CAMBRIDGE

Cambridge University Press
978-0-521-45901-3 - Algebraic Curves over Finite Fields
Carlos Moreno
Excerpt
More information

1

Algebraic curves and function fields

1.1 Geometric aspects

1.1.1 Introduction

In applications to arithmetical questions and coding theory, the basic field of constants will be the finite field $k = \mathbb{F}_0$ of characteristic p; in particular this will be apparent in the proof of the Riemann–Roch theorem as well as in the study of the zeta function of a curve. In the present chapter however the finite field $\mathbb{F}_0$ is replaced by its algebraic closure $\mathbb{F}$ which we can think of as the union of all finite extensions of $\mathbb{F}_0$. As a consequence of this choice of base field, the study of most of the geometric properties of curves and their connection with the algebraic properties of function fields can be guided by our geometric intuition as if we were working over the field of complex numbers.

In Section 1.1 we present the definitions necessary for an understanding of the fundamental properties of algebraic curves. The main result is Theorem 1.1 in Section 1.1.7 which establishes the existence of an algebraic curve which is a smooth model associated to a given function field K/k. We give there only a summary of the key results; the interested reader desiring more details is advised to consult the first chapter of Hartshorne's book [34] or Chapter II, Section 5 of Shafarevitch's book [76]. Section 1.2 is of a more technical nature and deals exclusively with the algebraic properties of the valuation rings of the function field of a curve. In a sense this part is a preparation for the proof of the Riemann–Roch theorem given in Chapter 2. The reader can find a more complete treatment in Chevalley ([11], Ch. I).

1.1.2 Affine varieties

Affine n-space over k is the set $\mathbb{A}^n$ consisting of all n-tuples of elements of k. If p is a point in $\mathbb{A}^n$ and $p = (a_1, \ldots, a_n)$, then the $a_i \in k$ are called the coordinates of p. $A = k[x_1, \ldots, x_n]$ denotes the polynomial ring in n variables over k. The evaluation of a polynomial $f \in A$ at points in $\mathbb{A}^n$ gives a map $f: \mathbb{A}^n \to k$. The set of points $p \in \mathbb{A}^n$ where $f(p) = 0$ is called the set of zeros of f. More generally if $T \subset A$, we associate with T the subset of $\mathbb{A}^n$ given by

$$Z(T) = \{p \in \mathbb{A} : f(p) = 0 \text{ for every } f \in T\}.$$

In particular if $\mathscr{S}$ is the ideal of A generated by T, we put $Z(T) = Z(\mathscr{S})$. A fundamental property of the ring A is its noetherian nature, which implies that any ideal $\mathscr{S}$ has a finite set of generators, i.e. $\mathscr{S} = (f_1, \ldots, f_r)$.

Definition 1.1 *A subset Y of $\mathbb{A}^n$ is called an algebraic subset if there exists a subset $T \subset A$ such that $Y = Z(T)$.*

Definition 1.2 *The Zariski topology on $\mathbb{A}^n$ is defined by taking the open subsets to be the complements of the algebraic sets.*

To see why this indeed defines a topology one needs to verify that the algebraic sets, which in this topology play the role of closed sets, satisfy the following properties: (i) the union of two algebraic sets is an algebraic set, (ii) the intersection of any family of algebraic sets is an algebraic set, (iii) the empty set and the whole space are algebraic sets. Only the second requirement is not obvious; it follows from the noetherian nature of A.

Example The affine line

Since $A = k[x]$ is a principal ideal domain, any ideal in A is of the form $(p(x))$, where $p(x)$ is a polynomial with coefficients in k. Since k is assumed to be algebraically closed, $p(x)$ splits into a finite number of linear factors. Hence the algebraic set associated with the ideal $(p(x))$ consists of the roots of $p(x)$. Therefore the closed sets of $\mathbb{A}^1$ are $\mathbb{A}^1$ itself and all finite subsets. Observe that any two open subsets in $\mathbb{A}^1$ always have a non-void intersection.

A non-empty subset Y of a topological space X is said to be *irreducible* if it cannot be expressed as the union $Y = Y_1 \cup Y_2$ of two proper subsets, each of which is closed in Y. The empty set is not considered to be irreducible.

Definition 1.3 *An affine variety is an irreducible closed subset of $\mathbb{A}^n$. An open subset of an affine variety is a quasi-affine variety.*

If Y is a subset of $\mathbb{A}^n$, we define the ideal of Y in $A = k[x_1, \ldots, x_n]$ by

$$I(Y) = \{f \in A : f(p) = 0 \text{ for all } p \in Y\}.$$

The Hilbert Nullstellensatz guarantees that the maps $Y \to I(Y)$ and $\mathscr{S} \to Z(\mathscr{S})$ defined above set up a one-to-one correspondence between algebraic sets in $\mathbb{A}^n$ and ideals $\mathscr{S}$ in A which satisfy

$$\mathscr{S} = \{f \in A : f^r \in \mathscr{S} \text{ for some integer } r > 0\},$$

i.e. $\mathscr{S}$ is its own radical. Under this correspondence an irreducible algebraic set in $\mathbb{A}^n$ is associated to a prime ideal.

Example Let f be an irreducible polynomial in $A = k[x, y]$. Since A is a unique factorization domain, f generates a prime ideal (f) and the corresponding algebraic set $Y = Z(f)$ is irreducible. If f is of degree d, then Y is said to be a curve of degree d.

A maximal ideal m of $A = k[x_1, \ldots, x_n]$ corresponds to a minimal irreducible closed subset of $\mathbb{A}^n$; in fact $Z(m)$ must be a point, say $p = (a_1, \ldots, a_n)$. Therefore every maximal ideal of A is of the form $m = (x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n$ in k.

Definition 1.4 *If $Y \subseteq \mathbb{A}^n$ is an affine algebraic set, we define the affine coordinate ring $A(Y)$ to be the quotient $A/I(Y)$.*

Remark If Y is an affine variety, then $I(Y)$ is a prime ideal and therefore $A(Y)$ is an integral domain. The coordinate ring $A(Y)$ of an affine algebraic set is a finitely generated k-algebra. Conversely, any finitely generated k-algebra which is a domain is the affine coordinate ring of some affine variety; in fact such a k-algebra is the quotient of a polynomial ring $A = k[x_1, \ldots, x_n]$ by an ideal $\mathscr{S}$, in which case we can take as affine variety $Y = Z(\mathscr{S})$.

A topological space Y is called noetherian if for any sequence $Y_1 \supseteq Y_2 \supseteq \cdots$ of closed subsets there is an integer r such that $Y_r = Y_{r+1} = \cdots$. A basic property of a noetherian space X is that every non-empty closed subset Y can be expressed uniquely as a finite union $Y = Y_1 \cup \cdots \cup Y_r$ where the Y_i are irreducible sets and $Y_i \supsetneq Y_j$ for $i \neq j$. The Y_i are called the irreducible components of Y. Since $\mathbb{A}^n$ is a noetherian space, a property inherited from the polynomial ring $A = k[x_1, \ldots, x_n]$, we see that every algebraic set can be represented uniquely as a union of varieties, no one containing another.

Definition 1.5 *If X is a topological space, we define the dimension of X to be the supremum of all integers n such that there exists a chain $Z_0 \subset Z_1 \subset \cdots \subset Z_n$ of distinct irreducible closed subsets of X. The dimension of an affine or quasi-affine variety is defined to be its dimension as a topological space.*

Example The dimension of the affine line $\mathbb{A}^1$ is clearly 1, since the only irreducible closed subsets of $\mathbb{A}^1$ are the whole space and the single points.

The dimension of an affine variety Y is also equal to the Krull dimension of its affine coordinate ring $A(Y)$. If k is a field, and B is a domain, which is also a finitely generated k-algebra, then the Krull dimension of B is equal to the transcendence degree of the quotient field $K(B)$ of B over k. For example $\dim \mathbb{A}^n = n$ since $K(\mathbb{A}^n) = k(x_1, \ldots, x_n)$ is of transcendence degree n over k.

Remark If Y is a quasi-affine variety, then $\dim Y = \dim \bar{Y}$, where $\bar{Y}$ is the closure of Y in the Zariski topology.

Since the noetherian integral domain $A = k[x_1, \ldots, x_n]$ is a unique factorization domain, a variety Y in $\mathbb{A}^n$ has dimension $n - 1$ if and only if it is the zero set $Z(f)$ of a single non-constant irreducible polynomial in A. Thus the algebraic curves in $\mathbb{A}^2$ are in one-to-one correspondence with the non-constant irreducible polynomials in $A = k[x, y]$.

1.1.3 Projective varieties

Projective n-space over k is the set $\mathbb{P}^n$ consisting of all equivalence classes of $(n+1)$-tuples $(a_0, \ldots, a_n)$ of elements of k, not all zero, under the equivalence relation given by $(a_0, \ldots, a_n) \sim (\lambda a_0, \ldots, \lambda a_n)$ for all $\lambda \in k$, $\lambda \neq 0$. As a set $\mathbb{P}^n$ can be identified as the space of all lines in $\mathbb{A}^{n+1}$ passing through the origin. An element in $\mathbb{P}^n$ is called a point. If $p \in \mathbb{P}^n$ is a point, then any $(n+1)$-tuple $(a_0, \ldots, a_n)$ in the equivalence class of p is called a *set of homogeneous coordinates* for p. On the polynomial ring $S = k[x_0, \ldots, x_n]$ we introduce a grading

$$S = \bigoplus_{d \geq 0} S_d,$$

where S_d is the set of all linear combinations of monomials of total weight d in $x_0, \ldots, x_n$. Clearly we have for any $d, e \geq 0$ that $S_d S_e \subseteq S_{d+e}$. An element of S_d is called a homogeneous polynomial of degree d. It is obvious that any element of S has a unique decomposition as a finite sum of homogeneous polynomials. An ideal $\mathcal{S} \subseteq S$ is called a homogeneous ideal if $\mathcal{S} = \bigoplus_{d \geq 0}(\mathcal{S} \cap S_d)$. It can be shown that an ideal is homogeneous if and only if it can be generated by homogeneous elements. The sum, product, intersection and radical of homogeneous ideals are homogeneous. To verify that a homogeneous ideal $\mathcal{S}$ in S is prime, it suffices to show for any two homogeneous elements f, g that $fg \in S$ implies $f \in \mathcal{S}$ or $g \in \mathcal{S}$.

If $f \in S_d$, i.e. $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$, then we have a well-defined map $f: \mathbb{P}^n \to \{0, 1\}$, where $f(p) = 0$ if $f(a_0, \ldots, a_n) = 0$ and $f(p) = 1$ if $f(a_0, \ldots, a_n) \neq 0$, where $(a_0, \ldots, a_n)$ is a set of homogeneous coordinates for p. If f is a homogeneous polynomial, we define the set of zeros of f to be the set of points p in $\mathbb{P}^n$ where $f(p) = 0$. If T is a set of homogeneous elements of S, we define the zero set of T to be

$$Z(T) = \{p \in \mathbb{P}^n : f(p) = 0 \text{ for all } f \in T\}.$$

If $\mathcal{S}$ is a homogeneous ideal in S, we define $Z(\mathcal{S}) = Z(T)$, where T is the set of all homogeneous elements in $\mathcal{S}$. Since S is a noetherian ring, we have as in the affine case, that any set T of homogeneous elements has a finite subset $f_1, \ldots, f_r$ such that $Z(T) = Z(f_1, \ldots, f_r)$.

Definition 1.6 *A subset Y of $\mathbb{P}^n$ is an algebraic set if there exists a set T of homogeneous elements of S such that $Y = Z(T)$.*

Definition 1.7 *The Zariski topology on $\mathbb{P}^n$ is defined by taking the open sets to be the complements of algebraic sets.*

Again to verify that indeed this definition makes sense one checks that: (i) the union of two algebraic sets is an algebraic set, (ii) the intersection of any family of algebraic sets is an algebraic set and (iii) the empty set and the whole space are algebraic sets.

Definition 1.8 *A projective variety is an irreducible algebraic set in $\mathbb{P}^n$, endowed with the induced topology. An open subset of a projective variety is called a quasi-projective variety.*

The dimension of a projective or quasi-projective variety is its dimension as a topological space. Let Y be any subset of $\mathbb{P}^n$; the homogeneous ideal of Y in S is the ideal $I(Y)$ generated by the set

$$\{f \in S : f \text{ is homogeneous and } f(p) = 0 \text{ for all } p \in Y\}.$$

If Y is an algebraic set, we define the homogeneous coordinate ring of Y to be $S(Y) = S/I(Y)$.

An important property of projective n-space $\mathbb{P}^n$ is that it has an open covering consisting of affine n-spaces. Let us see how this comes about. If f is a linear homogeneous polynomial then the zero set of f is called a *hyperplane*. In particular we denote the zero set of x_i by H_i for $i = 0, \ldots, n$. Let U_i be the open set $\mathbb{P}^n - H_i$. If p is any point in $\mathbb{P}^n$ with homogeneous coordinates $(a_0, \ldots, a_n)$, then $a_i \neq 0$ for at least one i and hence $p \in H_i$. This shows that $\mathbb{P}^n$ is covered by the open sets U_i. We now define a map

$$\varphi_i \colon U_i \to \mathbb{A}^n$$

as follows: if $p \in U_i$ has homogeneous coordinates $(a_0, \ldots, a_n)$, then $\varphi_i(p) = q$, where q is the point in $\mathbb{A}^n$ with affine coordinates

$$(a_0/a_i, \ldots, a_n/a_i),$$

with a_i/a_i omitted. The map φ_i is well defined since the ratios a_j/a_i are independent of the choice of homogeneous coordinates. The map φ_i is in fact a homeomorphism from U_i with its induced topology to $\mathbb{A}^n$ with its Zariski topology. This property of $\mathbb{P}^n$ is also inherited by projective and quasi-projective varieties: if Y is a projective (respectively, quasi-projective) variety, then Y is covered by the open sets $Y \cap U_i$, $i = 0, \ldots, n$ which are homomorphic to affine (respectively, quasi-affine) varieties via the map φ_i.

1.1.4 Morphisms

Let Y be a quasi-affine variety in $\mathbb{A}^n$.

Definition 1.9 *A function $f \colon Y \to k$ is regular at a point $p \in Y$ if there is an open neighborhood U with $p \in U \subseteq Y$, and polynomials $g, h \in k[x_1, \ldots, x_n]$ such that h is nowhere zero on U, and $f = g/h$ on U. We say f is regular on Y if it is regular at every point of Y.*

Remark If k is identified with the affine line $\mathbb{A}^1$ together with its Zariski topology, then a regular function $f \colon Y \to \mathbb{A}^1$ is continuous.

Let $Y \subseteq \mathbb{P}^n$ be a quasi-projective variety.

Definition 1.10 *A function $f \colon Y \to k$ is regular at a point $p \in Y$ if there is an open neighborhood U with $p \in U \subseteq Y$, and homogeneous polynomials $g, h \in S = k[x_0, \ldots, x_n]$ of the same degree, such that h is nowhere zero on U and $f = g/h$ on U. We say that f is regular on Y if it is regular at every point.*

In the following an affine, a quasi-affine, a projective or a quasi-projective variety will simply be referred to as a variety.

Definition 1.11 *If X, Y are two varieties, a morphism*

$$\varphi\colon X \to Y$$

is a continuous map such that for every open set $V \subseteq Y$, and for every regular function $f\colon V \to k$, the function $f \circ \varphi\colon \varphi^{-1}(V) \to k$ is regular.

Let Y be a variety. We denote by $\mathcal{O}(Y)$ the ring of all regular functions on Y. If p is a point of Y, we define the local ring of p on Y, $\mathcal{O}_{p,Y}$ (or simply $\mathcal{O}_p$) to be the local ring of germs of regular functions on Y near p. Recall that a germ of a regular function at p is the equivalence class of pairs $\langle U, f\rangle$, where U is an open subset of Y containing p, and f is a regular function on U, and where two such pairs $\langle U, f\rangle$ and $\langle V, g\rangle$ are said to be equivalent if $f = g$ on $U \cap V$. $\mathcal{O}_p$ is a local ring and its maximal ideal $\mathfrak{m}$ is the set of germs of regular functions which vanish at p. Since we are assuming that the base field k is algebraically closed, we have that the residue field $k_p = \mathcal{O}_p/\mathfrak{m}$ is isomorphic to k.

Definition 1.12 *The function field $K(Y)$ of a variety Y is the set of all equivalence classes of pairs $\langle U, f\rangle$ where U is a non-empty subset of Y, f is a regular function on U, and where we identify two pairs $\langle U, f\rangle$ and $\langle V, g\rangle$ if $f = g$ on $U \cap V$. The elements of $K(Y)$ are called the rational functions on Y.*

The natural maps $\mathcal{O}(Y) \to \mathcal{O}_p \to K(Y)$ are clearly injective. If $Y \subseteq \mathbb{A}^n$ is an affine algebraic variety, then its affine coordinate ring $A(Y)$ is isomorphic to the ring of all regular functions $\mathcal{O}(Y)$. If to each point $p \in Y$ we associate the ideal $\mathfrak{m}_p \subseteq A(Y)$ of functions vanishing at p, then the map $p \to \mathfrak{m}_p$ sets up a one-to-one correspondence between the points of Y and the maximal ideals of $A(Y)$. Furthermore, for each point p, the localization $A(Y)_{\mathfrak{m}_p}$ of $A(Y)$ at the ideal $\mathfrak{m}_p$ is isomorphic to the local ring $\mathcal{O}_p$. The quotient field of the affine coordinate ring $A(Y)$ is isomorphic to the function field $K(Y)$, and hence it is a finitely generated extension field of k of transcendence degree $= \dim Y$.

Consider $S = k[x_0, \ldots, x_n]$ as a graded ring and let $\mathcal{Q}$ be a homogeneous prime ideal in S, let T be the multiplicative subset of S consisting of the homogeneous elements not in $\mathcal{Q}$. The localization $S_{\mathcal{Q}} = T^{-1}S$ of S with respect to T has a natural grading given by $\deg(f/g) = \deg f - \deg g$ for f a homogeneous element on S and $g \in T$. The subring

$$S_{(\mathscr{Q})} = \{f/g \in T^{-1}S\colon \deg(f/g) = 0\}$$

is a local ring with maximal ideal $(\mathscr{Q} \cdot T^{-1}S) \cap S_{(\mathscr{Q})}$. If S is a domain and $\mathscr{Q} = (0)$, then $S_{(0)}$ is a field. If $f \in S$ is a homogeneous element, we denote by $S_{(f)}$ the subring of elements of degree 0 in the localized ring S_f.

Let $S(Y)$ be the homogeneous coordinate ring of a projective variety $Y \subseteq \mathbb{P}^n$. A characteristic property of such varieties is that the ring of all regular functions is identical to the field of constants:

$$\mathcal{O}(Y) = k,$$

i.e. the only functions which are regular everywhere on a projective variety are the constants. Let p be any point on Y and define the ideal

$$\mathscr{m}_p = \{f \in S(Y)\colon f \text{ homogeneous and } f(p) = 0\}.$$

We then have $\mathcal{O}_p = S(Y)_{(\mathscr{m}_p)}$. Furthermore if $K(Y)$ is the function field of Y, then $K(Y) \simeq S(Y)_{((0))}$.

Remark The correspondence $X \to A(X)$ which associates to a variety its coordinate ring and the analogous correspondence that sends a point $p \in X$ to its local ring $\mathcal{O}_p$ are the key to the reduction of geometric problems to questions about finitely generated k-algebras.

Finally we mention the well-known result concerning the finiteness of integral closure, a result that will be useful later on. Let A be an integral domain which is a finitely generated algebra over a field k. Let K be the quotient field of A, and let L be a finite algebraic extension of K. Then the integral closure A' of A in L is a finitely generated A-module, and is also a finitely generated k-algebra.

1.1.5 Rational maps

Let φ and ψ be two morphisms from the variety X to the variety Y. Suppose φ and ψ agree when restricted to a non-empty open subset. The image $(\varphi \times \psi)(U)$ of U under the product map $\varphi \times \psi\colon X \to Y \times Y$ $(\varphi \times \psi)(x) = (\varphi(x), \psi(x))$ is a dense subset of the diagonal $\Delta_Y = \{(y, y)\colon y \in Y\}$, which is itself a closed subset. The closure $(\varphi \times \psi)(X)$ is therefore also contained in Δ_Y. This shows that φ and ψ agree everywhere.

Definition 1.13 *Let X and Y be varieties. A rational map $\varphi\colon X \to Y$ is an equivalence class of pairs $\langle U, \varphi_U \rangle$, where U is a non-empty open subset of*

X, φ_U is a morphism of U to Y, and where $\langle U, \varphi_U \rangle$ and $\langle V, \varphi_V \rangle$ are equivalent if φ_U and φ_V agree on $U \cap V$. The rational map φ is dominant if for some pair $\langle U, \varphi_U \rangle$, the image of φ_U is dense in Y.

Definition 1.14 *Two varieties X and Y are called birationally isomorphic, or simply isomorphic if there is a rational map $\varphi: X \to Y$ which admits an inverse, namely a rational map $\psi: Y \to X$ such that $\psi \circ \varphi = id_X$ and $\varphi \circ \psi = id_Y$ as rational maps.*

Let $Y \subseteq \mathbb{A}^n$ be a hypersurface in affine space defined by the equation $f(x_1, \ldots, x_n) = 0$. Let $\mathbb{A}^n - Y$ be the set of points in $\mathbb{A}^n$ where $f \neq 0$; if $H \subseteq \mathbb{A}^{n+1}$ is the algebraic set defined by $H = \{(x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1}: x_{n+1} f(x_1, \ldots, x_n) = 1\}$, then the rational map $(x_1, \ldots, x_n) \to (x_1, \ldots, x_n, f^{-1})$ sets the algebraic sets $\mathbb{A}^n - Y$ and H in birational correspondence. In particular $\mathbb{A}^n - Y$ is affine and its affine coordinate ring is the local ring $k[x_1, \ldots, x_n]_f$. If p is a point of X and Y is a hypersurface which does not contain p, then the above fact shows that $X - (X \cap Y)$ contains an open neighborhood U with $p \in U$ and U is birationally isomorphic to an affine open subset. This shows that any variety X has a base for the Zariski topology consisting of affine open subsets.

Let X and Y be any two varieties. Let $\varphi: X \to Y$ be a dominant rational map represented by the pair $\langle U, \varphi_V \rangle$. Let $f \in K(Y)$ be a rational function represented by the pair $\langle V, f \rangle$, where $V \subseteq Y$ is an open subset and f is a regular function on V. Since $\varphi_U(U)$ is a dense subset of Y, the subset $\varphi_U^{-1}(V)$ is non-empty and open in X. Therefore the composite $f \circ \varphi_U$ represents a regular function on $\varphi_U^{-1}(V)$, i.e. $f \circ \varphi$ is a rational function on X. This construction gives a bijection between the set of dominant rational maps from X to Y and the set of k-algebra homomorphisms from $K(Y)$ to $K(X)$. In particular two varieties X and Y are birationally isomorphic if and only if their function fields $K(X)$ and $K(Y)$ are isomorphic as k-algebras.

Definition 1.15 *A field extension K/k is separably generated if there is a transcendence base $\{x_i\}$ for K/k such that K is a separable algebraic extension of $k(\{x_i\})$. Such a transcendence base is called a separating transcendence base.*

A basic property of a finitely and separably generated field extension K/k is that any set of generators always contains a subset which is a separating transcendence base. A field K is called *perfect* if the polynomials in $k[x]$ are separable, i.e. the irreducible factors of any polynomial in $k[x]$ have distinct roots. For example if k is algebraically closed, then it is perfect. If

Cambridge University Press
978-0-521-45901-3 - Algebraic Curves over Finite Fields
Carlos Moreno
Excerpt
More information

K/k is a finitely generated field extension over a perfect base field k, then it is separably generated. These results apply in particular to the function field K/k of an algebraic curve over the finite field of constants $k = \mathbb{F}_q$. The following result is the well-known theorem of the primitive element: if L is a finite separable extension of a field K, then there is an element α in L which generates L as an extension field of K. In fact if $\beta_1, \ldots, \beta_n$ is any set of generators of L over K, and if K is infinite, then α can be taken to be a linear combination $\alpha = c_1\beta_1 + \cdots + c_n\beta_n$ of the β_i with coefficients $c_i \in K$. An interesting application of this theorem is to the proof, which is now straightforward, that any variety of dimension r is birationally isomorphic to a hypersurface Y in $\mathbb{P}^{r+1}$.

1.1.6 Non-singular varieties

Let $Y \subseteq \mathbb{A}^n$ be an affine variety of dimension r, and let the ideal of Y be generated by the polynomials $f_1, \ldots, f_t \in k[x_1, \ldots, x_n]$, i.e. $I(Y) = (f_1, \ldots, f_t)$. Now the classical Jacobian criterion for a point $p \in Y$ to be simple is that the rank of the matrix $[(\partial f_j/\partial x_i)(p)]$ be $n - r$. Y is said to be non-singular if each of its points is simple. Recall that a noetherian local ring A with maximal ideal $\mathfrak{m}$ and residue field $k = A/\mathfrak{m}$ always satisfies $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq \dim A$; if strict equality holds, then A is called a *regular local ring*. This concept is of relevance in the study of non-singular varieties because if $Y \subseteq \mathbb{A}^n$ is an affine variety and $p \in Y$ is a point, then p is a simple point on Y if and only if the local ring $\mathcal{O}_{p,Y}$ is a regular local ring. This intrinsic characterization allows us to make the following definition.

Definition 1.16 *Let Y be any variety. Y is non-singular at a point $p \in Y$ if the local ring $\mathcal{O}_{p,Y}$ is a regular local ring. Y is non-singular if it is non-singular at every point.*

If Y is a variety then the set Sing Y of non-simple points of Y is a proper closed subset of Y. In particular if Y is a curve it can have at most a finite number of singular points. It is also clear that the projective line is non-singular. The completion of a local ring A with maximal ideal $\mathfrak{m}$ can be defined as the projective limit ([2], p. 100)

$$\hat{A} = \varprojlim_n A/\mathfrak{m}^n.$$

If A is a noetherian local ring with maximal ideal $\mathfrak{m}$, then its completion $\hat{A}$ is a local ring with maximal ideal $\hat{\mathfrak{m}} = \mathfrak{m} \cdot \hat{A}$ and there is a natural injective homomorphism $A \to \hat{A}$. We also have $\dim A = \dim \hat{A}$. If M is a finitely