Exercise 6.1 Recall that a curve is *rational* if it is birationally equivalent to $\mathbf{P}^1$ (Ex. 4.4). Let Y be a nonsingular rational curve which is not isomorphic to $\mathbf{P}^1$.

(a) Show that Y is isomorphic to an open subset of $\mathbf{A}^1$.

(b) Show that Y is affine.

(c) Show that $A(Y)$ is a unique factorization domain.

(a) Every nonsingular rational curve is isomorphic to an open subset of a nonsingular projective curve, which must be $\mathbf{P}^1$ (as it is unique in the birational equivalence class). As this open subset is not $\mathbf{P}^1$, it must be an open subset of $\mathbf{P}^1$ minus a point, which is $\mathbf{A}^1$.

(b) Let $Y \simeq \mathbf{A}^1 - \{a_1, \dots, a_n\}$, then it is isomorphic to the curve given parametrically by $(t, 1/(t-a_1), 1/(t-a_2), \dots, 1/(t-a_n))$ in $\mathbf{A}^{n+1}$.

(c) Under the above identification, $A(Y) \cong k[x, 1/(x-a_1), \dots, 1/(x-a_n)]$, in which elements all have the form $\frac{f(x)}{(x-a_1)^{k_1} \cdots (x-a_n)^{k_n}}$; the denominators are invertible so unique factorization follows from the fact that $k[x]$ is a unique factorization domain.

Exercise 6.2 *An Elliptic Curve.* Let Y be the curve $y^2 = x^3 - x$ in $\mathbf{A}^2$, and assume that the characteristic of the base field k is $\neq 2$. In this exercise we will show that Y is not a rational curve, and hence $K(Y)$ is not a pure transcendental extension of k.

(a) Show that Y is nonsingular, and deduce that $A = A(Y) \simeq k[x,y]/(y^2 - x^3 + x)$ is an integrally closed domain.

(b) Let $k[x]$ be the subring of $K = K(Y)$ generated by the image of x in A. Show that $k[x]$ is a polynomial ring, and that A is the integral closure of $k[x]$ in K.

(c) Show that there is an automorphism $\sigma : A \to A$ which sends y to $-y$ and leaves x fixed. For any $a \in A$, define the *norm* of a to be $N(a) = a \cdot \sigma(a)$. Show that $N(a) \in k[x]$, $N(1) = 1$, and $N(ab) = N(a) \cdot N(b)$ for any $a, b \in A$.

(d) Using the norm, show that the units in A are precisely the nonzero elements of k. Show that x and y are irreducible elements of A. Show that A is *not* a unique factorization domain.

(e) Prove that Y is not a rational curve (Ex. 6.1). See (II, 8.20.3) and (III, Ex. 5.3) for other proofs of this important result.

(a) Nonsingularity comes from the fact that the partial derivatives cannot both be zero. Every regular local ring is integrally closed (see exercse 5.13), so this curve is normal at each point, i.e. $A(Y)$ integrally closed (exercise 3.17 (d)).

(b) The map $k[x] \to k[x,y] \to k[x,y]/(y^2 - x^3 + x)$ is injective (as a multiple of $y^2 - x^3 + x$ cannot be a polynomial purely in x), so $k[x]$[1] is a polynomial ring. The integral closure of $k[x]$ contains y as $y^2 - x^3 + x = 0$ in K, so the integral closure of $k[x]$ is the integral closure of A, i.e. A itself.

(c) The automorphism $y \mapsto -y$ of $k[x,y]$ naturally induces $\sigma : A \to A$. It is clear that every element in A can be written as $f(x) + g(x)y$, therefore its norm is $f(x)^2 - g(x)^2 y^2 = f(x)^2 - g(x)^2(x^3 - x) \in k[x]$. It is obvious $N(1) = 1, N(ab) = N(a)N(b)$.

[1] Notation abuse here.

(d) The invertible elements must have invertible norms, but invertible elements in $k[x]$ are constants. We observe that the solution to $f(x)^2 - g(x)^2(x^3 - x) = C$ must have $g(x) = 0$ (compare the maximum degree term) so $f(x) = C'$, hence the invertible elements in A are constants. We have $N(x) = x^2, N(y) = x(1+x)(1-x)$, and none of their proper factors is of the form $f(x)^2 - g(x)^2(x^3 - x)$, so x, y are irreducible. We have $x|y^2$ but $x \nmid y$, thus x is not prime; therefore A is not a unique factorization domain.

(e) By exercise 6.1 the affine coordinate ring of a rational curve is a unique factorization domain, but $A(Y)$ is not.

Exercise 6.3 Show by example that the result of (6.8) is false if either (a) $\dim X \geq 2$, or (b) Y is not projective.

(a) The morphism $\mathbf{P}^2 - \{(0,0,1)\} \to \mathbf{P}^1 : (x, y, z) \mapsto (x, y)$ cannot be extended to $\mathbf{P}^2$.

(b) The morphism $\mathbf{A}^1 - \{0\} \to \mathbf{A}^1 : x \mapsto 1/x$ cannot be extended to $\mathbf{A}^1$.

Exercise 6.4 Let Y be a nonsingular projective curve. Show that every nonconstant rational function f on Y defines a surjective morphism $\varphi : Y \to \mathbf{P}^1$, and that for every $P \in \mathbf{P}^1$, $\varphi^{-1}(P)$ is a finite set of points.

By (6.8) f can be extended to a morphism $Y \to \mathbf{P}^1$; if it misses a point, then as $\mathbf{P}^1$ minus a point is isomorphic to $\mathbf{A}^1$, this gives a nonconstant global regular function on Y, which is impossible ($\mathcal{O}(Y) = k$). Hence it is surjective. The inverse image of a closed set $\{P\}$ is closed, hence is finite.

Exercise 6.5 Let X be a nonsingular projective curve. Suppose that X is a (locally closed) subvariety of a variety Y (Ex. 3.10). Show that X is in fact a closed subset of Y. See (II, Ex. 4.4) for generalization.

[2]By embedding Y into a projective space we might assume $Y = \mathbf{P}^n$. The condition translates to that a nonsingular curve $X \subseteq \mathbf{P}^m$ is isomorphic to a (quasi-)variety $X' \subseteq \mathbf{P}^n$, and we shall prove X' is in fact closed. Let $f : X \to X'$ be the isomorphism.

The subvariety $X \times X' \subseteq \mathbf{P}^m \times \mathbf{P}^n$ is closed, because it is closed in each affine cover $\mathbf{A}^m \times \mathbf{A}^n$, being cut out by polynomials $y_j = f_j(x_i)$ and those defining X. We shall only prove the projection $\mathbf{P}^m \times \mathbf{P}^n \to \mathbf{P}^n$ is closed, which reduces to proving $\mathbf{P}^m \times \mathbf{A}^n \to \mathbf{A}^n$ is closed.

A closed set C in $\mathbf{P}^m \times \mathbf{A}^n$ is defined by homogeneous polynomials in the projective variables with coefficients the polynomials in the affine variables. Thus by elimination theory (5.7A) there are polynomials in the coefficients that defines the image of C under the projection to $\mathbf{A}^n$, i.e. the image is closed.

Exercise 6.6 *Automorphisms of* $\mathbf{P}^1$. Think of $\mathbf{P}^1$ as $\mathbf{A}^1 \cup \{\infty\}$. Then we define a *fractional linear transformation* of $\mathbf{P}^1$ by sending $x \mapsto (ax+b)/(cx+d)$, for $a, b, c, d \in k, ad - bc \neq 0$.

(a) Show that a fractional linear transformation induces an *automorphism* of $\mathbf{P}^1$ (i.e., an isomorphism of $\mathbf{P}^1$ with itself). We denote the group of all these fractional linar transformations by $PGL(1)$.

(b) Let $\operatorname{Aut} \mathbf{P}^1$ denote the group of all automorphisms of $\mathbf{P}^1$. Show that $\operatorname{Aut} \mathbf{P}^1 \simeq \operatorname{Aut} k(x)$, the group of k-automorphisms of the field $k(x)$.

(c) Now show that every automorphism of $k(x)$ is a fractional linear transformation, and deduce that $PGL(1) \to \operatorname{Aut} \mathbf{P}^1$ is an isomorphism.

[2]This answer is based on this math stackexchange answer.

Note: We will see later (II, 7.1.1) that a similar result holds for $\mathbf{P}^n$: every automorphism is given by a linear transformation of the homogeneous coordinates.

(a) It is fairly easy to show that such a fractional linear transformation has an inverse that is also a fractional linear transformation, and that fractional linear transformations are morphisms (in homogeneous coordinates, $(x_0, x_1) \mapsto (ax_0 + bx_1, cx_0 + dx_1)$).

(b) This follows directly from the category equivalence of (6.12).

(c) We can see (e.g. from the geometric perspective) that all valuation rings of $k(x)$ is of the form $R_a = k[x]_{(x-a)}$ or $R_\infty = k[1/x]_{(1/x)}$. If $f = p/q$ with $p, a \in k[t], (p, q) = 1$, then $f \in \mathfrak{m}_{R_a} \iff x - a|p$, while $f \in \mathfrak{m}_{R_\infty} \iff \deg q - \deg p > 0$. Hence consider the set

$$\{f \in k(t) : \text{only appears in one of } \mathfrak{m}_{R_a} \text{ or } \mathfrak{m}_{R_\infty}\} = \{\text{nonconstant } p/q : \deg p, \deg q \leq 1\}$$

The automorphism must map the former set into itself, hence the image of its element x is still in it, i.e. the automorphism is a fractional linear transformation. When changing from $k(t)$ to $\mathbf{P}^1$, the fractional linear transformations are still fractional linear transformations, hence $PGL(1) \to \operatorname{Aut} \mathbf{P}^1$ is exactly the identity map.

Exercise 6.7 Let $P_1, \ldots, P_r, Q_1, \ldots, Q_s$ be distinct points of $\mathbf{A}^1$. If $\mathbf{A}^1 - \{P_1, \ldots, P_r\}$ is isomorphic to $\mathbf{A}^1 - \{Q_1, \ldots, Q_s\}$, show that $r = s$. Is the converse true? Cf. (Ex. 3.1).

The regular function ring of $\mathbf{A}^1 - \{P_1, \ldots, P_r\}$ is $k[x, 1/(x - p_1), \ldots, 1/(x - p_r)]$ where $p_i \in k$ corresponds to P_i. By embedding it into $\operatorname{Frac} k[x]$ we find that its units are given by $a \prod (x - p_i)^{\alpha_i}$, which means its unit group is isomorphic to $k^\times \times \mathbb{Z}^r$. A k-algebra isomorphism preserves the $k^\times$ factor in the unit group, hence by quotienting out we know $r = s$.

The converse is not true. An isomorphism from $\mathbf{A}^1 - \{P_1, \ldots, P_r\}$ to $\mathbf{A}^1 - \{Q_1, \ldots, Q_r\}$ is a birational map from $\mathbf{P}^1$ to itself, hence corresponds to an element of $\operatorname{Aut} k(x)$, i.e. a fractional lienar transformation (see exercise 6.6). A fractional linear transformation is uniquely determined by its value on three points, hence we can choose $r = s = 4$ such that the possible fractional linear transformations that map $\{P_1, P_2, P_3\}$ to $\{Q_1, Q_2, Q_3\}$ does not map P_4 to Q_4, which is a counterexample to the converse claim.