Chapter 1, Section 6

James Lee

April 23, 2025

2. *An Elliptic Curve.* Let Y be the curve $y^2 = x^3 - x$ in $\mathbb{A}^2$, 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 $N(a) = a\sigma(a)$. 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.

Proof.

(a) Let $f(x,y) = y^2 - x^3 + x$. Then, we have

$$\frac{\partial f}{\partial x} = -3x^2 + 1, \quad \frac{\partial f}{\partial y} = 2y.$$

If $(\partial f/\partial y)(P) = 0$ for some $P = (a,b) \in Y$, then $b = 0$, so either $a = 0$ or $a = \pm 1$. In any case, $(\partial f/\partial x)(P) \neq 0$ since char $k \neq 2$. Therefore, both partial derivatives of f do not vanish for any $P \in Y$, hence Y is nonsingular. This means the local ring $A_{\mathfrak{m}}$ for every maximal ideal $\mathfrak{m}$ of A is a regular local ring, and since A has dimension one by Krull's Hauptidealsatz, $A_{\mathfrak{m}}$ also has dimension one, hence $A_{\mathfrak{m}}$ is an integrally closed by (6.2A). Since being integrally closed is a local property by [AM p.63], A is also integrally closed.

(b) Since k is algebraically closed and $x \notin k$, x is transcendental over k, hence $k[x]$ is a polynomial ring. Since $y^2 - x^3 + x = 0$ in K, y is the integral closure of $k[x]$ in K. Thus, the integral closure of $k[x]$ contains A, and A itself is integrally closed, hence A is the integral closure of $k[x]$.

(c) The map σ is clearly bijective. To show it is an automorphism of A, it suffices to show σ as a map from $k[x,y]$ to itself fixes $y^2 - x^3 + x$, which it indeed does. An element of A is of the form $a = f + yg$ for some $f, g \in k[x]$, hence we have

$$N(a) = a\sigma(a) = (f + yg)(f - yg) = f^2 - y^2g^2 = f^2 - (x^3 - x)g^2 \in k[x].$$

The map σ is an isomorphism, so it fixes k; in particular it fixes 1, hence $N(1) = 1 \cdot 1 = 1$. Lastly, if $a, b \in A$, then

$$N(ab) = (ab)\sigma(ab) = (ab)(\sigma(a)\sigma(b)) = (a\sigma(a))(b\sigma(b)) = N(a) \cdot N(b).$$

(d) Let u be a unit in A and let u^{-1} be its inverses. By (c), we have $N(u)N(u^{-1}) = 1$, so $N(u)$, $N(u^{-1})$ are units in $k[x]$. Since $k[x]$ is a polynomial ring, the units are precisely the nonzero elements of k, that is $N(u) \in k$. Since the norm fixes the degree, we must have $u \in k$.

Suppose $x = ab$ for some $a, b \in A$. Then, $x^2 = N(a)N(b)$ and x is irreducible in $k[x]$, so either $N(a)$, $N(b)$ each are associates with x, or $N(a)$ is an associate of x^2 and $N(b)$ is a unit. It suffices to show N is not onto $k[x]$, that is there does not exist $c \in A$ such that $N(c) = x$. By the formula above, the degree of f^2 is even while $(x^3 - x)g^2$ has degree 0 or an odd number, so $f^2 - (x^3 - x)g^2$ must have degree greater than 1. Therefore, $N(b)$ is a unit, hence b is a unit. The case for y follows similarly, since $N(y) = x(1 + x)(1 - x)$, so if $y = ab$, then either $N(a)$ is associates with x or $x(1 + x)(1 - x)$, and the former case was shown to be impossible.

A is not a unique factorization domain since $y^2 = x(x + 1)(x - 1)$, and x, y are irreducible and hence prime but are not associates since the only units in A are the nonzero elements of k.

$\square$

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.

Proof.

(a) Consider the morphism $\mathbb{A}^2 - O \to \mathbb{P}^1$ defined by mapping (x, y) to a point in $\mathbb{P}^1$ with homogenous coordinates (x, y), where O is the origin.

(b) Let X be an abstract nonsingular curve isomorphic to $\mathbb{P}^1$ and write $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. Then, we have an isomorphism $\varphi : \mathbb{P}^1 - \infty \to \mathbb{A}^1$; however, φ clearly cannot be extended to ∞.

$\square$

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

Proof. Identifying k with the affine line, f is a rational map between quasi-projective curves. We first show that if f is nonconstant, then, f is a dominant rational map into $\mathbb{A}^1$. Since the closed subsets of $\mathbb{A}^1$ are either finite subsets or the entire line $\mathbb{A}^1$, it suffices to show $\operatorname{im} f$ is an infinite set of points. If $\operatorname{im} f$ is a finite set of points, then it must be of cardinality greater than 1 since f is nonconstant. Every nonsingular projective curve is isomorphic to an abstract nonsingular curve, so the closed subsets of Y are either finite set of points or the entire curve. If $\operatorname{im} f = \{P_1, \ldots, P_n\}$, $n > 1$, then $f^{-1}(P_i)$ cannot be the entire curve Y for any $1 \leq i \leq n$, thus $Y = f^{-1}(\operatorname{im} f) = f^{-1}(P_1) \cup \cdots \cup f^{-1}(P_n)$, which is a finite union of finite sets, implying Y is a finite set of points. This is clearly not true by Exercise 4.8. Therefore, $\operatorname{im} f$ is infinite set of points, so its closure is the entire affine line, hence f is a dominant rational map.

Then, $\mathbb{A}^1$ is a rational curve, in particular it is birationally equivalent to $\mathbb{P}^1$, so if U is the largest open affine subset of Y such that $f : U \to \mathbb{A}^1$ is defined as a morphism by Exercise 4.2, we have a dominant morphism $f' : U \to \mathbb{A}^1 \hookrightarrow \mathbb{P}^1$. Since U is open and nonempty, its complement $Y - U$ is closed and proper subset of Y, hence it is a finite set of points, so by (6.8) we can extend f' to be a dominant morphism $\varphi : Y \to \mathbb{P}^1$ between nonsingular projective curves.

It remains to show φ is surjective. A dominant morphism $\varphi : Y \to \mathbb{P}^1$ induces a k-homomorphism $\varphi^* : K(\mathbb{P}^1) \to K(Y)$ between function fields, where $K(\mathbb{P}^1) \simeq k(t)$ for some indeterminant t. Since $k(t)$ and $K(Y)$ both have transcendence degree 1, φ is injective; in particular every valuation ring of $k(t)$ can be extended to one of $K(Y)$ since $K(Y)$ is integrally closed over $k(t)$. The map φ induces a morphism between abstract nonsingular curves $\varphi_\# : C_{K(Y)} \to C_{k(x)}$, where for $P \in C_{K(Y)}$ we have $\varphi_\#(P) = P \cap C_{k(x)}$ (the point P can be identified with a valuation ring in $K(Y)$). Every valuation ring of $k(t)$ is the intersection of some valuation ring of $K(Y)$ and $k(t)$, which implies $\varphi_\#$ is surjective. Since we have the following commutative diagram

$$\begin{tikzcd} Y \arrow[r, "\varphi"] \arrow[d] & \mathbb{P}^1 \arrow[d] \\ C_{K(Y)} \arrow[r, "\varphi_\#"'] & C_{k(t)} \end{tikzcd}$$

where the vertical arrows are isomorphisms, φ is also surjective.

Every nonsingular projective curve is isomorphic to an abstract nonsingular curve, where its closed sets are either finite set of points or the entire curve. This implies $\varphi^{-1}(P)$ is either finite set of points or all of Y, and it cannot be Y since φ is surjective onto $\mathbb{P}^1$. $\square$