MODEL ANSWERS TO HWK #5

6.1. It is clear that $X \times \mathbb{P}^n_k$ is Noetherian and integral. The morphism $X \times \mathbb{P}^n_k \longrightarrow X$ is projective, whence separated. As the composition of separated morphisms is separated, $X \times \mathbb{P}^n_k$ is separated.
Suppose that $\eta \in X \times \mathbb{P}^n_k$ is a codimension one point, so that the closure of η is a prime divisor Y in $X \times \mathbb{P}^n_k$. We want to show that Y is defined by a single equation locally about η. So we may assume that X is affine and we are free to replace $\mathbb{P}^n_k$ by $\mathbb{A}^n_k$. We are reduced to the case $n = 1$ by induction on n.
If Y does not dominate X then Y is locally over the image of the form $W \times \mathbb{A}^1$, where W is a divisor in X. If $g \in A = A(X)$ defines W locally about the generic point of W then $g \in A[t] = A(X \times \mathbb{A}^1_k)$ also defines Y about the generic point η of Y.
Let ξ be the generic point of X, with residue field K. Then $Y' = Y \cap \mathbb{A}^1_K = \{\eta\}$ and we may easily find $f(x) \in K[x]$ which cuts out η.
Let $U = X \times \mathbb{A}^n_k$ be the open subset of $X \times \mathbb{P}^n_k$, given by one of the standard open affines $\mathbb{A}^n_k \subset \mathbb{P}^n_k$. Then $X \times \mathbb{P}^{n-1}$ is a prime divisor and so there is an exact sequence

$$\mathbb{Z} \longrightarrow \mathrm{Cl}(X \times \mathbb{P}^n_k) \longrightarrow \mathrm{Cl}(X \times \mathbb{A}^n_k) \longrightarrow 0.$$

We first check that

$$\mathrm{Cl}(X \times \mathbb{A}^n_k) = \mathrm{Cl}(X).$$

By induction on n we may assume that $n = 1$ and we may apply (II.6.6). Finally we check that we have injectivity on the left. This is clear if we restrict to $\{\eta\} \times \mathbb{P}^n$, since then Z is sent to the class of a hyperplane.
6.4. Let K be the field of fractions of A. Then

$$K = \frac{k(x_1, x_2, \dots, x_n)[z]}{\langle z^2 - f \rangle}.$$

This is a quadratic extension of the field $L = k(x_1, x_2, \dots, x_n)$. As the characteristic is not 2, K is the splitting field of $z^2 - f$ so that K/L is Galois, with Galois group $\mathbb{Z}/2\mathbb{Z}$ given by the involution $z \longrightarrow -z$.
Every element α of K is uniquely of the form $g + hz$, where g and $h \in k(x_1, x_2, \dots, x_n)$. Then the conjugate β of α is $g - hz$ so that

$$(X - \alpha)(X - \beta) = X^2 - (\alpha + \beta)X + (\alpha\beta) = X^2 - 2gX + (g^2 - h^2 f),$$

is the minimal polynomial of α. α is in the integral closure of $k[x_1, x_2, \dots, x_n]$ inside K if and only if $2g$ and $g^2 - h^2 f \in k[x_1, x_2, \dots, x_n]$. But

$2g \in k[x_1, x_2, \dots, x_n]$ if and only if $g \in k[x_1, x_2, \dots, x_n]$. In this case $g^2 - h^2 f \in k[x_1, x_2, \dots, x_n]$ if and only if $h^2 f \in k[x_1, x_2, \dots, x_n]$. As f is square free and $k[x_1, x_2, \dots, x_n]$ is a UFD this happens if and only if $h \in k[x_1, x_2, \dots, x_n]$. But then A is the integral closure of $k[x_1, x_2, \dots, x_n]$.

In particular A is integrally closed.

6.5. (a) Note that if $r \geq 2$ then $x_0^2 + x_1^2 + x_2^2 + \dots x_r^2$ is irreducible, as the characteristic is not two. In particular it is square free and we may apply (6.4).

(b) As k is algebraically closed there is an element i such that $i^2+1 = 0$. Consider the change of variables which replaces x_0 by ix_0 and fixes the other variables. This has the effect of replacing

$$x_0^2 + x_1^2 + x_2^2 + \dots x_r^2 \qquad \text{by} \qquad -x_0^2 + x_1^2 + x_2^2 + \dots + x_r^2.$$

Now consider the change of variables which sends

$$2x_0 \longrightarrow x_0 + x_1 \qquad \text{and} \qquad 2x_1 \longrightarrow x_0 - x_1,$$

and fixes the other variables. As

$$x_1^2 - x_0^2 = (x_0 + x_1)(x_1 - x_0),$$

this has the effect of replacing

$$-x_0^2 + x_1^2 + x_2^2 + \dots + x_r^2 \qquad \text{by} \qquad x_0 x_1 + x_2^2 + \dots + x_r^2.$$

Finally multiplying x_0 by -1 we can put the equation for X into the form

$$x_0 x_1 = x_2^2 + \dots + x_r^2.$$

(1) X is toric as it is defined by the binomial equation

$$x_0 x_1 = x_2^2.$$

If $n = r = 2$, then we have already proved that $\mathrm{Cl}(X) = \mathbb{Z}_2$. There are two ways to prove the general case. The first is directly, which basically repeats the same computation. On the other hand, note first that $X = Y \times \mathbb{G}_m^{n-r}$. Now

$$Y \times \mathbb{G}_m^{n-r} \subset Y \times \mathbb{A}_k^n,$$

is an open subset. It follows that there is a surjection

$$\mathrm{Cl}(Y \times \mathbb{A}_k^n) \longrightarrow \mathrm{Cl}(X).$$

But we have already seen that

$$\mathrm{Cl}(Y) = \mathrm{Cl}(Y \times \mathbb{A}_k^n),$$

and this easily implies that

$$\mathrm{Cl}(X) = \mathrm{Cl}(Y).$$

(2) Note that we can put X into the form

$$x_0x_1 = x_2x_3.$$

As this is a binomial equation it follows that X is again toric. As in (1) we are reduced to the case $n = r + 1 = 3$.
Pick four vectors v_0, v_1, v_2 and v_3 any three of which span the standard lattice in $N_{\mathbb{R}} = \mathbb{R}^3$ such that

$$v_0 + v_2 = v_1 + v_3,$$

and let σ be the cone spanned by these vectors. We compute the dual cone $\check{\sigma}$. σ has four faces and so there are four vectors w_0, w_1, w_2 and w_3 which span $\check{\sigma}$. It is easy to check that

$$\langle v_i, w_j \rangle = \delta_{ij}.$$

It follows easily from this that any three of the four vectors w_0, w_1, w_2 and w_3 span $M_{\mathbb{R}} = \mathbb{R}^3$ and that

$$w_0 + w_2 = w_1 + w_3.$$

Note that the equation for the associated affine toric variety is

$$x_0x_2 = x_1x_3,$$

which is obtained from the original equation by a simple permutation of the variables. There are four invariant divisors D_0, D_1, D_2 and D_3, corresponding to the four vectors v_0, v_1, v_2 and v_3, which are primitive generators of the rays they span. Dotting with $f_1 = w_0$, $f_2 = w_1$ and $f_3 = w_3 \in M$ gives three relations

$$D_0 = D_4, \qquad D_1 = D_4 \qquad \text{and} \qquad D_3 = D_4.$$

So

$$\mathrm{Cl}(X) = \mathbb{Z}.$$

(3) Note that the hyperplane $X_1 = 0$ intersects X in the closed set Z defined by $x_2^2 + x_3^2 + \cdots + x_r^2$, which is irreducible. Let U be the complement. Consider projection down to $\mathbb{P}^{n-1}_k$, from the point $[1 : 0 : 0 : \cdots : 0]$. Let $V \simeq \mathbb{A}^{n-1}_k \subset \mathbb{P}^{n-1}_k$ be the standard open subset where $X_1 \neq 0$. Given $[a_1 : a_2 : \cdots : a_n] \in V$, note that there is a unique point

$$a_0 = \frac{-1}{a_1}(a_2^2 + a_3^2 + \dots a_n^2),$$

such that $[a_0 : a_1 : \cdots : a_n] \in U$ projects down to V. It follows easily that $V \simeq U = \mathbb{A}^{n-1}_k$. In particular $\mathrm{Cl}(U) = 0$. On the other hand Z is linearly equivalent to zero so that $\mathrm{Cl}(X) = 0$ using the usual exact sequence.

(c) All of this follows from (II.6.3.b), except the first isomorphism (there are two abelian groups which are extensions of $\mathbb{Z}_2$ by $\mathbb{Z}$, $\mathbb{Z} \oplus \mathbb{Z}_2$ and $\mathbb{Z}$).
In fact cases (1) and (2) are toric varieties, so we reduce to the case when $n = r$. In case (1), we have $X_0X_1 = X_2^2$ in $\mathbb{P}^2$, which is a copy of $\mathbb{P}^1$. So the class group is $\mathbb{Z}$. It is clear that a line in $\mathbb{P}^2$ cuts out two points, that is, twice a generator.
(2) is the toric variety $\mathbb{P}^1 \times \mathbb{P}^1$. There are a million ways to check that the Class group is $\mathbb{Z}^2$.
(d) We already know that the homogeneous coordinate ring of Q is integrally closed and that the class group of the corresponding affine variety is zero. It follows that the homogeneous coordinate ring of Q is a UFD by (II.6.2).
$Y \sim dH$, for some positive integer d, as H generates $\mathrm{Cl}(Q)$. It follows that there is a rational function $f \in K(Q)$ such that $(f) = Y - dH$. Suppose that H is defined by the linear polynomial X_0. The restriction of f to the open affine $Q_0 = Q \cap U_0$ is a rational function with no poles. It follows that $Y \cap Q_0$ is a prime divisor which is linearly equivalent to zero. As $\mathrm{Cl}(Q_0) = 0$, the ideal of $Y_0 = Y \cap Q_0$ is principal. Thus there a polynomial g which defines Y_0. If we homogenize g then we get a homogeneous polynomial G which defines Y.
6.6. (a) We are given two group laws on C, one given by the rule,

$$(P, Q) \longrightarrow R,$$

where $(P - P_0) + (Q - P_0) \sim R - P_0$ and the other given by the rule

$$(P, Q) \longrightarrow R,$$

where P, Q and $-R$ are collinear. Suppose that P, Q and R are collinear. Then there a linear polynomial L such that $(L)_0 = P+Q+R$. On the other hand, the line $X = Z$ is a flex line to the cubic at P_0 so that $(X - Z) = 3P_0$. But then

$$(P - P_0) + (Q - P_0) + (R - P_0) = (L/(X - Z)) \sim 0.$$

But then it is clear that the two group laws are equivalent.
Or, to crack a nut using a sledgehammer, we could appeal to the fact that as C is projective, the two group laws makes C into two abelian varieties. The identity morphism of C clearly fixes the identity, and so it must be a group isomorphism, by rigidity (see the next hwk).
(b) By (a) $2P$ is equivalent to zero in the group law on X if and only if there is a line defined by a linear polynomial L such that $(L)_0 = 2P+P_0$. But the only line which intersects C in a point with multiplicity two is the tangent line.

(c) By (a) $3P$ is equivalent to zero in the group law on X if and only if there is a line defined by a linear polynomial such that $(L)_0 = 3P$. By (b) this line is the tangent line and by definition P is then an inflection point.
(d) It suffices to show that if P, Q and R are collinear and P and Q have their coordinates in $\mathbb{Q}$ then so does R. Suppose L is the line such that

$$L \cap C = P + Q + R.$$

Then L is the line spanned by P and Q. It follows that L is defined by an equation

$$aX + bY + cZ = 0,$$

where a, b and $c \in \mathbb{Q}$. Applying a rational change of coordinates, we may assume that L is the line $Z = 0$. This won't change the set of points with rational coordinates and the equation of C becomes a cubic $F \in \mathbb{Q}[X, Y, Z]$ with rational coefficients. Restricting to L we get a cubic $G(X, Y) = F(X, Y, 0) \in \mathbb{Q}[X, Y]$ with rational coefficients and two rational roots. It follows that the third root is rational, so that R has rational coordinates.
In retrospect the most sensible answer to this question is "No, I cannot determine the rational points." But let us suppose we are not sensible. If we dehomogenize we get the equation

$$y^2 = x^3 - x = x(x-1)(x+1).$$

If $y = 0$ then we get three points, $P = [0 : 0 : 1]$, $Q = [1 : 0 : 1]$, $R = [-1 : 0 : 1]$. The line through the point P and P_0 is the line $X = 0$. The cubic equation reduces to

$$Y^2 Z = 0.$$

This has a double root at $Y = 0$ so that this line is tangent to the cubic at P and P is torsion, $2P = 0$. Similarly the line through Q and P_0 is the line $X = Z$. The cubic equations reduces to

$$Y^2 X = X^3 - X^3 = 0.$$

This has a double root at $Y = 0$, so that the line $X = Z$ is tangent to Q and $2Q = 0$. As P, Q and R are collinear it follows that $P + Q + R = 0$ so that $2R = 0$. The group generated by P, Q and R is $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
Suppose that $[a : b : c]$ is a point with rational coordinates. We may assume that a, b and c are coprime integers. If one of a, b or c is zero, then we have one of the four points P_0, P, Q or R.
So we assume that $abc \neq 0$. We have

$$b^2 c = a(a-c)(a+c).$$

We will show that there is no such triple (a, b, c). Suppose that p is a prime factor of both b and c. Then p divides $a(a-c)(a+c)$ and so p divides a, which contradicts the fact that a, b and c are coprime. It follows that b and c are coprime.
Suppose we rewrite the equation above as

$$c(b^2 + ac) = a^3.$$

As c and b are coprime, c and $b^2 + ac$ are coprime. It follows that c is a cube.
Consider the two points on the cubic, $[a : b : c]$ and $[0 : 0 : 1]$. The line through these points is $bx = ay$ and this intersects the cubic in one more point. Solving we get

$$b^2x^2 = a^2y^2 = a^2(x^3 - x).$$

So

$$x^2 - \frac{b^2}{a^2}x - 1 = 0.$$

It follows that the other root is $x = -c/a$ and $y = -c/b^2$. So

$$[-bc : -ac : ab^2],$$

is a point of the cubic, with integer coordinates. By what we have already proved, it follows that a divides bc and in fact

$$[-bc/a : -c : b^2],$$

is a point of the cubic, with integer entries.
By what we have already proved, c is a cube. It follows that the second entry is always a cube (since the second entry is always equal to the third entry of some other rational point). But then the third entry is always a sixth power (it is the square of b, which is a cube). Continuing in this way, we see that b and c are arbitrary large powers of integers. It follows that b and c are both ± 1. But then

$$a(a-1)(a+1) = \pm 1.$$

It follows that $a = \pm 1$. But then either $a + c = 0$ or $a - c = 0$, and so $b^2c = 0$, a contradiction.
So the only rational points of the cubic have one entry zero and the group of rational points is isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.