DEPARTMENT OF MATHEMATICAL SCIENCES

SOLUTIONS S2 2004/5

MA30188 (now 40188)

SOLUTIONS JUNE '05 MA 30188

University of Bath

DEPARTMENT OF MATHEMATICAL SCIENCES
EXAMINATION

You have used an obsolete rubric.

If you are preparing a new exam, please check `examdoc` for the correct arguments to `\papertype`.

1. (a) C is rational if it is birationally equivalent to $\mathbb{P}^1$. It is nonsingular at P if T_PC is a line, that is, if the subvariety of $\mathbb{A}^2$ given by the vanishing of a local equation and its partial derivatives is empty.

[6, bookwork]

(b) On the affine piece $z = 1$ we have a singular point where $y^3 - x^4 + x^3 = 0$ and the two partials also vanish, i.e. $4x^3 - 3x^2 = 3y^2 = 0$. So $y = 0$ and then $x = 0$, so $(0 : 0 : 1)$ is the only singular point. On $y = 1$ we have $z - x^4 + x^3z = 1 + x^3 = -4x^3 + 3x^2 + z = 0$. But the first two give $x^3 = -1$ and $x^4 = 0$ which is impossible. On $x = 1$ we have $y^3z - 1 + z = 3y^2z = y^3 + 1 = 0$. The second tells us that $y = 0$ or $z = 0$; the first excludes $z = 0$ and the third excludes $y = 0$.

Thus the only singular point is $(0 : 0 : 1)$.

The points at infinity are given by $x^4 = 0$ in $\mathbb{P}^1$ with coordinates $(x : y : 0)$, so there is only one and it is $(0 : 1 : 0)$.

[8, unseen but not new]

(c) Project from the origin in the affine piece $z = 1$, so $y^3 - x^4 + x^3 = 0$. Put $y = tx$: we get $0 = t^3x^3 - x^4 + x^3 = x^3(t^3 + 1 - x)$. So the remaining point of intersection (there is only one) is at $(t^3 + 1, t^4 + t)$ and this gives a rational parametrisation, with inverse $(x, y) \mapsto y/x$.

[6, unseen]

2. (a) The group law is most simply defined by choosing an inflexion point (often done by choosing coordinates so that $(0:1:0)$ is the only point at infinity) and taking it to be the identity. Then three points P, Q, R on E sum to zero if and only if they are collinear.

[5, bookwork]

(b) Q is an inflexion point if the tangent to E at Q meets E to order at least 3: in other words, if we parametrise the tangent line L in such a way that the (linear) parameter t is zero at Q, then the equation of E restricted to L as a function of t is divisible by t^3.

[2, bookwork]

(c) First, $P \in E$ since $23^2 \equiv 11 \bmod 37$.

[1, unseen]

The tangent to E at P has slope $-\left(\frac{\partial f}{\partial x}|_P\right) / \left(\frac{\partial f}{\partial y}|_P\right) = -9/46 = -1$, so a point on the tangent is $(t, 23-t)$. Such a point is on E if

$$\begin{aligned} 0 &= (23-t)^2 - t^3 + 9t - 11 \\ &= 23^2 - 46t + t^2 - t^3 + 9t - 11 \\ &= t^2 - t^3 \end{aligned}$$

so the remaining point of intersection, which is Q, is given by $t = 1$. So $Q = (1, 22)$.

[5, unseen but seen examples]

(d) We can check that Q is an inflexion point by computing the Hessian or by calculating the tangent again. The latter has slope $-6/44 = -3/22 = -3/\sqrt{3} = -22$, so a point on it is $(1+t, 22(1-t))$. So it meets E when

$$\begin{aligned} 0 &= (22(1-t))^2 - (1+t)^3 + 9(1+t) - 11 \\ &= 3(1-t)^2 - (1+t)^3 + 9 + 9t - 11 \\ &= 3 - 6t + 3t^2 - 1 - 3t - 3t^2 - t^3 + 9 + 9t - 11 \\ &= -t^3 \end{aligned}$$

i.e. three times at Q.

[4, unseen]

Finally, $Q = -2P$ and since Q is an inflexion point $3Q$ is the identity. So $-6P = 0$; but $2P = -Q \neq 0$ and $3P \neq 0$ as P is not an inflexion point. So the order of P is 6.

[3, unseen]

3. (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 $f_1, \dots, f_m \in k[V]$ such that for all $P \in V$, $\big(f_1(P), \dots, f_m(P)\big) \in W$. 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 $\phi\psi = id_W$ and $\psi\phi = id_V$: then $\phi^*\colon k[W] \to k[V]$ is an isomorphism.

[8, bookwork]

(b) Certainly for any b such an a exists because k is algebraically closed, so Φ is surjective. Now $(X-a)^p = X^p - b + \sum_{0<r<p} \binom{p}{r} X^r a^{p-r}$ and all binomial coefficients $\binom{p}{r}$ with $0 < r < p$ are zero mod p because p divides the numerator and not the denominator. Thus if $x^p = b$ then $x = a$, so Φ is injective.

[6]

(c) $k[\mathbb{A}^1] = k[X]$ and Φ is given by the polynomial map $f(X) = X^p$, so Φ is a map of affine varieties. Φ is not an isomorphism because the image of Φ^* is $k[X^p]$ which is not the whole of $k[X]$

[6, unseen]

4. (a) Suppose $IA = A$: then we may write $a_i = \sum_j b_{ij} a_j$ with $b_{ij} \in I$. So $\sum_j (b_{ij} - \delta_{ij}) a_j = 0$, so $\det(b_{ij} - \delta_{ij}) = 0$. Expanding this gives

$$0 = \det(b_{ij} - \delta_{ij}) = 1 + \text{ terms involving } b_{ij} \in 1 + I$$

so $I = B$.

[8, on examples sheet]

(b) $k[V] = k[X_1, \dots, X_n]/I(V)$ where $I(V)$ is the ideal of polynomial vanishing on V.

[2, bookwork]

(c) ϕ is projection on the first coordinate.

[3, unseen]

(d) ϕ is surjective if $V_a = \{Q \in V \mid \phi(Q) = a\} \neq \emptyset$ for all $a \in k$. But $I(V_a) = I(V) + (X_1 - a)$, and by the Nullstellensatz $V_a \neq \emptyset$ if $I(V_a)$ is a proper ideal of $k[X_1, \dots, X_n]$. That is true if and only if $1 \notin (X_1 - a)k[V]$. The ideal generated by $X_1 - a$ is a proper ideal of $k[X_1]$ (in fact it is a maximal ideal) so Nakayama's Lemma tells us that $(X_1 - a)k[V] \neq k[V]$ and therefore $1 \notin (X_1 - a)k[V]$.

[7, unseen]