

Non-singular Points on Algebraic Curves and Codimension-1 primes

Chol Park

May. 13th. 2008

1 Varieties

Let K be a perfect field and \bar{K} be a fixed algebraic closure of K . We begin our study of algebraic geometry with affine n -space and its subsets defined by zeros of polynomials.

Affine n -space over K is the set of n -tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \dots, x_n) : x_i \in \bar{K}\}.$$

Similarly, the *set of K -rational points in \mathbb{A}^n* is the set

$$\mathbb{A}^n(K) = \{P = (x_1, \dots, x_n) : x_i \in K\}.$$

Let $\bar{K}[X] = \bar{K}[X_1, \dots, X_n]$ be a polynomial ring in n variables, and let $I \subseteq \bar{K}[X]$ be an ideal. To each such I we associate a subset of \mathbb{A}^n ,

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

An *algebraic set* is any set of the form V_I . If V is an algebraic set, the ideal of V is given by

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in V\}.$$

An algebraic set V is *defined over K* if its ideal $I(V)$ can be generated by polynomials in $K[X]$. We denote this by V/K . If V is defined over K , the *set of K -rational points of V* is the set

$$V(K) = V \cap \mathbb{A}^n(K).$$

An affine algebraic set V is called an *affine variety* if $I(V)$ is prime ideal in $\bar{K}[X]$. Let V/K be a variety defined over K . Then the *affine coordinate ring of V/K* is defined by

$$K[V] = \frac{K[X]}{I(V/K)}.$$

It is an integral domain; and its quotient field, denoted $K(V)$, is called the *function field of V/K* . Similarly $\bar{K}[V]$ and $\bar{K}(V)$ are defined by replacing K with \bar{K} . Note that since an element $f \in \bar{K}[V]$ is well-defined up to a polynomial vanishing on V , it induces a well-defined function $f : V \rightarrow \bar{K}$.

Definition 1.1. Let V be an affine variety. The *dimension* of V , denoted by $\dim(V)$, is the transcendence degree of $\overline{K}(V)$ over \overline{K} .

Example 1.2. The dimension of \mathbb{A}^n is n , since $\overline{K}(\mathbb{A}^n) = \overline{K}(X_1, \dots, X_n)$. Similarly, if $V \subset \mathbb{A}^n$ is given by a single non-constant polynomial equation

$$f(X_1, \dots, X_n) = 0,$$

then $\dim(V) = n - 1$. The converse is also true

Definition 1.3. Let V be an affine variety, $P \in V$, and $f_1, \dots, f_m \in \overline{K}[X]$ a set of generators for $I(V)$. Then V is *non-singular* (or *smooth*) at P if the $m \times n$ matrix

$$(\partial f_i / \partial X_j(P))_{1 \leq i \leq m, 1 \leq j \leq n}$$

has rank $n - \dim(V)$. If V is non-singular at every point, then we say that V is *non-singular* (or *smooth*).

Let $P \in V$, and define an ideal M_P of $\overline{K}[V]$ by

$$M_P = \{f \in \overline{K}[V] : f(P) = 0\}.$$

Notice that M_P is a maximal ideal, since there is an isomorphism

$$\overline{K}[V]/M_P \longrightarrow \overline{K} \quad \text{given by } f \rightarrow f(P).$$

The quotient M_P/M_P^2 is a finite dimensional \overline{K} -vector space.

Definition 1.4. The *local ring* of V at P , denoted $\overline{K}[V]_P$, is the localization of $\overline{K}[V]$ at M_P . In other words,

$$\overline{K}[V]_P = \{F \in \overline{K}(V) : F = f/g \text{ for some } f, g \in \overline{K}[V] \text{ with } g(P) \neq 0\}.$$

Notice that if $F = f/g \in \overline{K}[V]_P$, then $F(P) = f(P)/g(P)$ is well-defined. The functions in $\overline{K}[V]_P$ are said to be *regular* (or *defined*) at P .

There is another characterization of smoothness, in terms of the functions of the variety V , which is often quite useful.

Proposition 1.5. Let V be an affine variety. A point $P \in V$ is non-singular if and only if

$$\dim_{\overline{K}} M_P/M_P^2 = \dim(V).$$

proof Let P be the point (a_1, \dots, a_n) in $V \subset \mathbb{A}^n$, and let $I_P = (X_1 - a_1, \dots, X_n - a_n)$ be the corresponding maximal ideal in $\overline{K}[X]$. We define a linear map $\theta : \overline{K}[X] \rightarrow \overline{K}^n$ by

$$\theta(f) = \left(\frac{\partial f}{\partial x_1}(P), \dots, \frac{\partial f}{\partial x_n}(P) \right)$$

for any $f \in \overline{K}[X]$. Now it is clear that $\theta(X_i - a_i)$ for $i = 1, \dots, n$ form a basis for \overline{K}^n , and that $\theta(I_P^2) = 0$. Thus θ induces an isomorphism $\theta' : I_P/I_P^2 \rightarrow \overline{K}^n$. Now let f_1, \dots, f_m be a set of generators of $I(V) \subset I_P$. Then the rank of the Jacobian matrix

$$J = \left(\frac{\partial f_i}{\partial X_j}(P) \right)_{1 \leq i \leq m, 1 \leq j \leq n}$$

is just the dimension of $\theta(I(V))$ as a subspace of \overline{K}^n . Using the isomorphism θ' , this is the same as the dimension of the subspace $(I(V) + I_P^2)/I_P^2$ of I_P/I_P^2 . On the other hand, if \mathfrak{m}_P is the maximal ideal of $\overline{K}[V]_P$, we have

$$\mathfrak{m}_P/\mathfrak{m}_P^2 \cong I_P/(I(V) + I_P^2).$$

Counting dimensions of vector spaces, we have $\dim_{\overline{K}} \mathfrak{m}_P/\mathfrak{m}_P^2 = n - \text{rank} J$. Now let $\dim(V) = r$. Then $\overline{K}[V]_P$ is a local ring of dimension r , so $\dim_{\overline{K}} \mathfrak{m}_P/\mathfrak{m}_P^2 = \dim(V)$ if and only if $\dim_{\overline{K}} \mathfrak{m}_P/\mathfrak{m}_P^2 = r$. But this is equivalent to $\text{rank} J = n - r$, which says that P is a nonsingular point of V . Now the fact that $M_P/M_P^2 \cong \mathfrak{m}_P/\mathfrak{m}_P^2$ as \overline{K} -vector spaces completes the proposition.

Projective n -space over \overline{K} , denoted \mathbb{P}^n or $\mathbb{P}^n(\overline{K})$, is the set of all $(n + 1)$ -tuples

$$(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is non-zero, modulo the equivalence relation gives by

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

if there exists a $\lambda \in \overline{K}^*$ with $x_i = \lambda y_i$ for all i . An equivalence class $\{(\lambda x_0, \dots, \lambda x_n)\}$ is denoted $[x_0, \dots, x_n]$, and x_0, \dots, x_n are called *homogeneous coordinates* for the corresponding point in \mathbb{P}^n . The *set of K -rational points in \mathbb{P}^n* is the set

$$\mathbb{P}^n(K) = \{[x_1, \dots, x_n] \in \mathbb{P}^n : \text{all } x_i \in K\}.$$

A polynomial $f \in \overline{K}[X] = \overline{K}[X_0, \dots, X_n]$ is *homogeneous of degree d* if

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n)$$

for all $\lambda \in \overline{K}$. And ideal $I \subset \overline{K}[X]$ is *homogeneous* if it is generated by homogeneous polynomials. Note that for a homogeneous polynomial f , it makes sense to ask whether $f(P) = 0$ for a point $P \in \mathbb{P}^n$. To each homogeneous ideal I we associate a subset of \mathbb{P}^n ,

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}.$$

A *projective algebraic set* is any set of the form V_I . If V is a projective algebraic set, the *homogeneous ideal of V* , denoted $I(V)$, is the ideal in $\overline{K}[X]$ generated by

$$\{f \in \overline{K}[X] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\}.$$

Such a V is *defined over* K , denoted by V/K , if its ideal $I(V)$ can be generated by homogeneous polynomials in $K[X]$. If V is defined over K , the *set of K -rational points of V* is the set

$$V(K) = V \cap \mathbb{P}^n(K).$$

A projective algebraic set is called a *projective variety* if its homogeneous ideal $I(V)$ is a prime ideal in $\overline{K}[X]$.

It is clear that \mathbb{P}^n contains many copies of \mathbb{A}^n . For example, for each $0 \leq i \leq n$, there is an inclusion

$$\phi_i : \mathbb{A}^n \longrightarrow \mathbb{P}^n, \quad (y_1, \dots, y_n) \mapsto [y_1, \dots, y_{i-1}, 1, y_i, \dots, y_n].$$

If we let H_i denote the hyperplane in \mathbb{P}^n given by $X_i = 0$,

$$H_i = \{P = [x_0, \dots, x_n] \in \mathbb{P}^n : x_i = 0\};$$

and let U_i be the complement of H_i ,

$$U_i = \{P = [x_0, \dots, x_n] \in \mathbb{P}^n : x_i \neq 0\};$$

then there is a natural bijection

$$\phi_i^{-1} : U_i \longrightarrow \mathbb{A}^n, \quad [x_0, \dots, x_n] \mapsto \left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i} \right).$$

Having fixed an i , we will normally identify \mathbb{A}^n with the set U_i in \mathbb{P}^n via the map ϕ_i .

Now let V be a projective algebraic set with homogeneous ideal $I(V) \subset \overline{K}[X]$. Then $V \cap \mathbb{A}^n$ (by which we mean $\phi_i^{-1}(V \cap U_i)$) is an affine algebraic set with ideal $I(V \cap \mathbb{A}^n) \subset \overline{K}[Y]$ given by

$$I(V \cap \mathbb{A}^n) = \{f(Y_1, \dots, Y_{i-1}, 1, Y_{i+1}, \dots, Y_n) : f(X_0, \dots, X_n) \in I(V)\}.$$

The process of replacing $f(X_0, \dots, X_n)$ by $f(Y_1, \dots, Y_{i-1}, 1, Y_{i+1}, \dots, Y_n)$ is called *dehomogenization with respect to X_i* .

This process can be reversed. for any $f(Y) \in \overline{K}[Y]$, let

$$f^*(X_0, \dots, X_n) = X_i^d \left(\frac{X_0}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_n}{X_i} \right),$$

where $d = \deg(f)$ is the smallest integer for which f^* is a polynomial. We say that f^* is the *homogenization with respect to X_i* .

Definition 1.6. Let V be an affine algebraic set with ideal $I(V)$, and consider V as a subset of \mathbb{P}^n via the map

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n.$$

The *projective closure of V* , denoted \overline{V} , is the projective algebraic set whose homogeneous ideal $I(\overline{V})$ is generated by

$$\{f^* : f \in I(V)\}.$$

Most of the important properties of a projective variety V may now be defined in terms of the affine subvariety $V \cap \mathbb{A}^n$.

Definition 1.7. Let V/K be a projective variety, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ so that $V \cap \mathbb{A}^n \neq \emptyset$. The *dimension of V* is the dimension of $V \cap \mathbb{A}^n$. The *function field of V* , denoted $K(V)$, is the function field of $V \cap \mathbb{A}^n$; and similarly for $\overline{K}(V)$.

Remark 1.8. For different choices of \mathbb{A}^n , the different $K(V)$'s are canonically isomorphic, so we will always identify them.

Definition 1.9. Let V be a projective variety, $P \in V$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then V is *non-singular* (or *smooth*) at P if $V \cap \mathbb{A}^n$ is non-singular at P . The *local ring of V at P* , denoted $\overline{K}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P . A function $F \in \overline{K}(V)$ is *regular at P* if it is in $\overline{K}[V]_P$; in this case, it makes sense to evaluate F at P .

Definition 1.10. Let V_1 and $V_2 \subset \mathbb{P}^n$ be projective varieties. A *rational map from V_1 to V_2* is a map of the form

$$\phi : V_1 \longrightarrow V_2 \quad \phi = [f_0, \dots, f_n],$$

where $f_0, \dots, f_n \in \overline{K}(V_1)$ have the property that for every point $P \in V_1$ at which f_0, \dots, f_n are all defined,

$$\phi(P) = [f_0(P), \dots, f_n(P)] \in V_2.$$

Definition 1.11. A rational map

$$\phi = [f_0, \dots, f_n] : V_1 \longrightarrow V_2$$

is *regular at $P \in V_1$* if there is a function $g \in \overline{K}(V_1)$ such that

- (a) each gf_i is regular at P ; and
- (b) for some i , $(gf_i)(P) \neq 0$.

If such g exists, we set

$$\phi(P) = [gf_0(P), \dots, gf_n(P)].$$

A rational map which is regular at every point is called a *morphism*.

Example 1.12. Let V be a projective variety from

$$V : X^2 + Y^2 = 1.$$

Consider the rational map

$$\phi : V \longrightarrow \mathbb{P}^1, \quad \phi = \left[\frac{X+1}{Y}, 1 \right].$$

Clearly ϕ is regular at every point of V except possibly $(-1, 0)$. But using

$$(X+1)(X-1) \equiv -Y^2 \pmod{I(V)},$$

we have

$$\phi = \left[\frac{X+1}{Y}, 1 \right] = \left[\frac{-Y}{X-1}, 1 \right] = [-Y, X-1].$$

Thus

$$\phi([-1, 0, 1]) = [0, -2] = [0, 1].$$

2 Algebraic Curves

By a *curve* we will always mean an projective variety of dimension 1. We start by describing the local rings of a smooth curve.

Let R be an integral domain, K its field of fraction. R is a *valuation ring of K* if, for each $x \neq 0$, either $x \in R$ or $x^{-1} \in R$

Proposition 2.1. Let C be a curve and $P \in C$ a smooth point. Then $\overline{K}[C]_P$ is a discrete valuation ring.

proof It is immediate from Proposition 1.5 and the lemma 2.3.

Example 2.2. Consider the two curves

$$C_1 : Y^2 = X^3 + X \quad \text{and} \quad C_2 : Y^2 = X^3 + X^2.$$

Let $P = (0, 0)$. Then C_1 is smooth at P and C_2 is not. The maximal ideal M_P of $\overline{K}[C_1]_P$ has the property that M_P/M_P^2 is generated by Y , so for example

$$\text{ord}_P(Y) = 1 \quad \text{ord}_P(X) = 2 \quad \text{ord}_P(2Y^2 - X) = 2.$$

On the other hand, $\overline{K}[C_2]_P$ is not a discrete valuation ring.

Lemma 2.3. Let R be a Noetherian local domain of dimension one, \mathfrak{m} its maximal ideal, and $k = R/\mathfrak{m}$. Then the following are equivalent:

- (a) R is a discrete valuation ring;
- (b) R is integrally closed;
- (c) \mathfrak{m} is an principal ideal;
- (d) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$;
- (e) Every non-zero ideal is a power of \mathfrak{m} ;
- (f) There exists $x \in R$ such that every non-zero ideal is of the form (x^k) , $k \geq 0$.

proof Before we start going the rounds, we make two remarks (A) and (B):

(A) If I is an non-zero proper ideal, then I is \mathfrak{m} -primary and $I \supseteq \mathfrak{m}^n$ for some n . Since A is Noetherian I has a primary decomposition and so $\sqrt{I} = \mathfrak{m}$ for \mathfrak{m} is the only nonzero prime ideal. Then it is immediate from the following sublemma.

sublemma 2.4. Let A be a Noetherian ring, \mathfrak{m} a maximal ideal of A , I any ideal of A . Then the following are equivalent:

- (1) I is \mathfrak{m} -primary;

- (2) $\sqrt{I} = \underline{\mathfrak{m}}$;
(3) $\underline{\mathfrak{m}}^n \subset I \subset \underline{\mathfrak{m}}$ for some $n > 0$.
proof Atiyah-MacDonald [Cor 7.16 p.83]

(B) $\underline{\mathfrak{m}}^n \neq \underline{\mathfrak{m}}^{n+1}$ for all $n \geq 0$.

It is immediate from the following lemma.

sublemma 2.5. Let A be a Noetherian local ring, $\underline{\mathfrak{m}}$ its maximal ideal. Then exactly one of the following two statements is true:

- (1) $\underline{\mathfrak{m}}^n \neq \underline{\mathfrak{m}}^{n+1}$ for all n ;
(2) $\underline{\mathfrak{m}}^n = 0$ for some n , in which case A is an Artin local ring.

proof Atiyah-MacDonald[Prop 8.6 p. 90]

(a) \Rightarrow (b) Let $x \in K$ be integral over R , where K is a field of quotients of R . Then we have

$$x^n + b_1x^{n-1} + \dots + b_n = 0$$

with the $b_i \in R$. If $x \in R$ there is nothing to prove. If not, then $x^{-1} \in R$, and so $x = -(b_1 + b_2x^{-1} + \dots + b_nx^{1-n}) \in R$.

(b) \Rightarrow (c) Let $a \in \underline{\mathfrak{m}}$ and $a \neq 0$. By remark (A) there exists an integer n such that $\underline{\mathfrak{m}}^n \subseteq (a)$ but $\underline{\mathfrak{m}}^{n-1} \not\subseteq (a)$. Choose $b \in \underline{\mathfrak{m}}^{n-1}$ and $b \notin (a)$, and let $x = a/b \in K$. We have $x^{-1} \notin R$ since $b \notin (a)$, hence x^{-1} is not integral over R , and therefore by the following sublemma we have $x^{-1}\underline{\mathfrak{m}} \not\subseteq \underline{\mathfrak{m}}$; for if $x^{-1}\underline{\mathfrak{m}} \subset \underline{\mathfrak{m}}$, $\underline{\mathfrak{m}}$ would be a faithful $R[x^{-1}]$ -module, finitely generated as an R -module. But $x^{-1}\underline{\mathfrak{m}} \subset R$ by construction of x , hence $x^{-1}\underline{\mathfrak{m}} = R$ and therefore $\underline{\mathfrak{m}} = Rx = (x)$. Recall that $\underline{\mathfrak{m}}$ is *faithful* if $\text{Ann}(\underline{\mathfrak{m}}) = 0$.

sublemma 2.6. The following are equivalent:

- (1) $x \in B$ is integral over A ;
(2) $A[x]$ is a finitely generated A -module;
(3) $A[x]$ is contained in a subring C of B such that C is a finitely generated A -module;
(4) There exists a faithful $A[x]$ -module M which is finitely generated as an A -module.

proof Atiyah-MacDonald[Prop 5.1 p59]

(c) \Rightarrow (d) It is easy to see that $x + \underline{\mathfrak{m}}^2$ generates $\underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2$ as $k = A/\underline{\mathfrak{m}}$ -vector space. So we have $\dim_k(\underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2) \leq 1$, and by remark (B), $\underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2 \neq 0$.

(d) \Rightarrow (e) Let I be a non-zero proper ideal of R . By remark (A) we have $I \supseteq \underline{\mathfrak{m}}^n$ for some n ; from the following sublemma applied to $R/\underline{\mathfrak{m}}^n$, which is an Artin local ring, it follows that I is a power of $\underline{\mathfrak{m}}$.

sublemma 2.7. Let A be an Artin local ring, $\underline{\mathfrak{m}}$ its maximal ideal, $k = A/\underline{\mathfrak{m}}$ its residue field. Then the following are equivalent:

- (1) every ideal in A is principal and a power of $\underline{\mathfrak{m}}$;
(2) the maximal ideal $\underline{\mathfrak{m}}$ principal;
(3) $\dim_k(\underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2) \leq 1$.

proof Atiyah-MacDonald[Prop 8.8 p91]

(e) \Rightarrow (f) By remark (B), $\underline{\mathfrak{m}} \neq \underline{\mathfrak{m}}^2$, hence there exists $x \in \underline{\mathfrak{m}}$, $x \notin \underline{\mathfrak{m}}^2$. But $(x) = \underline{\mathfrak{m}}^r$ by hypothesis, hence $r = 1$, $(x) = \underline{\mathfrak{m}}$, $(x^k) = \underline{\mathfrak{m}}^k$.

(f) \Rightarrow (a) Clearly $(x) = \underline{\mathfrak{m}}$, hence $(x^k) \neq (x^{k+1})$ by remark (B), hence if a is any non-zero element of R , we have $(a) = (x^k)$ for exactly one value of $k \geq 0$. Define $v(a) = k$ and extend v to K^* by defining $v(ab^{-1}) = v(a) - v(b)$. Check that v is well-defined and is a discrete valuation, and that R is the valuation ring of v .

Corollary 2.8. Let R be a normal Noetherian domain. Then every localization of R at a height-1 prime is a discrete valuation ring.

proof If a prime \mathfrak{p} has height 1, $R_{\mathfrak{p}}$ is a normal Noetherian local domain of dimension 1, and so by the previous lemma it is a discrete valuation ring.

Definition 2.9. Let C be a curve and $P \in C$ a smooth point. The (*normalized*) valuation on $\overline{K}[C]_P$ is given by

$$\begin{aligned} \text{ord}_P : \overline{K}[C]_P &\longrightarrow \{0, 1, 2, \dots\} \cup \{\infty\} \\ \text{ord}_P(f) &= \max\{d \in \mathbb{Z} : f \in M_P^d\}. \end{aligned}$$

Using $\text{ord}_P(f/g) = \text{ord}_P(f) - \text{ord}_P(g)$, we extend ord_P to $\overline{K}(C)$,

$$\text{ord}_P : \overline{K}(C) \longrightarrow \mathbb{Z} \cup \{\infty\}.$$

A *uniformizer* for C at P is a function $t \in \overline{K}(C)$ with $\text{ord}_P(t) = 1$.

Proposition 2.10. Let C/K be a curve, and let $t \in K(C)$ be a uniformizer at some non-singular point $P \in C$. Then $K(C)$ is a finite separable extension of $K(t)$.

proof $K(C)$ is clearly a finite extension of $K(t)$, since it is finitely generated over K , has transcendence degree 1 over K , and $t \notin K$. Now let $x \in K(C)$. We will show that x is separable over $K(t)$.

In any case, x is algebraic over $K(t)$, so it satisfies some polynomial relation

$$\sum a_{ij} t^i x^j = 0, \quad \text{where } \Phi(T, X) = \sum a_{ij} T^i X^j \in K[X, Y].$$

We may further assume that Φ is chosen so as to have minimal degree in X . Let $p = \text{char}(K)$. If Φ contains a non-zero term $a_{ij} T^i X^j$ with $p \nmid j$, then $\frac{\partial \Phi(T, X)}{\partial X}$ is not identically 0, so x is separable over $K(t)$. Suppose now that $\Phi(T, X) = \Psi(T, X^p)$. We proceed to derive a contradiction.

The main point to note is that if $F(T, X) \in K[T, X]$ is any polynomial, then $F(T^p, X^p)$ is a p^{th} -power. Thus if $F(T, X) = \sum \alpha_{ij} T^i X^j$, then writing $\alpha_{ij} = \beta_{ij}^p$ gives $F(T^p, X^p) = (\sum \beta_{ij} T^i X^j)^p$. We now regroup the terms in $\Phi(T, X) = \Psi(T, X^p)$ according to powers of T modulo p :

$$\Phi(T, X) = \Psi(T, X^p) = \sum_{k=0}^{p-1} \left(\sum_{i,j} b_{ijk} T^{ip} X^{jp} \right) T^k = \sum_{k=0}^{p-1} \phi_k(T, X)^p T^k.$$

Now by assumption, $\Phi(t, x) = 0$. On the other hand, since t is a uniformizer at P , we have

$$\text{ord}_P(\phi_k(t, x)^p t^k) = p \text{ord}_P(\phi_k(t, x)) + k \text{ord}_P(t) \equiv k \pmod{p}.$$

Thus each of the terms in the sum $\sum \phi_k(t, x)^p t^k$ has a distinct order at P , so every term must vanish:

$$\phi_0(t, x) = \phi_1(t, x) = \dots = \phi_{p-1}(t, x) = 0.$$

But one of the $\phi_k(T, X)$'s must involve X ; and for that k , the relation $\phi_k(t, x) = 0$ contradicts the fact that we chose $\Phi(t, X)$ to be a minimal polynomial for x over $K(t)$. Note that $\deg_X(\phi_k(T, X)) \leq \deg_X(\Phi(T, X))/p$. This contradiction completes the proof that x is separable over $K(t)$.

Proposition 2.11. Let C be a curve, $V \subset \mathbb{P}^N$ a variety, $P \in C$ a smooth point, and $\phi : C \rightarrow V$ a rational map. Then ϕ is regular at P . In particular, if C is smooth, then ϕ is a morphism.

proof Write $\phi = [f_0, \dots, f_N]$ with $f_i \in \overline{K}(C)$, and choose a uniformizer $t \in \overline{K}(C)$ for C at P . Let

$$n = \min_{1 \leq i \leq N} \{\text{ord}_P f_i\}.$$

Then

$$\text{ord}_P(t^{-n} f_i) \geq 0 \text{ for all } i \quad \text{and} \quad \text{ord}_P(t^{-n} f_j) = 0 \text{ for some } j,$$

so each $t^{-n} f_i$ is regular at P and $t^{-n} f_j(P) \neq 0$. Therefore ϕ is regular at P .

Example 2.12. Let V be a projective variety

$$V : Y^2 = X^3 + X^2,$$

and consider the rational maps

$$\phi : V \rightarrow \mathbb{P}^1, \quad \phi = [Y, X]$$

and

$$\psi : \mathbb{P}^1 \rightarrow V, \quad \psi = [(S^2 - T^2)T, (S^2 - T^2)S, T^3].$$

Then since \mathbb{P}^1 is a smooth curve ψ is a morphism, while ϕ is not regular at $[0, 0, 1]$.

3 More about height-1 primes

First we prove the following theorem. Then we are going to look at the geometric version of the theorem.

Theorem 3.1. If R is a normal Noetherian domain, then R is the intersection of its localizations at height-1 primes.

Lemma 3.2. If R is a Noetherian domain, then R is the intersection of its localizations at every prime associated to principal ideal in R .

proof Suppose a/u is in $Q(R) - R$, then $a \notin (u)$. We need to show that there is an associated prime \mathfrak{p} of (u) such that $a \notin (u)_{\mathfrak{p}} \subset R_{\mathfrak{p}}$, which implies $a/u \notin R_{\mathfrak{p}}$. Let $(u) = I_1 \cap I_2 \cap \dots \cap I_n$ be a primary decomposition of (u) , where I_i is a \mathfrak{q}_i -primary. Suppose $a \in (u)_{\mathfrak{q}_i}$ for all i . Then for all i there exists $t_i \in R - \mathfrak{q}_i$ such that $t_i a = u x_i \in I_i$. Thus $a \in I_i$ for all i , contracting $a \notin (u)$

Proposition 3.3. A Noetherian domain R is normal if and only if for every prime \mathfrak{p} associated to a principal ideal, $\mathfrak{p}_{\mathfrak{p}}$ is principal.

proof Suppose first that R is a normal domain and that \mathfrak{p} is a prime of R associated to a principal ideal (a) ; say \mathfrak{p} is the annihilator of $b \bmod (a)$, with $b \in R - (a)$. Then $\mathfrak{p}_{\mathfrak{p}} = ((a)_{\mathfrak{p}} : b)$. We shall show that $\mathfrak{p}_{\mathfrak{p}}$ is principal. Let $K = Q(R) = Q(R_{\mathfrak{p}})$, and consider the set $\mathfrak{p}_{\mathfrak{p}}^{-1} = \{r \in K : r\mathfrak{p}_{\mathfrak{p}} \subset R_{\mathfrak{p}}\}$. We clearly have $\mathfrak{p}_{\mathfrak{p}} \subset \mathfrak{p}_{\mathfrak{p}}^{-1}\mathfrak{p}_{\mathfrak{p}} \subset R_{\mathfrak{p}} \subset \mathfrak{p}_{\mathfrak{p}}^{-1}$, and since $\mathfrak{p}_{\mathfrak{p}}$ is maximal, this leaves only the possibilities $\mathfrak{p}_{\mathfrak{p}}^{-1}\mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$ and $\mathfrak{p}_{\mathfrak{p}}^{-1}\mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}}$. If $\mathfrak{p}_{\mathfrak{p}}^{-1}\mathfrak{p}_{\mathfrak{p}} = \mathfrak{p}_{\mathfrak{p}}$, then by the sublemma 2.6 the elements of $\mathfrak{p}_{\mathfrak{p}}^{-1}$ are integral over $R_{\mathfrak{p}}$ since for each $r \in \mathfrak{p}_{\mathfrak{p}}^{-1}$, $\mathfrak{p}_{\mathfrak{p}}[r]$ is finitely generated $R_{\mathfrak{p}}$ -module. Since $R_{\mathfrak{p}}$ is normal, $\mathfrak{p}_{\mathfrak{p}}^{-1} = R_{\mathfrak{p}}$. But $\mathfrak{p}_{\mathfrak{p}}b \subset (a)_{\mathfrak{p}}$, so $b/a \in \mathfrak{p}_{\mathfrak{p}}^{-1} = R_{\mathfrak{p}}$, whence $b \in (a)_{\mathfrak{p}}$ contracting our assumption. Thus $\mathfrak{p}_{\mathfrak{p}}^{-1}\mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}}$; that is, $\mathfrak{p}_{\mathfrak{p}}$ is invertible. Since $R_{\mathfrak{p}}$ is local, $\mathfrak{p}_{\mathfrak{p}}^{-1}\mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}}$ implies that for some $r \in \mathfrak{p}_{\mathfrak{p}}^{-1}$ we have $r\mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}}$. Consequently, $\mathfrak{p}_{\mathfrak{p}} = R_{\mathfrak{p}}r^{-1}$ is principal. Conversely, we show that the given conditions imply that R is normal. Since an intersection of normal domains with a common quotient field is obviously normal, it will be enough to show that R is the intersection of its localizations at primes associated to principal ideals. Thus lemma 3.2 completes the proof.

Lemma 3.4. Any prime properly contained in a proper principal ideal in a Noetherian ring R has height 0.

proof If on the contrary, $\mathfrak{q} \subsetneq \mathfrak{p} \subsetneq (x)$ in a ring R with \mathfrak{q} and \mathfrak{p} prime ideals, then factoring out \mathfrak{q} we can assume that $\mathfrak{q} = 0$, and thus that R is a domain. If $y \in \mathfrak{p}$, then $y = ax$ for some a , and since $x \notin \mathfrak{p}$ it follows that $a \in \mathfrak{p}$; thus $\mathfrak{p} = x\mathfrak{p}$. By the sublemma below $(1-b)\mathfrak{p} = 0$ for some $b \in (x)$. Since R is a domain, we must have $b = 1$, so (x) is not proper, a contradiction.

sublemma 3.5. If M is a finitely generated R -module and I is an ideal of R such that $IM = M$, then there is an element $r \in I$ that $(1-r)M = 0$.

proof Atiyah-MacDonald[Cor 2.5, p 21].

Lemma 3.6. every height 1 prime \mathfrak{p} in a domain R is minimal to a principal ideal.

proof Let x be a nonzero element in \mathfrak{p} . Then \mathfrak{p} is a minimal prime to (x) since \mathfrak{p} has height 1.

proof of theorem 3.1 By lemma 3.2, any Noetherian domain is the intersection of its localizations at the primes associated to principal ideals. If R is normal and \mathfrak{p} is a prime

associated to a principal ideal, then by proposition 3.3, $\mathfrak{p}_{\mathfrak{p}}$ is principal. Thus by lemma 3.4 \mathfrak{p} has codimension 1. Finally lemma 3.6 completes proof.

As I mentioned above, the geometric version of theorem 3.1 is quite useful:

Theorem 3.7. let V be a normal variety and W be a subvariety of codimension at least 2. Then every regular function on $V - W$ can extend to a regular function on V .

proof A function f in $\overline{K}(V)$ is regular at a point P if and only if $f \in \overline{K}[V]_P$. Thus if $f \in \overline{K}(V)$ is regular on $V - W$ then $f \in \overline{K}[V]_P$ for every point $P \in V - W$. We need to show that for each point $P \in V$, $f \in \overline{K}[V]_P$. Let $Q \in W$. Then by Theorem 3.1

$$\overline{K}[V]_Q = \bigcap_{\substack{\mathfrak{p} \in \overline{K}[V]_Q \\ ht=1}} (\overline{K}[V]_Q)_{\mathfrak{p}\overline{K}[V]_Q}.$$

By the identity $(A_{\mathfrak{P}})_{\mathfrak{p}A_{\mathfrak{P}}} = A_{\mathfrak{p}}$ for prime ideals $\mathfrak{p} \subset \mathfrak{P} \subset A$,

$$\overline{K}[V]_Q = \bigcap_{M_Q \supseteq \mathfrak{p} \quad ht=1} \overline{K}[V]_{\mathfrak{p}}.$$

Since height of \mathfrak{p} is 1 and height of $I(W)$ is larger than or equal to 2, then $V_{\mathfrak{p}} - W \neq \emptyset$, say $P_0 \in V_{\mathfrak{p}} - W$, that is, $P_0 \in V - W$. So $M_{P_0} \supset \mathfrak{p}$ and so $f \in \overline{K}[V]_{P_0} \subset \overline{K}[V]_{\mathfrak{p}}$. Hence

$$f \in \overline{K}[V]_Q.$$

Example 3.8. Consider $A = k[x, y]$. Let $V = \mathbb{A}^2(k)$ and $W = \{(0, 0)\}$. Then $I(V) = (0)$ and $I(W) = (x, y)$. Since A is a UFD, V is normal, and W has height 2. So by Theorem 3.7, every regular function on $V - W$ can extend to a regular function on V .

4 Some interesting examples of varieties

Example 4.1. A factorial variety which is singular. Take $\sum_{i=1}^5 x_i^2 = 0$ in \mathbb{A}^5 .

Example 4.2. A normal variety which is not factorial. Take the cone $xy = z^2$ in \mathbb{A}^3

Example 4.3. A variety not non-singular in codimension 1. Take $y^2 = x^3$ in \mathbb{A}^2 .

References

- [1] Silvermann/The arithmetic of Elliptic Curves.
- [2] Harshone/Algebraic Geometry.
- [3] Atiyah and MacDonald/Introduction to commutative Algebra.
- [4] Eisenbud/Commutative Algebra.