University of Bath

DEPARTMENT OF MATHEMATICAL SCIENCES EXAMINATION

MA40188: ALGEBRAIC CURVES

May 2009

No calculators may be brought in and used.

Full marks will be given for correct answers to THREE questions.
Only the best three answers will contribute towards the assessment.

1. (a) If K is an algebraically closed field and I is an ideal of $K[x_1,\dots,x_n]$ such that $V(I)=\emptyset$ in $\mathbb{A}^n_K$, then $1\in I$. [3, bookwork]

(b) $\sqrt{I}=\{a\in R \mid a^n\in I \text{ for some } n\in\mathbb{N}\}$. It is an ideal because if $a^n\in I$ and $r\in R$ then $(ra)^n\in I$ and if $a^n,\ b^m\in I$ then

$$(a+b)^{n+m}=\sum\binom{n+m}{r}a^r b^{n+m-r}\in I$$

since either $r\geq n$ or $n+m-r\geq m$. [4, unseen but hint given in lectures.]

(c) $V(I)=\{(a_1,\dots,a_n)\in\mathbb{A}^n \mid f(a_1,\dots,a_n)=0 \text{ for all } f\in I\}$, and $I(V)=\{f\in K[x_1,\dots,x_n] \mid f(a_1,\dots,a_n) \text{ for all } a_1,\dots a_n\in V\}$.
If $n=1$ and $I=\langle x^2\rangle$ then $V(I)=\{0\}\subset\mathbb{A}^1$ but $I(V(I))=\langle x\rangle$. [3, bookwork]

(d) Suppose $f\in A=K[x_1,\dots,x_n]$. Consider the ring $B=A[y]=K[x_1,\dots,x_n,y]$, and the ideal $I^+=IB+(yf-1)B$ of B.
Notice that $Q\in\mathbb{A}^{n+1}$ is in $V(I^+)$ if and only if the point $P\in\mathbb{A}^n$ got by taking the first n coordinates of Q is in $V(I)$ and, in addition, the last coordinate of Q is $1/f(P)$ (in particular $f(P)\neq 0$). The set $(f\neq 0)\subset V(I)$ is empty when $f=0$ everywhere on $V(I)$, i.e. when $f\in I(V(I))$. So suppose $f(P)=0$ for all $P\in V(I)$: that means that $V(I^+)=\emptyset$. By the Nullstellensatz, that implies that $1\in I^+$, and because I^+ is generated by I and $yf-1$ we can find polynomials $g_0,g_1,\dots g_k\in B$ such that

$$g_0(yf-1)+g_1f_1+\cdots+g_kf_k=1,$$

where $f_1,\dots,f_k$ are generators for the ideal I.
This equation is an identity, so writing $1/f$ instead of y we have

$$\sum_{i=1}^{k} g_i\big(x_1,\dots,x_n,1/f(x_1,\dots,x_n)\big)f_i(x_1,\dots,x_n)=1.$$

The left-hand side is a rational function with denominator f^N where N is the maximum of the degrees of the g_i in y), so

$$g_i\big(x_1,\dots,x_n,1/f(x_1,\dots,x_n)\big)=h_i(x_1,\dots,x_n)/\big(f(x_1,\dots,x_n)\big)^N$$

for some polynomials h_i. If we multiply through by f^N we get

$$\sum_{i=1}^{k} h_i(x_1,\dots,x_n,1)f_i(x_1,\dots,x_n)=f(x_1,\dots,x_n)^N$$

so $f\in\sqrt{I}$ as claimed. [10, bookwork]

2. Let E be the projective curve over a field K in $\mathbb{P}^2$ given in affine coordinates by

$$y^2 = x^3 + ax + b.$$

(a) The group law on E is given by the rule "three collinear points add to zero" and the identity element is the point at infinity, $(0 : 1 : 0)$. The point $-P$ is $(p, -q)$. [4, bookwork]

(b) The tangent line ℓ_P to E at $P = (p, q)$ has equation

$$2q(y - q) = (3p^2 + a)(x - p).$$

[4, unseen but standard]

(c) On ℓ_P we have $y = \frac{(3p^2+a)(x-p)}{2q} + q$. Hence

$$y^2 = \frac{(3p^2 + a)^2(x - p)^2}{4q^2} + (3p^2 + a)(x - p) + q^2$$

on ℓ_P, so ℓ_P meets E where

$$x^3 + ax + b - \frac{(3p^2 + a)^2(x - p)^2}{4q^2} - (3p^2 + a)(x - p) - q^2 = 0.$$

This cubic equation in x has three solutions, two of which are $x = p$. Let the third solution be $x = r$: then

$$(x - p)^2(x - r) = x^3 + ax + b - \frac{(3p^2 + a)^2(x - p)^2}{4q^2} - (3p^2 + a)(x - p) - q^2 = 0.$$

Comparing the x^2 terms we have

$$-r - 2p = -\frac{(3p^2 + a)^2}{4q^2}$$

so, using $q^2 = p^3 + ap + b$ (since $P \in E$)

$$\begin{aligned} r &= \frac{(3p^2 + a)^2}{4q^2} - 2p \\ &= \frac{(3p^2 + a)^2 - 8pq^2}{4q^2} \\ &= \frac{(3p^2 + a)^2 - 8p(p^3 + ap + b)}{4q^2} \\ &= \frac{p^4 - 2p^2a + a^2 - 8pb}{4q^2} \\ &= \frac{(p^2 - a)^2 - 8pb}{4q^2}. \end{aligned}$$

[7, unseen]

Question 2 continues on next page . . .

Question 2 continued ...

(d) First, $P \in E$ because $b = 19 = -4$ and $1^3 + 9 \times 1 - 4 = 6 = 11^2 \pmod{23}$. By the formula, the x-coordinate of $-2P$ is

$$\begin{aligned} \frac{(1^2-9)^2 - 8 \times 1 \times (-4)}{24} &= \frac{64+32}{1} \\ &= 96 \\ &= 4 \bmod 23. \end{aligned}$$

So the x-coordinate of $4P$ is

$$\begin{aligned} \frac{(4^2-9)^2 - 8 \times 4 \times (-4)}{4 \times (4^3 + 9 \times 4 - 4)} &= \frac{49 + 4 \times 32}{16} \\ &= \frac{49 + 4 \times 9}{16} \\ &= \frac{3+36}{16} \\ &= \frac{16}{16} \\ &= 1. \end{aligned}$$

Therefore $4P = \pm P$, but if $4P = P$ then $2P = -P$; but we have already seen that P and $2P$ have different x-coordinates, whereas P and $-P$ have the same x-coordinate. So $4P = -P$, so $5P = 0$. [7, unseen]

3. (a) A *rational map* $\phi\colon V \dashrightarrow W$ is given by $\phi = (f_0 : \ldots : f_n)$ with $f_i \in K[x_0, \ldots, x_n]$ all homogeneous of the same degree, such that the f_i are not all in the homogenous ideal of V and $\phi(x) \in W$ if $x \in V$ and $\phi(x)$ is defined. [3, bookwork]

(b) V and W are *birationally equivalent* if there exist rational maps $\phi\colon V \dashrightarrow W$ and $\psi\colon W \dashrightarrow V$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity where they are defined. [2, bookwork]

(c) V is *rational* if V is birationally equivalent to some $\mathbb{P}^r$. [2, bookwork]

(d) $P \in V$ is singular if $\dim T_P V > \dim T_Q V$ for some $Q \in V$. [2, bookwork]

(e) The singular points of the curve C in $\mathbb{P}^2$ given by

$$f = x^2(x-y)(x+y)z + x^5 + 3y^5 = 0$$

are found by setting $z = 1$ and $f_x = f_y = 0$ (writing f_x for $\frac{\partial f}{\partial x}$), and similarly for y and z.

It is easiest to begin with $y = 1$. Then $f = x^4 z - x^2 z + x^5 + 3$, so $f_z = x^4 - x^2$ and $f_x = 4x^3 z - 2x + 5x^4$. The equation $f_z = 0$ gives $x = 0$, $x = 1$ or $x = -1$: but none of these satisfy both $f = 0$ and $f_x = 0$.

If $y \neq 1$ then $y = 0$ and on that line the equation is $x^4 z + x^5 = 0$, so $x = 0$ or $x = -z$, i.e. the points $(0 : 0 : 1)$ and $(-1 : 0 : 1)$. So we can check these on the $z = 1$ part, where we have $f = x^4 - x^2y^2 + x^5 + 3y^5$, $f_x = 4x^3 - 2xy^2 + 5x^4$ and $f_y = -2x^2y + 15y^4$. At the point $(-1 : 0 : 1)$, f_x does not vanish so that is not a singular point, but all three vanish at $(0 : 0 : 1)$ which is thus the only singular point of C. [6, unseen]

(f) Projecting from the singular point gives a birational map $\pi\colon C \dashrightarrow \mathbb{P}^1$. We may do this on the part $z = 1$, since the line $z = 0$ is not contained in C. Then the line of slope t has $y = tx$ and passes through C where $x^4(1 - t^2) + x^5(1 + 3t^5) = 0$, so the unique nonzero point is at $x = \frac{t^2-1}{3t^5+1}$ and this gives a birational map $\mathbb{P}^1 \dashrightarrow C$. inverse to π. [5, unseen]

4. (a) If $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ are irreducible then a map $\phi\colon V \to W$ is given by m elements $f_1,\ ldots, f_m \in K[V]$ such that for all $P \in V$, $(f_1(P), \ldots, f_m(P)) \in W$. ϕ^* is given by composition with ϕ. The map ϕ is an isomorphism if there exists a map $\psi\colon W \to V$ such that $\phi\psi = \mathrm{id}_w$ and $\psi\phi = \mathrm{id}_V$: then $\phi^*\colon K[W] \to K[V]$ is an isomorphism. [8, bookwork]

(b) $(x-a)^p = x^p - b + \sum_{0<r<p} \binom{p}{r} x^r a^{p-r} a^p$ and since the binomial coefficients are zero mod p we have $(x-a)^p = x^p - b$. [3, unseen]

(c) Certainly for any b such an a exists because K is algebraically closed, so Φ is surjective. But because $(x-a)^p = x^p - b$. Hence if $x^p = b$ then $x = a$, so Φ is injective. [3, unseen]

(d) $K[\mathbb{A}^1] = K[x]$ and Φ is given by the polynomial map $f(x) = x^p$, so Φ is a map of affine varieties. $\Phi^*\colon K[x] \to K[x]$ is $x \mapsto x^p$. Hence Φ is not an isomorphism because the image of Φ^* is $K[x^p]$, which is not the whole of $K[x]$. [6, unseen]