Chapter 8

Rational Maps on Curves and Divisors

The purpose of this chapter is to develop some tools in the theory of algebraic curves that are needed for the applications (especially, hyperelliptic curve cryptography). The technical machinery in this chapter is somewhat deeper than the previous one and readers can skip this chapter if they wish.

The reader should note that the word "curve" in this chapter always refers to a non-singular curve.

8.1 Rational Maps of Curves and the Degree

Lemma 8.1.1. *Let C be a curve over $\Bbbk$ and $f \in \Bbbk(C)$. One can associate with f a rational map $\phi : C \to \mathbb{P}^1$ over $\Bbbk$ by $\phi = (f : 1)$. (Indeed, this is a morphism by Lemma 7.3.6.) Denote by ∞ the constant map $\infty(P) = (1 : 0)$. Then there is a one-to-one correspondence between $\Bbbk(C) \cup \{\infty\}$ and the set of morphisms $\phi : C \to \mathbb{P}^1$.*

Exercise 8.1.2. Prove Lemma 8.1.1.

Note that since $\Bbbk(C) \cup \{\infty\}$ is not a field, it does not make sense to interpret the set of rational maps $\phi : C \to \mathbb{P}^1$ as a field.

Lemma 8.1.3. *Let C_1 and C_2 be curves over $\Bbbk$ (in particular, non-singular and projective) and let $\phi : C_1 \to C_2$ be a non-constant rational map over $\Bbbk$. Then ϕ is a dominant morphism.*

Proof: By Lemma 7.3.6, ϕ is a morphism. By Lemma 5.5.17 and Exercise 5.5.19 we know that the Zariski closure Z of $\phi(C_1)$ is an irreducible algebraic set. Suppose $Z \neq C_2$. We may intersect with an affine space so that $Z \cap \mathbb{A}^n \neq \varnothing$. It follows that $Z \cap \mathbb{A}^n \neq C_2 \cap \mathbb{A}^n$

(otherwise their projective closures are equal and $Z = C_2$). Hence $I_{\overline{\Bbbk}}(C_2) \subsetneq I_{\overline{\Bbbk}}(Z)$. By Theorem 5.6.8 it follows that $\dim(Z) = 0$ and so, by Exercise 5.6.6, $Z = \{P\}$ for some $P \in C_2(\overline{\Bbbk})$. □

The notion of degree of a mapping is fundamental in algebra and topology; a degree d map is "d-to-one on most points".

Example 8.1.4. Let $\Bbbk$ be a field of characteristic not equal to 2. The morphism $\phi : \mathbb{A}^1(\Bbbk) \to \mathbb{A}^1(\Bbbk)$ given by $\phi(x) = x^2$ is clearly two-to-one away from the point $x = 0$. We say that ϕ has degree 2.

Example 8.1.4 suggests several possible definitions for degree: the first in terms of the number of pre-images of a general point in the image; the second in terms of the degrees of the polynomials defining the map. A third definition is to recall the injective field homorphism $\phi^* : \Bbbk(\mathbb{A}^1) \to \Bbbk(\mathbb{A}^1)$. One sees that $\phi^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(x^2) \subseteq \Bbbk(x)$ and that $[\Bbbk(x) : \Bbbk(x^2)] = 2$. This latter formulation turns out to be a suitable definition for degree.

Theorem 8.1.5. *Let C_1, C_2 be curves over $\Bbbk$. Let $\phi : C_1 \to C_2$ be a non-constant rational map over $\Bbbk$. Then $\Bbbk(C_1)$ is a finite algebraic extension of $\phi^*(\Bbbk(C_2))$.*

Proof: By Lemma 8.1.3, ϕ is a dominant morphism and hence by Theorem 5.5.24, $\phi^* : \Bbbk(C_2) \to \Bbbk(C_1)$ is an injective field homorphism. It follows that $\phi^*(\Bbbk(C_2))$ is a subfield of $\Bbbk(C_1)$. Since $\phi^*(\Bbbk(C_2))$ is isomorphic to $\Bbbk(C_2)$ it has transcendence degree 1. Since $\Bbbk(C_1)$ also has transcendence degree 1 it follows from Theorem A.6.5 that $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$ is an algebraic extension. Finally, $\Bbbk(C_1)$ is a finite algebraic extension of $\phi^*(\Bbbk(C_2))$ since $\Bbbk(C_1)$ is finitely generated over $\Bbbk$. □

Definition 8.1.6. Let $\phi : C_1 \to C_2$ be a non-constant rational map of curves over $\Bbbk$. The **degree** of ϕ is $[\Bbbk(C_1) : \phi^*(\Bbbk(C_2))]$.

Let F be a field such that $\phi^*(\Bbbk(C_2)) \subset F \subset \Bbbk(C_1)$ and $\Bbbk(C_1)/F$ is separable and $F/\phi^*(\Bbbk(C_2))$ is purely inseparable (recall the notion of separability from Section A.6). The **separable degree** of ϕ is $\deg_s(\phi) = [\Bbbk(C_1) : F]$ and the **inseparable degree** of ϕ is $\deg_i(\phi) = [F : \phi^*(\Bbbk(C_2))]$.

A non-constant rational map of curves is called **separable** (respectively, **inseparable**) if its inseparable (resp., separable) degree is 1.

Example 8.1.7. Let $\Bbbk = \mathbb{F}_p$. The **Frobenius map** $\pi_p : \mathbb{A}^1(\overline{\Bbbk}) \to \mathbb{A}^1(\overline{\Bbbk})$ is given by $\pi_p(x) = x^p$. Since $\Bbbk(\mathbb{A}^1) = \Bbbk(x)$ and $\pi_p^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(x^p)$ it follows that $\Bbbk(x)/\pi_p^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(x)/\Bbbk(x^p)$ is inseparable of degree p. Hence $\deg_s(\pi_p) = 1$ and $\deg(\pi_p) = \deg_i(\pi_p) = p$. Note that π_p is one-to-one on $\mathbb{A}^1(\overline{\mathbb{F}}_p)$, not p-to-one.

Lemma 8.1.8. *Let $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ be a non-constant morphism over $\Bbbk$ given by $\phi(x) = a(x)$ for some polynomial $a(x) \in \Bbbk[x]$. Then $\deg(\phi) = \deg_x(a(x))$.*

Proof: Let $\theta = a(x)$. We have $\phi^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(\theta) \subseteq \Bbbk(x)$ and we are required to determine $[\Bbbk(x) : \Bbbk(\theta)]$. We claim the minimal polynomial of x over $\Bbbk(\theta)$ is given by

$$F(T) = a(T) - \theta.$$

First, it is clear that $F(x) = 0$. Second, it follows from Eisenstein's criteria (see Proposition III.1.14 of [589], Theorem IV.3.1 of [367] or Theorem III.6.15 of [301]), taking for example the place (i.e., valuation) at infinity in $\Bbbk(\theta)$, that $F(T)$ is irreducible. Since $\deg_T(F(T)) = \deg_x(a(x))$ the result follows. □

Lemma 8.1.9. *Let $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ be a non-constant rational map over $\Bbbk$ given by $\phi(x) = a(x)/b(x)$ where $\gcd(a(x), b(x)) = 1$. Then $\deg(\phi) = \max\{\deg_x(a(x)), \deg_x(b(x))\}$.*

Proof: Let $\theta = a(x)/b(x)$ so that $\phi^*(\Bbbk(\mathbb{A}^1)) = \Bbbk(\theta) \subseteq \Bbbk(x)$. Since $\Bbbk(\theta) = \Bbbk(1/\theta)$ we may assume $\deg_x(a(x)) \geq \deg_x(b(x))$. If these degrees are equal then one can reduce the degree of $a(x)$ by using $\Bbbk(a(x)/b(x)) = \Bbbk((a(x) - cb(x))/b(x))$ for a suitable $c \in \Bbbk$; replacing θ by $1/\theta$ again we may assume that $\deg_x(a(x)) > \deg_x(b(x))$. We may also assume that $a(x)$ and $b(x)$ are monic.

We claim the minimal polynomial of x over $\Bbbk(\theta)$ is given by

$$F(T) = a(T) - \theta b(T).$$

To see this, first note that $F(x) = 0$. Now, $a(T) - \theta b(T)$ is irreducible in $\Bbbk[\theta, T]$ since it is linear in θ. The irreducibility of $F(T)$ in $\Bbbk(\theta)[T]$ then follows from the Gauss Lemma (see, for example, Lemma III.6.13 of Hungerford [301]). □

Exercise 8.1.10. Let $C_1 : y^2 = x^3$ and $C_2 : Y^2 = X$ over a field $\Bbbk$ of characteristic not equal to 2 and consider the map $\phi : C_1 \to C_2$ such that $\phi(x, y) = (x, y/x)$. Show that $\deg(\phi) = 1$.

Exercise 8.1.11. Let $C_1 : y^2 = x^6 + 2x^2 + 1$ and $C_2 : Y^2 = X^3 + 2X + 1$ over a field $\Bbbk$ of characteristic not equal to 2 and consider the map $\phi : C_1 \to C_2$ such that $\phi(x, y) = (x^2, y)$. Show that $\deg(\phi) = 2$.

Exercise 8.1.12. Let C_1, C_2 and C_3 be curves over $\Bbbk$ and let $\psi : C_1 \to C_2$ and $\phi : C_2 \to C_3$ be morphisms over $\Bbbk$. Show that $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$.

Lemma 8.1.13. *Let C_1 and C_2 be curves over $\Bbbk$ (in particular, smooth and projective). Let $\phi : C_1 \to C_2$ be a birational map over $\Bbbk$. Then ϕ has degree 1.*

Proof: Write ϕ^{-1} for the rational map from C_2 to C_1 such that $\phi^{-1} \circ \phi$ is the identity on an open subset of C_1. Then $(\phi^{-1} \circ \phi)^*$ is the identity map on $\Bbbk(C_1)$ and it also factors as $\phi^* \circ (\phi^{-1})^*$. Since $1 = [\Bbbk(C_1) : (\phi^{-1} \circ \phi)^*\Bbbk(C_1)] = [\Bbbk(C_1) : \phi^*\Bbbk(C_2)][\Bbbk(C_2) : (\phi^{-1})^*\Bbbk(C_1)]$ the result follows. □

For Lemma 8.1.15 (and Lemma 8.2.6) we need the following technical result. This is a special case of weak approximation; see Stichtenoth [589] for a presentation that uses similar techniques to obtain most of the results in this chapter.

Lemma 8.1.14. *Let C be a curve over $\Bbbk$ and let $Q, Q' \in C(\overline{\Bbbk})$ be distinct points. Then there is a function $f \in \overline{\Bbbk}(C)$ such that $v_Q(f) = 0$ and $v_{Q'}(f) > 0$.*

Proof: By Lemma 7.1.19 we have $\mathcal{O}_{Q',\overline{\Bbbk}} \not\subseteq \mathcal{O}_{Q,\overline{\Bbbk}}$ (and vice versa). Hence, there exists a function $u \in \mathcal{O}_{Q,\overline{\Bbbk}} - \mathcal{O}_{Q',\overline{\Bbbk}}$. Then $v_Q(u) \geq 0$ while $v_{Q'}(u) < 0$. If $u(Q) = -1$ then set $f = 1/(1 + u^2)$ else set $f = 1/(1 + u)$. Then $v_Q(f) = 0$ and $v_{Q'}(f) > 0$ as required. □

Lemma 8.1.15. *Let C_1 and C_2 be curves over $\Bbbk$ (in particular, smooth and projective). Let $\phi : C_1 \to C_2$ be a rational map over $\Bbbk$ of degree 1. Then ϕ is an isomorphism.*

Proof: Since ϕ has degree 1 it follows that $\phi^*(\Bbbk(C_2)) = \Bbbk(C_1)$ and so $\Bbbk(C_2) \cong \Bbbk(C_1)$. The inverse of ϕ^* induces a rational map $\phi^{-1} : C_2 \to C_1$. Since C_1 and C_2 are non-singular and projective it follows from Lemma 7.3.6 that $\phi : C_1 \to C_2$ and $\phi^{-1} : C_2 \to C_1$ are actually morphisms. It follows that $\phi^{-1} \circ \phi : C_1 \to C_1$ and $\phi \circ \phi^{-1} : C_2 \to C_2$ are morphisms.

It remains to show that these maps are both the identity. Without loss of generality we consider $\psi = \phi^{-1} \circ \phi$. Suppose for contradiction that there are points $P, Q \in C_1(\overline{\Bbbk})$ such that $\psi(P) = Q \neq P$. There exists a function f on C_1 such that $f(P) = 0$ and $f(Q) \neq 0$ (see Lemma 8.1.14). But ψ^* is the identity map on $\Bbbk(C_1)$. Hence $\psi^*(f) = f$. But $\psi^*(f) = f \circ \psi$ and so $0 = f(P) = (f \circ \psi)(P) = f(Q) \neq 0$, which is a contradiction. □

8.2 Extensions of Valuations

Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Then $F_1 = \Bbbk(C_1)$ is a finite extension of $F_2 = \phi^*(\Bbbk(C_2))$. We now study the preimages of points $Q \in C_2(\overline{\Bbbk})$ under ϕ and a notion of multiplicity of preimages of Q (namely, ramification indices). The main result is Theorem 8.2.12.

There are several approaches to these results in the literature. One method, which unifies algebraic number theory and the theory of curves, is to note that if U is an open subset of C then $\Bbbk[U]$ is a Dedekind domain. The splitting of the maximal ideal $\mathfrak{m}_Q$ of $\Bbbk[U]$ (for $Q \in U$) in the integral closure of $\phi^*(\Bbbk[U])$ in $\Bbbk(C_1)$ yields the results. Details of this approach are given in Section VII.5 of Lorenzini [394], Section I.4 of Serre [542] (especially Propositions I.10 and I.11), Chapter 1 of Lang [365] and Chapter XII of Lang [367]. An analogous ring-theoretic formulation is used in Proposition II.6.9 of Hartshorne [278]. A different method is to study extensions of valuations directly, for example see Section III.1 of Stichtenoth [589]. Note that, since we consider points over $\overline{\Bbbk}$, the notion of residue degree does not arise, which simplifies the presentation compared with many texts.

Definition 8.2.1. Let F_2 be a field of transcendence degree 1 over $\overline{\Bbbk}$. Let F_1/F_2 be a finite extension. Let v be a discrete valuation on F_2. A valuation v' on F_1 is an **extension** of v (or, v is the **restriction** of v') if $\{f \in F_2 : v(f) \geq 0\} = \{f \in F_2 : v'(f) \geq 0\}$. We write $v' \mid v$ if this is the case.

Note that if v' is an extension of v as above then one does not necessarily have $v'(f) = v(f)$ for all $f \in F_2$ (indeed, we will see later that $v'(f) = ev(f)$ for some $e \in \mathbb{N}$).

Lemma 8.2.2. *Let F_1/F_2 be a finite extension and let $v' \mid v$ be valuations on F_1 and F_2 respectively. Then R_v is a subring of $R_{v'}$, $R_v = R_{v'} \cap F_2$ and $\mathfrak{m}_v = \mathfrak{m}_{v'} \cap F_2$. In particular, for $f \in F_2$, $v(f) = 0$ if and only if $v'(f) = 0$.*

Exercise 8.2.3. Prove Lemma 8.2.2.

Theorem 8.2.4. *Let F_1/F_2 be a finite extension of fields and let v be a valuation on F_2. Then there is at least one (and only finitely many) valuation v' of F_1 such that $v' \mid v$.*

Proof: See Theorem XII.4.1 and Corollary XII.4.9 of Lang [367] or Proposition III.1.7(b) of Stichtenoth [589]. □

Let $\phi : C_1 \to C_2$ be a morphism of curves and let $F_2 = \phi^*(\Bbbk(C_2))$ and $F_1 = \Bbbk(C_1)$. We now explain the relation between extensions of valuations from F_2 to F_1 and pre-images of points under ϕ.

Lemma 8.2.5. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$ (this is short-hand for C_1, C_2 and ϕ all being defined over $\Bbbk$). Let $P \in C_1(\overline{\Bbbk})$ and $Q \in C_2(\overline{\Bbbk})$. Denote by v the valuation on $\phi^*(\Bbbk(C_2)) \subseteq \Bbbk(C_1)$ defined by $v(\phi^*(f)) = v_Q(f)$ for $f \in \Bbbk(C_2)$. If $\phi(P) = Q$ then v_P is an extension of v.*

Proof: Let $f \in \Bbbk(C_2)$. Since $\phi(P) = Q$ we have $\phi^*(f) = f \circ \phi$ regular at P if and only if f is regular at Q. Hence $v_P(\phi^*(f)) \geq 0$ if and only if $v_Q(f) \geq 0$. It follows that $v_P \mid v$. □

Lemma 8.2.6. *Let the notation be as in Lemma 8.2.5. In particular, $P \in C_1(\overline{\Bbbk}), Q \in C_2(\overline{\Bbbk}), v_P$ is the corresponding valuation on $F_1 = \overline{\Bbbk}(C_1)$ and v is the valuation on $\phi^*(\overline{\Bbbk}(C_2))$ corresponding to v_Q on $\overline{\Bbbk}(C_2)$. Then $v_P \mid v$ implies $\phi(P) = Q$.*

Proof: Suppose $\phi(P) = Q' \neq Q$. By Lemma 8.1.14 there is some $f \in \overline{\Bbbk}(C_2)$ such that $f(Q) \neq 0$ and $f(Q') = 0$. Then $0 = v_Q(f) = v(\phi^*(f)) = v_P(\phi^*(f))$ (the last equality

by Lemma 8.2.2 and since $v_P \mid v$). But $\phi^*(f)(P) = f \circ \phi(P) = f(Q') = 0$, which is a contradiction. □

In other words, Lemmas 8.2.5 and 8.2.6 show that $\phi(P) = Q$ if and only if the maximal ideal $\mathfrak{m}_P$ in $\mathcal{O}_P \subseteq \mathbb{k}(C_1)$ contains $\phi^*(\mathfrak{m}_Q)$ where $\mathfrak{m}_Q$ is the maximal ideal in $\mathcal{O}_Q \subseteq \mathbb{k}(C_2)$. This is the connection between the behaviour of points under morphisms and the splitting of ideals in Dedekind domains.

We already know that a non-constant morphism of curves is dominant, but the next result makes the even stronger statement that a morphism is surjective.

Theorem 8.2.7. *Let C_1 and C_2 be curves over $\mathbb{k}$ (in particular, they are projective and non-singular). Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\mathbb{k}$. Then ϕ is surjective from $C_1(\overline{\mathbb{k}})$ to $C_2(\overline{\mathbb{k}})$.*

Proof: Let $Q \in C_2(\overline{\mathbb{k}})$ and let v be the corresponding valuation on $\phi^*(\overline{\mathbb{k}}(C_2))$. By Theorem 8.2.4 there is a valuation v' on $\overline{\mathbb{k}}(C_1)$ that extends v. Theorem 7.5.2 shows that $v' = v_P$ for some $P \in C_1(\overline{\mathbb{k}})$. Finally, Lemma 8.2.6 shows that $\phi(P) = Q$. □

Definition 8.2.8. Let C_1 and C_2 be curves over $\mathbb{k}$ and let $\phi : C_1 \to C_2$ be a non-constant rational map over $\mathbb{k}$. Let $P \in C_1(\overline{\mathbb{k}})$. The **ramification index** of ϕ at P is

$$e_\phi(P) = v_P(\phi^*(t_{\phi(P)}))$$

where $t_{\phi(P)}$ is a uniformizer on C_2 at $\phi(P)$. If $e_\phi(P) = 1$ for all $P \in C_1(\overline{\mathbb{k}})$ then ϕ is **unramified**.

We now show that this definition agrees with Definition III.1.5 of Stichtenoth [589].

Lemma 8.2.9. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\mathbb{k}$. Let $P \in C_1(\overline{\mathbb{k}})$, $Q = \phi(P) \in C_2(\overline{\mathbb{k}})$ and $f \in \overline{\mathbb{k}}(C_2)$. Then*

$$v_P(\phi^*(f)) = e_\phi(P) v_Q(f).$$

Proof: Let $v_Q(f) = n$ and write $f = t_Q^n h$ for some $h \in \overline{\mathbb{k}}(C_2)$ such that $h(Q) \neq 0$. Then $\phi^*(f) = \phi^*(t_Q)^n \phi^*(h)$ and $v_P(\phi^*(h))) = 0$. The result follows since $v_P(\phi^*(t_Q)^n) = n v_P(\phi^*(t_Q))$. □

Exercise 8.2.10. Let $\phi : C_1 \to C_2$ be a non-constant rational map of curves over $\mathbb{k}$. Let $P \in C_1(\overline{\mathbb{k}})$, $Q = \phi(P)$, and suppose $e_\phi(P) = 1$. Show that $t \in \overline{\mathbb{k}}(C_2)$ is a uniformizer at Q if and only if $\phi^*(t)$ is a uniformizer at P.

Exercise 8.2.11. Let $\phi : C_1 \to C_2$ be an isomorphism of curves over $\mathbb{k}$. Show that ϕ is unramified.

The following result is of fundamental importance.

Theorem 8.2.12. *Let C_1 and C_2 be curves over $\mathbb{k}$ and let $\phi : C_1 \to C_2$ be a non-constant rational map over $\mathbb{k}$. Then for all $Q \in C_2(\overline{\mathbb{k}})$ we have*

$$\sum_{P \in C_1(\overline{\mathbb{k}}) : \phi(P) = Q} e_\phi(P) \quad = \quad \deg(\phi).$$

Proof: As mentioned above, one can see this by noting that $\phi^*(\mathcal{O}_Q)$ and $\phi^*(\mathbb{k}[U])$ (for an open set $U \subseteq C_2$ with $Q \in U$) are Dedekind domains and studying the splitting of $\mathfrak{m}_Q$ in their integral closures in $\mathbb{k}(C_1)$. For details see any of Proposition 1.10 and 1.11 of Serre [542], Corollary XII.6.3 of Lang [367], Proposition I.21 of Lang [365], Theorem III.3.5 of Lorenzini [394], Proposition II.6.9 of Hartshorne [278], or Theorem III.1.11 of Stichenoth [589]. □

Corollary 8.2.13. *If $\phi : C_1 \to C_2$ is a rational map of degree d and $Q \in C_2(\overline{\Bbbk})$ then there are at most d points $P \in C_1(\overline{\Bbbk})$ such that $\phi(P) = Q$.*

Furthermore, if ϕ is separable then there is an open subset $U \subseteq C_2$ such that for all $Q \in U$ one has $\#\phi^{-1}(Q) = d$.

Proof: The first statement is immediate. The second follows by choosing U to be the complement of points corresponding to factors of the discriminant of $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$; see Proposition VII.5.7 of Lorenzini [394]. □

Example 8.2.14. Consider $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ given by $\phi(x) = x^2$ as in Example 8.1.4. This extends to the morphism $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ given by $\phi((x : z)) = (x^2/z^2 : 1)$, which is regular at $\infty = (1 : 0)$ via the equivalent formula $(1 : z^2/x^2)$. One has $\phi^{-1}((a : 1)) = \{(\sqrt{a} : 1), (-\sqrt{a} : 1)\}$, $\phi^{-1}((0 : 1)) = \{(0 : 1)\}$ and $\phi^{-1}((1 : 0)) = \{(1 : 0)\}$. At a point $Q = (a : 1)$ with $a \neq 0$ one has uniformizer $t_Q = x/z - a$ and

$$\phi^*(t_Q) = x^2/z^2 - a = (x/z - \sqrt{a})(x/z + \sqrt{a}).$$

Writing $P = (\sqrt{a} : 1)$ one has $\phi(P) = Q$ and $e_\phi(P) = 1$. However, one can verify that $e_\phi((0 : 1)) = e_\phi((1 : 0)) = 2$.

Lemma 8.2.15. *Let $\phi : C_1 \to C_2$ and $\psi : C_2 \to C_3$ be non-constant morphisms of curves over $\Bbbk$. Let $P \in C_1(\overline{\Bbbk})$. Then $e_{\psi\circ\phi}(P) = e_\phi(P)e_\psi(\phi(P))$.*

Exercise 8.2.16. Prove Lemma 8.2.15.

Exercise 8.2.17. Let $\phi : C_1 \to C_2$ be defined over $\Bbbk$. Let $P \in C_1(\overline{\Bbbk})$ and let $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Show that $e_\phi(\sigma(P)) = e_\phi(P)$.

8.3 Maps on Divisor Classes

We can now define some important maps on divisors that will be used in several proofs later. In particular, this will enable an elegant proof of Theorem 7.7.11 for general curves.

Definition 8.3.1. Let $\phi : C_1 \to C_2$ be a non-constant morphism over $\Bbbk$. Define the **pullback**

$$\phi^* : \mathrm{Div}_{\overline{\Bbbk}}(C_2) \to \mathrm{Div}_{\overline{\Bbbk}}(C_1)$$

as follows. For $Q \in C_2(\overline{\Bbbk})$ define $\phi^*(Q) = \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P)$ and extend ϕ^* to $\mathrm{Div}_{\overline{\Bbbk}}(C_2)$ by linearity, i.e.,

$$\phi^*\left(\sum_{Q \in C_2(\overline{\Bbbk})} n_Q(Q)\right) = \sum_{Q \in C_2(\overline{\Bbbk})} n_Q \phi^*(Q).$$

Note that, since $\mathrm{Div}_{\overline{\Bbbk}}(C_2)$ and $\mathrm{Div}_{\overline{\Bbbk}}(C_1)$ are not varieties, it does not make sense to ask whether ϕ^* is a rational map or morphism.

Example 8.3.2. Consider $\phi : \mathbb{A}^1 \to \mathbb{A}^1$ given by $\phi(x) = x^2$. Let $D = (0) + (1)$ be a divisor on $\mathbb{A}^1$. Then $\phi^*(D) = 2(0) + (1) + (-1)$.

Let $\phi : C_1 \to C_2$ be a non-constant morphism over $\Bbbk$ and let $P \in C_2(\overline{\Bbbk})$. Then the divisor $\phi^*(P)$ is also called the **conorm** of P with respect to $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$ (see Definition III.1.8 of Stichtenoth [589]).

Lemma 8.3.3. *Let C be a curve over $\Bbbk$ and let $f \in \Bbbk(C)^*$ be a non-constant rational function. Define the rational map $\phi : C \to \mathbb{P}^1$ by $\phi = (f : 1)$ (in future we will write f instead of ϕ). Then ϕ is a morphism and* $\mathrm{div}(f) = \phi^*((0 : 1) - (1 : 0))$.

Proof: That ϕ is a morphism follows from Lemma 7.3.6. Let $P \in C(\overline{\Bbbk})$ be such that $f(P) = 0$ (i.e., $\phi(P) = (0:1)$). We prove that $v_P(f) = e_\phi(P)$. Recall that $t = x/z$ is a uniformizer at $(0:1)$. By definition, $e_\phi(P) = v_P(t \circ \phi)$. Now $t \circ \phi = x(f:1)/z(f:1) = f/1 = f$. Hence, $e_\phi(P) = v_P(f)$. One handles poles of f analogously using the formula $e_\phi(P) = v_P(1/f)$. □

There is a natural map ϕ_* on divisors that is called the **pushforward** (it is called the **divisor-norm map** in Section VII.7 of Lorenzini [394]).

Definition 8.3.4. Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves. Define the **pushforward**

$$\phi_* : \mathrm{Div}_{\overline{\Bbbk}}(C_1) \to \mathrm{Div}_{\overline{\Bbbk}}(C_2)$$

by $\phi_*(P) = \phi(P)$ and extend to the whole of $\mathrm{Div}_{\overline{\Bbbk}}(C_1)$ by linearity.

It remains to find a map from $\Bbbk(C_1)$ to $\Bbbk(C_2)$ that corresponds (in the sense of property 4 of Theorem 8.3.8) to the pushforward. This is achieved using the norm map with respect to the extension $\Bbbk(C_1)/\phi^*(\Bbbk(C_2))$. As we will show in Lemma 8.3.13 this norm satisfies, for $f \in \Bbbk(C_1)$ and $Q \in C_2(\overline{\Bbbk})$, $\mathrm{N}_{\Bbbk(C_1)/\phi^*(\Bbbk(C_2))}(f)(Q) = \prod_{\phi(P)=Q} f(P)^{e_\phi(P)}$.

Definition 8.3.5. Let C_1, C_2 be curves over $\Bbbk$ and let $\phi : C_1 \to C_2$ be a non-constant rational map. Let $N_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}$ be the usual norm map in field theory (see Section A.6). Define

$$\phi_* : \Bbbk(C_1) \to \Bbbk(C_2)$$

by $\phi_*(f) = (\phi^*)^{-1}(\mathrm{N}_{\Bbbk(C_1)/\phi^*(\Bbbk(C_2))}(f))$.

Note that the definition of $\phi_*(f)$ makes sense since $\mathrm{N}_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}(f) \in \phi^*(\Bbbk(C_2))$ and so is of the form $h \circ \phi$ for some $h \in \Bbbk(C_2)$. So $\phi_*(f) = h$.

Example 8.3.6. Let $C_1 = C_2 = \mathbb{A}^1$ and $\phi : C_1 \to C_2$ be given by $\phi(x) = x^2$. Then $\phi^*(\Bbbk(C_2)) = \Bbbk(x^2)$ and $\Bbbk(C_1) = \phi^*(\Bbbk(C_2))(x)$. Let $f(x) = x^2/(x-1)$. Then

$$\mathrm{N}_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}(f) = f(x)f(-x) = \frac{x^2}{(x-1)}\frac{(-x)^2}{(-x-1)} = \frac{x^4}{-x^2+1},$$

which is $h \circ \phi$ for $h(X) = X^2/(1-X)$. Hence $\phi_*(f(x)) = -f(x)$.

Exercise 8.3.7. Let $C_1 = V(y^2 = x^2 + 1) \subseteq \mathbb{A}^2$, $C_2 = \mathbb{A}^1$ and let $\phi : C_1 \to C_2$ be given by $\phi(x, y) = x$. Let $f(x, y) = x/y$. Show that

$$\mathrm{N}_{\Bbbk(C_1)/\phi^*\Bbbk(C_2)}(f) = \frac{-x^2}{x^2+1}$$

and so $\phi_*(f) = h(X)$ where $h(X) = -X^2/(X^2+1)$.

We now state the main properties of the pullback and pushforward.

Theorem 8.3.8. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Then*

1. $\deg(\phi^*(D)) = \deg(\phi)\deg(D)$ *for all* $D \in \mathrm{Div}(C_2)$.
2. $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$ *for all* $f \in \Bbbk(C_2)^*$.
3. $\deg(\phi_*(D)) = \deg(D)$ *for all* $D \in \mathrm{Div}(C_1)$.
4. $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_*(f))$ *for all* $f \in \Bbbk(C_1)^*$.
5. $\phi_*(\phi^*(D)) = \deg(\phi)D$ *for* $D \in \mathrm{Div}(C_2)$.

6. *If $\psi : C_2 \to C_3$ is another non-constant rational map of curves over $\Bbbk$ then $(\psi\circ\phi)^* = \phi^* \circ \psi^*$ and $(\psi \circ \phi)_* = \psi_* \circ \phi_*$.*

Proof: (Sketch)

1. Follows from Theorem 8.2.12.
2. Follows from Lemma 8.2.9.
3. Follows directly from the definition.
4. First note that

$$\phi_*(\mathrm{div}(f)) = \sum_{P \in C_1(\overline{\Bbbk})} v_P(f)(\phi(P)) = \sum_{Q \in C_2(\overline{\Bbbk})} \left(\sum_{P \in C_1(\overline{\Bbbk}) : \phi(P) = Q} v_P(f) \right) (Q).$$

   To complete the proof it suffices to show that $\sum_{P \in C_1(\overline{\Bbbk}):\phi(P)=Q} v_P(f) = v_Q(\phi_*(f))$. This requires some theory that has not been presented in the book, so we sketch the details here.
   Write $L = \overline{\Bbbk}(C_1)$, $K = \phi^*(\overline{\Bbbk}(C_2)) \subseteq L$. Fix $Q \in C_2(\overline{\Bbbk})$ and write v for the valuation on K corresponding to v_Q on $\overline{\Bbbk}(C_2)$. Write $A = \phi^*(\mathcal{O}_{Q,\overline{\Bbbk}}(C_2)) \subseteq K$, which is a Dedekind domain, and let B be the integral closure of A in L. Write $\mathfrak{m}$ for the maximal ideal of A corresponding to $\mathfrak{m}_{Q,\overline{\Bbbk}}(C_2)$. If $P \in C_1(\overline{\Bbbk})$ is such that $\phi(P) = Q$ then $\mathfrak{m} = \mathfrak{m}_{P,\overline{\Bbbk}}(C_1) \cap A$. Suppose first that L/K is Galois. Then for any B-ideal I one can define the norm $\mathrm{N}_{L/K}(I) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(I)$. Lemma IV.6.4 of Lorenzini [394] implies that $\mathrm{N}_{L/K}(\mathfrak{m}_{P,\overline{\Bbbk}}(C_1)) = \mathfrak{m}$. When L/K is not Galois then one can define $\mathrm{N}_{L/K}$ by $\mathrm{N}_{L/K}(\mathfrak{m}_{P,\overline{\Bbbk}}(C_1)) = \mathfrak{m}$. Proposition IV.6.9 of [394] shows (also see Proposition I.22 of [365] in the case when L/K is separable) that $\mathrm{N}_{L/K}((f)) = (\mathrm{N}_{L/K}(f))$, where (f) denotes the principal B-ideal generated by f and where $\mathrm{N}_{L/K}(f)$ denotes the usual field-theoretic norm. Since

$$\mathrm{N}_{L/K}((f)) = \prod_{\mathfrak{m}_P \supseteq \mathfrak{m}} \mathfrak{m}_P^{v_P(f)} \qquad \text{and} \qquad (\mathrm{N}_{L/K}(f)) = \mathfrak{m}^{v\left(\mathrm{N}_{L/K}(f)\right)}$$

   (where the latter are A-ideals) the result follows.
5. Follows easily from Theorem 8.2.12.
6. The first statement follows from Lemma 8.2.15 and the second is straightforward from the definition.

□

Exercise 8.3.9. Give all the details in the proof of Theorem 8.3.8.

Corollary 8.3.10. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Then the induced maps $\phi^* : \mathrm{Pic}^0_{\Bbbk}(C_2) \to \mathrm{Pic}^0_{\Bbbk}(C_1)$ and $\phi_* : \mathrm{Pic}^0_{\Bbbk}(C_1) \to \mathrm{Pic}^0_{\Bbbk}(C_2)$ on divisor class groups are well-defined group homomorphisms.*

Proof: The maps ϕ^* and ϕ_* are well-defined on divisor classes by parts 2 and 4 of Theorem 8.3.8. The homomorphic property follows from the linearity of the definitions. □

Exercise 8.3.11. Show that if $\phi : C_1 \to C_2$ is an isomorphism of curves over $\Bbbk$ then $\mathrm{Pic}^0_{\Bbbk}(C_1) \cong \mathrm{Pic}^0_k(C_2)$ (isomorphic as groups). Give an example to show that the converse is not true.

A further corollary of this result is that a rational map $\phi : E_1 \to E_2$ between elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is automatically a group homomorphism (see Theorem 9.2.1).

Exercise 8.3.12. Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be defined by $\phi((x : z)) = (x^2/z^2 : 1)$. Let $D = (-1 : 1) + (1 : 0) - (0 : 1)$. Compute $\phi_*(D)$, $\phi^*(D)$, $\phi_*\phi^*(D)$ and $\phi^*\phi_*(D)$.

We now make an observation that was mentioned when we defined ϕ_* on $\mathbb{k}(C_1)$.

Lemma 8.3.13. *Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\mathbb{k}$. Let $f \in \mathbb{k}(C_1)^*$ and $Q \in C_2(\overline{\mathbb{k}})$. Suppose that $v_P(f) = 0$ for all points $P \in C_1(\overline{\mathbb{k}})$ such that $\phi(P) = Q$. Then*

$$\mathrm{N}_{\mathbb{k}(C_1)/\phi^*(\mathbb{k}(C_2))}(f)(Q) = \prod_{P \in C_1(\overline{\mathbb{k}}) : \phi(P) = Q} f(P)^{e_\phi(P)}.$$

(Later in the book we will introduce the notation $f(\phi^*(Q))$ for the right hand side.) Another formulation would be "f of conorm of Q equals norm of f at Q".

Proof: (Sketch) This uses similar ideas to the proof of part 4 of Theorem 8.3.8. We work over $\overline{\mathbb{k}}$.

As always, $\overline{\mathbb{k}}(C_1)$ is a finite extension of $\phi^*(\overline{\mathbb{k}}(C_2))$. Let $A = \phi^*(\mathcal{O}_Q(C_2))$ and let B be the integral closure of A in $\mathbb{k}(C_1)$. Then B is a Dedekind domain and the ideal $\phi^*(\mathfrak{m}_Q)$ splits as a product $\prod_i \mathfrak{m}_{P_i}^{e_\phi(P_i)}$ where $P_i \in C_1(\overline{\mathbb{k}})$ are distinct points such that $\phi(P_i) = Q$.

By assumption, f has no poles at P_i and so $f \in B$. Note that $f(P_i) = c_i \in \overline{\mathbb{k}}$ if and only if $f \equiv c_i \pmod{\mathfrak{m}_{P_i}}$. Hence, the right hand side is

$$\prod_i f(P_i)^{e_\phi(P_i)} = \prod_i c_i^{e_\phi(P_i)} = \prod_i (f \pmod{\mathfrak{m}_{P_i}})^{e_\phi(P_i)}.$$

It remains to prove that this is equal to the norm of f evaluated at Q and we sketch this when the extension is Galois and cyclic (the general case is simple linear algebra). The elements $\sigma \in \mathrm{Gal}(\overline{\mathbb{k}}(C_1)/\phi^*(\overline{\mathbb{k}}(C_2)))$ permute the $\mathfrak{m}_{P_i}$ and the ramification indices $e_\phi(P_i)$ are all equal. Since $c_i \in \overline{\mathbb{k}} \subset \phi^*(\mathbb{k}(C_2))$ we have $f \equiv c_i \pmod{\mathfrak{m}_{P_i}}$ if and only if $\sigma(f) \equiv c_i \pmod{\sigma(\mathfrak{m}_{P_i})}$. Hence

$$\mathrm{N}_{\mathbb{k}(C_1)/\phi^*(\mathbb{k}(C_2))}(f) = \prod_{\sigma \in \mathrm{Gal}(\overline{\mathbb{k}}(C_1)/\phi^*(\overline{\mathbb{k}}(C_2)))} \sigma(f) \equiv \prod_i c_i^{e_\phi(P_i)} \pmod{\mathfrak{m}_{P_1}}$$

and since $\mathrm{N}_{\mathbb{k}(C_1)/\phi^*(\mathbb{k}(C_2))}(f) \in \phi^*(\mathbb{k}(C_2))$ this congruence holds modulo $\phi^*(\mathfrak{m}_Q)$. The result follows. □

We now give an important application of Theorem 8.3.8, already stated as Theorem 7.7.11.

Theorem 8.3.14. *Let C be a curve over $\mathbb{k}$ and let $f \in \mathbb{k}(C)^*$. Then f has only finitely many zeroes and poles (i.e., $\mathrm{div}(f)$ is a divisor) and $\deg(\mathrm{div}(f)) = 0$.*

Proof: Let $D = (0 : 1) - (1 : 0)$ on $\mathbb{P}^1$. Interpreting f as a rational map $f : C \to \mathbb{P}^1$ as in Lemma 8.1.1 we have $\mathrm{div}(f) = f^*(D)$ and, by part 1 of Theorem 8.3.8, $\deg(f^*(D)) = \deg(f)\deg(D) = 0$. One also deduces that f has, counting with multiplicity, $\deg(f)$ poles and zeroes. □

Exercise 8.3.15. Let $\phi : C_1 \to C_2$ be a rational map over $\mathbb{k}$. Show that if $D \in \mathrm{Div}_{\mathbb{k}}(C_1)$ (respectively, $D \in \mathrm{Div}_{\mathbb{k}}(C_2)$) then $\phi_*(D)$ (resp., $\phi^*(D)$) is defined over $\mathbb{k}$.

8.4 Riemann-Roch Spaces

Definition 8.4.1. Let C be a curve over $\Bbbk$ and let $D = \sum_P n_P(P)$ be a divisor on C. The **Riemann-Roch space** of D is

$$\mathcal{L}_\Bbbk(D) = \{f \in \Bbbk(C)^* : v_P(f) \geq -n_P \text{ for all } P \in C(\overline{\Bbbk})\} \cup \{0\}.$$

We denote $\mathcal{L}_{\overline{\Bbbk}}(D)$ by $\mathcal{L}(D)$.

Lemma 8.4.2. *Let C be a curve over $\Bbbk$ and let D be a divisor on C. Then*

1. *$\mathcal{L}_\Bbbk(D)$ is a $\Bbbk$-vector space.*
2. *$D \leq D'$ implies $\mathcal{L}_\Bbbk(D) \subseteq \mathcal{L}_\Bbbk(D')$.*
3. *$\mathcal{L}_\Bbbk(0) = \Bbbk$, $\mathcal{L}_\Bbbk(D) = \{0\}$ if $\deg(D) < 0$.*
4. *Let $P_0 \in C(\overline{\Bbbk})$. Then $\dim_\Bbbk(\mathcal{L}_\Bbbk(D+P_0)/\mathcal{L}_\Bbbk(D)) \leq 1$ and if $D' \geq D$ then $\dim_\Bbbk(\mathcal{L}_\Bbbk(D')/\mathcal{L}_\Bbbk(D)) \leq \deg(D') - \deg(D)$.*
5. *$\mathcal{L}_\Bbbk(D)$ is finite dimensional and if $D = D_+ - D_-$, where D_+, D_- are effective, then $\dim_\Bbbk \mathcal{L}_\Bbbk(D) \leq \deg(D_+) + 1$.*
6. *If $D' = D + \operatorname{div}(f)$ for some $f \in \Bbbk(C)^*$ then $\mathcal{L}_\Bbbk(D)$ and $\mathcal{L}_\Bbbk(D')$ are isomorphic as $\Bbbk$-vector spaces.*

Proof: (Sketch)

1. Straightforward from the definition and part 3 of Lemma 7.4.14.
2. Write $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ and $D' = \sum_P n'_P(P)$. Then $D \leq D'$ implies $n_P \leq n'_P$. If $f \in \mathcal{L}_\Bbbk(D)$ then $v_P(f) \geq -n_P \geq n'_P$ and so $f \in \mathcal{L}_\Bbbk(D')$.
3. Clearly $\Bbbk \subseteq \mathcal{L}_\Bbbk(0)$. The converse follows from Corollary 7.7.13. The second statement follows since $\deg(\operatorname{div}(f)) = 0$.
4. Write $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$. Note that $\mathcal{L}_\Bbbk(D)$ is a $\Bbbk$-vector subspace of $\mathcal{L}_\Bbbk(D + P_0)$. Let $t \in \Bbbk(C)^*$ be a function such that $v_{P_0}(f) = n_{P_0} + 1$ (e.g., take t to be a power of a uniformizer at P_0). If $f \in \mathcal{L}_\Bbbk(D + P_0)$ then $ft \in \mathcal{O}_{P,\Bbbk}(C)$. We therefore have a $\Bbbk$-linear map $\psi : \mathcal{L}_\Bbbk(D + P_0) \to \Bbbk$ given by $\psi(f) = (ft)(P_0)$. The kernel of ψ is $\mathcal{L}_\Bbbk(D)$ and the first part of the statement follows. The second statement follows by induction.
5. First, note that $\mathcal{L}_\Bbbk(D) \subseteq \mathcal{L}_\Bbbk(D_+)$. We then compute $\dim_\Bbbk \mathcal{L}_\Bbbk(D_+) = 1 + \dim_\Bbbk(\mathcal{L}_\Bbbk(D_+)/\mathcal{L}_\Bbbk(0))$. By the previous part this is $\leq 1 + \deg(D_+) - \deg(0) = 1 + \deg(D_+)$.
6. The linear map $\mathcal{L}_\Bbbk(D) \to \mathcal{L}_\Bbbk(D')$ is given by $h \mapsto h/f$.

□

Exercise 8.4.3. Fill in the gaps in the proof of Lemma 8.4.2.

Exercise 8.4.4. Let $D = \sum_{P \in C(\overline{\Bbbk})} n_P(P)$ be a divisor on C. Explain why $\{f \in \Bbbk(C)^* : v_P(f) = n_P \text{ for all } P \in C(\overline{\Bbbk})\} \cup \{0\}$ is not usually a $\Bbbk$-vector space.

Definition 8.4.5. Let C be a curve over $\Bbbk$ and let D be a divisor on C. Define

$$\ell_\Bbbk(D) = \dim_\Bbbk \mathcal{L}_\Bbbk(D).$$

Write $\ell(D) = \ell_{\overline{\Bbbk}}(D)$.

Exercise 8.4.6. Show that $\ell_{\Bbbk}(0) = 1$ and, for $f \in \Bbbk(C)$, $\ell_{\Bbbk}(\mathrm{div}(f)) = 1$.

Theorem 8.4.7. *(Riemann's theorem) Let C be a curve over $\Bbbk$ (in particular, non-singular and projective) . Then there exists a unique minimal integer g such that, for all divisors D on C over $\overline{\Bbbk}$*

$$\ell_{\overline{\Bbbk}}(D) \geq \deg(D) + 1 - g.$$

Proof: See Proposition I.4.14 of Stichtenoth [589], Section 8.3 (page 196) of Fulton [216] or Theorem 2.3 of Moreno [439]. □

Definition 8.4.8. The number g in Theorem 8.4.7 is called the **genus** of C.

Note that the genus is independent of the model of the curve C and so one can associate the genus with the function field or birational equivalence class of the curve.

Exercise 8.4.9. Show that on $\mathbb{P}^1$ over $\Bbbk$ one has $\ell_{\overline{\Bbbk}}(D) = \deg(D) + 1$ for all divisors D and so the genus of $\mathbb{P}^1$ is zero. Note that if D is defined over $\Bbbk$ then $\ell_{\Bbbk}(D) = \deg(D) + 1$ too. (More results about genus zero are given in Section 8.6.)

Exercise 8.4.10. Let $\Bbbk$ be a field and let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\Bbbk$. Determine the spaces $\mathcal{L}_{\Bbbk}(n\mathcal{O}_E)$ and their dimensions $\ell_{\Bbbk}(n\mathcal{O}_E)$ for $n = 0, 1, 2, 3, 4, 5, 6$.

Remark 8.4.11. We give an alternative justification for Remark 5.4.14. Suppose $f \in \overline{\Bbbk}(C)$ is such that $\sigma(f) = f$ for all $\sigma \in \mathrm{Gal}(\overline{\Bbbk}/\Bbbk)$. Write $D = \mathrm{div}(f)$. Note that D is defined over $\Bbbk$. Then $f \in \mathcal{L}_{\overline{\Bbbk}}(D)$, which has dimension 1 by Exercise 8.4.6. Now, performing the Brill-Noether proof of Riemann's theorem (e.g., see Section 8.5 of Fulton [216]) one can show that $\mathcal{L}_{\Bbbk}(D)$ contains a function $h \in \Bbbk(C)$. It follows that $\mathrm{div}(h) = D$ and that $f = ch$ for some $c \in \Bbbk$. Hence Theorem 7.8.3 is proved.

8.5 Derivations and Differentials

Differentials arise in differential geometry: a manifold is described by open patches homeomorphic to $\mathbb{R}^n$ (or $\mathbb{C}^n$ for complex manifolds) with coordinate functions $x_1, \ldots, x_n$ and the differentials dx_i arise naturally. It turns out that differentials can be described in a purely formal way (i.e., without reference to limits).

When working over general fields (such as finite fields) it no longer makes sense to consider differentiation as a process defined by limits. But the formal description of differentials makes sense and the concept turns out to be useful.

We first explain how to generalise partial differentiation to functions on curves. We can then define differentials. Throughout this section, if $F(x, y)$ is a polynomial or rational function then $\partial F/\partial x$ denotes standard undergraduate partial differentiation.

Definition 8.5.1. Let C be a curve over $\Bbbk$. A **derivation** on $\Bbbk(C)$ is a $\Bbbk$-linear map (treating $\Bbbk(C)$ as a $\Bbbk$-vector space) $\delta : \Bbbk(C) \to \Bbbk(C)$ such that $\delta(f_1f_2) = f_1\delta(f_2) + f_2\delta(f_1)$.

Lemma 8.5.2. *Let $\delta : \Bbbk(C) \to \Bbbk(C)$ be a derivation. Then*

1. *If $c \in \Bbbk$ then $\delta(c) = 0$.*
2. *If $x \in \Bbbk(C)$ and $n \in \mathbb{Z}$ then $\delta(x^n) = nx^{n-1}\delta(x)$.*
3. *If $\mathrm{char}(\Bbbk) = p$ and $x \in \Bbbk(C)$ then $\delta(x^p) = 0$.*
4. *If $h \in \Bbbk(C)$ then $\delta'(f) = h\delta(f)$ is a derivation.*

5. *If $x, y \in \Bbbk(C)$ then $\delta(x/y) = (y\delta(x) - x\delta(y))/y^2$.*
6. *If $x, y \in \Bbbk(C)$ and $F(u, v) \in \Bbbk[u, v]$ is a polynomial then $\delta(F(x, y)) = (\partial F/\partial x)\delta(x) + (\partial F/\partial y)\delta(y)$.*

Exercise 8.5.3. Prove Lemma 8.5.2.

Definition 8.5.4. Let C be a curve over $\Bbbk$. A function $x \in \Bbbk(C)$ is a **separating element** (or **separating variable**) if $\Bbbk(C)$ is a finite separable extension of $\Bbbk(x)$.

Note that if $x \in \Bbbk(C)$ is such that $x \notin \overline{\Bbbk}$ then $\Bbbk(C)/\Bbbk(x)$ is finite; hence the non-trivial condition is that $\Bbbk(C)/\Bbbk(x)$ is separable.

Example 8.5.5. For $\mathbb{P}^1(\mathbb{F}_p)$, x is a separating element (since $\Bbbk(\mathbb{P}^1) = \Bbbk(x)$) and x^p is not a separating element (since $\Bbbk(\mathbb{P}^1)/\Bbbk(x^p) = \Bbbk(x)/\Bbbk(x^p)$ is not separable). The mapping $\delta(f) = \partial f/\partial x$ is a derivation.

The following exercise shows that separating elements exist for elliptic and hyperelliptic curves. For general curves we need Lemma 8.5.7.

Exercise 8.5.6. Let $\Bbbk$ be any field and let C be a curve given by an equation of the form $y^2 + H(x)y = F(x)$ with $H(x), F(x) \in \Bbbk[x]$. Show that if either $H(x) \neq 0$ or if $\mathrm{char}(\Bbbk) \neq 2$ then x is a separating element of $\Bbbk(C)$.

Lemma 8.5.7. *Let C be a curve over $\Bbbk$, where $\Bbbk$ is a perfect field. Then there exists a separating element $x \in \Bbbk(C)$.*

Proof: Let $L = \Bbbk(x_1, \ldots, x_n)$ be any field extension of transcedence degree 1 of a perfect field $\Bbbk$. We show that L is a separable extension of $\Bbbk(x)$ for some x. First, note that either $\{x_1, \ldots, x_n\}$ is algebraically dependent (and so there is a polynomial $F(x_1, \ldots, x_n) = 0$ of minimal degree, hence irreducible), or else $L = \Bbbk(x_1)$ and we're done. In the former case, write $F = \sum_i f_i m_i$ where $f_i \in \Bbbk$ and m_i are monomials in $x_1, \ldots, x_n$.

We claim that F is separable in at least one variable (i.e., $\partial F/\partial x_i \neq 0$). To show this, suppose F is not separable in any variable. Then all monomials are p-powers, $m_i = n_i^p$. Since $\Bbbk$ is perfect $f_i^{1/p} \in \Bbbk$. Hence $F = (\sum_i f_i^{1/p} n_i)^p$ is not irreducible.

Re-order the variables so that F is separable in x_n. Then $\Bbbk(x_1, \ldots, x_n)/\Bbbk(x_1, \ldots, x_{n-1})$ is a separable extension. Applying the argument inductively to $\Bbbk(x_1, \ldots, x_{n-1})$ proves the result. □

Lemma 8.5.8. *Let C be a curve over $\Bbbk$, let $P \in C(\Bbbk)$ and let t_P be a uniformizer at P. Then t_p is a separating element of $\Bbbk(C)$.*

Proof: Let $p = \mathrm{char}(\Bbbk)$. Then $v_P(t_P) = 1 \not\equiv 0 \pmod{p}$ and so, by Proposition III.9.2(a) of Stichtenoth [589], t_P is a separating element. □

Suppose now that C is a curve over $\Bbbk$ and x is a separating element. We wish to extend $\delta(f) = \partial f/\partial x$ from $\Bbbk(x)$ to the whole of $\Bbbk(C)$. The natural approach is to use property 6 of Lemma 8.5.2: If $f \in \Bbbk(C)$ then $\Bbbk(x, f)/\Bbbk(x)$ is finite and separable; write $F(T)$ for the minimal polynomial of f over $\Bbbk(x)$ in $\Bbbk(C)$; since the extension is separable we have $\partial F/\partial T \neq 0$; as a function on C we have $F(x, f) = 0$ and so

$$0 = \delta(F(x, f)) = \frac{\partial F}{\partial x}\delta(x) + \frac{\partial F}{\partial T}\delta(f). \tag{8.1}$$

This motivates the following definition.

Definition 8.5.9. Let C be a curve over $\Bbbk$ and let $x \in \Bbbk(C)$ be a separating element. Let $y \in \Bbbk(C)$. Let $F(x,T)$ be a rational function such that $F(x,y) = 0$. Define

$$\frac{\partial y}{\partial x} = -(\partial F/\partial x)/(\partial F/\partial T)$$

evaluated at y.

Lemma 8.5.10. *The value $\partial y/\partial x$ in Definition 8.5.9 is well-defined. More precisely, if F and F' are rational functions (hopefully the notation is not confusing; here F' is* not *the derivative of F) such that $F(x,y) = F'(x,y) = 0$ then $(\partial F/\partial x)/(\partial F/\partial y) = (\partial F'/\partial x)/(\partial F'/\partial y)$ and if $z \equiv y$ in $\Bbbk(C)$ then $\partial z/\partial x \equiv \partial y/\partial x$.*

Proof: The first claim follows from equation (8.1). For the second claim, if $z = y$ in $\Bbbk(C)$ then they satisfy the same minimal polynomial. □

It remains to show that this construction does give a derivation.

Lemma 8.5.11. *Let C be a curve over $\Bbbk$ and $x \in \Bbbk(C)$ a separating element. The function $\delta : \Bbbk(C) \to \Bbbk(C)$ defined by $\delta(y) = \partial y/\partial x$ as in Definition 8.5.9 is $\Bbbk$-linear and satisfies the product rule.*

Furthermore, if $f = H(y) \in \Bbbk(C)$ is another function, where $H(T) \in \Bbbk(x)[T]$ is a polynomial, then

$$\delta(f) = \frac{\partial H}{\partial x} - (\partial F/\partial x)/(\partial F/\partial T)\frac{\partial H}{\partial T} \tag{8.2}$$

evaluated at y, where F is as in Definition 8.5.9.

Proof: (Sketch; see Proposition IV.1.4 of Stichtenoth for details.)

Consider the two maps $D_1, D_2 : \Bbbk(x)[T] \to \Bbbk(x)[T]$ defined by

$$D_1\left(\sum_i u_i T^i\right) = \sum_i \frac{\partial u_i}{\partial x} T^i \ , \qquad D_2\left(\sum_i u_i T^i\right) = \sum_i i u_i T^{i-1}.$$

(So D_1 corresponds to $\partial/\partial x$ while D_2 will correspond to $\partial/\partial y$.) One can verify that D_1 and D_2 are $\Bbbk$-linear maps. Furthermore, one can verify that if $u, v \in \Bbbk(x)[T]$ then $D_1(uv) = uD_1(v) + vD_1(u)$ and $D_2(uv) = uD_2(v) + vD_2(u)$.

We re-write equation (8.2) as

$$\delta(f) = D_1(H) - D_1(F)/D_2(F)D_2(H) \tag{8.3}$$

evaluated at y. One can show that δ is well-defined, in the sense that if $H(T) = Q(T)F(T) + R(T)$ for $Q, R \in \Bbbk(x)[T]$ then $f = H(y) = R(y)$ and the value of $\delta(f)$ is the same regardless of whether H or R is used to compute it.

Let y be such that $\Bbbk(C) = \Bbbk(x)(y)$ and write $F(T) \in \Bbbk(x)[T]$ for the minimal polynomial of y. For any $f \in \Bbbk(C)$ we have $f = H(y)$ for some polynomial $H(T) \in \Bbbk(x)[T]$ and so define $\delta(f)$ using equation (8.3). We show that δ is a derivation. The $\Bbbk$-linearity of δ is clear. To show that δ satisfies the product rule let $g, h \in \Bbbk(C)$ and write $g = G(y)$ and $h = H(y)$ for $G[T], H[T] \in \Bbbk(x)[T]$. Then note that

$$\begin{aligned}
\delta(gh) &= D_1(GH) - \frac{D_1(F)}{D_2(F)} D_2(GH) \\
&= GD_1(H) + HD_1(G) - \frac{D_1(F)}{D_2(F)}(GD_2(H) + HD_2(G)) \\
&= G\left(D_1(H) - \frac{D_1(F)}{D_2(F)} D_2(H)\right) + H\left(D_1(G) - \frac{D_1(F)}{D_2(F)} D_2(G)\right) \\
&= g\delta(h) + h\delta(g).
\end{aligned}$$

The equivalence of the two definitions (i.e., equations (8.2) and (8.3)) follows from the uniqueness of derivations extending $\Bbbk(x)$ (Lemma IV.1.3 of Stichtenoth [589]). □

Example 8.5.12. Let $C : y^2 = x^3 + x + 1$ over $\mathbb{Q}$. Note that x is a separating element. To compute $\partial y/\partial x$ one uses the fact that $F(x, y) = y^2 - (x^3 + x + 1) = 0$ in $\Bbbk(C)$ and so $\partial y/\partial x = (3x^2 + 1)/(2y)$.

Consider the function $f(x, y) = xy$ and let $\delta(f) = \partial f/\partial x$. Then $\delta(f) = x\delta(y) + y = x(3x^2 + 1)/(2y) + y = (3x^3 + x + 2y^2)/(2y) = (5x^3 + 3x + 2)/(2y)$.

Exercise 8.5.13. Let $\Bbbk(C)$ be as in Example 8.5.12. Show that $\delta(y/x) = (x^3 - x - 2)/(2yx^2)$.

Lemma 8.5.14. *Let C be a curve over $\Bbbk$ and let $x, y \in \Bbbk(C)$ be separating elements. Then the corresponding derivations on $\Bbbk(C)$ satisfy the chain rule, namely*

$$\frac{\partial f}{\partial y} = \frac{\partial f}{\partial x}\frac{\partial x}{\partial y}.$$

In particular, if $x, y \in \Bbbk(C)$ are separating elements then $\partial x/\partial y = 1/(\partial y/\partial x) \neq 0$.

Let $t \in \Bbbk(C)$. Then $\partial t/\partial x = 0$ if and only if t is not a separating element.

Proof: See Lemma IV.1.6 of Stichtenoth [589]. □

Exercise 8.5.15. Let $C = \mathbb{P}^1$ over $\mathbb{F}_p$ with variable x and let $\delta(f) = \partial f/\partial x$. Show that $\delta(x^p) = 0$.

Now we have defined $\partial f/\partial x$ for general $f \in \Bbbk(C)$ we can introduce the differentials on a curve over a field. Our definition is purely formal and the symbol dx is not assumed to have any intrinsic meaning. We essentially follow Section IV.1 of Stichtenoth [589]; for a slightly different approach see Section 8.4 of Fulton [216].

Definition 8.5.16. Let C be a curve over $\Bbbk$. The set of **differentials** $\Omega_{\Bbbk}(C)$ (some authors write $\Omega^1_{\Bbbk}(C)$) is the quotient of the free $\Bbbk(C)$-module on symbols dx for $x \in \Bbbk(C)$ under the relations

1. $dx \neq 0$ if x is a separating element,
2. If x is a separating element and $h_1, h_2 \in \Bbbk(C)$ then $h_1 dx + h_2 dx = (h_1 + h_2)dx$.
3. If x is a separating element and $y \in \Bbbk(C)$ then $dy = (\partial y/\partial x)dx$,

In other words, differentials are equivalence classes of formal symbols

$$\left\{ \sum_{i=1}^{m} h_i dx_i : x_i, h_i \in \Bbbk(C) \right\}$$

where one may assume the x_i are all separating elements.

Lemma 8.5.17. *Let C be a curve over $\Bbbk$ and $x, y \in \Bbbk(C)$ separating elements.*

1. *$dx = 0$ if x is not a separating element.*
2. *$d(x + y) = dx + dy$.*
3. *$d(\lambda x) = \lambda dx$ and $d\lambda = 0$ for all $\lambda \in \Bbbk$.*
4. *$d(xy) = xdy + ydx$.*
5. *If x is a separating element and $y \in \Bbbk(C)$ then $dx + dy = (1 + (\partial y/\partial x))dx$.*

6. *For $n \in \mathbb{Z}$, $d(x^n) = nx^{n-1}dx$.*
7. *$d(x/y) = (ydx - xdy)/y^2$*
8. *If $f \in \Bbbk(C)$ then $d(f(x)) = (\partial f/\partial x)dx$.*
9. *For $i \in \mathbb{Z}$, $d(f(x)y^i) = (\partial f/\partial x)y^i dx + f(x)iy^{i-1}dy$.*
10. *If $F(x,y)$ is a rational function in x and y then $dF(x,y) = (\partial F/\partial x)dx + (\partial F/\partial y)dy$.*

Exercise 8.5.18. Prove Lemma 8.5.17.

Exercise 8.5.19. Let C be a curve over $\Bbbk$. Let $x_1, x_2 \in \Bbbk(C)$ be separating elements and $h_1, h_2 \in \Bbbk(C)$. Show that $h_1 dx_1$ is equivalent to $h_2 dx_2$ if and only if

$$h_2 = h_1 \frac{\partial x_1}{\partial x_2}.$$

Example 8.5.20. We determine $\Omega_{\Bbbk}(\mathbb{P}^1)$. Since $\Bbbk(\mathbb{P}^1) = \Bbbk(x)$ the differentials are $d(f(x)) = (\partial f/\partial x)dx$ for $f(x) \in \Bbbk(x)$. Hence, they are a 1-dimensional vector space over $\Bbbk(C)$.

The following theorem, that all differentials on a curve are multiples of dx where x is a separating element, is a direct consequence of the definition.

Theorem 8.5.21. *Let C be a curve over $\Bbbk$ and let x be a separating element. Let $\omega \in \Omega_{\Bbbk}(C)$. Then $\omega = hdx$ for some $h \in \Bbbk(C)$.*

Exercise 8.5.22. Prove Theorem 8.5.21.

This result shows that $\Omega_{\Bbbk}(C)$ is a $\Bbbk(C)$-vector space of dimension 1 (we know that $\Omega_{\Bbbk}(C) \neq \{0\}$ since $dx \neq 0$ if x is a separating element). Therefore, for any $\omega_1, \omega_2 \in \Omega_{\Bbbk}(C)$ with $\omega_2 \neq 0$ there is a unique function $f \in \Bbbk(C)$ such that $\omega_1 = f\omega_2$. We define ω_1/ω_2 to be f. (See Proposition II.4.3 of Silverman [564]).

We now define the divisor of a differential by using uniformizers. Recall from Lemma 8.5.8 that a uniformizer t_P is a separating element and so $dt_P \neq 0$.

Definition 8.5.23. Let C be a curve over $\Bbbk$. Let $\omega \in \Omega_{\Bbbk}(C)$, $\omega \neq 0$ and let $P \in C(\overline{\Bbbk})$ have uniformizer $t_P \in \overline{\Bbbk}(C)$. Then the **order** of ω at P is $v_P(\omega) := v_P(\omega/dt_P)$. The **divisor of a differential** is

$$\operatorname{div}(\omega) = \sum_{P \in C(\overline{\Bbbk})} v_P(\omega)(P).$$

Lemma 8.5.24. *Let C be a curve over $\Bbbk$ and let ω be a differential on C. Then $v_P(\omega) \neq 0$ for only finitely many $P \in C(\overline{\Bbbk})$ and so $\operatorname{div}(\omega)$ is a divisor.*

Proof: See Proposition II.4.3(e) of Silverman [564]. □

Exercise 8.5.25. Show that $v_P(hdx) = v_P(h) + v_P(dx)$ and $v_P(df) = v_P(\partial f/\partial t_P)$.

Lemma 8.5.26. *The functions $v_P(\omega)$ and $\operatorname{div}(\omega)$ in Definition 8.5.23 are well-defined (both with respect to the choice of representative for ω and choice of t_P).*

Exercise 8.5.27. Prove Lemma 8.5.26.

Lemma 8.5.28. *Let C be a curve over $\Bbbk$ and $\omega, \omega' \in \Omega_{\Bbbk}(C)$. Then*

1. $\deg(\operatorname{div}(\omega)) = \deg(\operatorname{div}(\omega'))$.

2. $\mathrm{div}(\omega)$ *is well-defined up to principal divisors (i.e.,* $\mathrm{div}(\omega) = \mathrm{div}(\omega') + \mathrm{div}(f)$ *for some* $f \in \Bbbk(C)^*$*).*

Exercise 8.5.29. Prove Lemma 8.5.28.

Definition 8.5.30. Any divisor $\mathrm{div}(\omega)$ is called a **canonical divisor**. The set $\{\mathrm{div}(\omega) : \omega \in \Omega_{\Bbbk}(C)\}$ is the **canonical divisor class**.

Example 8.5.31. We determine the canonical class of $C = \mathbb{P}^1$.

Let $\omega = dx$. Since x is a uniformizer at the point 0 we have $v_0(\omega) = v_0(dx/dx) = 0$. More generally, for $P \in \Bbbk$ we have $(x - P)$ a uniformizer and $v_P(\omega) = v_P(dx/d(x-P)) = v_P(1) = 0$. Finally, a uniformizer at ∞ is $t = 1/x$ and $dt = (-x^{-2})dx$ so $v_\infty(\omega) = v_\infty(-x^2) = -2$. Hence $\mathrm{div}(\omega) = -2\infty$ and the degree of $\mathrm{div}(\omega)$ is -2.

Example 8.5.32. We determine the divisor of a differential on an elliptic curve E in Weierstrass form. Rather than computing $\mathrm{div}(dx)$ it is easier to compute $\mathrm{div}(\omega)$ for

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

Let $P \in E(\overline{\Bbbk})$. There are three cases, if $P = \mathcal{O}_E$ then one can take uniformizer $t = x/y$, if $P = (x_P, y_P) = \iota(P)$ then take uniformizer $(y - y_P)$ (and note that $v_P(2y + a_1x + a_3) = 1$ in this case) and otherwise take uniformizer $(x - x_P)$ and note that $v_P(2y + a_1x + a_3) = 0$.

We deal with the general case first. Since $dx/d(x - x_P) = \partial x/\partial(x - x_P) = 1$ it follows that $v_P(\omega) = 0$. For the case, $P = \mathcal{O}_E$ write $x = t^{-2}f$ and $y = t^{-3}h$ for some functions $f, h \in \Bbbk(E)$ regular at $\mathcal{O}_E$ and with $f(\mathcal{O}_E), h(\mathcal{O}_E) \neq 0$. One can verify that

$$\frac{\omega}{dt} = \frac{-2t^{-3}f + t^{-2}f'}{2t^{-3}h + a_1t^{-2}f + a_3} = \frac{-2f + tf'}{2h + a_1tf + a_3t^3}$$

and so $v_{\mathcal{O}_E}(\omega) = 0$. Finally, when $P = \iota(P)$ we must consider

$$\frac{dx}{d(y - y_P)} = \frac{1}{\partial y/\partial x} = \frac{2y + a_1x + a_3}{3x^2 + 2a_2x + a_4}.$$

It follows that $\omega = (1/(3x^2 + 2a_2x + a_4))d(y - y_P)$ and, since P is not a singular point, $3x_P^2 + 2a_2x_P + a_4 \neq 0$ and so $v_P(\omega) = 0$.

In other words, we have shown that $\mathrm{div}(\omega) = 0$. One can verify that

$$\mathrm{div}(dx) = (P_1) + (P_2) + (P_3) - 3(\mathcal{O}_E)$$

where P_1, P_2, P_3 are the three affine points of order 2 in $E(\overline{\Bbbk})$.

Exercise 8.5.33. Show that

$$\frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

on an elliptic curve.

Definition 8.5.34. Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves over $\Bbbk$. Define the function $\phi^* : \Omega_{\Bbbk}(C_2) \to \Omega_{\Bbbk}(C_1)$ by

$$\phi^*(f dx) = \phi^*(f) d(\phi^*(x)).$$

Lemma 8.5.35. *The function* ϕ^* *of Definition 8.5.34 is* $\Bbbk$*-linear and* ϕ^* *is injective (= non-zero) if and only if* ϕ *is separable.*

Proof: The linearity follows since dx is $\Bbbk$-linear. The second part follows since if x is separating for $\Bbbk(C_2)$ and ϕ is separable then $\Bbbk(C_1)/\phi^*\Bbbk(C_2)$ and $\phi^*\Bbbk(C_2)/\Bbbk(\phi^*(x))$ are separable. Hence, $\phi^*(x)$ is a separating element for $\Bbbk(C_1)$ and $d\phi^*(x) \neq 0$. The reverse implication is also straightforward. □

Lemma 8.5.36. *Let $\phi : C_1 \to C_2$ be an unramified morphism of curves over $\Bbbk$ and let $\omega \in \Omega_{\Bbbk}(C_2)$. Then $\phi^*(\mathrm{div}(\omega)) = \mathrm{div}(\phi^*(\omega))$.*

Proof: Let $P \in C_1(\overline{\Bbbk})$ and $Q = \phi(P)$. Let t_Q be a uniformizer at Q. Since ϕ is unramified it follows (Lemma 8.2.9) that $t_P = \phi^*(t_Q)$ is a uniformizer at P. Let $f \in \Bbbk(C_2)$. It suffices to show that $v_P(\phi^*(df)) = v_Q(df)$.

Recall from Exercise 8.5.25 that $v_Q(df) = v_Q(\partial f/\partial t_Q)$, and by Definition 8.5.9 this is equal to $-(\partial F/\partial x)/(\partial F/\partial T)$ evaluated at (t_Q, f), where $F(x, T)$ is a rational function such that $F(t_Q, f) = 0$. Write

$$-(\partial F/\partial x)/(\partial F/\partial T)(t_Q, f) = t_Q^n u$$

for some $n \in \mathbb{Z}$ and $u \in \overline{\Bbbk}(C_2)$ such that $u(Q) \neq 0$.

Now if $F(t_Q(R), f(R)) = 0$ for all $R \in C_2$ then $F(t_Q(\phi(S)), f(\phi(S))) = 0$ for all $S \in C_1$. Hence $F(t_P, \phi^*(f)) = 0$. It follows that

$$\partial\phi^*(f)/\partial t_P = -(\partial F/\partial x)/(\partial F/\partial y)$$

evaluated at the point $(\phi^*(t_Q), \phi^*(f))$, so this is a function on C_1. Write it as $t_P^m v$ for some $v \in \overline{\Bbbk}(C_1)$ such that $v(P) \neq 0$. Since $t_P = \phi^*(t_Q)$ it follows that $m = n$ and $v = \phi^*(u)$. Hence, $v_P(\partial\phi^*(f)/\partial t_P) = v_Q(\partial f/\partial t_Q)$ and so $v_P(d\phi^*(f)) = v_Q(df)$. □

Corollary 8.5.37. *Let $\phi : C_1 \to C_2$ be an isomorphism of curves over $\Bbbk$ and let $\omega \in \Omega_{\Bbbk}(C_2)$. Then* $\deg(\mathrm{div}(\omega)) = \deg(\mathrm{div}(\phi^*(\omega)))$.

8.6 Genus Zero Curves

Theorem 8.6.1. *Let C be a curve over $\Bbbk$ (i.e., projective non-singular). The following are equivalent.*

1. *C is birationally equivalent over $\Bbbk$ to $\mathbb{P}^1$.*
2. *The divisor class group of C over $\Bbbk$ is trivial and $\#C(\Bbbk) \geq 2$.*
3. *There is a point $P \in C(\Bbbk)$ with $\ell_{\Bbbk}(P) \geq 2$.*

Proof: (1 ⇒ 2): Let C be birational to $\mathbb{P}^1$ over $\Bbbk$. By Lemma 7.3.6 there is a morphism from $\mathbb{P}^1$ to C and by Lemma 8.2.7 it is surjective. Since $\#\mathbb{P}^1(\Bbbk) \geq 2$ it follows that $\#C(\Bbbk) \geq 2$. Also, since the divisor class group of $\mathbb{P}^1$ is trivial it follows from Exercise 8.3.11 that $\mathrm{Pic}^0_{\Bbbk}(C) = \{0\}$.

(2 ⇒ 3): Let $P, Q \in C(\Bbbk)$ be distinct. Since $(Q) - (P)$ is principal there exists a function h with $\mathrm{div}(h) = (Q) - (P)$ and so $\ell_{\Bbbk}(P)$ is spanned by at least $\{1, h\}$ (which is a linearly independent set).

(3 ⇒ 1): Let $P_0 \in C(\Bbbk)$ be such that $\ell_{\Bbbk}(P_0) \geq 2$. Then there is some function $h \in \Bbbk(C)$ and a point $P \in C(\Bbbk)$ such that $\mathrm{div}(h) = (P) - (P_0)$. For any $R \in C(\Bbbk)$, $R \neq P_0$, the function $h - h(R)$ has a simple pole at P_0 and a simple zero at R. One can therefore deduce that h gives an injective rational map $h : C \to \mathbb{P}^1$. Unfortunately, it is not trivial to write down the inverse rational map $h' : \mathbb{P}^1 \to C$, so to complete the proof we show that $\Bbbk(C) \cong \Bbbk(\mathbb{P}^1)$.

Let f be any function on C. Then $g = fh^{v_{P_0}(f)}$ has no zero or pole at P_0. Write

$$g' = \prod_{R \in C(\Bbbk)} (h - h(R))^{v_R(g)}.$$

Then $v_R(g) = v_R(g')$ and so $\mathrm{div}(g') = \mathrm{div}(g)$ and $g' = cg$ for some $c \in \Bbbk^*$. In other words, f is a rational function of h, and so $f \in \Bbbk(h)$. Since f was arbitrary, $\Bbbk(C) = \Bbbk(h)$ and so, by Theorem 5.5.28, C is birational to $\mathbb{P}^1$. □

Definition 8.6.2. A curve satisfying any of the above equivalent conditions is called a **genus 0 curve**.

Exercise 8.6.3. Write down a curve C over a field $\Bbbk$ such that the divisor class group $\mathrm{Pic}^0_\Bbbk(C)$ is trivial but C is not birationally equivalent over $\Bbbk$ to $\mathbb{P}^1$.

Theorem 8.6.4. *An elliptic curve does not have genus 0.*

Proof: We have seen in Examples 8.5.31 and 8.5.32 that the canonical divisor classes on $\mathbb{P}^1$ and an elliptic curve have different degree. It follows that $\mathbb{P}^1$ is not isomorphic to an elliptic curve. And since a birational map of smooth projective curves is an isomorphism (Lemma 8.1.13 and Lemma 8.1.15) the result follows from Corollary 8.5.37.

There are a number of other proofs of this result: For example, Lemma 11.3 of Washington [626] gives an elementary one; it also follows from the general theorem that a non-singular plane curve of degree d has genus $d(d-1)/2$ or from the Hurwitz genus formula (see below). □

Corollary 8.6.5. *Let E be an elliptic curve and $P_1, P_2 \in E(\Bbbk)$. If $P_1 \neq P_2$ then $(P_1) - (P_2)$ is not a principal divisor.*

8.7 Riemann-Roch Theorem and Hurwitz Genus Formula

In this section we state, without proof, two very important results in algebraic geometry. Neither will play a crucial role in this book.

Lemma 8.7.1. *Let C be a curve over $\Bbbk$ of genus g and let $\omega \in \Omega_\Bbbk(C)$. Then*

1. $\deg(\mathrm{div}(\omega)) = 2g - 2$.
2. $\ell_\Bbbk(\mathrm{div}(\omega)) = g$.

Proof: See Corollary I.5.16 of Stichtenoth [589] or Corollary 11.16 of Washington [626]. For non-singular plane curves see Sections 8.5 and 8.6 of Fulton [216]. □

Theorem 8.7.2. *(Riemann-Roch) Let C be a non-singular projective curve over $\Bbbk$ of genus g, $\omega \in \Omega_\Bbbk(C)$ a differential and D a divisor. Then*

$$\ell_\Bbbk(D) = \deg(D) + 1 - g + \ell_\Bbbk(\mathrm{div}(\omega) - D).$$

Proof: There are several proofs. Section 8.6 of Fulton [216] gives the Brill-Noether proof for non-singular plane curves. Theorem I.5.15 of Stichtenoth [589] and Theorem 2.5 of Moreno [439] give proofs using repartitions. □

Some standard applications of the Riemann-Roch theorem are to prove that every genus 1 curve with a rational point is birational to an elliptic curve in Weierstrass form, and to prove that every hyperelliptic curve of genus g is birational to an affine curve of the form $y^2 + H(x)y = F(x)$ with $\deg(H(x)) \leq g + 1$ and $\deg(F(x)) \leq 2g + 2$.

Theorem 8.7.3. *(Hurwitz genus formula) Let $\phi : C_1 \to C_2$ be a rational map of curves over $\Bbbk$. Let g_i be the genus of C_i. Suppose that $\Bbbk$ is a field of characteristic zero or characteristic coprime to all $e_\phi(P)$. Then*

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

Proof: See Theorem III.4.12 and Corollary III.5.6 of Stichtenoth [589], Theorem II.5.9 of Silverman [564] or Exercise 8.36 of Fulton [216]. □

A variant of the above formula is known in the case where some of the $e_\phi(P)$ are divisible by $\mathrm{char}(\Bbbk)$.