity of the original affine piece X. Let $f = y^2 - (x^3 + ax + b)$. We have $\frac{\partial f}{\partial x} = -3x^2 - a$ and $\frac{\partial f}{\partial y} = 2y$. When both partial derivatives vanish, we have $x^2 = -\frac{1}{3}a$ and $y = 0$. Then $f = 0$ implies $\frac{1}{3}ax - ax - b = 0$. Case 1: $a = 0$. If $b \neq 0$, then there is no solution hence no singular point. If $b = 0$, then $x = y = 0$ is the only point at which f and its two derivatives vanish. Case 2: If $a \neq 0$, then $x = -3b/2a$. Hence $x^2 = 9b^2/4a^2 = -\frac{1}{3}a$, which is possible if and only if $4a^3 + 27b^2 = 0$. When this condition is met, $(x, y) = (-3b/2a, 0)$ is a singular point on X. Combining the two cases, $\overline{X}$ is non-singular, or equivalently X is non-singular if and only if $4a^3 + 27b^2 \neq 0$. [unseen, 4]

Problem 4

(a) Given two points $A, B \in C$, if the line AB meets the cubic C at a third point R, and the line OR meets the cubic C at a third point $\overline{R}$, then the sum $A + B = \overline{R}$. If $A = B$, then we use the tangent line $T_A C$ for AB; if $O = R$, then we use the tangent line $T_O C$ for OR. [bookwork, 4]

(b) In the affine curve $C_0 = \mathbb{V}(y^2 - x^3 + 4x - 1)$, the non-homogeneous coordinates of the two points are $A = (2, 1)$ and $B = (-2, -1)$. The line AB is given by $x = 2y$. To find its third intersection points with C_0, we solve $y^2 - 8y^3 + 8y - 1 = 0$ to get $y = \pm 1$ and $y = \frac{1}{8}$. Therefore the third intersection point is $(\frac{1}{4}, \frac{1}{8})$, whose reflection across the x-axis is the sum of A and B; that is $A + B = (\frac{1}{4}, -\frac{1}{8})$, or $[\frac{1}{4} : -\frac{1}{8} : 1]$ in homogeneous coordinates. The inverse $-B$ is the reflection of B across the x-axis, so $-B = (-2, 1)$, or $[-2 : 1 : 1]$ in homogeneous coordinates. [exercise sheet, 4]

(c) Define rational maps $\varphi : \mathbb{P}^1 \dashrightarrow C$ by $\varphi([u : v]) = [uv^2 : v^3 : u^3]$ and $\psi : C \dashrightarrow \mathbb{P}^1$ by $\psi([x : y : z]) = [x : y]$. To show φ is a rational map, we observe: all components are homogeneous of degree 3; φ is defined at every point $[u : v] \in \mathbb{P}^1$ since either u^3 or v^3 is non-zero; the image $[uv^2 : v^3 : u^3]$ is a point in C since it satisfies the defining equation of C. To show ψ is a rational map, we observe: all components are homogeneous of degree 1; ψ is well-defined at every point on C except $[0 : 0 : 1]$; image of ψ is clearly in $\mathbb{P}^1$. It remains to show φ and ψ are mutually inverse to each other. For every $[u : v] \in \mathbb{P}^1$ where $\psi \circ \varphi$ is defined, we have $(\psi \circ \varphi)([u : v]) = \psi([uv^2 : v^3 : u^3]) = [uv^2 : v^3] = [u : v]$. For every $[x : y : z] \in C$ where $\varphi \circ \psi$ is defined, we have $(\varphi \circ \psi)([x : y : z]) = \varphi([x : y]) = [xy^2 : y^3 : x^3] = [xy^2 : y^3 : y^2 z] = [x : y : z]$. Therefore C is birational to $\mathbb{P}^1$, hence is rational. [exercise sheet, 4]

(d) Assume $L = \mathbb{V}(ax + by + cz)$ where a, b and c are not simultaneously zero. Without loss of generality, we can assume $c \neq 0$. Then a point $p \in L$ can be written as $p = [x : y : -\frac{a}{c}x - \frac{b}{c}y]$. Assume $D = \mathbb{V}(f)$ where $f(x, y, z)$ is a non-zero homogeneous polynomial of degree d. Then $p \in D$ if and only if $f\left(x, y, -\frac{a}{c}x - \frac{b}{c}y\right) = 0$. The left-hand side is a homogeneous polynomial of degree d in x and y, which can be factored into a product of d homogeneous factors of degree 1 as $f\left(x, y, -\frac{a}{c}x - \frac{b}{c}y\right) = (r_1 x + s_1 y) \cdots (r_d x + s_d y) = 0$. Each factor $r_i x + s_i y$ determines a solution $[x : y] = [-s_i : r_i]$ which gives point $p_i = [-s_i : r_i : \frac{a}{c}s_i - \frac{b}{c}r_i] \in L \cap D$. Some of these points may be the same, so L and D meet in at most d points. When counting with the number of times each point occurs as a solution, we have precisely d points. [bookwork, 4]

(e) For any point $P \in C$, let Q be the third intersection point of $T_P C$ with C, and $\overline{Q}$ the third intersection point of OQ with C, then $\overline{Q} = P + P$. Since O is an inflection point, let $\overline{P}$ be the third intersection point of OP with C, then $\overline{P} = -P$. For one direction, if P is an inflection point, then $Q = P$. It follows $\overline{Q} = \overline{P}$, which implies $P + P = -P$. Hence P is 3-torsion. For the other direction, if P is 3-torsion, then $P + P = -P$ which implies $\overline{Q} = \overline{P}$. It follows $Q = P$, hence P is an inflection point. [unseen, 4]