ALGEBRAIC CURVES (MA40188): SOLUTIONS TO 2007 EXAM

1. (a): an ideal is a nonempty subset $I \subset R$ such that if $a,\ b \in I$ and $r \in R$ then $a+b \in I$ and $ra \in I$. It is a prime ideal if $rs \in I$ implies $r \in I$ or $s \in I$.
(b): an affine variety V is a subset of $\mathbb{A}^n$ such that there exists an ideal I of $K[t_1, \ldots, t_n]$ for which $V = V(I)$, i.e. $V = \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ for } f \in I\}$. It is irreducible if it is not the union of two proper subvarieties.
The first part of (c) is also bookwork. A polynomial map $f\colon V \to W$ is a collection $f = (f_1, \ldots, f_m)$ of elements $f_i \in K[t_1, \ldots, t_n]$ such that if $P \in V \subset \mathbb{A}^n$ then $f(P) \in W \subset \mathbb{A}^m$. It induces $f*$ by composition: an element of $K[W]$ is a map $g\colon W \to \mathbb{A}^1$ and $f^*(g) = g \circ f$. For the last part of (c), notice that W is irreducible if and only if $K[W]$ is a domain. Suppose $K[W]$ is not a domain, so we have $0 \neq a,\ b \in K[W]$ with $ab = 0$. Then $0 = f^*(ab) = f^*(a)f^*(b)$ and since f^* is injective $f(a) \neq 0$ and $f(b) \neq 0$. So $K[V]$ is not a domain, i.e. V is reducible.
For (d), the last two equations give $y = z^2$ and $x = z^3$ if $(x, y, z) \in W$, so $(x, y, z) \mapsto z$ is a morphism $W \to \mathbb{A}^1$ with inverse $z \mapsto (z^3, z^2, z)$. But the equations in (e) also allow $x = y = 0$, $z =$anything, i.e. $W' = W \cup \{(0, 0, z)\}$ which is reducible.
2. (a) The function field of a projective variety V is the field of fractions of the integral domain $K[t_0, \ldots, t_n]/I(V)$.
(b) A rational map $\phi\colon V \dashrightarrow W$, where $V \subseteq \mathbb{P}^n$, $W \subseteq \mathbb{P}^m$ are irreducible projective varieties, is an equivalence class of $m+1$ polynomials $f_0, \ldots, f_m$ in $n+1$ variables, all of the same degree, where $\{f_i\}$ and $\{g_i\}$ are equivalent if $f_i g_j - f_j g_i \in I(V)$ for all $i,\ j$, such that the f_i can be chosen so that they do not all vanish simultaneously on the whole of V and such that if $P \in V$ and $(f_0(P) : \ldots : f_m(P)) \in \mathbb{P}^m$ then $(f_0(P) : \ldots : f_m(P)) \in W$.
ϕ is regular at P if there is a representation $\phi = (f_0 : \ldots : f_m)$ such that $f_i(P)$ are not all zero. It is dominating if the image of ϕ is Zariski dense in W, i.e. is not contained in any proper subvariety of W. It is birational if it is dominating and there is a dominating rational map $\psi\colon W \dashrightarrow V$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are both the identity on the (dense) sets where they are defined.
(c) A curve C, projective or affine, is rational if there is a birational rational map $\phi\colon C \dashrightarrow \mathbb{P}^1$ (or $\mathbb{A}^1$). curves.
For (d), consider the plane $y = \lambda x$, whose points are $(t, \lambda t, s)$ with $s,\ t \in K$. This meets C_0 when $st = \lambda t$ and $t = s^2(s-1)$, i.e. at $(\lambda^2(\lambda-1), \lambda^3(\lambda-1), \lambda)$ so the map $\mathbb{A}^1 \to C_0$ given by $\lambda \mapsto (\lambda^2(\lambda-1), \lambda^3(\lambda-1), \lambda)$ has rational inverse $(x, y, z) \mapsto z$. Hence C_0 is rational.
For (e), consider the projection map $p\colon \mathbb{A}^3 \to \mathbb{A}^2$ given by $p\colon (x, y, z) \mapsto (x, y)$. This maps

C_0 to C_1 (if $(x, y, z) \in C_0$ then $(x, y) \in C_1$) and it has rational inverse $(x, y) \mapsto (x, y, y/x)$ defined away from $(x, y) = (0, 0)$ (the only point of C_1 where $x = 0$ is $(0, 0)$).

3. (a) $\mathbb{A}^n$ is simply K^n. $\mathbb{P}^n$ is K^{n+1}/K^*, where K^* acts by coordinatewise multiplication in K.

(b) A polynomial is said to be homogeneous of degree d if it is a sum of degree d monomials. And ideal I of $K[t_0, \ldots, t_n]$ is called a homogeneous ideal if it can be generated by homogeneous polynomials (possibly of different degrees).

(c) If I is a homogeneous ideal generated by $f_1, \ldots, f_k$ homogeneous of degrees d_i then the projective variety $V(I)$ is the image in $\mathbb{P}^n$ of the variety $f_1 = \cdots = f_k = 0$ in $\mathbb{A}^{n+1}$, which is also $\{(x_0 : \ldots : x_n) \mid f_i(x_0, \ldots, x_n) = 0,\ i = 1, \ldots, k\}$. Note that this makes sense because if $f_i(x_0, \ldots, x_n) = 0$ then $f_i(\lambda x_0, \ldots, \lambda x_n) = \lambda^{d_i} f_i(x_0, \ldots, x_n) = 0$ also.

(d) If $V \subset \mathbb{A}^n$ is an affine variety given by $f_i(t_1, \ldots, t^n) = 0$ its projective closure is the variety $\bar{V} \subset \mathbb{P}^n$ given by $\bar{f}_I(t_0, t_1, \ldots, t_n) = 0$, where $\bar{f}$ is the polynomial obtained from f by homogenising with respect to t_0: that is, any monomial of degree $d < \deg f$ is multiplied by $t_0^{\deg f - d}$. The points at infinity are the solutions of $\bar{f}_i(0, t_1, \ldots, t_n) = 0$.

(e) If V is a projective variety and $P \in V$, we say that P is singular if the dimension of the tangent space to V at P is greater that the dimension of the tangent space to V at some other point $Q \in V$.

Only (f) is not bookwork. V is given by homogenising: $x^4+x^2y^2-3x^2z^2+3y^2z^2+8yz^3+6z^4$. To find the points at infinity, put $z = 0$: we get $x^4 + x^2y^2 = 0$ so $x = 0$ or $x = \pm y$, so the points are $(0 : 1 : 0)$, $(1 : 1 : 0)$ and $(1 : -1 : 0)$.

To find the singular points, differentiate the equation given and set both partial derivatives equal to zero. That gives

$$2x(2x^2 + y^2 - 6) = 2y(x^2 + 3) + 8 = 0.$$

Since $x = 0$ gives $y = -4$ from the second equation and $(0, -4)$ is not on the curve, we may divide out the x from the first equation and substitute $y = -8/(x^2 + 3)$ from the second ($x = \pm\sqrt{-3}$ does not give a point of the curve either). That gives the equation in the hint; dividing out the $x^2 - 1$ leaves $2x^4 + 11x^2 + 11$. But we don't need to solve that: taking $x = 1$ gives $y = -1$ and taking $x = -1$ gives $y = 1$ also. So two of the singular points are $(1 : 1 : 1)$ and $(-1 : 1 : 1)$, and $(0 : 1 : 0)$ is singular also so that is the lot as the question says there are only three.

4. Main points are:

Smooth plane cubic curves are not rational;

As long as the characteristic is not 2 they are up to change of coordinate of the form $y^2 = x^3 + ax + b$;
They have a group law, which with the equation above is given by taking the point at infinity to be the origin and making three points on a line add to zero;
The group law is associative (and commutative), and this is an algebraic fact not depending on the ground field, which may not be algebraically closed.
Optional extras would include singular cases, what happens over $\mathbb{C}$, cryptography,...