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. $\quad\square$

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

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

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

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

A *uniformizer for C at P* is any function $t \in \bar{K}(C)$ with $\mathrm{ord}_P(t) = 1$, 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 $\mathrm{ord}_P(f)$. If $\mathrm{ord}_P(f) > 0$, then f has a *zero* at P, and if $\mathrm{ord}_P(f) < 0$, then f has a *pole* at P. If $\mathrm{ord}_P(f) \geq 0$, 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,

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

(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

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

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 $p = \text{char}(K)$. If Φ contains a nonzero term $a_{ij}T^i X^j$ 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 pth power. This is true because we have assumed that K is perfect, which implies that every element of K is a pth power. Thus if $F(T, X) = \sum \alpha_{ij}T^i X^j$, then writing $\alpha_{ij} = \beta_{ij}^p$ gives $F(T^p, X^p) = \left(\sum \beta_{ij}T^i X^j\right)^p$.

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

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

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

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

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

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

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 $\deg_X \phi_k(T, X) \leq \frac{1}{p}\deg_X \Phi(T, X)$.) This contradiction completes the proof that x is separable over $K(t)$. $\qquad\square$

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

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

Then

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

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

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

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 $C_2 \subset \mathbb{P}^N$, 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. $\qquad\square$

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.2.4b), 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. $\qquad\square$

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.)

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

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

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

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

$$C_0 : y^2 = f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_d.$$

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 $\mathrm{disc}(f) \neq 0$, 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

$$C_0 : y^2 = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4.$$

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

$$F = X_3 X_0 - X_1^2,$$
$$G = X_2^2 X_0^2 - a_0 X_1^4 - a_1 X_1^3 X_0 - a_2 X_1^2 X_0^2 - a_3 X_1 X_0^3 - a_4 X_0^4.$$

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 $X_1^2 = X_0 X_3$ into G and cancel an X_0^2 to obtain the quadratic polynomial

$$H = X_2^2 - a_0 X_3^2 - a_1 X_1 X_3 - a_2 X_0 X_3 - a_3 X_0 X_1 - a_4 X_0^2.$$

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 $z = X_3/X_0$)

$$z = x^2 \qquad \text{and} \qquad y^2 = a_0 z^2 + a_1 xz + a_2 z + a_3 x + a_4.$$

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 $[0, 0, \pm\sqrt{a_0}, 1]$ 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

$$u = v^2 \qquad \text{and} \qquad w^2 = a_0 + a_1 v + a_2 u + a_3 uv + a_4 u^2,$$

from which we obtain the single affine equation

$$w^2 = a_0 + a_1 v + a_2 v^2 + a_3 v^3 + a_4 v^4.$$

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 $\mathrm{disc}(f) \neq 0$. 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 $f(x) = a_0 x^4 + \cdots + a_4$. 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

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

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 $Y = C_2$ and $D = (Q)$, 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

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

which is the desired result. $\square$

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

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

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 $e_\phi(P) \geq 1$, this occurs if and only if each $e_\phi(P) = 1$. $\square$

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

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

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

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

so

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

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

The Frobenius Map

Assume that $\text{char}(K) = p > 0$ 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 qth 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 qth-*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

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

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

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

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

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

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 qth-power Frobenius morphism.*
(a) *$\phi^* K(C^{(q)}) = K(C)^q = \{f^q : f \in K(C)\}$.*
(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

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

However, since K is perfect, we know that every element of K is a qth power, so

$$\left(K[X_0, \ldots, X_n]\right)^q = K[X_0^q, \ldots, X_n^q].$$

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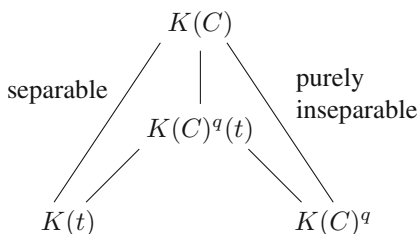
It follows that $K(C) = K(C)^q(t)$, so from (a),

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

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. $\qquad\square$

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 qth-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,

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

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

$$C_1 \xrightarrow{\ \phi\ } C_1^{(q)} \xrightarrow{\ \lambda\ } C_2$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad}_{\psi}$$

$\square$

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

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

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

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 $\mathrm{div}(f) \in \mathrm{Div}_K(C)$.

Since each ord_P is a valuation, the map

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

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 $D \in \mathrm{Div}(C)$ is *principal* if it has the form $D = \mathrm{div}(f)$ 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 $\mathrm{Pic}(C)$, is the quotient of $\mathrm{Div}(C)$ by its subgroup of principal divisors. We let $\mathrm{Pic}_K(C)$ be the subgroup of $\mathrm{Pic}(C)$ fixed by $G_{\bar{K}/K}$. N.B. In general, $\mathrm{Pic}_K(C)$ is not the quotient of $\mathrm{Div}_K(C)$ by its subgroup of principal divisors. But see exercise 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) $\mathrm{div}(f) = 0$ *if and only if $f \in \bar{K}^*$.*
(b) $\deg\big(\mathrm{div}(f)\big) = 0$.

PROOF. (a) If $\mathrm{div}(f) = 0$, 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 $\deg : \mathrm{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ is an isomorphism. The converse is also true, i.e., if C is a smooth curve and $\mathrm{Pic}(C) \cong \mathbb{Z}$, then C is isomorphic to $\mathbb{P}^1$.

Example 3.3. Assume that $\mathrm{char}(K) \neq 2$. 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

$$\mathrm{div}(x - e_i) = 2(P_i) - 2(P_\infty),$$
$$\mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

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

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

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*

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

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. $\qquad\qquad\square$

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 $\bar{K}(C)$-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

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

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

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

Definition. Let $\omega \in \Omega_C$ with $\omega \neq 0$. 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

$$\mathrm{ord}_\alpha(dt) = \mathrm{ord}_\alpha\big(d(t - \alpha)\big) = 0.$$

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

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

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

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

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

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

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

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

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 $\mathrm{Div}(C)$ 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 $D_1, D_2 \in \mathrm{Div}(C)$, 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

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

Similarly,

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

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

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

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 $D \in \mathrm{Div}(C)$.*
(a) *If $\deg D < 0$, then*

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

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

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

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

$$0 = \deg \mathrm{div}(f) \geq \deg(-D) = -\deg D,$$

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

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

is an isomorphism.   □

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

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

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

$$\mathrm{div}(f) \geq -\mathrm{div}(\omega), \qquad so \quad \mathrm{div}(f\omega) \geq 0.$$

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 $g \geq 0$, called the* genus *of C, such that for every divisor $D \in \mathrm{Div}(C)$,*

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

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 $\deg D \geq -1$, 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

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

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

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

We consider several special cases.

(i) Let $P \in C$. Then $\ell((P)) = 1$. But $\mathcal{L}((P))$ 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 $\ell(2(P_\infty)) = 2$, and $\{1, x\}$ provides a basis for $\mathcal{L}(2(P_\infty))$.

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

(iv) Now we observe that the seven functions $1, x, y, x^2, xy, x^3, y^2$ are all in $\mathcal{L}(6(P_\infty))$, but $\ell(6(P_\infty)) = 6$, 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. $\qquad \square$

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*

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

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 $\{\alpha_1, \ldots, \alpha_n\}$ be a basis for L/K, and let $\{\sigma_1, \ldots, \sigma_n\} = G_{L/K}$. 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 $(\alpha_i^{\sigma_j})_{1 \le i, j \le n}$ 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.) $\qquad \square$

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*

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

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

PROOF. Let $\omega \in \Omega_{C_2}$ be a nonzero differential, let $P \in C_1$, and let $Q = \phi(P)$. Since ϕ is separable, (II.4.2c) tells us that $\phi^*\omega \neq 0$. We need to relate the values of $\mathrm{ord}_P(\phi^*\omega)$ and $\mathrm{ord}_Q(\omega)$. 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 $u(P) \neq 0, \infty$. 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 $\mathrm{ord}_P(du/ds) \geq 0$ from (II.4.3b), so we see that

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

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

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

Hence adding over all $P \in C_1$ yields

$$\deg \mathrm{div}(\phi^*\omega) \geq \sum_{P \in C_1} \big[e_\phi(P)\,\mathrm{ord}_{\phi(P)}(\omega) + e_\phi(P) - 1 \big]$$

$$= \sum_{Q \in C_2} \sum_{P \in \phi^{-1}(Q)} e_\phi(P)\,\mathrm{ord}_Q(\omega) + \sum_{P \in C_1} \big(e_\phi(P) - 1 \big)$$

$$= (\deg \phi)(\deg \mathrm{div}(\omega)) + \sum_{P \in C_1} \big(e_\phi(P) - 1 \big),$$

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

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

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):

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

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

(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 $D \in \mathrm{Div}(C)$. 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

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

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

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

(*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 $\text{genus}(C_1) \geq \text{genus}(C_2)$.
(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 a, b, c pairwise relatively prime, 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 $D = \sum n_P(P) \in \text{Div}(C)$ 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 $\text{div}(f)$ 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 $D \in \text{Div}(C_2)$.
(b) $f(\phi_*D) = (\phi^*f)(D)$ for all $f \in \bar{K}(C_2)^*$ and all $D \in \text{Div}(C_1)$.

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

$$f(\text{div}(g)) = g(\text{div}(f))$$

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:

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

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

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

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

$$C_0 : y^2 = f(x) = a_0 x^d + a_1 x^{d-1} + \cdots + a_{d-1}x + a_d,$$

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

$$f^*(v) = v^{2g+2} f(1/v) = \begin{cases} a_0 + a_1 v + \cdots + a_{d-1}v^{d-1} + a_d v^d & \text{if } d \text{ is even}, \\ a_0 v + a_1 v^2 + \cdots + a_{d-1}v^d + a_d v^{d+1} & \text{if } d \text{ is odd}. \end{cases}$$

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

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

(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.