Chapter I

Algebraic Varieties

In this chapter we describe the basic objects that arise in the study of algebraic geometry. We set the following notation, which will be used throughout this book.

K	a perfect field, i.e., every algebraic extension of K is separable.
$\bar{K}$	a fixed algebraic closure of K.
$G_{\bar{K}/K}$	the Galois group of $\bar{K}/K$.

For this chapter, we also let m and n denote positive integers.

The assumption that K is a perfect field is made solely to simplify our exposition. However, since our eventual goal is to do arithmetic, the field K will eventually be taken to be an algebraic extension of $\mathbb{Q}$, $\mathbb{Q}_p$, or $\mathbb{F}_p$. Thus this restriction on K need not concern us unduly.

For a more extensive exposition of the basic concepts that appear in this chapter, we refer the reader to any introductory book on algebraic geometry, such as [95], [109], [111], or [243].

I.1 Affine Varieties

We begin our study of algebraic geometry with Cartesian (or affine) n-space and its subsets defined by zeros of polynomials.

Definition. *Affine n-space (over K)* is the set of n-tuples

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

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

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

J.H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, Graduate Texts in Mathematics 106, DOI 10.1007/978-0-387-09494-6_I,

Notice that the Galois group $G_{\bar{K}/K}$ acts on $\mathbb{A}^n$; for $\sigma \in G_{\bar{K}/K}$ and $P \in \mathbb{A}^n$,

$$P^\sigma = (x_1^\sigma, \dots, x_n^\sigma).$$

Then $\mathbb{A}^n(K)$ may be characterized by

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

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

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

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

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

An algebraic set 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, then the *set of K-rational points of* V is the set

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

Remark 1.1. Note that by the Hilbert basis theorem [8, 7.6], [73, §1.4], all ideals in $\bar{K}[X]$ and $K[X]$ are finitely generated.

Remark 1.2. Let V be an algebraic set, and consider the ideal $I(V/K)$ defined by

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

Then we see that V is defined over K if and only if

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

Now suppose that V is defined over K and let $f_1, \dots, f_m \in K[X]$ be generators for $I(V/K)$. Then $V(K)$ is precisely the set of solutions $(x_1, \dots, x_n)$ to the simultaneous polynomial equations

$$f_1(X) = \cdots = f_m(X) = 0 \quad \text{with } x_1, \dots, x_n \in K.$$

Thus one of the fundamental problems in the subject of *Diophantine geometry*, namely the solution of polynomial equations in rational numbers, may be said to be the problem of describing sets of the form $V(K)$ when K is a number field.

Notice that if $f(X) \in K[X]$ and $P \in \mathbb{A}^n$, then for any $\sigma \in G_{\bar{K}/K}$,

$$f(P^\sigma) = f(P)^\sigma.$$

Hence if V is defined over K, then the action of $G_{\bar{K}/K}$ on $\mathbb{A}^n$ induces an action on V, and clearly

$$V(K) = \{P \in V : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Example 1.3.1. Let V be the algebraic set in $\mathbb{A}^2$ given by the single equation

$$X^2 - Y^2 = 1.$$

Clearly V is defined over K for any field K. Let us assume that $\mathrm{char}(K) \neq 2$. Then the set $V(K)$ is in one-to-one correspondence with $\mathbb{A}^1(K) \smallsetminus \{0\}$, one possible map being

$$\begin{aligned} \mathbb{A}^1(K) \smallsetminus \{0\} &\longrightarrow V(K), \\ t &\longmapsto \left(\frac{t^2+1}{2t}, \frac{t^2-1}{2t} \right). \end{aligned}$$

Example 1.3.2. The algebraic set

$$V : X^n + Y^n = 1$$

is defined over $\mathbb{Q}$. Fermat's last theorem, proven by Andrew Wiles in 1995 [291, 311], states that for all $n \geq 3$,

$$V(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\} & \text{if } n \text{ is odd,} \\ \{(\pm 1,0),(0,\pm 1)\} & \text{if } n \text{ is even.} \end{cases}$$

Example 1.3.3. The algebraic set

$$V : Y^2 = X^3 + 17$$

has many $\mathbb{Q}$-rational points, for example

$$(-2,3) \qquad (5234, 378661) \qquad \left(\frac{137}{64}, \frac{2651}{512} \right).$$

In fact, the set $V(\mathbb{Q})$ is infinite. See (I.2.8) and (III.2.4) for further discussion of this example.

Definition. An affine algebraic set V is called an (*affine*) *variety* if $I(V)$ is a prime ideal in $\bar{K}[X]$. Note that if V is defined over K, it is not enough to check that $I(V/K)$ is prime in $K[X]$. For example, consider the ideal $(X_1^2 - 2X_2^2)$ in $\mathbb{Q}[X_1, X_2]$.

Let V/K be a variety, i.e., V is a variety defined over K. Then the *affine coordinate ring of* V/K is defined by

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

The ring $K[V]$ is an integral domain. Its quotient field (field of fractions) is denoted by $K(V)$ and 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 adding a polynomial vanishing on V, it induces a well-defined function $f : V \to \bar{K}$. If $f(X) \in \bar{K}[X]$ is any polynomial, then $G_{\bar{K}/K}$ acts on f by acting on its coefficients. Hence if V is defined over K, so $G_{\bar{K}/K}$ takes $I(V)$ into itself, then we obtain an action of $G_{\bar{K}/K}$ on $\bar{K}[V]$ and $\bar{K}(V)$. One can check (Exercise 1.12) that $K[V]$ and $K(V)$ are, respectively, the subsets of $\bar{K}[V]$ and $\bar{K}(V)$ fixed by $G_{\bar{K}/K}$. We denote the action of $\sigma \in G_{\bar{K}/K}$ on f by $f \mapsto f^\sigma$. Then for all points $P \in V$,

$$\bigl(f(P)\bigr)^\sigma = f^\sigma(P^\sigma).$$

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

Example 1.4. The dimension of $\mathbb{A}^n$ is n, since $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, \ldots, X_n)$. Similarly, if $V \subset \mathbb{A}^n$ is given by a single nonconstant polynomial equation

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

then $\dim(V) = n - 1$. (The converse is also true; see [111, I.1.2].) In particular, the examples described in (I.1.3.1), (I.1.3.2), and (I.1.3.3) all have dimension one.

In studying a geometric object, we are naturally interested in whether it looks reasonably "smooth." The next definition formalizes this notion in terms of the usual Jacobian criterion for the existence of a tangent plane.

Definition. Let V be a variety, $P \in V$, and $f_1, \ldots, f_m \in \bar{K}[X]$ a set of generators for $I(V)$. Then V is *nonsingular* (or *smooth*) *at* P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

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

Example 1.5. Let V be given by a single nonconstant polynomial equation

$$f(X_1, \ldots, X_n) = 0.$$

Then (I.1.4) tells us that $\dim(V) = n-1$, so $P \in V$ is a singular point if and only if

$$\frac{\partial f}{\partial X_1}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

Since P also satisfies $f(P) = 0$, this gives $n + 1$ equations for the n coordinates of any singular point. Thus for a "randomly chosen" polynomial f, one would expect V to be nonsingular. We will not pursue this idea further, but see Exercise 1.1.

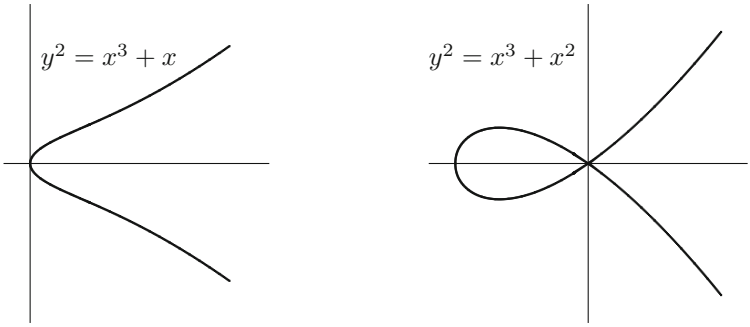


Figure 1.1: A smooth curve and a singular curve.

Example 1.6. Consider the two varieties

$$V_1 : Y^2 = X^3 + X \qquad \text{and} \qquad V_2 : Y^2 = X^3 + X^2.$$

Using (I.1.5), we see that any singular points on V_1 and V_2 satisfy, respectively,

$$V_1^{\text{sing}} : 3X^2 + 1 = 2Y = 0 \qquad \text{and} \qquad V_2^{\text{sing}} : 3X^2 + 2X = 2Y = 0.$$

Thus V_1 is nonsingular, while V_2 has one singular point, namely $(0, 0)$. The graphs of $V_1(\mathbb{R})$ and $V_2(\mathbb{R})$ illustrate the difference; see Figure 1.1.

There is another characterization of smoothness, in terms of the functions on the variety V, that is often quite useful. For each point $P \in V$, we define an ideal M_P of $\bar{K}[V]$ by

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

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

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

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

Proposition 1.7. *Let V be a variety. A point $P \in V$ is nonsingular if and only if*

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

PROOF. [111, I.5.1]. (See Exercise 1.3 for a special case.) □

Example 1.8. Consider the point $P = (0, 0)$ on the varieties V_1 and V_2 of (I.1.6). In both cases, M_P is the ideal of $\bar{K}[V]$ generated by X and Y, and M_P^2 is the ideal generated by X^2, XY, and Y^2. For V_1 we have

$$X = Y^2 - X^3 \equiv 0 \pmod{M_P^2},$$

so M_P/M_P^2 is generated by Y alone. On the other hand, for V_2 there is no nontrivial relationship between X and Y modulo M_P^2, so M_P/M_P^2 requires both X and Y as generators. Since each V_i has dimension one, (I.1.7) implies that V_1 is smooth at P and V_2 is not.

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

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

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

I.2 Projective Varieties

Historically, projective space arose through the process of adding "points at infinity" to affine space. We define projective space to be the collection of lines through the origin in affine space of one dimension higher.

Definition. *Projective n-space* (*over K*), denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\bar{K})$, 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 nonzero, modulo the equivalence relation

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

if there exists a $\lambda \in \bar{K}^*$ such that $x_i = \lambda y_i$ for all i. An equivalence class

$$\big\{(\lambda x_0, \dots, \lambda x_n) : \lambda \in \bar{K}^*\big\}$$

is denoted by $[x_0, \dots, x_n]$, and the individual $x_0, \dots, x_n$ 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

$$\mathbb{P}^n(K) = \big\{[x_0, \dots, x_n] \in \mathbb{P}^n : \text{all } x_i \in K\big\}.$$

Remark 2.1. Note that if $P = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$, it does not follow that each $x_i \in K$. However, choosing some i with $x_i \neq 0$, it does follow that $x_j/x_i \in K$ for every j.

Definition. Let $P = [x_0, \dots, x_n] \in \mathbb{P}^n(\bar{K})$. The *minimal field of definition for P* (*over K*) is the field

$$K(P) = K(x_0/x_i, \dots, x_n/x_i) \quad \text{for any } i \text{ with } x_i \neq 0.$$

The Galois group $G_{\bar{K}/K}$ acts on $\mathbb{P}^n$ by acting on homogeneous coordinates,

$$[x_0, \dots, x_n]^\sigma = [x_0^\sigma, \dots, x_n^\sigma].$$

This action is well-defined, independent of choice of homogeneous coordinates, since

$$[\lambda x_0, \dots, \lambda x_n]^\sigma = [\lambda^\sigma x_0^\sigma, \dots, \lambda^\sigma x_n^\sigma] = [x_0^\sigma, \dots, x_n^\sigma].$$

It is not difficult to check that

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\},$$

and that

$$K(P) = \text{fixed field of } \{\sigma \in G_{\bar{K}/K} : P^\sigma = P\};$$

see Exercise 1.12.

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

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n) \quad \text{for all } \lambda \in \bar{K}.$$

An ideal $I \subset \bar{K}[X]$ is *homogeneous* if it is generated by homogeneous polynomials.

Let f be a homogeneous polynomial and let $P \in \mathbb{P}^n$. It makes sense to ask whether $f(P) = 0$, since the answer is independent of the choice of homogeneous coordinates for P. To each homogeneous ideal I we associate a subset of $\mathbb{P}^n$ by the rule

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

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

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

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, then the *set of* K*-rational points of* V is the set

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

As usual, $V(K)$ may also be described as

$$V(K) = \{P \in V : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Example 2.2. A *line* in $\mathbb{P}^2$ is an algebraic set given by a linear equation

$$aX + bY + cZ = 0$$

with $a, b, c \in \bar{K}$ not all zero. If, say, $c \neq 0$, then such a line is defined over any field containing a/c and b/c. More generally, a *hyperplane* in $\mathbb{P}^n$ is given by an equation

$$a_0X_0 + a_1X_1 + \cdots + a_nX_n = 0$$

with $a_i \in \bar{K}$ not all zero.

Example 2.3. Let V be the algebraic set in $\mathbb{P}^2$ given by the single equation

$$X^2 + Y^2 = Z^2.$$

Then for any field K with $\operatorname{char}(K) \neq 2$, the set $V(K)$ is isomorphic to $\mathbb{P}^1(K)$, for example by the map

$$\mathbb{P}^1(K) \longrightarrow V(K), \qquad [s,t] \longmapsto [s^2 - t^2, 2st, s^2 + t^2].$$

(For the precise definition of "isomorphic," see (I.3.5).)

Remark 2.4. A point of $\mathbb{P}^n(\mathbb{Q})$ has the form $[x_0,\dots,x_n]$ with $x_i \in \mathbb{Q}$. Multiplying by an appropriate $\lambda \in \mathbb{Q}$, we can clear denominators and common factors from the x_i's. In other words, every $P \in \mathbb{P}^n(\mathbb{Q})$ may be written with homogeneous coordinates $[x_0,\dots,x_n]$ satisfying

$$x_0,\dots,x_n \in \mathbb{Z} \quad \text{and} \quad \gcd(x_0,\dots,x_n) = 1.$$

Note that the x_i's are determined by P up to multiplication by -1.

Thus if an ideal of an algebraic set $V/\mathbb{Q}$ is generated by homogeneous polynomials $f_1,\dots,f_m \in \mathbb{Q}[X]$, then describing $V(\mathbb{Q})$ is equivalent to finding the solutions to the homogeneous equations

$$f_1(X_0,\dots,X_n) = \cdots = f_m(X_0,\dots,X_n) = 0$$

in relatively prime integers $x_0,\dots,x_n$.

Example 2.5. The algebraic set

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

is defined over $\mathbb{Q}$. However, $V(\mathbb{Q}) = \emptyset$. To see this, suppose that $[x,y,z] \in V(\mathbb{Q})$ with $x,y,z \in \mathbb{Z}$ and $\gcd(x,y,z) = 1$. Then

$$x^2 + y^2 \equiv 0 \pmod 3,$$

so the fact that -1 is not a square modulo 3 implies that

$$x \equiv y \equiv 0 \pmod 3.$$

Hence x^2 and y^2 are divisible by 3^2. It follows from the equation for V that 3 also divides z, which contradicts the assumption that $\gcd(x,y,z) = 1$.

This example illustrates a fundamental tool used in the study of Diophantine equations.

> *In order to show that an algebraic set $V/\mathbb{Q}$ has no $\mathbb{Q}$-rational points, it suffices to show that the corresponding homogeneous polynomial equations have no nonzero solutions modulo p for any one prime p (or even for one prime power p^r).*

A more succinct way to phrase this is to say that if $V(\mathbb{Q})$ is nonempty, then $V(\mathbb{Q}_p)$ is nonempty for every p-adic field $\mathbb{Q}_p$. Similarly, $V(\mathbb{R})$ would also be nonempty. One of the reasons that the study of Diophantine equations is so difficult is that the converse to this statement, which is called the *Hasse principle*, does not hold in general. An example, due to Selmer [225, 227], is the equation

$$V : 3X^3 + 4Y^2 + 5Z^3 = 0.$$

One can check that $V(\mathbb{Q}_p)$ is nonempty for every prime p, yet $V(\mathbb{Q})$ is empty. See, e.g., [41, §4] for a proof. Other examples are given in (X.6.5).

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

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

$$\begin{aligned} \phi_i : \mathbb{A}^n &\longrightarrow \mathbb{P}^n, \\ (y_1, \dots, y_n) &\longmapsto [y_1, y_2, \dots, y_{i-1}, 1, y_i, \dots, y_n]. \end{aligned}$$

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

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

and we let U_i be the complement of H_i,

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

There is a natural bijection

$$\begin{aligned} \phi_i^{-1} : U_i &\longrightarrow \mathbb{A}^n, \\ [x_0, \dots, x_n] &\longmapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i},\right). \end{aligned}$$

(Note that for any point of $\mathbb{P}^n$ with $x_i \neq 0$, the quantities x_j/x_i are well-defined.) For a fixed 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 $I(V) \subset \bar{K}[X]$. Then $V \cap \mathbb{A}^n$, by which we mean $\phi_i^{-1}(V \cap U_i)$ for some fixed i, is an affine algebraic set with ideal $I(V \cap \mathbb{A}^n) \subset \bar{K}[Y]$ given by

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

Notice that the sets $U_0, \dots, U_n$ cover all of $\mathbb{P}^n$, so any projective variety V is covered by subsets $V \cap U_0, \dots, V \cap U_n$, each of which is an affine variety via an appropriate ϕ_i^{-1}. The process of replacing the polynomial $f(X_0, \dots, X_n)$ with the polynomial $f(Y_1, \dots, Y_{i-1}, 1, Y_{i+1}, \dots, Y_n)$ is called *dehomogenization with respect to* X_i.

This process can be reversed. For any $f(Y) \in \bar{K}[Y]$, we define

$$f^*(X_0, \dots, X_n) = X_i^d f\left(\frac{X_0}{X_i}, \frac{X_1}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_n}{X_i}\right),$$

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

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

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

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

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

Proposition 2.6. (a) *Let V be an affine variety. Then $\bar{V}$ is a projective variety, and*

$$V = \bar{V} \cap \mathbb{A}^n.$$

(b) *Let V be a projective variety. Then $V \cap \mathbb{A}^n$ is an affine variety, and either*

$$V \cap \mathbb{A}^n = \emptyset \qquad \text{or} \qquad V = \overline{V \cap \mathbb{A}^n}.$$

(c) *If an affine (respectively projective) variety V is defined over K, then $\bar{V}$ (respectively $V \cap \mathbb{A}^n$) is also defined over K.*

PROOF. See [111, I.2.3] for (a) and (b). Part (c) is clear from the definitions. □

Remark 2.7. In view of (I.2.6), each affine variety may be identified with a unique projective variety. Notationally, since it is easier to deal with affine coordinates, we will often say "let V be a projective variety" and write down some inhomogeneous equations, with the understanding that V is the projective closure of the indicated affine variety W. The points of $V \smallsetminus W$ are called the *points at infinity* on V.

Example 2.8. Let V be the projective variety given by the equation

$$V : Y^2 = X^3 + 17.$$

This really means that V is the variety in $\mathbb{P}^2$ given by the homogeneous equation

$$\bar{Y}^2\bar{Z} = \bar{X}^3 + 17\bar{Z}^3,$$

the identification being

$$X = \bar{X}/\bar{Z}, \qquad Y = \bar{Y}/\bar{Z}.$$

This variety has one point at infinity, namely $[0, 1, 0]$, obtained by setting $\bar{Z} = 0$. Thus, for example,

$$V(\mathbb{Q}) = \big\{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : y^2 = x^3 + 17\big\} \cup \big\{[0, 1, 0]\big\}.$$

In (I.1.3.3) we listed several points in $V(\mathbb{Q})$. The reader may verify (Exercise 1.5) that the line connecting any two points of $V(\mathbb{Q})$ intersects V in a third point of $V(\mathbb{Q})$ (provided that the line is not tangent to V). Using this secant line procedure repeatedly leads to infinitely many points in $V(\mathbb{Q})$, although this is by no means obvious. The variety V is an *elliptic curve*, and as such, it provides the first example of the varieties that will be our principal object of study in this book. See (III.2.4) for further discussion of this example.

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

Definition. Let V/K be a projective variety and choose $\mathbb{A}^n \subset \mathbb{P}^n$ such 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 by $K(V)$, is the function field of $V \cap \mathbb{A}^n$, and similarly for $\bar{K}(V)$. We note that for different choices of $\mathbb{A}^n$, the different $K(V)$ are canonically isomorphic, so we may identify them. (See (I.2.9) for another description of $K(V)$.)

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

Remark 2.9. The function field of $\mathbb{P}^n$ may also be described as the subfield of $\bar{K}(X_0, \dots, X_n)$ consisting of rational functions $F(X) = f(X)/g(X)$ for which f and g are *homogeneous* polynomials of the *same* degree. Such an expression gives a well-defined function on $\mathbb{P}^n$ at all point P where $g(P) \neq 0$. Similarly, the function field of a projective variety V is the field of rational functions $F(X) = f(X)/g(X)$ such that:

(i) f and g are homogeneous of the same degree;

(ii) $g \notin I(V)$;

(iii) two functions f_1/g_1 and f_2/g_2 are identified if $f_1 g_2 - f_2 g_1 \in I(V)$.

I.3 Maps Between Varieties

In this section we look at algebraic maps between projective varieties. These are maps that are defined by rational functions.

Definition. 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

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

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

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

If V_1 and V_2 are defined over K, then $G_{\bar{K}/K}$ acts on ϕ in the obvious way,

$$\phi^\sigma(P) = \big[f_0^\sigma(P), \dots, f_n^\sigma(P)\big].$$

Notice that we have the formula

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma) \qquad \text{for all } \sigma \in G_{\bar{K}/K} \text{ and } P \in V_1.$$

If, in addition, there is some $\lambda \in \bar{K}^*$ such that $\lambda f_0, \dots, \lambda f_n \in K(V_1)$, then ϕ is said to be *defined over* K. Note that $[f_0, \dots, f_n]$ and $[\lambda f_0, \dots, \lambda f_n]$ give the same map on points. As usual, it is true that ϕ is defined over K if and only if $\phi = \phi^\sigma$ for all $\sigma \in G_{\bar{K}/K}$; see Exercise 1.12c.

Remark 3.1. A rational map $\phi : V_1 \to V_2$ is not necessarily a well-defined function at every point of V_1. However, it may be possible to evaluate $\phi(P)$ at points P of V_1 where some f_i is not regular by replacing each f_i by gf_i for an appropriate $g \in \bar{K}(V_1)$.

Definition. A rational map

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

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

(i) each gf_i is regular at P;

(ii) there is some i for which $(gf_i)(P) \neq 0$.

If such a g exists, then we set

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

N.B. It may be necessary to take different g's for different points. A rational map that is regular at every point is called a *morphism*.

Remark 3.2. Let $V_1 \subset \mathbb{P}^m$ and $V_2 \subset \mathbb{P}^n$ be projective varieties. Recall (I.2.9) that the functions in $\bar{K}(V_1)$ may be described as quotients of homogeneous polynomials in $\bar{K}[X_0, \ldots, X_m]$ having the same degree. Thus by multiplying a rational map $\phi = [f_0, \ldots, f_n]$ by a homogeneous polynomial that "clears the denominators" of the f_i's, we obtain the following alternative definition:

A *rational map* $\phi : V_1 \to V_2$ is a map of the form

$$\phi = \big[\phi_0(X), \ldots, \phi_n(X)\big],$$

where

(i) the $\phi_i(X) \in \bar{K}[X] = \bar{K}[X_0, \ldots, X_n]$ are homogeneous polynomials, not all in $I(V_1)$, having the same degree;

(ii) for very $f \in I(V_2)$,

$$f\big(\phi_0(X), \ldots, \phi_n(X)\big) \in I(V_1).$$

Clearly, $\phi(P)$ is well-defined provided that some $\phi_i(P) \neq 0$. However, even if all $\phi_i(P) = 0$, it may be possible to alter ϕ so as to make sense of $\phi(P)$. We make this precise as follows:

A rational map $\phi = [\phi_0, \ldots, \phi_n] : V_1 \to V_2$ as above is *regular* (or *defined*) at $P \in V_1$ if there exist homogeneous polynomials $\psi_0, \ldots, \psi_n \in \bar{K}[X]$ such that

(i) $\psi_0, \ldots, \psi_n$ have the same degree;

(ii) $\phi_i\psi_j \equiv \phi_j\psi_i \pmod{I(V_1)}$ for all $0 \leq i, j \leq n$;

(iii) $\psi(P) \neq 0$ for some i.

If this occurs, then we set

$$\phi(P) = \big[\psi_0(P), \dots, \psi_n(P)\big].$$

As above, a rational map that is everywhere regular is called a *morphism*.

Remark 3.3. Let $\phi = [\phi_0, \dots, \phi_n] : \mathbb{P}^m \to \mathbb{P}^n$ be a rational map as in (I.3.2), where the $\phi_i \in \bar{K}[X]$ are homogeneous polynomials of the same degree. Since $\bar{K}[X]$ is a unique factorization domain (UFD), we may assume that the ϕ_i's have no common factor. Then ϕ is regular at a point $P \in \mathbb{P}^m$ if and only if some $\phi_i(P) \neq 0$. (Note that $I(\mathbb{P}^m) = (0)$, so there is no way to alter the ϕ_i's.) Hence ϕ is a morphism if and only if the ϕ_i's have no common zero in $\mathbb{P}^m$.

Definition. Let V_1 and V_2 be varieties. We say that V_1 and V_2 are *isomorphic*, and write $V_1 \cong V_2$, if there are morphisms $\phi : V_1 \to V_2$ and $\psi : V_2 \to V_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on V_1 and V_2, respectively. We say that V_1/K and V_2/K are *isomorphic over* K if ϕ and ψ can be defined over K. Note that both ϕ and ψ must be morphisms, not merely rational maps.

Remark 3.4. If $\phi : V_1 \to V_2$ is an isomorphism defined over K, then ϕ identifies $V_1(K)$ with $V_2(K)$. Hence for Diophantine problems, it suffices to study any one variety in a given K-isomorphism class of varieties.

Example 3.5. Assume that $\operatorname{char}(K) \neq 2$ and let V be the variety from (I.2.3),

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

Consider the rational map

$$\phi : V \longrightarrow \mathbb{P}^1, \qquad \phi = [X + Z, Y].$$

Clearly ϕ is regular at every point of V except possibly at $[1, 0, -1]$, i.e., at the point where $X + Z = Y = 0$. However, using

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

we have

$$\phi = [X + Z, Y] = [X^2 - Z^2, Y(X - Z)] = [-Y^2, Y(X - Z)] = [-Y, X - Z].$$

Thus

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

so ϕ is regular at every point of V, i.e., ϕ is a morphism. One easily checks that the map

$$\psi : \mathbb{P}^1 \longrightarrow V, \qquad \psi = [S^2 - T^2, 2ST, S^2 + T^2],$$

is a morphism and provides an inverse for ϕ, so V and $\mathbb{P}^1$ are isomorphic.

Example 3.6. Using (I.3.3), we see that the rational map

$$\phi : \mathbb{P}^2 \longrightarrow \mathbb{P}^2, \qquad \phi = [X^2, XY, Z^2],$$

is regular everywhere except at the point $[0, 1, 0]$.

Example 3.7. Let V be the variety

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

and consider the rational maps

$$\begin{aligned} &\psi : \mathbb{P}^1 \to V, && \psi = \big[(S^2 - T^2)T, (S^2 - T^2)S, T^3\big], \\ &\phi : V \to \mathbb{P}^1, && \phi = [Y, X]. \end{aligned}$$

Here ψ is a morphism, while ϕ is not regular at $[0, 0, 1]$. Not coincidentally, the point $[0, 0, 1]$ is a singular point of V; see (II.2.1). We emphasize that although the compositions $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map wherever they are defined, the maps ϕ and ψ are not isomorphisms, because ϕ is not a morphism.

Example 3.8. Consider the varieties

$$V_1 : X^2 + Y^2 = Z^2 \qquad \text{and} \qquad V_2 : X^2 + Y^2 = 3Z^2.$$

They are not isomorphic over $\mathbb{Q}$, since $V_2(\mathbb{Q}) = \emptyset$ from (I.2.5), while $V_1(\mathbb{Q})$ contains lots of points. (More precisely, $V_1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Q})$ from (I.3.5).) However, the varieties V_1 and V_2 are isomorphic over $\mathbb{Q}(\sqrt{3}\,)$, an isomorphism being given by

$$\phi : V_2 \longrightarrow V_1, \qquad \phi = [X, Y, \sqrt{3}\,Z].$$

Exercises

1.1. Let $A, B \in \bar{K}$. Characterize the values of A and B for which each of the following varieties is singular. In particular, as (A, B) ranges over $\mathbb{A}^2$, show that the "singular values" lie on a one-dimensional subset of $\mathbb{A}^2$, so "most" values of (A, B) give a nonsingular variety.
(a) $V : Y^2Z + AXYZ + BYZ^2 = X^3$.
(b) $V : Y^2Z = X^3 + AXZ^2 + BZ^3$. (You may assume that $\operatorname{char}(K) \neq 2$.)

1.2. Find the singular point(s) on each of the following varieties. Sketch $V(\mathbb{R})$.
(a) $V : Y^2 = X^3$ in $\mathbb{A}^2$.
(b) $V : 4X^2Y^2 = (X^2 + Y^2)^3$ in $\mathbb{A}^2$.
(c) $V : Y^2 = X^4 + Y^4$ in $\mathbb{A}^2$.
(d) $V : X^2 + Y^2 = (Z - 1)^2$ in $\mathbb{A}^3$.

1.3. Let $V \subset \mathbb{A}^n$ be a variety given by a single equation as in (I.1.4). Prove that a point $P \in V$ is nonsingular if and only if

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

(*Hint*. Let $f = 0$ be the equation of V and define the *tangent plane of* V *at* P by

$$T = \left\{ (y_1, \dots, y_n) \in \mathbb{A}^n : \sum_{i=1}^{n} \left(\frac{\partial f}{\partial X_i}(P) \right) y_i = 0 \right\}.$$

Show that the map

$$M_P/M_P^2 \times T \longrightarrow \bar{K}, \qquad (g, y) \longmapsto \sum_{i=1}^{n} \left(\frac{\partial g}{\partial X_i}(P) \right) y_i,$$

is a well-defined perfect pairing of $\bar{K}$-vector spaces. Now use (I.1.5).)

1.4. Let $V/\mathbb{Q}$ be the variety

$$V : 5X^2 + 6XY + 2Y^2 = 2YZ + Z^2.$$

Prove that $V(\mathbb{Q}) = \emptyset$.

1.5. Let $V/\mathbb{Q}$ be the projective variety

$$V : Y^2 = X^3 + 17,$$

and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be distinct points of V. Let L be the line through P_1 and P_2.

(a) Show that $V \cap L = \{P_1, P_2, P_3\}$ and express $P_3 = (x_3, y_3)$ in terms of P_1 and P_2. (If L is tangent to V, then P_3 may equal P_1 or P_2.)
(b) Calculate P_3 for $P_1 = (-1, 4)$ and $P_2 = (2, 5)$.
(c) Show that if $P_1, P_2 \in V(\mathbb{Q})$, then $P_3 \in V(\mathbb{Q})$.

1.6. Let V be the variety

$$V : Y^2Z = X^3 + Z^3.$$

Show that the map

$$\phi : V \longrightarrow \mathbb{P}^2, \qquad \phi = [X^2, XY, Z^2],$$

is a morphism. (Notice that ϕ does not give a morphism $\mathbb{P}^2 \to \mathbb{P}^2$.)

1.7. Let V be the variety

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

and let ϕ be the map

$$\phi : \mathbb{P}^1 \longrightarrow V, \qquad \phi = [S^2T, S^3, T^3].$$

(a) Show that ϕ is a morphism.
(b) Find a rational map $\psi : V \to \mathbb{P}^1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map wherever they are defined.
(c) Is ϕ an isomorphism?

1.8. Let $\mathbb{F}_q$ be a finite field with q elements and let $V \subset \mathbb{P}^n$ be a variety defined over $\mathbb{F}_q$.

(a) Prove that the q^{th}-power map

$$\phi = [X_0^q, \dots, X_n^q]$$

is a morphism $\phi : V \to V$. It is called the *Frobenius morphism*.
(b) Prove that ϕ is one-to-one and onto.
(c) Prove that ϕ is not an isomorphism.

(d) Prove that $V(\mathbb{F}_q) = \big\{P \in V : \phi(P) = P\big\}$.

1.9. If $m > n$, prove that there are no nonconstant morphisms $\mathbb{P}^m \to \mathbb{P}^n$. (*Hint*. Use the dimension theorem [111, I.7.2].)

1.10. For each prime $p \geq 3$, let $V_p \subset \mathbb{P}^2$ be the variety given by the equation

$$V_p : X^2 + Y^2 = pZ^2.$$

(a) Prove that V_p is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ if and only if $p \equiv 1 \pmod 4$.
(b) Prove that for $p \equiv 3 \pmod 4$, no two of the V_p's are isomorphic over $\mathbb{Q}$.

1.11. (a) Let $f \in K[X_0, \ldots, X_n]$ be a homogeneous polynomial, and let

$$V = \big\{P \in \mathbb{P}^n : f(P) = 0\big\}$$

be the hypersurface defined by f. Prove that if a point $P \in V$ is singular, then

$$\frac{\partial f}{\partial X_0}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

Thus for hypersurfaces in projective space, we can check for smoothness using homogeneous coordinates.

(b) Let $n \geq 1$, and let $W \subset \mathbb{P}^n$ be a smooth algebraic set, each of whose component varieties has dimension $n-1$. Prove that W is a variety. (*Hint*. First use Krull's Hauptidealsatz [8, page 122], [73, Theorem 10.1], to show that W is the zero of a single homogeneous polynomial.)

1.12. (a) Let V/K be an affine variety. Prove that

$$K[V] = \big\{f \in \bar{K}[V] : f^\sigma = f \text{ for all } \sigma \in G_{\bar{K}/K}\big\}.$$

(*Hint*. One inclusion is clear. For the other, choose some polynomial $F \in \bar{K}[X]$ with $F \equiv f \pmod{I(V)}$. Show that the map $G_{\bar{K}/K} \to I(V)$ defined by $\sigma \mapsto F^\sigma - F$ is a 1-cocycle; see (B §2). Now use (B.2.5a) to conclude that there exists a $G \in I(V)$ such that $F + G \in K[X]$.)

(b) Prove that

$$\mathbb{P}^n(K) = \big\{P \in \mathbb{P}^n(\bar{K}) : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\big\}.$$

(*Hint*. Write $P = [x_0, \ldots, x_n]$. If $P = P^\sigma$, then there is a $\lambda_\sigma \in \bar{K}^*$ such that $x_i^\sigma = \lambda_\sigma x_i$ for all $0 \leq i \leq n$. Show that the map $\sigma \mapsto \lambda_\sigma$ gives a 1-cocycle from $G_{\bar{K}/K}$ to $\bar{K}^*$. Now use Hilbert's Theorem 90 (B.2.5b) to find an $\alpha \in \bar{K}^*$ such that $[\alpha x_0, \ldots, \alpha x_n] \in \mathbb{P}^n(K)$.)

(c) Let $\phi : V_1 \to V_2$ be a rational map of projective varieties. Prove that ϕ is defined over K if and only if $\phi^\sigma = \phi$ for every $\sigma \in G_{\bar{K}/K}$. (*Hint*. Use (a) and (b).)

Chapter II

Algebraic Curves

In this chapter we present basic facts about algebraic curves, i.e., projective varieties of dimension one, that will be needed for our study of elliptic curves. Actually, since elliptic curves are curves of genus one, one of our tasks will be to define the genus of a curve. As in Chapter I, we give references for those proofs that are not included. There are many books in which the reader will find more material on the subject of algebraic curves, for example [111, Chapter IV], [133], [180], [243], [99, Chapter 2], and [302].

We recall the following notation from Chapter I that will be used in this chapter. Here C denotes a curve and $P \in C$ is a point of C.

C/K	C is defined over K.
$\bar{K}(C)$	the function field of C over $\bar{K}$.
$K(C)$	the function field of C over K.
$\bar{K}[C]_P$	the local ring of C at P.
M_P	the maximal ideal of $\bar{K}[C]_P$.

II.1 Curves

By a *curve* we will always mean a projective variety of dimension one. We generally deal with curves that are smooth. Examples of smooth curves include $\mathbb{P}^1$, (I.2.3), and (I.2.8). We start by describing the local rings at points on a smooth curve.

Proposition 1.1. *Let C be a curve and $P \in C$ a smooth point. Then $\bar{K}[C]_P$ is a discrete valuation ring.*

PROOF. From (I.1.7), the vector space M_P/M_P^2 is a one-dimensional vector space over the field $\bar{K} = \bar{K}[C]_P/M_P$. Now use [8, Proposition 9.2] or Exercise 2.1. □

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

J.H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, Graduate Texts in Mathematics 106, DOI 10.1007/978-0-387-09494-6_II,

$$\operatorname{ord}_P : \bar{K}[C]_P \longrightarrow \{0,1,2,\ldots\} \cup \{\infty\},$$
$$\operatorname{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\}.$$

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

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

A *uniformizer for C at P* is any function $t \in \bar{K}(C)$ with $\operatorname{ord}_P(t) = 1$, i.e., a generator for the ideal M_P.

Remark 1.1.1. If $P \in C(K)$, then it is not hard to show that $K(C)$ contains uniformizers for P; see Exercise 2.16.

Definition. Let C and P be as above, and let $f \in \bar{K}(C)$. The *order of f at P* is $\operatorname{ord}_P(f)$. If $\operatorname{ord}_P(f) > 0$, then f has a *zero* at P, and if $\operatorname{ord}_P(f) < 0$, then f has a *pole* at P. If $\operatorname{ord}_P(f) \geq 0$, then f is *regular* (or *defined*) at P and we can evaluate $f(P)$. Otherwise f has a pole at P and we write $f(P) = \infty$.

Proposition 1.2. *Let C be a smooth curve and $f \in \bar{K}(C)$ with $f \neq 0$. Then there are only finitely many points of C at which f has a pole or zero. Further, if f has no poles, then $f \in \bar{K}$.*

PROOF. See [111, I.6.5], [111, II.6.1], or [243, III §1] for the finiteness of the number of poles. To deal with the zeros, look instead at $1/f$. The last statement is [111, I.3.4a] or [243, I §5, Corollary 1]. □

Example 1.3. Consider the two curves

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

(Remember our convention (I.2.7) concerning affine equations for projective varieties. Each of C_1 and C_2 has a single point at infinity.) Let $P = (0,0)$. Then C_1 is smooth at P and C_2 is not (I.1.6). The maximal ideal M_P of $\bar{K}[C_1]_P$ has the property that M_P/M_P^2 is generated by Y (I.1.8), so for example,

$$\operatorname{ord}_P(Y) = 1, \qquad \operatorname{ord}_P(X) = 2, \qquad \operatorname{ord}_P(2Y^2 - X) = 2.$$

(For the last, note that $2Y^2 - X = 2X^3 + X$.) On the other hand, $\bar{K}[C_2]_P$ is not a discrete valuation ring.

The next proposition is useful in dealing with curves over fields of characteristic $p > 0$. (See also Exercise 2.15.)

Proposition 1.4. *Let C/K be a curve, and let $t \in K(C)$ be a uniformizer at some nonsingular point $P \in C(K)$. Then $K(C)$ is a finite separable extension of $K(t)$.*

PROOF. The field $K(C)$ is clearly a finite (algebraic) extension of $K(t)$, since it is finitely generated over K, has transcendence degree one over K (since C is a curve), and $t \notin K$. Let $x \in K(C)$. We claim that x is separable over $K(t)$.

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

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

We may further assume that Φ is chosen so as to have minimal degree in X, i.e., $\Phi(t,X)$ is a minimal polynomial for x over $K(t)$. Let $p = \operatorname{char}(K)$. If Φ contains a nonzero term $a_{ij}T^iX^j$ with $j \not\equiv 0 \pmod p$, then $\partial\Phi(t,X)/\partial X$ is not identically 0, so x is separable over $K(t)$.

Suppose instead 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. This is true because we have assumed that K is perfect, which implies that every element of K is a p^{th} power. Thus if $F(T,X) = \sum \alpha_{ij}T^iX^j$, then writing $\alpha_{ij} = \beta_{ij}^p$ gives $F(T^p,X^p) = \bigl(\sum \beta_{ij}T^iX^j\bigr)^p$.

We regroup the terms in $\Phi(T,X) = \Psi(T,X^p)$ according to powers of T modulo p. Thus

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

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

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

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

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

But at least one of the $\phi_k(T,X)$'s must involve X, and for that k, the relation $\phi_k(t,x) = 0$ contradicts our choice of $\Phi(t,X)$ as a minimal polynomial for x over $K(t)$. (Note that $\deg_X \phi_k(T,X) \le \frac{1}{p}\deg_X \Phi(T,X)$.) This contradiction completes the proof that x is separable over $K(t)$. □

II.2 Maps Between Curves

We start with the fundamental result that for smooth curves, a rational map is defined at every point.

Proposition 2.1. *Let C be a curve, let $V \subset \mathbb{P}^N$ be a variety, let $P \in C$ be a smooth point, and let $\phi : C \to V$ be 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 functions $f_i \in \bar{K}(C)$, and choose a uniformizer $t \in \bar{K}(C)$ for C at P. Let

$$n = \min_{0 \le i \le N} \operatorname{ord}_P(f_i).$$

Then

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

Hence every $t^{-n} f_i$ is regular at P, and $(t^{-n} f_j)(P) \ne 0$. Therefore ϕ is regular at P. □

See (I.3.6) and (I.3.7) for examples where (II.2.1) is false if P is not smooth or if C has dimension greater than 1.

Example 2.2. Let C/K be a smooth curve and let $f \in K(C)$ be a function. Then f defines a rational map, which we also denote by f,

$$f : C \longrightarrow \mathbb{P}^1, \qquad P \longmapsto \big[f(P), 1\big].$$

From (II.2.1), this map is actually a morphism. It is given explicitly by

$$f(P) = \begin{cases} \big[f(P), 1\big] & \text{if } f \text{ is regular at } P, \\ [1, 0] & \text{if } f \text{ has a pole at } P. \end{cases}$$

Conversely, let

$$\phi : C \longrightarrow \mathbb{P}^1, \qquad \phi = [f, g],$$

be a rational map defined over K. Then either $g = 0$, in which case ϕ is the constant map $\phi = [1, 0]$, or else ϕ is the map corresponding to the function $f/g \in K(C)$. Denoting the former map by ∞, we thus have a one-to-one correspondence

$$K(C) \cup \{\infty\} \longleftrightarrow \{\text{maps } C \to \mathbb{P}^1 \text{ defined over } K\}.$$

We will often implicitly identify these two sets.

Theorem 2.3. *Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.*

PROOF. See [111, II.6.8] or [243, I §5, Theorem 4]. □

Let C_1/K and C_2/K be curves and let $\phi : C_1 \to C_2$ be a nonconstant rational map defined over K. Then composition with ϕ induces an injection of function fields fixing K,

$$\phi^* : K(C_2) \longrightarrow K(C_1), \qquad \phi^* f = f \circ \phi.$$

Theorem 2.4. *Let C_1/K and C_2/K be curves.*

(a) *Let $\phi : C_1 \to C_2$ be a nonconstant map defined over K. Then $K(C_1)$ is a finite extension of $\phi^*(K(C_2))$.*

(b) *Let $\iota : K(C_2) \to K(C_1)$ be an injection of function fields fixing K. Then there exists a unique nonconstant map $\phi : C_1 \to C_2$ (defined over K) such that $\phi^* = \iota$.*

(c) *Let $\mathbb{K} \subset K(C_1)$ be a subfield of finite index containing K. Then there exist a smooth curve C'/K, unique up to K-isomorphism, and a nonconstant map $\phi : C_1 \to C'$ defined over K such that $\phi^* K(C') = \mathbb{K}$.*

PROOF. (a) [111, II.6.8].
(b) Let $C_1 \subset \mathbb{P}^N$, and for each i, let $g_i \in K(C_2)$ be the function on C_2 corresponding to X_i/X_0. (Relabeling if necessary, we may assume that C_2 is not contained in the hyperplane $X_0 = 0$.) Then

$$\phi = \big[1, \iota(g_1), \dots, \iota(g_N)\big]$$

gives a map $\phi : C_1 \to C_2$ with $\phi^* = \iota$. (Note that ϕ is not constant, since the g_i's cannot all be constant and ι is injective.) Finally, if $\psi = [f_0, \dots, f_N]$ is another map with $\psi^* = \iota$, then for each i,

$$f_i/f_0 = \psi^* g_i = \phi^* g_i = \iota(g_i),$$

which shows that $\psi = \phi$.
(c) See [111, I.6.12] for the case that K is algebraically closed. The general case can be proven similarly, or it may be deduced from the algebraically closed case by examining $G_{\bar{K}/K}$-invariants. □

Definition. Let $\phi : C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the *degree of* ϕ to be 0. Otherwise we say that ϕ is a *finite map* and we define its *degree* to be

$$\deg \phi = \big[K(C_1) : \phi^* K(C_2)\big].$$

We say that ϕ is *separable*, *inseparable*, or *purely inseparable* if the field extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property, and we denote the separable and inseparable degrees of the extension by $\deg_s \phi$ and $\deg_i \phi$, respectively.

Definition. Let $\phi : C_1 \to C_2$ be a nonconstant map of curves defined over K. From (II.2.4a) we know that $K(C_1)$ is a finite extension of $\phi^* K(C_2)$. We use the norm map relative to ϕ^* to define a map in the other direction,

$$\phi_* : K(C_1) \longmapsto K(C_2), \qquad \phi_* = (\phi^*)^{-1} \circ \mathrm{N}_{K(C_1)/\phi^* K(C_2)}.$$

Corollary 2.4.1. *Let C_1 and C_2 be smooth curves, and let $\phi : C_1 \to C_2$ be a map of degree one. Then ϕ is an isomorphism.*

PROOF. By definition, $\deg \phi = 1$ means that $\phi^* \bar{K}(C_2) = \bar{K}(C_1)$, so ϕ^* is an isomorphism of function fields. Hence from (II.2.5b), corresponding to the inverse map $(\phi^*)^{-1} : \bar{K}(C_1) \xrightarrow{\sim} \bar{K}(C_2)$, there is a rational map $\psi : C_2 \to C_1$ such that $\psi^* = (\phi^*)^{-1}$. Further, since C_2 is smooth, (II.2.1) tells us that ψ is actually a morphism. Finally, since $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ is the identity map on $\bar{K}(C_2)$, and similarly $(\psi \circ \phi)^* = \phi^* \circ \psi^*$ is the identity map on $\bar{K}(C_1)$, the uniqueness assertion of (II.2.4b) implies that $\phi \circ \psi$ and $\psi \circ \phi$ are, respectively, the identity maps on C_2 and C_1. Hence ϕ and ψ are isomorphisms. □

Remark 2.5. The above result (II.2.4) shows the close connection between (smooth) curves and their function fields. This can be made precise by stating that the following map is an equivalence of categories. (See [111, I §6] for details.)

$$\left[\begin{array}{l}\textit{Objects}\text{: smooth curves}\\ \text{defined over } K\\ \textit{Maps}\text{: nonconstant rational}\\ \text{maps (equivalently}\\ \text{surjective morphisms)}\\ \text{defined over } K\end{array}\right] \rightsquigarrow \left[\begin{array}{l}\textit{Objects}\text{: finitely generated}\\ \text{extensions } \mathbb{K}/K \text{ of}\\ \text{transcendence degree one with}\\ \mathbb{K}\cap\bar{K}=K\\ \textit{Maps}\text{: field injections fixing } K\end{array}\right]$$

$$C/K \rightsquigarrow K(C)$$

$$\phi : C_1 \to C_2 \rightsquigarrow \phi^* : K(C_2) \to K(C_1)$$

Example 2.5.1. *Hyperelliptic Curves*. We assume that $\operatorname{char}(K) \neq 2$. We choose a polynomial $f(x) \in K[x]$ of degree d and consider the *affine* curve C_0/K given by the equation

$$C_0 : y^2 = f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_d.$$

Suppose that the point $P = (x_0, y_0) \in C_0$ is singular. Then

$$2y_0 = f'(x_0) = 0,$$

which means that $y_0 = 0$ and x_0 is a double root of $f(x)$. Hence, if we assume that $\operatorname{disc}(f) \neq 0$, then the affine curve $y^2 = f(x)$ will be nonsingular.

If we treat C_0 as a curve in $\mathbb{P}^2$ by homogenizing its affine equation, then one easily checks that the point(s) at infinity are singular whenever $d \geq 4$. On the other hand, (II.2.4c) assures us that there exists some smooth projective curve C/K whose function field equals $K(C_0) = K(x, y)$. The problem is that this smooth curve is not a subset of $\mathbb{P}^2$.

For example, consider the case $d = 4$. (See also Exercise 2.14.) Then C_0 has an affine equation

$$C_0 : y^2 = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4.$$

We define a map

$$[1, x, y, x^2] : C_0 \longrightarrow \mathbb{P}^3.$$

Letting $[X_0, X_1, X_2, X_3] = [1, x, y, x^2]$, the ideal of the image clearly contains the two homogeneous polynomials

$$\begin{aligned} F &= X_3X_0 - X_1^2,\\ G &= X_2^2X_0^2 - a_0X_1^4 - a_1X_1^3X_0 - a_2X_1^2X_0^2 - a_3X_1X_0^3 - a_4X_0^4. \end{aligned}$$

However, the zero set of these two polynomials cannot be the desired curve C, since it includes the line $X_0 = X_1 = 0$. So we substitute $X_1^2 = X_0X_3$ into G and cancel an X_0^2 to obtain the quadratic polynomial

$$H = X_2^2 - a_0X_3^2 - a_1X_1X_3 - a_2X_0X_3 - a_3X_0X_1 - a_4X_0^2.$$

We claim that the ideal generated by F and H gives a smooth curve C.

To see this, note first that if $X_0 \neq 0$, then dehomogenization with respect to X_0 gives the affine curve (setting $x = X_1/X_0$, $y = X_2/X_0$, and $z = X_3/X_0$)

$$z = x^2 \qquad \text{and} \qquad y^2 = a_0z^2 + a_1xz + a_2z + a_3x + a_4.$$

Substituting the first equation into the second gives us back the original curve C_0. Thus $C_0 \cong C \cap \{X_0 \neq 0\}$.

Next, if $X_0 = 0$, then necessarily $X_1 = 0$, and then $X_2 = \pm\sqrt{a_0}\,X_3$. Thus C has two points $\left[0, 0, \pm\sqrt{a_0}, 1\right]$ on the hyperplane $X_0 = 0$. (Note that $a_0 \neq 0$, since we have assumed that $f(x)$ has degree exactly four.) To check that C is nonsingular at these two points, we dehomogenize with respect to X_3, setting $u = X_0/X_3$, $v = X_1/X_3$, and $w = X_2/X_3$. This gives the equations

$$u = v^2 \qquad \text{and} \qquad w^2 = a_0 + a_1v + a_2u + a_3uv + a_4u^2,$$

from which we obtain the single affine equation

$$w^2 = a_0 + a_1v + a_2v^2 + a_3v^3 + a_4v^4.$$

Again using the assumption that the polynomial $f(x)$ has no double roots, we see that the points $(v, w) = \left(0, \pm\sqrt{a_0}\right)$ are nonsingular.

We summarize the preceding discussion in the following proposition, which will be used in Chapter X.

Proposition 2.5.2. *Let $f(X) \in K[x]$ be a polynomial of degree 4 with $\operatorname{disc}(f) \neq 0$. There exists a smooth projective curve $C \subset \mathbb{P}^3$ with the following properties*:

(i) *The intersection of C with $\mathbb{A}^3 = \{X_0 \neq 0\}$ is isomorphic to the affine curve $y^2 = f(x)$.*

(ii) *Let $f(x) = a_0x^4 + \cdots + a_4$. Then the intersection of C with the hyperplane $X_0 = 0$ consists of the two points $\left[0, 0, \pm\sqrt{a_0}, 1\right]$.*

We next look at the behavior of a map in the neighborhood of a point.

Definition. Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves, and let $P \in C_1$. The *ramification index of ϕ at P*, denoted by $e_\phi(P)$, is the quantity

$$e_\phi(P) = \operatorname{ord}_P\left(\phi^* t_{\phi(P)}\right),$$

where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$. Note that $e_\phi(P) \geq 1$. We say that ϕ is *unramified at P* if $e_\phi(P) = 1$, and that ϕ is *unramified* if it is unramified at every point of C_1.

Proposition 2.6. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves.*

(a) *For every $Q \in C_2$,*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

(b) *For all but finitely many $Q \in C_2$,*

$$\#\phi^{-1}(Q) = \deg_s(\phi).$$

(c) *Let $\psi : C_2 \to C_3$ be another nonconstant map of smooth curves. Then for all $P \in C_1$,*

$$e_{\psi\circ\phi}(P) = e_\phi(P)e_\psi(\phi P).$$

PROOF. (a) Use [111, II.6.9] with $Y = \mathbb{P}^1$ and $D = (0)$, or see [142, Proposition 2], [233, I Proposition 10], or [243, III §2, Theorem 1].
(b) See [111, II.6.8].
(c) Let $t_{\phi P}$ and $t_{\psi\phi P}$ be uniformizers at the indicated points. By definition, the functions

$$t_{\phi P}^{e_\psi(\phi P)} \quad \text{and} \quad \psi^* t_{\psi\phi P}$$

have the same order at $\phi(P)$. Applying ϕ^* and taking orders at P yields

$$\operatorname{ord}_P\left(\phi^* t_{\phi P}^{e_\psi(\phi P)}\right) = \operatorname{ord}_P\big((\psi\phi)^* t_{\psi\phi P}\big),$$

which is the desired result. □

Corollary 2.7. *A map a $\phi : C_1 \to C_2$ is unramified if and only if*

$$\#\phi^{-1}(Q) = \deg(\phi) \qquad \textit{for all } Q \in C_2.$$

PROOF. From (II.2.6a), we see that $\#\phi^{-1}(Q) = \deg(\phi)$ if and only if

$$\sum_{P\in\phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q).$$

Since $e_\phi(P) \ge 1$, this occurs if and only if each $e_\phi(P) = 1$. □

Remark 2.8. The content of (II.2.6) is exactly analogous to the theorems describing the ramification of primes in number fields. Thus let L/K be number fields. Then (II.2.6a) is the analogue of the $\sum e_i f_i = [K : \mathbb{Q}]$ theorem ([142, I, Proposition 21], [233, I, Proposition 10]), while (II.2.6b) is analogous to the fact that only finitely many primes of K ramify in L, and (II.2.6c) gives the multiplicativity of ramification degrees in towers of fields. Of course, (II.2.6) and the analogous results for number fields are both merely special cases of the basic theorems describing finite extensions of Dedekind domains.

Example 2.9. Consider the map

$$\phi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1, \qquad \phi\big([X,Y]\big) = [X^3(X-Y)^2, Y^5].$$

Then ϕ is ramified at the points $[0,1]$ and $[1,1]$. Further,

$$e_\phi\big([0,1]\big) = 3 \qquad \text{and} \qquad e_\phi\big([1,1]\big) = 2,$$

so

$$\sum_{P\in\phi^{-1}([0,1])} e_\phi(P) = e_\phi\big([0,1]\big) + e_\phi\big([1,1]\big) = 5 = \deg\phi,$$

which is in accordance with (II.2.6a).

The Frobenius Map

Assume that $\operatorname{char}(K) = p > 0$ and let $q = p^r$. For any polynomial $f \in K[X]$, let $f^{(q)}$ be the polynomial obtained from f by raising each coefficient of f to the q^{th} power. Then for any curve C/K, we can define a new curve $C^{(q)}/K$ as the curve whose homogeneous ideal is given by

$$I(C^{(q)}) = \text{ideal generated by } \{f^{(q)} : f \in I(C)\}.$$

Further, there is a natural map from C to $C^{(q)}$, called the q^{th}*-power Frobenius morphism*, given by

$$\phi : C \longrightarrow C^{(q)}, \qquad \phi\big([x_0, \ldots, x_n]\big) = [x_0^q, \ldots, x_n^q].$$

To see that ϕ maps C to $C^{(q)}$, it suffices to show that for every point

$$P = [x_0, \ldots, x_n] \in C,$$

the image $\phi(P)$ is a zero of each generator $f^{(q)}$ of $I(C^{(q)})$. We compute

$$\begin{aligned} f^{(q)}\big(\phi(P)\big) &= f^{(q)}(x_0^q, \ldots, x_n^q) \\ &= \big(f(x_0, \ldots, x_n)\big)^q && \text{since } \operatorname{char}(K) = p, \\ &= 0 && \text{since } f(P) = 0. \end{aligned}$$

Example 2.10. Let C be the curve in $\mathbb{P}^2$ given by the single equation

$$C : Y^2Z = X^2 + aXZ^2 + bZ^3.$$

Then $C^{(q)}$ is the curve given by the equation

$$C^{(q)} : Y^2Z = X^2 + a^qXZ^2 + b^qZ^3.$$

The next proposition describes the basic properties of the Frobenius map.

Proposition 2.11. *Let K be a field of characteristic $p > 0$, let $q = p^r$, let C/K be a curve, and let $\phi : C \to C^{(q)}$ be the q^{th}-power Frobenius morphism.*

(a) $\phi^*K(C^{(q)}) = K(C)^q = \big\{f^q : f \in K(C)\big\}$.

(b) *ϕ is purely inseparable.*

(c) $\deg \phi = q$.

(*N.B. We are assuming that K is perfect. If K is not perfect, then* (*b*) *and* (*c*) *remain true, but* (*a*) *must be modified.*)

PROOF. (a) Using the description (I.2.9) of $K(C)$ as consisting of quotients f/g of homogeneous polynomials of the same degree, we see that $\phi^*K(C^{(q)})$ is the subfield of $K(C)$ given by quotients

$$\phi^*\left(\frac{f}{g}\right) = \frac{f(X_0^q, \ldots, X_n^q)}{g(X_0^q, \ldots, X_n^q)}.$$

Similarly, $K(C)^q$ is the subfield of $K(C)$ given by quotients

$$\frac{f(X_0,\dots,X_n)^q}{g(X_0,\dots,X_n)^q}.$$

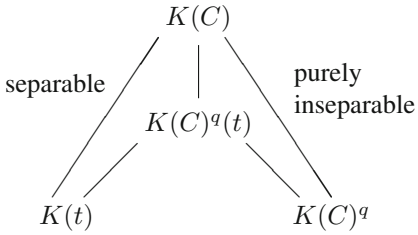
However, since K is perfect, we know that every element of K is a q^{th} power, so

$$\big(K[X_0,\dots,X_n]\big)^q = K[X_0^q,\dots,X_n^q].$$

Thus the set of quotients $f(X_i^q)/g(X_i^q)$ and the set of quotients $f(X_i)^q/g(X_i)^q$ give the exact same subfield of $K(C)$.

(b) Immediate from (a).

(c) Taking a finite extension of K if necessary, we may assume that there is a smooth point $P \in K(C)$. Let $t \in K(C)$ be a uniformizer at P (II.1.1.1). Then (II.1.4) says that $K(C)$ is separable over $K(t)$. Consider the tower of fields



It follows that $K(C) = K(C)^q(t)$, so from (a),

$$\deg\phi = \big[K(C)^q(t) : K(C)^q\big].$$

Now $t^q \in K(C)^q$, so in order to prove that $\deg\phi = q$, we need merely show that $t^{q/p} \notin K(C)^q$. But if $t^{q/p} = f^q$ for some $f \in K(C)$, then

$$\frac{q}{p} = \operatorname{ord}_P(t^{q/p}) = q\operatorname{ord}_P(f),$$

which is impossible, since $\operatorname{ord}_P(f)$ must be an integer. □

Corollary 2.12. *Every map $\psi : C_1 \to C_2$ of (smooth) curves over a field of characteristic $p > 0$ factors as*

$$C_1 \xrightarrow{\ \phi\ } C_1^{(q)} \xrightarrow{\ \lambda\ } C_2,$$

where $q = \deg_i(\psi)$, the map ϕ is the q^{th}-power Frobenius map, and the map λ is separable.

PROOF. Let $\mathbb{K}$ be the separable closure of $\psi^*K(C_2)$ in $K(C_1)$. Then $K(C_1)/\mathbb{K}$ is purely inseparable of degree q, so $K(C_1)^q \subset \mathbb{K}$. From (II.2.11a,c) we have,

$$K(C_1)^q = \phi^*\big(K(C_1^{(q)})\big) \qquad \text{and} \qquad \big[K(C_1) : \phi^*(K(C_1^{(q)}))\big] = q.$$

Comparing degrees, we conclude that $\mathbb{K} = \phi^*(C_1^{(q)})$. We now have a tower of function fields

$$K(C_1) \;/\; \phi^*K(C_1^{(q)}) \;/\; \psi^*K(C_2),$$

and from (II.2.4b), this corresponds to maps

$$C_1 \xrightarrow{\;\phi\;} C_1^{(q)} \xrightarrow{\;\lambda\;} C_2 \qquad (\psi : C_1 \to C_2)$$

□

II.3 Divisors

The *divisor group of a curve* C, denoted by $\mathrm{Div}(C)$, is the free abelian group generated by the points of C. Thus a divisor $D \in \mathrm{Div}(C)$ is a formal sum

$$D = \sum_{P \in C} n_P(P),$$

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$. The *degree of* D is defined by

$$\deg D = \sum_{P \in C} n_P.$$

The *divisors of degree* 0 form a subgroup of $\mathrm{Div}(C)$, which we denote by

$$\mathrm{Div}^0(C) = \big\{D \in \mathrm{Div}(C) : \deg D = 0\big\}.$$

If C is defined over K, we let $G_{\bar{K}/K}$ act on $\mathrm{Div}(C)$ and $\mathrm{Div}^0(C)$ in the obvious way,

$$D^\sigma = \sum_{P \in C} n_P(P^\sigma).$$

Then D is *defined over* K if $D^\sigma = D$ for all $\sigma \in G_{\bar{K}/K}$. We note that if $D = n_1(P_1) + \cdots + n_r(P_r)$ with $n_1, \ldots, n_r \neq 0$, then to say that D is defined over K does *not* mean that $P_1, \ldots, P_r \in C(K)$. It suffices for the group $G_{\bar{K}/K}$ to permute the P_i's in an appropriate fashion. We denote the *group of divisors defined over* K by $\mathrm{Div}_K(C)$, and similarly for $\mathrm{Div}^0_K(C)$.

Assume now that the curve C is smooth, and let $f \in \bar{K}(C)^*$. Then we can associate to f the divisor $\mathrm{div}(f)$ given by

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

This is a divisor by (II.1.2). If $\sigma \in G_{\bar{K}/K}$, then it is easy to see that

$$\mathrm{div}(f^\sigma) = \big(\mathrm{div}(f)\big)^\sigma.$$

In particular, if $f \in K(C)$, then $\operatorname{div}(f) \in \operatorname{Div}_K(C)$.

Since each ord_P is a valuation, the map

$$\operatorname{div} : \bar{K}(C)^* \longrightarrow \operatorname{Div}(C)$$

is a homomorphism of abelian groups. It is analogous to the map that sends an element of a number field to the corresponding fractional ideal. This prompts the following definitions.

Definition. A divisor $D \in \operatorname{Div}(C)$ is *principal* if it has the form $D = \operatorname{div}(f)$ for some $f \in \bar{K}(C)^*$. Two divisors are *linearly equivalent*, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The *divisor class group* (or *Picard group*) of C, denoted by $\operatorname{Pic}(C)$, is the quotient of $\operatorname{Div}(C)$ by its subgroup of principal divisors. We let $\operatorname{Pic}_K(C)$ be the subgroup of $\operatorname{Pic}(C)$ fixed by $G_{\bar{K}/K}$. N.B. In general, $\operatorname{Pic}_K(C)$ is not the quotient of $\operatorname{Div}_K(C)$ by its subgroup of principal divisors. But see exericse 2.13 for a case in which this is true.

Proposition 3.1. *Let C be a smooth curve and let $f \in \bar{K}(C)^*$.*

(a) $\operatorname{div}(f) = 0$ *if and only if* $f \in \bar{K}^*$.

(b) $\deg\bigl(\operatorname{div}(f)\bigr) = 0$.

PROOF. (a) If $\operatorname{div}(f) = 0$, then f has no poles, so the associated map $f : C \to \mathbb{P}^1$ as defined in (II.2.2) is not surjective. Then (II.2.3) tells us that the map is constant, so $f \in \bar{K}^*$. The converse is clear.

(b) See [111, II.6.10], [243, III 2, corollary to Theorem 1], or (II.3.7). □

Example 3.2. On $\mathbb{P}^1$, every divisor of degree 0 is principal To see this, suppose that $D = \sum n_P(P)$ has degree 0. Writing $P = [\alpha_P, \beta_P] \in \mathbb{P}^1$, we see that D is the divisor of the function

$$\prod_{P \in \mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}.$$

Note that $\sum n_P = 0$ ensures that this function is in $K(\mathbb{P}^1)$. It follows that the degree map $\deg : \operatorname{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ is an isomorphism. The converse is also true, i.e., if C is a smooth curve and $\operatorname{Pic}(C) \cong \mathbb{Z}$, then C is isomorphic to $\mathbb{P}^1$.

Example 3.3. Assume that $\operatorname{char}(K) \neq 2$. Let $e_1, e_2, e_3 \in \bar{K}$ be distinct, and consider the curve

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

One can check that C is smooth and that it has a single point at infinity, which we denote by P_∞. For $i = 1, 2, 3$, let $P_i = (e_i, 0) \in C$. Then

$$\begin{aligned} \operatorname{div}(x - e_i) &= 2(P_i) - 2(P_\infty), \\ \operatorname{div}(y) &= (P_1) + (P_2) + (P_3) - 3(P_\infty). \end{aligned}$$

Definition. It follows from (II.3.1b) that the principal divisors form a subgroup of $\operatorname{Div}^0(C)$. We define the *degree-0 part of the divisor class group of C* to be the quotient of $\operatorname{Div}^0(C)$ by the subgroup of principal divisors. We denote this group by $\operatorname{Pic}^0(C)$. Similarly, we write $\operatorname{Pic}^0_K(C)$ for the subgroup of $\operatorname{Pic}^0(C)$ fixed by $G_{\bar{K}/K}$.

Remark 3.4. The above definitions and (II.3.1) may be summarized by saying that there is an exact sequence

$$1 \longrightarrow \bar{K}^* \longrightarrow \bar{K}(C)^* \xrightarrow{\text{div}} \text{Div}^0(C) \longrightarrow \text{Pic}^0(C) \longrightarrow 0.$$

This sequence is the function field analogue of the fundamental exact sequence in algebraic number theory, which for a number field K reads

$$1 \longrightarrow \begin{pmatrix}\text{units}\\ \text{of } K\end{pmatrix} \longrightarrow K^* \longrightarrow \begin{pmatrix}\text{fractional}\\ \text{ideals of } K\end{pmatrix} \longrightarrow \begin{pmatrix}\text{ideal class}\\ \text{group of } K\end{pmatrix} \longrightarrow 1.$$

Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves. As we have seen, ϕ induces maps on the function fields of C_1 and C_2,

$$\phi^* : \bar{K}(C_2) \longrightarrow \bar{K}(C_1) \qquad \text{and} \qquad \phi_* : \bar{K}(C_1) \longrightarrow \bar{K}(C_2).$$

We similarly define maps of divisor groups as follows:

$$\begin{aligned} \phi^* : \text{Div}(C_2) &\longrightarrow \text{Div}(C_1), & \phi_* : \text{Div}(C_1) &\longrightarrow \text{Div}(C_2),\\ (Q) &\longmapsto \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P), & (P) &\longmapsto (\phi P), \end{aligned}$$

and extend $\mathbb{Z}$-linearly to arbitrary divisors.

Example 3.5. Let C be a smooth curve, let $f \in \bar{K}(C)$ be a nonconstant function, and let $f : C \to \mathbb{P}^1$ be the corresponding map (II.2.2). Then directly from the definitions,

$$\text{div}(f) = f^*\big((0) - (\infty)\big).$$

Proposition 3.6. *Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves.*

(a) $\deg(\phi^* D) = (\deg \phi)(\deg D)$ *for all* $D \in \text{Div}(C_2)$.

(b) $\phi^*(\text{div}\, f) = \text{div}(\phi^* f)$ *for all* $f \in \bar{K}(C_2)^*$.

(c) $\deg(\phi_* D) = \deg D$ *for all* $D \in \text{Div}(C_1)$.

(d) $\phi_*(\text{div}\, f) = \text{div}(\phi_* f)$ *for all* $f \in \bar{K}(C_1)^*$.

(e) $\phi_* \circ \phi^*$ *acts as multiplication by* $\deg \phi$ *on* $\text{Div}(C_2)$.

(f) *If $\psi : C_2 \to C_3$ is another such map, then*

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* \quad \textit{and} \quad (\psi \circ \phi)_* = \psi_* \circ \phi_*.$$

PROOF. (a) Follows directly from (II.2.6a).

(b) Follows from the definitions and the easy fact (Exercise 2.2) that for all $P \in C_1$,

$$\text{ord}_P(\phi^* f) = e_\phi(P)\, \text{ord}_{\phi P}(f).$$

(c) Clear from the definitions.

(d) See [142, Chapter 1, Proposition 22] or [233, I, Proposition 14].

(e) Follows directly from (II.2.6a).

(f) The first equality follows from (II.2.6c). The second is obvious. □

Remark 3.7. From (II.3.6) we see that ϕ^* and ϕ_* take divisors of degree 0 to divisors of degree 0, and principal divisors to principal divisors. They thus induce maps

$$\phi^* : \mathrm{Pic}^0(C_2) \longrightarrow \mathrm{Pic}^0(C_1) \qquad \text{and} \qquad \phi_* : \mathrm{Pic}^0(C_1) \longrightarrow \mathrm{Pic}^0(C_2).$$

In particular, if $f \in \bar{K}(C)$ gives the map $f : C \to \mathbb{P}^1$, then

$$\deg \mathrm{div}(f) = \deg f^*\big((0) - (\infty)\big) = \deg f - \deg f = 0.$$

This provides a proof of (II.3.1b)

II.4 Differentials

In this section we discuss the vector space of differential forms on a curve. This vector space serves two distinct purposes. First, it performs the traditional calculus role of linearization. (See (III §5), especially (III.5.2).) Second, it gives a useful criterion for determining when an algebraic map is separable. (See (II.4.2) and its utilization in the proof of (III.5.5).) Of course, the latter is also a familiar use of calculus, since a field extension is separable if and only if the minimal polynomial of each element has a nonzero derivative

Definition. Let C be a curve. The *space of* (*meromorphic*) *differential forms* on C, denoted by Ω_C, is the $\bar{K}$-vector space generated by symbols of the form dx for $x \in \bar{K}(C)$, subject to the usual relations:

(i) $d(x+y) = dx + dy$ for all $x, y \in \bar{K}(C)$.

(ii) $d(xy) = x\,dy + y\,dx$ for all $x, y \in \bar{K}(C)$.

(iii) $da = 0$ for all $a \in \bar{K}$.

Remark 4.1. There is, of course, a functorial definition of Ω_C. See, for example, [164, Chapter 10], [111, II.8], or [210, II §3].

Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. The associated function field map $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$ induces a map on differentials,

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}, \qquad \phi^*\left(\sum f_i\,dx_i\right) = \sum (\phi^* f_i) d(\phi^* x_i).$$

This map provides a useful criterion for determining when ϕ is separable.

Proposition 4.2. *Let C be a curve.*

(a) *Ω_C is a 1-dimensional $\bar{K}(C)$-vector space.*

(b) *Let $x \in \bar{K}(C)$. Then dx is a $\bar{K}(C)$-basis for Ω_C if and only if $\bar{K}(C)/\bar{K}(x)$ is a finite separable extension.*

(c) *Let $\phi : C_1 \to C_2$ be a nonconstant map of curves. Then ϕ is separable if and only if the map*

$$\phi^* : \Omega_{C_2} \longrightarrow \Omega_{C_1}$$

is injective (*equivalently, nonzero*).

PROOF. (a) See [164, 27.A,B], [210, II.3.4], or [243, III §4, Theorem 3].
(b) See [164, 27A,B] or [243, III §4, Theorem 4].
(c) Using (a) and (b), choose $y \in \bar{K}(C_2)$ such that $\Omega_{C_2} = \bar{K}(C_2)\,dy$ and such that $\bar{K}(C_2)/\bar{K}(y)$ is a separable extension. Note that $\phi^*\bar{K}(C_2)$ is then separable over $\phi^*\bar{K}(y) = \bar{K}(\phi^* y)$. Now

$$\begin{aligned}
\phi^* \text{ is injective} &\iff d(\phi^* y) \neq 0 \\
&\iff d(\phi^* y) \text{ is a basis for } \Omega_{C_1} \text{ (from (a))}, \\
&\iff \bar{K}(C_1)/\bar{K}(\phi^* y) \text{ is separable (from (b))}, \\
&\iff \bar{K}(C_1)/\phi^*\bar{K}(C_2) \text{ is separable},
\end{aligned}$$

where the last equivalence follows because we already know that $\phi^*\bar{K}(C_2)/\bar{K}(\phi^* y)$ is separable. □

Proposition 4.3. *Let C be a curve, let $P \in C$, and let $t \in \bar{K}(C)$ be a unformizer at P.*

(a) *For every $\omega \in \Omega_C$ there exists a unique function $g \in \bar{K}(C)$, depending on ω and t, satisfying*

$$\omega = g\,dt.$$

We denote g by ω/dt.

(b) *Let $f \in \bar{K}(C)$ be regular at P. Then df/dt is also regular at P.*

(c) *Let $\omega \in \Omega_C$ with $\omega \neq 0$. The quantity*

$$\operatorname{ord}_P(\omega/dt)$$

depends only on ω and P, independent of the choice of uniformizer t. We call this value the order of ω at P *and denote it by* $\operatorname{ord}_P(\omega)$.

(d) *Let $x, f \in \bar{K}(C)$ with $x(P) = 0$, and let $p = \operatorname{char} K$. Then*

$$\begin{aligned}
&\operatorname{ord}_P(f\,dx) = \operatorname{ord}_P(f) + \operatorname{ord}_P(x) - 1, && \text{if } p = 0 \text{ or } p \nmid \operatorname{ord}_P(x), \\
&\operatorname{ord}_P(f\,dx) \geq \operatorname{ord}_P(f) + \operatorname{ord}_P(x), && \text{if } p > 0 \text{ and } p \mid \operatorname{ord}_P(x).
\end{aligned}$$

(e) *Let $\omega \in \Omega_C$ with $\omega \neq 0$. Then*

$$\operatorname{ord}_P(\omega) = 0 \qquad \text{for all but finitely many } P \in C.$$

PROOF. (a) This follows from (II.1.4) and (4.2ab).
(b) See [111, comment following IV.2.1] or [210, II.3.10].
(c) Let t' be another uniformizer at P. Then from (b) we see that dt/dt' and dt'/dt are both regular at P, so $\operatorname{ord}_P(dt'/dt) = 0$. The desired result then follows from

$$\omega = g\,dt' = g(dt'/dt)\,dt.$$

(d) Write $x = ut^n$ with $n = \operatorname{ord}_P(x) \geq 1$, so $\operatorname{ord}_P(u) = 0$. Then

$$dx = \left[nut^{n-1} + (du/dt)t^n\right] dt.$$

From (b) we know that du/dt is regular at P. Hence if $n \neq 0$, then the first term dominates, which gives the desired equality

$$\operatorname{ord}_P(f\,dx) = \operatorname{ord}_P(fnut^{n-1}\,dt) = \operatorname{ord}_P(f) + n - 1.$$

On the other hand, if $p > 0$ and $p \mid n$, then the first term vanishes and we find that

$$\operatorname{ord}_P(f\,dx) = \operatorname{ord}_P(f(du/dt)t^n\,dt) \geq \operatorname{ord}_P(f) + n.$$

(e) Choose some $x \in \bar{K}(C)$ such that $\bar{K}(C)/\bar{K}(x)$ is separable and write $\omega = f\,dx$. From [111, IV.2.2a], the map $x : C \to \mathbb{P}^1$ ramifies at only finitely many points of C. Hence discarding finitely many points, we may restrict attention to points $P \in C$ such that

$$f(P) \neq 0, \quad f(P) \neq \infty, \quad x(P) \neq \infty,$$

and the map $x : C \to \mathbb{P}^1$ is unramified at P. The two conditions on x imply that $x - x(P)$ is a uniformizer at P, so

$$\operatorname{ord}_P(\omega) = \operatorname{ord}_P\bigl(f\,d(x - x(P))\bigr) = 0.$$

Hence $\operatorname{ord}_P(\omega) = 0$ for all but finitely many P. □

Definition. Let $\omega \in \Omega_C$. The *divisor associated to* ω is

$$\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega)(P) \in \operatorname{Div}(C).$$

The differential $\omega \in \Omega_C$ is *regular* (or *holomorphic*) if

$$\operatorname{ord}_P(\omega) \geq 0 \qquad \text{for all } P \in C.$$

It is *nonvanishing* if

$$\operatorname{ord}_P(\omega) \leq 0 \qquad \text{for all } P \in C.$$

Remark 4.4. If $\omega_1, \omega_2 \in \Omega_C$ are nonzero differentials, then (II.4.2a) implies that there is a function $f \in \bar{K}(C)^*$ such that $\omega_1 = f\omega_2$. Thus

$$\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_2),$$

which shows that the following definition makes sense.

Definition. The *canonical divisor class on* C is the image in $\operatorname{Pic}(C)$ of $\operatorname{div}(\omega)$ for any nonzero differential $\omega \in \Omega_C$. Any divisor in this divisor class is called a *canonical divisor*.

Example 4.5. We are going to show that there are no holomorphic differentials on $\mathbb{P}^1$. First, if t is a coordinate function on $\mathbb{P}^1$, then

$$\operatorname{div}(dt) = -2(\infty).$$

To see this, note that for all $\alpha \in \bar{K}$, the function $t - \alpha$ is a uniformizer at α, so

$$\operatorname{ord}_\alpha(dt) = \operatorname{ord}_\alpha\bigl(d(t-\alpha)\bigr) = 0.$$

However, at $\infty \in \mathbb{P}^1$ we need to use a function such as $1/t$ as our uniformizer, so

$$\operatorname{ord}_\infty(dt) = \operatorname{ord}_\infty\left(-t^2\, d\left(\frac{1}{t}\right)\right) = -2.$$

Thus dt is not holomorphic. But now for any nonzero $\omega \in \Omega_{\mathbb{P}^1}$, we can use (II.4.3a) to compute

$$\deg \operatorname{div}(\omega) = \deg \operatorname{div}(dt) = -2,$$

so ω cannot be holomorphic either.

Example 4.6. Let C be the curve

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

where we continue with the notation from (II.3.3). Then

$$\operatorname{div}(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

(Note that $dx = d(x - e_i) = -x^2\, d(1/x)$.) We thus see that

$$\operatorname{div}(dx/y) = 0.$$

Hence the differential dx/y is both holomorphic and nonvanishing.

II.5 The Riemann–Roch Theorem

Let C be a curve. We put a partial order on $\operatorname{Div}(C)$ in the following way.

Definition. A divisor $D = \sum n_P(P)$ is *positive* (or *effective*), denoted by

$$D \geq 0,$$

if $n_P \geq 0$ for every $P \in C$. Similarly, for any two divisors $D_1, D_2 \in \operatorname{Div}(C)$, we write

$$D_1 \geq D_2$$

to indicate that $D_1 - D_2$ is positive.

Example 5.1. Let $f \in \bar{K}(C)^*$ be a function that is regular everywhere except at one point $P \in C$, and suppose that it has a pole of order at most n at P. These requirements on f may be succinctly summarized by the inequality

$$\operatorname{div}(f) \geq -n(P).$$

Similarly,

$$\operatorname{div}(f) \geq (Q) - n(P)$$

says that in addition, f has a zero at Q. Thus divisorial inequalities are a useful tool for describing poles and/or zeros of functions.

Definition. Let $D \in \operatorname{Div}(C)$. We associate to D the set of functions

$$\mathcal{L}(D) = \big\{ f \in \bar{K}(C)^* : \operatorname{div}(f) \ge -D \big\} \cup \{0\}.$$

The set $\mathcal{L}(D)$ is a finite-dimensional $\bar{K}$-vector space (see (II.5.2b) below), and we denote its dimension by

$$\ell(D) = \dim_{\bar{K}} \mathcal{L}(D).$$

Proposition 5.2. *Let $D \in \operatorname{Div}(C)$.*
(a) *If $\deg D < 0$, then*

$$\mathcal{L}(D) = \{0\} \qquad \textit{and} \qquad \ell(D) = 0.$$

(b) *$\mathcal{L}(D)$ is a finite-dimensional $\bar{K}$-vector space.*
(c) *If $D' \in \operatorname{Div}(C)$ is linearly equivalent to D, then*

$$\mathcal{L}(D) \cong \mathcal{L}(D'), \qquad \textit{and so} \qquad \ell(D) = \ell(D').$$

PROOF. (a) Let $f \in \mathcal{L}(D)$ with $f \ne 0$. Then (II.3.1b) tells us that

$$0 = \deg \operatorname{div}(f) \ge \deg(-D) = -\deg D,$$

so $\deg D \ge 0$.
(b) See [111, II.5.19] or Exercise 2.4.
(c) If $D = D' + \operatorname{div}(g)$, then the map

$$\mathcal{L}(D) \longrightarrow \mathcal{L}(D'), \qquad f \longmapsto fg$$

is an isomorphism. □

Example 5.3. Let $K_C \in \operatorname{Div}(C)$ be a canonical divisor on C, say

$$K_C = \operatorname{div}(\omega).$$

Then each function $f \in \mathcal{L}(K_C)$ has the property that

$$\operatorname{div}(f) \ge -\operatorname{div}(\omega), \qquad \text{so} \quad \operatorname{div}(f\omega) \ge 0.$$

In other words, $f\omega$ is holomorphic. Conversely, if the differential $f\omega$ is holomorphic, then $f \in \mathcal{L}(K_C)$. Since every differential on C has the form $f\omega$ for some f, we have established an isomorphism of $\bar{K}$-vector spaces,

$$\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ is holomorphic}\}.$$

The dimension $\ell(K_C)$ of these spaces is an important invariant of the curve C.

We are now ready to state a fundamental result in the algebraic geometry of curves. Its importance, as we will see amply demonstrated in (III §3), lies in its ability to tell us that there are functions on C having prescribed zeros and poles.

Theorem 5.4. (Riemann–Roch) *Let C be a smooth curve and let K_C be a canonical divisor on C. There is an integer $g \ge 0$, called the* genus of C*, such that for every divisor $D \in \operatorname{Div}(C)$,*

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

PROOF. For a fancy proof using Serre duality, see [111, IV §1]. A more elementary proof, due to Weil, is given in [136, Chapter 1]. □

Corollary 5.5. (a) $\ell(K_C) = g$.
(b) $\deg K_C = 2g - 2$.
(c) *If* $\deg D > 2g - 2$*, then*

$$\ell(D) = \deg D - g + 1.$$

PROOF. (a) Use (II.5.4) with $D = 0$. Note that $\mathcal{L}(0) = \bar{K}$ from (II.1.2), so $\ell(0) = 1$.
(b) Use (a) and (II.5.4) with $D = K_C$.
(c) From (b) we have $\deg(K_C - D) < 0$. Now use (II.5.4) and (II.5.2a). □

Example 5.6. Let $C = \mathbb{P}^1$. Then (II.4.5) says that there are no holomorphic differentials on C, so using the identification from (II.5.3), we see that $\ell(K_C) = 0$. Then (II.5.5a) says that $\mathbb{P}^1$ has genus 0, and the Riemann–Roch theorem reads

$$\ell(D) - \ell(-2(\infty) - D) = \deg D + 1.$$

In particular, if $\deg D \ge -1$, then

$$\ell(D) = \deg D + 1.$$

(See Exercise 2.3b.)

Example 5.7. Let C be the curve

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3),$$

where we continue with the notation of (II.3.3) and (II.4.6). We have seen in (II.4.6) that

$$\operatorname{div}(dx/y) = 0,$$

so the canonical class on C is trivial, i.e., we may take $K_C = 0$. Hence using (II.5.5a) we find that

$$g = \ell(K_C) = \ell(0) = 1,$$

so C has genus one. The Riemann–Roch theorem (II.5.5c) then tells us that

$$\ell(D) = \deg D \qquad \text{provided } \deg D \ge 1.$$

We consider several special cases.

(i) Let $P \in C$. Then $\ell\big((P)\big) = 1$. But $\mathcal{L}\big((P)\big)$ certainly contains the constant functions, which have no poles, so this shows that there are no functions on C having a single simple pole.

(ii) Recall that P_∞ is the point at infinity on C. Then $\ell\big(2(P_\infty)\big) = 2$, and $\{1, x\}$ provides a basis for $\mathcal{L}\big(2(P_\infty)\big)$.

(iii) Similarly, the set $\{1, x, y\}$ is a basis for $\mathcal{L}\big(3(P_\infty)\big)$, and $\{1, x, y, x^2\}$ is a basis for $\mathcal{L}\big(4(P_\infty)\big)$.

(iv) Now we observe that the seven functions $1, x, y, x^2, xy, x^3, y^2$ are all in $\mathcal{L}\big(6(P_\infty)\big)$, but $\ell\big(6(P_\infty)\big) = 6$, so these seven functions must be $\bar{K}$-linearly dependent. Of course, the equation $y^2 = (x - e_1)(x - e_2)(x - e_3)$ used to define C gives an equation of linear dependence among them.

The next result says that if C and D are defined over K, then so is $\mathcal{L}(D)$.

Proposition 5.8. *Let C/K be a smooth curve and let $D \in \mathrm{Div}_K(C)$. Then $\mathcal{L}(D)$ has a basis consisting of functions in $K(C)$.*

PROOF. Since D is defined over K, we have

$$f^\sigma \in \mathcal{L}(D^\sigma) = \mathcal{L}(D) \qquad \text{for all } f \in \mathcal{L}(D) \text{ and all } \sigma \in G_{\bar{K}/K}.$$

Thus $G_{\bar{K}/K}$ acts on $\mathcal{L}(D)$, and the desired conclusion follows from the following general lemma. □

Lemma 5.8.1. *Let V be a $\bar{K}$-vector space, and assume that $G_{\bar{K}/K}$ acts continuously on V in a manner compatible with its action on $\bar{K}$. Let*

$$V_K = V^{G_{\bar{K}/K}} = \{\mathbf{v} \in V : \mathbf{v}^\sigma = \mathbf{v} \textit{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Then

$$V \cong \bar{K} \otimes_K V_K,$$

i.e., the vector space V has a basis of $G_{\bar{K}/K}$-invariant vectors.

PROOF. It is clear that V_K is a K-vector space, so it suffices to show that every $\mathbf{v} \in V$ is a $\bar{K}$-linear combination of vectors in V_K. Let $\mathbf{v} \in V$ and let L/K be a finite Galois extension such that $\mathbf{v}$ is fixed by $G_{\bar{K}/L}$. (The assumption that $G_{\bar{K}/K}$ acts continuously on V means precisely that the subgroup $\{\sigma \in G_{\bar{K}/K} : \mathbf{v}^\sigma = \mathbf{v}\}$ has finite index in K, so we can take L to be the Galois closure of its fixed field.) Let $\{\alpha_1, \dots, \alpha_n\}$ be a basis for L/K, and let $\{\sigma_1, \dots, \sigma_n\} = G_{L/K}$. For each $1 \le i \le n$, consider the vector

$$\mathbf{w}_i = \sum_{j=1}^{n} (\alpha_i \mathbf{v})^{\sigma_j} = \mathrm{Trace}_{L/K}(\alpha_i \mathbf{v}).$$

It is clear that $\mathbf{w}_i$ is $G_{\bar{K}/K}$ invariant, so $\mathbf{w}_i \in V_K$. A basic result from field theory [142, III, Proposition 9] says that the matrix $\big(\alpha_i^{\sigma_j}\big)_{1 \le i,j \le n}$ is nonsingular, so each $\mathbf{v}^{\sigma_j}$, and in particular $\mathbf{v}$, is an L-linear combination of the $\mathbf{w}_i$'s. (For a fancier proof, see Exercise 2.12.) □

We conclude this section with a classic relationship connecting the genera of curves linked by a nonconstant map.

Theorem 5.9. (Hurwitz) *Let $\phi : C_1 \to C_2$ be a nonconstant separable map of smooth curves of genera g_1 and g_2, respectively. Then*

$$2g_1 - 2 \ge (\deg \phi)(2g_2 - 2) + \sum_{P \in C_1} \big(e_\phi(P) - 1\big).$$

Further, equality holds if and only if one of the following two conditions is true:
(i) $\operatorname{char}(K) = 0$.
(ii) $\operatorname{char}(K) = p > 0$ *and p does not divide $e_\phi(P)$ for all $P \in C_1$.*

PROOF. Let $\omega \in \Omega_C$ be a nonzero differential, let $P \in C_1$, and let $Q = \phi(P)$. Since ϕ is separable, (II.4.2c) tells us that $\phi^*\omega \ne 0$. We need to relate the values of $\operatorname{ord}_P(\phi^*\omega)$ and $\operatorname{ord}_Q(\omega)$. Write $\omega = f\,dt$ with $t \in \bar{K}(C_2)$ a uniformizer at Q. Letting $e = e_\phi(P)$, we have $\phi^*t = us^e$, where s is a uniformizer at P and $u(P) \ne 0, \infty$. Hence

$$\phi^*\omega = (\phi^*f)d(\phi^*t) = (\phi^*f)d(us^e) = (\phi^*f)\big[eus^{e-1} + (du/ds)s^e\big]\,ds.$$

Now $\operatorname{ord}_P(du/ds) \ge 0$ from (II.4.3b), so we see that

$$\operatorname{ord}_P(\phi^*\omega) \ge \operatorname{ord}_P(\phi^*f) + e - 1,$$

with equality if and only if $e \ne 0$ in K. Further,

$$\operatorname{ord}_P(\phi^*f) = e_\phi(P)\operatorname{ord}_Q(f) = e_\phi(P)\operatorname{ord}_Q(\omega).$$

Hence adding over all $P \in C_1$ yields

$$\begin{aligned}
\deg \operatorname{div}(\phi^*\omega) &\ge \sum_{P \in C_1} \big[e_\phi(P)\operatorname{ord}_{\phi(P)}(\omega) + e_\phi(P) - 1\big] \\
&= \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\operatorname{ord}_Q(\omega) + \sum_{P \in C_1} \big(e_\phi(P) - 1\big) \\
&= (\deg \phi)(\deg \operatorname{div}(\omega)) + \sum_{P \in C_1} \big(e_\phi(P) - 1\big),
\end{aligned}$$

where the last equality follows from (II.2.6a). Now Hurwitz's formula is a consequence of (II.5.5b), which says that on a curve of genus g, the divisor of any nonzero differential has degree $2g - 2$. □

Exercises

2.1. Let R be a Noetherian local domain that is not a field, let $\mathfrak{M}$ be its maximal ideal, and let $k = R/\mathfrak{M}$ be its residue field. Prove that the following are equivalent:
(i) R is a discrete valuation ring.

(ii) $\mathfrak{M}$ is principal.
(iii) $\dim_k \mathfrak{M}/\mathfrak{M}^2 = 1$.
(Note that this lemma was used in (II.1.1) to show that on a smooth curve, the local rings $\bar{K}[C]_P$ are discrete valuation rings.)

2.2. Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves, let $f \in \bar{K}(C_2)^*$, and let $P \in C_1$. Prove that

$$\operatorname{ord}_P(\phi^* f) = e_\phi(P) \operatorname{ord}_{\phi(P)}(f).$$

2.3. Verify directly that each of the following results from the text is true for the particular case of the curve $C = \mathbb{P}^1$.
(a) Prove the two parts of (II.2.6):

$$\text{(i)} \quad \sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi \qquad \text{for all } Q \in \mathbb{P}^1.$$

$$\text{(ii)} \quad \#\phi^{-1}(Q) = \deg_s(\phi) \qquad \text{for all but finitely many } Q \in \mathbb{P}^1.$$

(b) Prove the Riemann–Roch theorem (II.5.4) for $\mathbb{P}^1$.
(c) Prove Hurwitz's theorem (II.5.9) for a nonconstant separable map $\phi : \mathbb{P}^1 \to \mathbb{P}^1$.

2.4. Let C be a smooth curve and let $D \in \operatorname{Div}(C)$. Without using the Riemann–Roch theorem, prove the following statements.
(a) $\mathcal{L}(D)$ is a $\bar{K}$-vector space.
(b) If $\deg D \geq 0$, then

$$\ell(D) \leq \deg D + 1.$$

2.5. Let C be a smooth curve. Prove that the following are equivalent (over $\bar{K}$):
(i) C is isomorphic to $\mathbb{P}^1$.
(ii) C has genus 0.
(iii) There exist distinct points $P, Q \in C$ satisfying $(P) \sim (Q)$.

2.6. Let C be a smooth curve of genus one, and fix a base point $P_0 \in C$.
(a) Prove that for all $P, Q \in C$ there exists a unique $R \in C$ such that

$$(P) + (Q) \sim (R) + (P_0).$$

Denote this point R by $\sigma(P, Q)$.
(b) Prove that the map $\sigma : C \times C \to C$ from (a) makes C into an abelian group with identity element P_0.
(c) Define a map

$$\kappa : C \longrightarrow \operatorname{Pic}^0(C), \qquad P \longmapsto \text{divisor class of } (P) - (P_0).$$

Prove that κ is a bijection of sets, and hence that κ can be used to make C into a group via the rule

$$P + Q = \kappa^{-1}\big(\kappa(P) + \kappa(Q)\big).$$

(d) Prove that the group operations on C defined in (b) and (c) are the same.

2.7. Let $F(X,Y,Z) \in K[X,Y,Z]$ be a homogeneous polynomial of degree $d \geq 1$, and assume that the curve C in $\mathbb{P}^2$ given by the equation $F = 0$ is nonsingular. Prove that

$$\operatorname{genus}(C) = \frac{(d-1)(d-2)}{2}.$$

(*Hint*. Define a map $C \to \mathbb{P}^1$ and use (II.5.9).)

2.8. Let $\phi : C_1 \to C_2$ be a nonconstant separable map of smooth curves.

(a) Prove that $\operatorname{genus}(C_1) \geq \operatorname{genus}(C_2)$.

(b) Prove that if C_1 and C_2 have the same genus g, then one of the following is true:

(i) $g = 0$.

(ii) $g = 1$ and ϕ is unramified.

(iii) $g \geq 2$ and ϕ is an isomorphism.

2.9. Let a, b, c, d be squarefree integers with $a > b > c > 0$, and let C be the curve in $\mathbb{P}^2$ given by the equation

$$C : aX^3 + bY^3 + cZ^3 + dXYZ = 0.$$

Let $P = [x, y, z] \in C$ and let L be the tangent line to C at P.

(a) Show that $C \cap L = \{P, P'\}$ and calculate $P' = [x', y', z']$ in terms of a, b, c, d, x, y, z.

(b) Show that if $P \in C(\mathbb{Q})$, then $P' \in C(\mathbb{Q})$.

(c) Let $P \in C(\mathbb{Q})$. Choose homogeneous coordinates for P and P' that are integers satisfying $\gcd(x, y, z) = 1$ and $\gcd(x', y', z') = 1$. Prove that

$$|x'y'z'| > |xyz|.$$

(Note the strict inequality.)

(d) Conclude that either $C(\mathbb{Q}) = \emptyset$ or else $C(\mathbb{Q})$ is an infinite set.

(e) ****** Characterize, in terms of a, b, c, d, whether $C(\mathbb{Q})$ contains any points.

2.10. Let C be a smooth curve. The *support* of a divisor $D = \sum n_P(P) \in \operatorname{Div}(C)$ is the set of points $P \in C$ for which $n_P \neq 0$. Let $f \in \bar{K}(C)^*$ be a function such that $\operatorname{div}(f)$ and D have disjoint supports. Then it makes sense to define

$$f(D) = \prod_{P \in C} f(P)^{n_P}.$$

Let $\phi : C_1 \to C_2$ be a nonconstant map of smooth curves. Prove that the following two equalities are valid in the sense that if both sides are well-defined, then they are equal.

(a) $f(\phi^* D) = (\phi_* f)(D)$ for all $f \in \bar{K}(C_1)^*$ and all $D \in \operatorname{Div}(C_2)$.

(b) $f(\phi_* D) = (\phi^* f)(D)$ for all $f \in \bar{K}(C_2)^*$ and all $D \in \operatorname{Div}(C_1)$.

2.11. Let C be a smooth curve and let $f, g \in \bar{K}(C)^*$ be functions such that $\operatorname{div}(f)$ and $\operatorname{div}(g)$ have disjoint support. (See Exercise 2.10.) Prove *Weil's reciprocity law*

$$f\big(\operatorname{div}(g)\big) = g\big(\operatorname{div}(f)\big)$$

using the following two steps:

(a) Verify Weil's reciprocity law directly for $C = \mathbb{P}^1$.

(b) Now prove it for arbitrary C by using the map $g : C \to \mathbb{P}^1$ to reduce to (a).

2.12. Use the extension of Hilbert's Theorem 90 (B.3.2), which says that

$$H^1\big(G_{\bar{K}/K}, \mathrm{GL}_n(\bar{K})\big) = 0,$$

to give another proof of (II.5.8.1).

2.13. Let C/K be a curve.

(a) Prove that the following sequence is exact:

$$1 \longrightarrow K^* \longrightarrow K(C)^* \longrightarrow \mathrm{Div}^0_K(C) \longrightarrow \mathrm{Pic}^0_K(C).$$

(b) Suppose that C has genus one and that $C(K) \neq \emptyset$. Prove that the map

$$\mathrm{Div}^0_K(C) \longrightarrow \mathrm{Pic}^0_K(C)$$

is surjective.

2.14. For this exercise we assume that $\mathrm{char}\, K \neq 2$. Let $f(x) \in K[x]$ be a polynomial of degree $d \geq 1$ with nonzero discriminant, let C_0/K be the affine curve given by the equation

$$C_0 : y^2 = f(x) = a_0x^d + a_1x^{d-1} + \cdots + a_{d-1}x + a_d,$$

and let g be the unique integer satisfying $d - 3 < 2g \leq d - 1$.

(a) Let C be the closure of the image of C_0 via the map

$$[1, x, x^2, \ldots, x^{g-1}, y] : C_0 \longrightarrow \mathbb{P}^{g+2}.$$

Prove that C is smooth and that $C \cap \{X_0 \neq 0\}$ is isomorphic to C_0. The curve C is called a *hyperelliptic curve*.

(b) Let

$$f^*(v) = v^{2g+2}f(1/v) = \begin{cases} a_0 + a_1v + \cdots + a_{d-1}v^{d-1} + a_dv^d & \text{if } d \text{ is even,} \\ a_0v + a_1v^2 + \cdots + a_{d-1}v^d + a_dv^{d+1} & \text{if } d \text{ is odd.} \end{cases}$$

Show that C consists of two affine pieces

$$C_0 : y^2 = f(x) \qquad \text{and} \qquad C_1 : w^2 = f^*(v),$$

"glued together" via the maps

$$\begin{aligned} C_0 &\longrightarrow C_1, \\ (x, y) &\longmapsto (1/x, y/x^{g+1}), \end{aligned} \qquad\qquad \begin{aligned} C_1 &\longrightarrow C_0, \\ (v, w) &\longmapsto (1/v, w/v^{g+1}). \end{aligned}$$

(c) Calculate the divisor of the differential dx/y on C and use the result to show that C has genus g. Check your answer by applying Hurwitz's formula (II.5.9) to the map $[1, x] : C \to \mathbb{P}^1$. (Note that Exercise 2.7 does not apply, since $C \not\subset \mathbb{P}^2$.)

(d) Find a basis for the holomorphic differentials on C. (*Hint.* Consider the set of differential forms $\{x^i\, dx/y : i = 0, 1, 2, \ldots\}$. How many elements in this set are holomorphic?)

2.15. Let C/K be a smooth curve defined over a field of characteristic $p > 0$, and let $t \in K(C)$. Prove that the following are equivalent:

(i) $K(C)$ is a finite separable extension of $K(t)$.

(ii) For all but finitely many points$P \in C$, the function $t - t(P)$ is a uniformizer at P.

(iii) $t \notin K(C)^p$.

2.16. Let C/K be a curve that is defined over K and let $P \in C(K)$. Prove that $K(C)$ contains uniformizers for C at P, i.e., prove that there are uniformizers that are defined over K.