Chapter 8 THE RIEMANN-ROCH THEOREM FOR CURVES

curves version 53

We study smooth projective curves in this chapter. Smooth affine curves were discussed in Chapter 5, and a curve is smooth if it has an open covering by smooth affine curves. Our main goal is to prove the Riemann-Roch Theorem, which describes the dimension of the space of rational functions with prescribed poles on a smooth projective curve. Some other facts will be derived from the theorem, among them:

- With its classical topology, a smooth projective curve is a connected manifold.
- The topological genus and the arithmetic genus of a smooth projective curve are equal: $g = p_a$.

8.1 Modules on a Curve

curvemodules

Finite modules on a smooth curve have a relatively simple structure, and we make a start at describing their structure here. Recall that a *torsion element* of a module M over a domain A is an element m such that $am = 0$ for some nonzero element a of A, and that a module is *torsion-free* if its only torsion element is 0. These definitions are extended to $\mathcal{O}$-modules by the standard procedure.

tfreelfree **8.1.1. Proposition.** *A torsion-free $\mathcal{O}$-module $\mathcal{M}$ on a smooth curve Y is locally free: There is an open covering $\{Y^i\}$ of Y such that, for every i, the restriction of $\mathcal{M}$ to Y^i is a free module.*

proof. A discrete valuation ring R is a principal ideal domain. Every finite R-module is a direct sum of its torsion submodule module and a free module, and every finite, torsion-free R module is free. If Y is a smooth curve, its localization at a point p will be a discrete valuation ring. So the localization at p of a torsion-free $\mathcal{O}$-module $\mathcal{M}$ will be free. It follows from the general principle (5.2.4) that $\mathcal{M}$ will be free in a neighborhood of p. We'll verify the principle in this case. We replace Y by an affine open neighborhood of p, say $Y = \operatorname{Spec} A$. Let $M = \mathcal{M}(Y)$, and let S be the complement of the maximal ideal $\mathfrak{m}$ of A at p, so that $R = AS^{-1}$. The localization MS^{-1} of M will be a free module; let $(x_1, ..., x_n)$ be a basis. Then $x_i = s_i^{-1} m_i$, where s_i is an element of A not in the maximal ideal $\mathfrak{m}$ of p and m_i is in M. The set $(m_1, ..., m_n)$ is also a basis for MS^{-1}. We inspect the homomorphism $A^r \xrightarrow{\varphi} M$ that sends $(a_1, ..., a_n)$ to $\sum a_i m_i$. The kernel K and the cokernel C of φ are finite A-modules. Since $(m_1, ..., m_n)$ is a basis for MS^{-1}, the localized map $R^r \xrightarrow{\varphi'} MS^{-1}$ is an isomorphism. Then, since localization is an exact operation (5.2.6), the localizations KS^{-1} and CS^{-1} are zero. Let $v_1, ..., v_n$ be generators for the finite module K. An element $v \in K$ maps to zero in KS^{-1} if it is annihilated by an element $s \in S$. So there is an element $s_i \in S$ such that $s_i v_i = 0$, and by taking a common multiple, we may choose an element $s \in S$ such that $sv_i = 0$ for all i. Then the simple localization K_s will be zero. Similarly, there is an element $s \in S$ such that $C_s = 0$, and we may choose an element s so that both K_s and C_s are zero. Then the module M_s will be free. □

Later in the chapter, we will need to know about the module of homomorphisms from one $\mathcal{O}$-module to another.

Let M and N be modules over a ring A. The set of A-module homomorphisms $M \to N$, which is denoted by

$$\mathrm{Hom}_A(M, N)$$

becomes an A-module with some fairly obvious laws of composition: If f and g are homomorphisms and a is an element of A, then $f+g$ and af are defined by

$$[f+g](m) = f(m) + g(m) \quad \text{and} \quad [af](m) = a[f(m)] \quad \big(= f(am)\big)$$

homfinite **8.1.2. Lemma.**
(i) Hom_A *is a left exact, contravariant functor of the first variable. An exact sequence* $M_1 \to M_2 \to M_3 \to 0$ *of A-modules produces an exact sequence*

$$0 \to \mathrm{Hom}_A(M_3, N)\, \mathrm{Hom}_A(M_2, N) \to \mathrm{Hom}_A(M_1, N)$$

(ii) Hom_A *is a left exact covariant functor in the second variable. An exact sequence* $0 \to N_1 \to N_1 \to N_3$ *of A-modules produces an exact squence*

$$0 \to \mathrm{Hom}_A(M, N_1) \to \mathrm{Hom}_A(M, N_2) \to \mathrm{Hom}_A(M, N_3)$$

proof. **(i)** The map $\mathrm{Hom}_A(M_1, N) \leftarrow \mathrm{Hom}_A(M_2, N)$ is defined to be composition with the map $M_1 \to M_2$. We verify exactness at $\mathrm{Hom}_A(M_2, N)$. A homomorphism $M_2 \xrightarrow{f} N$ such that the composition $M_3 \to M_2 \to N$ is zero induces a map $\overline{f}$ as in the diagram below

$$\begin{array}{ccccccc} M_1 & \longrightarrow & M_2 & \longrightarrow & M_3 & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \overline{f}} & & . \\ 0 & \longrightarrow & N & = & N & \longrightarrow & 0 \end{array}$$

We omit the proof of **(ii)**. □

homfinitetwo **8.1.3. Lemma.** *Let A be a noetherian ring.*
(i) *For any finite A-module M, there is an exact sequence* $A^\ell \to A^k \to M \to 0$.
(ii) *If M and N are finite A-modules, then* $\mathrm{Hom}_A(M, N)$ *is a finite A-module.*

proof. **(i)** A set $m_1, ..., m_k$ that generates the finite module M will define a surjective map $A^k \to M$. Since A is noetherian, the kernel N of this map will be a finite A-module. A set $n_1, ..., n_\ell$ that generates N will define a surjective map $A^\ell \to N$. Then the sequence $A^\ell \to A^k \to M \to 0$ will be exact.

(ii) We choose a surjection $A^k \xrightarrow{\pi} M$. Lemma 8.1.2 **(i)** tells us that the induced map $\mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(A^k, N)$ is injective. We note that $\mathrm{Hom}_A(A^k, N) \approx \mathrm{Hom}_A(A, N)^k \approx N^k$. So $\mathrm{Hom}_A(M, N)$ is isomorphic to a submodule of the finite module N^k. Since A is noetherian, $\mathrm{Hom}_A(M, N)$ is a finite module. □

The $\mathcal{O}$-module $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M}, \mathcal{N})$ of homomorphisms of $\mathcal{O}$-modules on a variety Y is defined using the standard procedure: If $Y' = \operatorname{Spec} A$ is an affine open subset of Y, and if $\mathcal{M}(Y') = M$ and $\mathcal{N}(Y') = N$, then the module of sections of $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M}, \mathcal{N})$ on Y' is $\mathrm{Hom}_A(M, N)$.

HomON **8.1.4. Lemma.** **(i)** *For any $\mathcal{O}$-module $\mathcal{N}$,* $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{O}, \mathcal{N}) \approx \mathcal{N}$.
(ii) *In particular, a homomorphism $\mathcal{O} \to \mathcal{N}$ is defined by a global section of $\mathcal{N}$.*

proof. This follows from the fact that $\mathrm{Hom}_A(A, N) \approx N$, but let's spell it out: A section n of $\mathcal{N}$ on an open set U defines a homomorphism $\mathcal{O}|_U \xrightarrow{\varphi} \mathcal{N}|_U$ of restrictions to U in this way: Let V be an open set that is contained in U. Then φ must give us a homomorphism of $\mathcal{O}(V)$-modules $\mathcal{O}(V) \to \mathcal{N}(V)$. Let's denote this homomorphism, yet to be defined, by φ'. We restrict n to the open set V, obtaining an element of $\mathcal{N}(V)$. We usually denote this element by n too, but let's denote it by n' here. The definition of φ' is that, if f is a regular function on V, then $\varphi'(f) = fn'$. □

homloc **8.1.5. Proposition.** *If $\mathcal{M}$ and $\mathcal{N}$ are finite $\mathcal{O}$-modules on a variety Y, $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M},\mathcal{N})$ is also a finite $\mathcal{O}$-module.*

proof. The fact that $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M},\mathcal{N})$ is a finite module is Lemma 8.1.3 and Proposition 6.3.10. We verify the sheaf and coherence properties.

For the coherence property, we must show that if s is a nonzero element of a noetherian domain A, there is a canonical isomorphism

$$(\mathrm{Hom}_A(M,N))_s \xrightarrow{\epsilon} \mathrm{Hom}_{A_s}(M_s,N_s)$$

The fact that localization is a functor gives us a module homomorphism $\mathrm{Hom}_A(M,N) \to \mathrm{Hom}_{A_s}(M_s,N_s)$. Since s is invertible in $\mathrm{Hom}_{A_s}(M_s,N_s)$, this homomorphism defines the map ϵ. To show that ϵ is an isomorphism, we choose a presentation $A^\ell \to A^k \to M \to 0$ as in (8.1.2) **(i)**. Since $\mathrm{Hom}_A(A^k,N) \approx N^k$, it is true that the map $\mathrm{Hom}_A(A^k,N)_s \overset{\to}{\mathrm{Hom}}_{A_s}(A^k_s,N_s)$ is an isomorphism. Then the fact that ϵ is an isomorphism follows from Lemma 8.1.2 **(i)**.

We omit the proof of the sheaf property. It uses (8.1.3) **(i)** to reduce the problem to the case that $\mathcal{M} = \mathcal{O}$, for which it becomes the sheaf property of $\mathcal{N}$. □

dualmodule **(8.1.6) the dual module**

The *rank* of a locally free module $\mathcal{M}$ is the rank of its free localizations.

Because $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{O},\mathcal{N}) \approx \mathcal{N}$, $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{O}^n,\mathcal{O}^m)$ is the free $\mathcal{O}$-module $\mathcal{O}^{m\times n}$ of $m\times n$ matrices. Consequently, if $\mathcal{M}$ and $\mathcal{N}$ are locally free, then $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M},\mathcal{N})$ will also be locally free, and if $\mathcal{M}$ and $\mathcal{N}$ have ranks m and n, respectively, the rank of $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M},\mathcal{N})$ will be mn.

The *dual module* $\mathcal{M}^*$ of a locally free $\mathcal{O}$-module $\mathcal{M}$ is the locally free module $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M},\mathcal{O})$. The duality between $\mathcal{M}$ and $\mathcal{M}^*$ can be expressed as the $\mathcal{O}$-bilinear form

$$\mathcal{M}^* \times \mathcal{M} \to \mathcal{O}$$

defined by $\langle\varphi,m\rangle = \varphi(m)$, or by the $\mathcal{O}$-module homomorphism

$$\mathcal{M}^* \otimes_{\mathcal{O}} \mathcal{M} \to \mathcal{O}$$

that sends $\varphi\otimes m$ to $\varphi(m)$. The symmetry of these expressions shows that a locally free $\mathcal{O}$-module $\mathcal{M}$ is canonically isomorphic to its double dual $\mathcal{M}^{**}$.

We will often work with $\mathcal{O}$-modules that are locally free, of rank one. They are often called *invertible* modules, one reason being that the phrase "locally free, rank one" is lengthy. So an invertible $\mathcal{O}$-module $\mathcal{L}$ will be isomorphic to the $\mathcal{O}$-module $\mathcal{O}$ in a neighborhood of any point. The term "invertible" is justified by the fact that if $\mathcal{L}$ is invertible, the map $\mathcal{L}^*\otimes_{\mathcal{O}}\mathcal{L} \to \mathcal{O}$ will be an isomorphism.

Suppose given a nonzero global section s of an invertible module $\mathcal{L}$ on a smooth curve Y. The homomorphism $\mathcal{O} \xrightarrow{s} \mathcal{L}$ will be injective because $\mathcal{L}$ will be torsion-free, and its cokernel C will be supported on a finite set of points of Y. One says that a section s on an open set U is *zero* at a point p of U if p is in the support of C. This is justified by the fact that when we look locally, where $\mathcal{L}$ is isomorphic to $\mathcal{O}$, the section corresponds to a regular function f on U, and the zeros of s correspond to the zeros of f. Wherever a section s of $\mathcal{L}$ isn't zero, the map $\mathcal{O} \xrightarrow{s} \mathcal{L}$ will be bijective. A bijective map $\mathcal{O}\to\mathcal{L}$ to an invertible module $\mathcal{L}$ is given by a global section s of $\mathcal{L}$ that is nowhere zero.

8.2 Divisors

divisors

The next proposition describes the ideals in the structure sheaf of a of a smooth curve Y in terms of finite subsets with multiplicities. This extends the description of closed subsets of $\mathbb{P}^1$ given in (**??**).

idealincurve **8.2.1. Proposition.** *Let $\mathcal{I}$ be a nonzero ideal in the structure sheaf $\mathcal{O}$ of a smooth curve Y. There are points $p_1,...,p_k$ of Y and integers $r_1,...,r_k$ such that $\mathcal{I}$ is the product $\mathfrak{m}_1^{r_1}\cdots\mathfrak{m}_k^{r_k}$ of the maximal ideals $\mathfrak{m}_i$ at p_i.*

proof. Because Y has dimension one, the support of the quotient algebra $\mathcal{O}/\mathcal{I}$ is a finite set $\{p_1, ..., p_k\}$ of points of Y. To show that $\mathcal{I} = \mathfrak{m}_1^{r_1} \cdots \mathfrak{m}_k^{r_k}$, it is enough to show that there is an open covering on which those ideals are equal. Therefore it suffices to prove the assertion for an affine open set $Y' = \operatorname{Spec} A$ that contains just one of the points $p = p_i$, with maximal ideal $\mathfrak{m}$. Then it follows from Proposition 5.4.5. □

A *divisor* on a smooth curve Y is a finite integer combination of points: $r_1p_1 + \cdots + r_kp_k$, with $r_i \in \mathbb{Z}$ and $p_i \in Y$. A divisor will often be denoted by a capital letter such as D. The *degree* of $D = \sum r_ip_i$ is the sum $\sum r_i$. It will be denoted by $\deg D$.

A divisor $D = \sum r_ip_i$ is *effective* if $r_i \geq 0$ for all i, and D is *effective on an open subset* V if $r_i \geq 0$ for all p_i that are points of V.

The local rings of Y are discrete valuation rings, and we denote the valuation that corresponds to a point q by v_q, as before. Recall that a nonzero rational function f is zero at q if $\mathrm{v}_q(f) > 0$, and that it has a pole at q if $\mathrm{v}_q(f) < 0$. The *divisor* of a rational function f is

$$\operatorname{div}(f) = \sum_q \mathrm{v}_q(f)\, q$$

This divisor is written as a sum over all points of Y, but because f has finitely many zeros and poles of f, the coefficient $\mathrm{v}_q(f)$ will be zero at all other points. So the divisor is actually a finite sum. Speaking loosely, $\operatorname{div}(f) = \{\text{zeros of } f\} - \{\text{poles of } f\}$. The divisor of a function is called a *principal divisor*.

Let D and E be two divisors. By allowing zero coefficients, we can suppose they are combinations of the same finite set $p_1, ..., p_k$ of points, say $D = \sum r_ip_i$ and $E = \sum s_ip_i$. These divisors are *linearly equivalent* if their difference $D - E = \sum (r_i - s_i)p_i$ is a principal divisor.

OofD **(8.2.2) the modules $\mathcal{O}(D)$**

The invertible $\mathcal{O}$-module $\mathcal{O}(D)$ associated to a divisor D on a smooth curve Y, is the module whose sections are the rational functions whose poles are bounded by D. More precisely, the sections of $\mathcal{O}(D)$ on an open subset V of Y consist of zero and of the rational functions f such that the the divisor $\operatorname{div}(f) + D$ is effective on V. The points of Y that are not in V impose no conditions on the sections of $\mathcal{O}(D)$ on V.

Say that $D = \sum r_ip_i$ and that p_i is a point of an open set V. If $r_i > 0$, the sections of $\mathcal{O}(D)$ on V have poles of order at most r_i at p_i and if $r_i < 0$, they have zeros of order at least $-r_i$ at p_i.

For example, suppose that $D = p$. If an open set V contains p, the nonzero sections of $\mathcal{O}(p)$ on V are the rational functions with a pole of order at most 1 at p, that are regular at every other point of V, and that can have arbitrary zeros or poles at points not in V. If V does't contain p, the sections of $\mathcal{O}(p)$ on V are the regular functions on V.

The module $\mathcal{O}(-p)$ is the maximal ideal at p. If an open set V contains p, the sections of $\mathcal{O}(-p)$ on V are the regular functions on V that vanish at p, and if p doesn't contain V, the sections of $\mathcal{O}(-p)$ on V are the regular functions on V.

The fact that a section of $\mathcal{O}(D)$ is allowed to have a pole at p_i if $r_i > 0$ contrasts with the divisor of a function. If $\operatorname{div}(f) = \sum a_ip_i$, then $a_i > 0$ means that f has a zero at p_i. Thus, if $D = \operatorname{div}(f)$, f will be a global section of $\mathcal{O}(-D)$.

Let D and E be divisors. It is obvious that $\mathcal{O}(D)$ is a subset of $\mathcal{O}(E)$ if and only if $E - D$ is effective. However, when regarded simply as $\mathcal{O}$-modules, there may be other homomorphisms between them. Thus multiplication by a global section f of $\mathcal{O}(D)$ defines a homomorphism $\mathcal{O} \xrightarrow{f} \mathcal{O}(D)$. The analogous statement is true for global sections of any $\mathcal{O}$-module. Conversely, any homomorphism $\mathcal{O} \xrightarrow{\varphi} \mathcal{O}(D)$ is multiplication by the global section $f = \varphi(1)$. For instance, regular functions f on Y correspond bijectively to module homomorphisms $\mathcal{O} \xrightarrow{f} \mathcal{O}$.

Various facts about these modules $\mathcal{O}(D)$ are collected below. The proofs are all easy.

OtoOD **8.2.3. Proposition. (i)** *For any divisor D, $\mathcal{O}(D)$ is an invertible $\mathcal{O}$-module.*

(ii) *If D and E are divisors, $\mathcal{O}(D+E)$ is canonically isomorphic to $\mathcal{O}(D) \otimes_{\mathcal{O}} \mathcal{O}(E)$.*

(iii) *Let f be a rational function and let $D = \operatorname{div}(f)$ be its divisor. Multiplication by f defines an isomorphism $\mathcal{O}(D) \xrightarrow{f} \mathcal{O}$.*

(iv) *If D and E are divisors, the modules $\mathcal{O}(D)$ and $\mathcal{O}(E)$ are isomorphic if and only if D and E are linearly equivalent. If $D - E = \operatorname{div}(f)$, multiplication by f defines an isomorphism $\mathcal{O}(D) \xrightarrow{f} \mathcal{O}(E)$.*

(v) *Suppose that Y is a closed subvariety of projective space $X = \mathbb{P}^n$. The module $\mathcal{O}_Y(k) = \mathcal{O}_X(k) \otimes_{\mathcal{O}_X} \mathcal{O}_Y$ is invertible, and it has the form $\mathcal{O}_Y(kH)$, where H is the locus $\{x_0 = 0\}$ in Y, viewed as a divisor.*

(vi) *Every nonzero ideal of $\mathcal{O}$ is isomorphic to $\mathcal{O}(-D)$ for some divisor $D \geq 0$.*

(vii) *Every invertible $\mathcal{O}$-module $\mathcal{L}$ is isomorphic to a module of the form $\mathcal{O}(D)$.*

We verify **(vi)** and **(vii)**, and omit the other proofs.

(vi) Proposition 8.2.1 **(ii)** tells us that $\mathcal{I} = \mathfrak{m}_1^{r_1} \cdots \mathfrak{m}_k^{r_k}$ for some points $p_1, ..., p_k$. Then if $D = \sum r_i p_i$, sections of $\mathcal{I}$ on U are regular functions that have zeros of orders at least r_i at the points p_i that are in U. This is also the module of sections of $\mathcal{O}(-D)$ on U.

(vii) Since $\mathcal{L}$ is invertible, so is its dual module $\mathcal{L}^*$, and $\mathcal{O}^* \approx \mathcal{O}$. For large k, the module $\mathcal{L}^*(k)$ will have a global section, which will define a map $\mathcal{O} \to \mathcal{L}^*(k)$. Its dual is a map $\mathcal{L}(-k) \to \mathcal{O}$ that represents $\mathcal{L}(-k)$ as an ideal. By **(v)**, $\mathcal{L}(-k) = \mathcal{O}(-D)$ for some effective divisor D. Then with H is as in **(vii)**, $\mathcal{L} = \mathcal{O}(-D - kH)$. □

8.3 Cohomology

cohcurve Let Y be a smooth projective curve. A we saw in Chapter 7, the cohomology $H^q(Y, \mathcal{M})$ of an $\mathcal{O}$-module $\mathcal{M}$ is zero when $q > 1$ and if $\mathcal{M}$ is a finite module, then $H^0(Y, \mathcal{M})$ and $H^1(Y, \mathcal{M})$ are finite dimensional vector spaces. The *Euler characteristic* of a finite $\mathcal{O}$-module $\mathcal{M}$ is

chicurve (8.3.1) $$\chi(\mathcal{M}) = \dim H^0(Y, \mathcal{M}) - \dim H^1(Y, \mathcal{M}).$$

In particular,

$$\chi(\mathcal{O}_Y) \;=\; \dim H^0(Y, \mathcal{O}_Y) - \dim H^1(Y, \mathcal{O}_Y)$$

We will see below that $H^0(Y, \mathcal{O}_Y) = \mathbb{C}$, and by definition, $\dim H^1(Y, \mathcal{O}_Y) = p_a$ is the *arithmetic genus* of Y. Thus

$$\chi(\mathcal{O}_Y) \;=\; 1 - p_a$$

To determine the effect on the cohomology of an $\mathcal{O}$-module $\mathcal{O}(D)$ when we allow one more zero or pole, we consider the inclusion map $\mathcal{O}(D-p) \xrightarrow{\varphi} \mathcal{O}(D)$ and form a short exact sequence

$$0 \to \mathcal{O}(D-p) \to \mathcal{O}(D) \to \epsilon \to 0$$

where ϵ is the cokernel of φ. Recall that $\mathcal{O}(-p) = \mathfrak{m}_p$. So this sequence above can be obtained from the sequence

$$0 \to \mathcal{O}(-p) \to \mathcal{O} \to \kappa_p \to 0$$

by tensoring with $\mathcal{O}(D)$. Since $\mathcal{O}(D)$ is locally isomorphic to $\mathcal{O}$, $\epsilon = \kappa_p \otimes_{\mathcal{O}} \mathcal{O}(D)$ is a one-dimensional vector space supported on the point p. Therefore $H^0(X, \epsilon)$ has dimension 1 and $H^1(X, \epsilon) = 0$.

Let's abbreviate by writing [1] for the one-dimensional space $H^0(Y, \epsilon)$. The cohomology sequence of the sequence above becomes

addpoint (8.3.2) $$0 \to H^0(Y, \mathcal{O}(D-p)) \to H^0(Y, \mathcal{O}(D)) \to [1] \to H^1(Y, \mathcal{O}(D-p)) \to H^1(Y, \mathcal{O}(D)) \to 0$$

Consequently, when we change a divisor by adding a point, one of two things happens: Either the dimension of H^0 increases by 1, or the dimension of H^1 decreases by 1. In either case,

chichange (8.3.3) $$\chi(\mathcal{O}(D)) = \chi(\mathcal{O}(D-p)) + 1.$$

Moreover, when we add an infinite sequence of points in succession, then because H^1 is finite-dimensional, its dimension can decrease only finitely often. Therefore H^0 will tend to infinity.

RRcurve **8.3.4. Riemann-Roch Theorem (version 1).** *Let $D = \sum r_i p_i$ be a divisor on a smooth projective curve Y. Then*

$$\chi(\mathcal{O}(D)) \quad = \quad \chi(\mathcal{O}) + \deg\, D$$

The theorem follows from (8.3.3), because we can get from $\mathcal{O}$ to $\mathcal{O}(D)$ by a finite number of operations, each of which changes the divisor by adding or subtracting a point. □

The full Riemann-Roch Theorem is more precise than this version. It describes the Euler characteristic of a locally free $\mathcal{O}$-module $\mathcal{M}$, and it identifies the cohomology $H^1(Y, \mathcal{M})$ as the dual space to the space of global sections of another locally free $\mathcal{O}$-module $\mathcal{M}^D$, the *Serre dual* of $\mathcal{M}$ (see Section 8.7 below). However, the weaker version 1 has important consequences.

RRcor **8.3.5. Corollary.** *Let Y be a smooth projective curve.*

(i) *The divisor* $\operatorname{div}(f)$ *of a nonzero rational function f has degree zero: The number of zeros of f is equal to the number of its poles. Therefore linearly equivalent divisors have equal degrees.*

(ii) *A nonconstant rational function f on Y takes every value, including infinity, the same number of times.*

(iii *A rational function that is regular at every point of Y is a constant: $H^0(Y, \mathcal{O}) = \mathbb{C}$.*

(iv) *If D is a divisor on Y, then* $\dim H^0(Y, \mathcal{O}(D)) \geq \deg\, D + 1 - p_a$.

(v) *If* $\deg\, D \geq p_a$, *then* $H^0(Y, \mathcal{O}(D)) \neq 0$.

(vi) *If* $\deg\, D < 0$, *then* $H^0(Y, \mathcal{O}(D)) = 0$.

proof. **(i)** Let $D = \operatorname{div}(f)$. Multiplication by f defines an isomorphism $\mathcal{O}(D) \to \mathcal{O}$ (8.2.3), so $\chi(\mathcal{O}(D)) = \chi(\mathcal{O})$. On the other hand, by Riemann-Roch, $\chi(\mathcal{O}(D)) = \chi(\mathcal{O}) + \deg\, D$. Therefore $\deg\, D = 0$.

(ii) For any complex number c, the functions f and $f - c$ have the same poles. Therefore the number of zeros of $f - c$, which is the number of points at which f takes the value c, is equal to the number of poles of f.

(iii) According to **(ii)**, a nonconstant function must have a pole.

(iv),(v) follow directly from **(iii)** and the Riemann-Roch formula.

(v) This follows from **(ii)** because, when $\deg\, D < 0$, a global section of $\mathcal{O}(D)$ would have more zeros than poles. □

Corollary 8.3.5 **(iii)** and Proposition 8.2.3 **(iii)** allow us to define the *degree* $\deg \mathcal{L}$ of an invertible $\mathcal{O}$-module $\mathcal{L}$. It is the degree of a divisor D such that $\mathcal{L} \approx \mathcal{O}(D)$. With this definition of degree, Riemann-Roch for $\mathcal{L}$ becomes

RRL (8.3.6)
$$\chi(\mathcal{L}) = \chi(\mathcal{O}) + \deg\, \mathcal{L}$$

curveconn **8.3.7. Theorem.** *With its classical topology, a smooth projective curve Y is connected.*

The proof that Y is a compact orientable manifold can be adapted from the case of plane curves (see **??**).

proof. This is a proof by contradiction. Suppose that the curve is the union of disjoint closed subsets: $Y = Y_1 \cup Y_2$. Both Y_1 and Y_2 will be compact manifolds. We choose a point p of Y_1. Riemann-Roch shows that $H^0(Y, \mathcal{O}(np))$ isn't zero, if n is sufficiently large. So there will be a nonconstant rational function f that is regular on the complement of p. Then f will have no pole on Y_2. It will be a bounded analytic function on that compact space. The maximum principle for analytic functions shows that f will be constant on Y_2. We may subtract this constant, to construct a nonzero rational function that is identically zero on Y_2. Similarly, there is a nonzero rational function g that is identically zero on Y_1. Then $fg = 0$. This is impossible because the rational functions form a field. □

8.4 Curves as Coverings of $\mathbb{P}^1$, again

covercurve We will want to view a smooth projective curve Y as a covering of the projective line $X = \mathbb{P}^1$, as we did with plane curves in the first chapter. If Y is a closed subvariety of $\mathbb{P}^n$, we can construct a morphism $Y \xrightarrow{\pi} X$

by restriction from the projection $\mathbb{P}^n \to \mathbb{P}^1$ that sends $(x_0, ..., x_n)$ to (x_0, x_1). The center of projection, the locus where the projection isn't defined, is the linear subspace L of points $(0, 0, x_2, ..., x_n)$. It is defined by two equations $x_0 = x_1 = 0$. Provided that coordinates are in general position, Y will meet the hyperplane $\{x_0 = 0\}$ in a finite number of points, none of which are in the locus $\{x_1 = 0\}$. Then $Y \cap L$ will be empty, and π will be a finite morphism (Chevalley Finiteness Theorem 4.5.2). It will present Yas a branched covering of X. The direct image $\pi_*\mathcal{O}_Y$ will be a finite torsion-free, and therefore locally free, $\mathcal{O}_X$-module. Its rank as $\mathcal{O}_X$-module is the *degree* of the covering. Let's denote the degree by n.

The inverse image $\pi^{-1}X'$ of an affine open subset $X' = \operatorname{Spec} A'$ of X will be a smooth affine curve $Y' = \operatorname{Spec} B'$, and B' will be a finite, locally free A'-algebra whose rank is the degree n of Y over X. Proposition 8.4.2 below shows that, if one localizes suitably, one can generate B' as A'-algebra by a single element.

We appologize that what follows is rather technical.

We arrange coordinates so that p is the origin $x = 0$ in the affine line $\mathbb{U}^0 = \operatorname{Spec} A$, with $A = \mathbb{C}[x]$. We relabel $\mathbb{U}^0$ as X, and its inverse image by Y. Then Y will be an affine variety $\operatorname{Spec} B$, where B is a finite A-algebra. Let p be a point of X, let $q_1, ..., q_k$ be the points of Y over p, and let v_i be the valuation associated to q_i. The integer $\mathrm{v}_i(x) = e_i$ is the *ramification index* of the covering Y of X at q_i. The maximal ideals of B that contain x are the maximal ideals $\mathfrak{m}_i$ at q_i, and the ideal xB is the product $\mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k}$. This follows from Proposition **??**.

Let $\overline{B}$ denote quotient algebra B/xB. Since $xB = \mathfrak{m}_1^{e_1} \cdots \mathfrak{m}_k^{e_k}$ and since the powers $\mathfrak{m}_i^{e_i}$ are comaximal, the Chinese Remainder Theorem tells us that $\overline{B}$ is the direct sum $\overline{B}_1 \oplus \cdots \oplus \overline{B}_k$, where $\overline{B}_i = B/\mathfrak{m}_i^{e_i}$. Moreover, $\overline{B}_i$ is a truncated polynomial ring $\mathbb{C}[t_i]/(t_i^{e_i})$ (Proposition 5.4.5 **(iii)**).

sumei **8.4.1. Corollary.** *The sum* $\sum e_i$ *is the degree* n *of* Y *over* X. □

oneelement-generates **8.4.2. Proposition** *Let* $Y \to X$ *be as above. There is an affine open neighborhood* $X' = \operatorname{Spec} A'$ *of* p *whose inverse image* Y' *has the form* $\operatorname{Spec} B'$*, where* B' *is a finite* A'*-algebra with the following properties:*

(a) *As* A'*-algebra,* B' *is generated by one element:* $B' = A'[y]$.

(b) B' *is a simple localization of an algebra of the form* $B_0 = \mathbb{C}[x, y]/(F)$*, where* F *is an irreducible polynomial in* $\mathbb{C}[x, y]$.

The curve $Y_0 = \operatorname{Spec} B_0$, which is the locus $F = 0$ in the plane $\mathbb{A}^2_{x,y}$, is closely related to the curve Y. Its nomalization will be an open subset V of Y. However, its image Y_0 in the plane may have picked up some singularities. So Y_0 needn't be an open subset of Y.

proof. We begin by noting that $\overline{B}$ is generated, as $\mathbb{C}$-algebra, by one element. To generate this algebra, we distribute the factors $\overline{B}_i$ along the affine y-line. We let $\overline{y}$ be the element $(t_1 - c_1) \oplus \cdots \oplus (t_k - c_k)$, with distinct elements $c_i \in \mathbb{C}$. The polynomial in y of lowest degree that evaluates to zero with the substitution $y = \overline{y}$ is $\prod (y + c_i)^{e_i}$. Therefore the subalgebra $\mathbb{C}[\overline{y}]$ of $\overline{B}$ has dimension $e_1 + \cdots + e_k$, the same as the dimension of $\overline{B}$, and $\mathbb{C}[\overline{y}] = \overline{B}$.

Now that we have $\overline{B} = \mathbb{C}[\overline{y}]$, we choose an element $y \in B$ that maps to $\overline{y}$ in $\overline{B}$, and we let B_0 denote the subalgebra $A[y] = \mathbb{C}[x, y]$ of B generated by y. This algebra is a quotient of $\mathbb{C}[x, y]$ of Krull dimension one, so it has the form $B_0 = \mathbb{C}[x, y]/P$, where P is a principal prime ideal, say the ideal generated by the polynomial $F(x, y)$. (see (2.3.1)).

Since $\overline{y}$ generates $\overline{B}$, the map $B_0 \to \overline{B}$ is surjective. Let $\overline{B}_0 = B_0/xB_0$ and $M = B/B_0$. We form a diagram of finite A-modules

$$\begin{array}{ccccc} B_0 & \xrightarrow{x} & B_0 & \longrightarrow & \overline{B}_0 \\ \downarrow & & \downarrow & & \downarrow \\ B & \xrightarrow{x} & B & \longrightarrow & \overline{B} \\ \downarrow & & \downarrow & & \downarrow \\ M & \xrightarrow{x} & M & \longrightarrow & 0 \end{array}$$

The two top rows form short exact sequences when zeros are added at the ends, and the bottom row is the sequence of cokernels. The zero in the corner is justified by the fact that $B_0 \to \overline{B}$ is surjective, which implies that $\overline{B}_0 \to \overline{B}$ is surjective. The Snake Lemma shows that multiplication by x defines a surjective map $M \to M$, i.e., that $xM = M$. By the Nakayama Lemma, there is a nonzero element $z \in xA$ such that $s = 1 - z$ annihilates M. Then the localizations $(B_0)_s$ and $(B)_s$ are equal, and $B_s = A_s[y]$. Then $A' = A_s$ and $B' = B_s$ are as required. □

workonX **8.4.3. Notation.** When considering a smooth projective curve Y as a covering of $X = \mathbb{P}^1$, it will be convenient to work primarily on X, and we will often pass between an $\mathcal{O}_Y$-module $\mathcal{M}$ and its direct image $\pi_*\mathcal{M}$. Recall that if X' is open in X, then $[\pi_*\mathcal{M}](X') = \mathcal{M}(Y')$, where $Y' = \pi^{-1}X'$.

If we restrict the $\mathcal{O}$-module by looking only at open subsets of Y of the form $Y' = \pi^{-1}X'$, the only difference between $\pi_*\mathcal{M}$ and $\mathcal{M}$ will be that $\mathcal{M}(X')$ gets relabelled as $\mathcal{M}(\pi^{-1}X')$.

So one can think of the direct image $\pi_*\mathcal{M}$ as working with $\mathcal{M}$, but looking only at open subsets of Y that are inverse images of open subsets of X. To simplify notation, we omit the symbol π_*, and simply write $\mathcal{M}$ for $\pi_*\mathcal{M}$. If X' is open in X, $\mathcal{M}(X')$ will stand for $\mathcal{M}(\pi^{-1}X')$. To eliminate confusion, we may refer to an $\mathcal{O}_Y$-module $\mathcal{M}$ as an $\mathcal{O}_X$-module when thinking of its direct image. Because $H^q(X, \pi_*\mathcal{M}) = H^q(Y, \mathcal{M})$ (7.4.18), dropping the symbol π_* won't get us into trouble with cohomology.

In accordance with this convention, we will also write $\mathcal{O}_Y$ for $\pi_*\mathcal{O}_Y$. In order not to confuse $\mathcal{O}_Y$ with $\mathcal{O}_X$, we must be careful to include the subscripts.

locfreeonY **8.4.4. Lemma.** **(i)** *Let X be a variety, let $\mathcal{M}$ be a locally free $\mathcal{O}_X$-module, and let $S = \{p_1, ..., p_k\}$ be a finite set of points of X. There is an open set X' that contains S on which $\mathcal{M}$ is a free $\mathcal{O}_X$-module.*

(ii) *Let $Y \to X$ be a map from a smooth projective curve to $\mathbb{P}^1$, and let $\mathcal{M}$ be a locally free $\mathcal{O}_Y$-module. If p is a point of X, there is an open subset X' that contains p, such that $\mathcal{M}$ is a free $\mathcal{O}_Y$-module on the inverse image $Y' = \pi^{-1}(X')$.*

(iii) *The direct image of a locally free $\mathcal{O}_Y$-module $\mathcal{M}$ is a locally free $\mathcal{O}_X$-module. If $\mathcal{M}$ is a locally free $\mathcal{O}_Y$-module of rank r, and if the degree of the covering $Y \to X$ is n, then $\mathcal{M}$ will have rank nr as $\mathcal{O}_X$-module. In particular, $\mathcal{O}_Y$ is a locally free $\mathcal{O}_X$-module of rank n.*

proof. **(i)** We show first that there is an affine open set that contains S. Since X is quasiprojective, its closure $\overline{X}$ in $\mathbb{P}^n$ will be a projective variety. Let C be the closed complement $\overline{X} - X$ of X in $\overline{X}$. We may choose a homogeneous polynomial f that vanishes on C but doesn't vanish at any point of S. Let Z be the hypersurface $\{f = 0\}$. The complement of Z in $\mathbb{P}^n$ is an affine open subset V of $\mathbb{P}^n$ that contains S (**??**), and $U = V \cap \overline{X} = V \cap X$ is an affine open subset of X that contains S.

So we may assume that X is affine, say $X = \operatorname{Spec} B$. Let $M = \mathcal{M}(X)$, and suppose that $\mathcal{M}$ is free on an open set that contains the first n points $q_1, ..., q_n$, with basis $v = (v_1, ..., v_r)$. Let $v' = (v_1', ..., v_r')$ be a local basis for $\mathcal{M}$ at the next point q_{n+1}. We may clear denominators, so that the basis elements v_i and v_i' are in M. Then $v' = vP$, where P is a matrix whose entries are rational functions that are regular at $q_1, ..., q_n$, and similarly, $v = v'P^{-1}$, and the entries of P^{-1} are regular at q_{n+1}. Let $w_i = cv_i + c'v_i'$. Then $w = v(cI + c'P)$ and also $w = v'(cP^{-1} + c'I)$. For most choices of c and c', the matrix $cI + c'P$ will be invertible at the points q_i, and the matrix $cP^{-1} + c'I$ will be invertible at q_{n+1}. Then w will be a basis for $\mathcal{M}$ at the points $q_1, ..., q_{n+1}$.

We omit the proofs of **(ii)** and **(iii)**. □

8.5 Differentials

diff

We introduce differentials because they are important for understanding the duality in the Riemann-Roch Theorem. Exactly why they enter into Riemann-Roch is a bit of a mystery.

Let M be a module over an algebra A. A *derivation* $A \xrightarrow{\delta} M$ is a $\mathbb{C}$-linear map such that

deriv (8.5.1) $$\delta(ab) = a\,\delta b + b\,\delta a$$

for all a, b in A, and $\delta c = 0$ for all c in $\mathbb{C}$. For example, let A be the polynomial ring $\mathbb{C}[x_1, ..., x_n]$, and let $m_1, ..., m_n$ be elements of an A-module M. The map $A \xrightarrow{\delta} M$ defined by $\delta(f) = \sum \frac{\partial f}{\partial x_i} m_i$ is a derivation.

The *module of differentials* Ω_A of the algebra A, also called *Kähler differentials.* is an A-module generated by elements denoted by da, one for each a in A, with the relations that make the map $A \xrightarrow{d} \Omega_A$ that sends a to da a derivation:

$$d(ab) = a\,db + b\,da \text{ for } a, b \text{ in } A, \text{and } dc = 0 \text{ for } c \text{ in } \mathbb{C}$$

These relations show by induction that $dx^k = kx^{k-1}dx$, and that if $f(x)$ is a polynomial, then $df = \frac{df}{dx}dx$.

omegafree **8.5.2. Proposition.** *Let R denote the polynomial ring $\mathbb{C}[x_1, ..., x_n]$. The R-module Ω_R of differentials is a free R-module with basis $dx_1, ..., dx_n$.*

proof. The formula $df = \sum \frac{\partial f}{\partial x_i} dx_i$ shows that the elements $dx_1, ..., dx_n$ generate Ω_R as R-module. If F denotes the free R-module with basis $v_1, ..., v_n$, then sending $f \rightsquigarrow \sum \frac{\partial f}{\partial x_i} v_i$ is a derivation that induces a surjective module homomorphism $\Omega_R \xrightarrow{\varphi} F$. Since F is free, φ is an isomorphism. □

homomderiv **8.5.3. Lemma.** **(i)** *Composition with the derivation $A \xrightarrow{d} \Omega_A$ defines a bijection between homomorphisms of A-modules $\Omega_A \xrightarrow{\varphi} M$ and derivations $A \xrightarrow{\delta} M$.*
(ii) *An algebra homomorphism $A \xrightarrow{\varphi} B$ induces a module homomorphism $\Omega_A \xrightarrow{d\varphi} \Omega_B$ making a diagram*

$$\begin{array}{ccc} B & \xrightarrow{d} & \Omega_B \\ {\scriptstyle\varphi}\uparrow & & \uparrow{\scriptstyle d\varphi} \\ A & \xrightarrow{d} & \Omega_A \end{array}$$

commutes.

proof. **(i)** This follows from the defining relations for Ω_A.

(ii) This follows from the mapping property **(i)**, because the composed map $A \xrightarrow{\varphi} B \xrightarrow{d} \Omega_B$ will be a derivation. □

8.5.4. Lemma. **(i)** *Let I be an ideal of an algebra R, and let $A = R/I$. Suppose that I is generated by*
omegafreetwo *elements $f = (f_1, ..., f_r)$ of R. Then Ω_A is the quotient of Ω_R obtained from Ω_R by introducing the two rules:*

- *multiplication by f_i is zero, and*
- *$df_i = 0$*

(ii) *Let S be a multiplicative system in a domain A. There is a canonical isomorphism $\Omega_A S^{-1} \to \Omega_{AS^{-1}}$. In particular, if K is the field of fractions of A, then $\Omega_K \approx \Omega_A \otimes_A K$.*

proof. The statment can be summed up by an exact sequence

omegasequence (8.5.5) $$I \xrightarrow{d} \Omega_R \otimes_R A \to \Omega_A \to 0$$

in which the map labeled d sends an element g of I to $dg \otimes 1$.

The explanation of this sequence is this: $\Omega_R \otimes_R A \approx \Omega_R / I\Omega_R$ is the result of declaring that multiplication by f_i is zero. Then the assertion becomes that killing the image dI of I in $\Omega_R \otimes_R A$ produces Ω_A. To see this, let S denote the module obtained from $\Omega_R \otimes_R A$ by killing dI. We note first that multiplication by f_i and df_i must be zero in Ω_A. Therefore there is a canonical module homomorphism $S \to \omega_A$. Conversely the composed map $R \xrightarrow{d} \Omega_R \to S$ is a derivation, and I is in its kernel. Let's denote that derivation by $\overline{d}$. We define a derivation $A \xrightarrow{\delta} S$ as follows: Given $a \in A$, we represent a by an element $r \in R$, and we define $\delta(a) = \overline{d}(r)$. This is well-defined because, if $r \in I$, then because $dI = 0$, $\overline{d}(r) = 0$. Then δ is a derivation because $\overline{d}$ is one. By the universal property of Ω_A, the map $S \to \Omega_A$ is invertible.

(ii) The composition $A \to AS^{-1} \to \Omega_{AS^{-1}}$ is a derivation. It defines an A-module map $\Omega_A \to \Omega_{AS^{-1}}$, and therefore an AS^{-1}-module map $S^{-1}\Omega_A \to \Omega_{AS^{-1}}$. To invert this map, we define a derivation $AS^{-1} \xrightarrow{\delta} \Omega_A S^{-1}$. Setting $d(s^{-1}) = -s^{-2}ds$ for s in S, we define δ by

$$\delta(as^{-1}) = (ds^{-1})a + s^{-1}da = s^{-2}(-a\,ds + s\,da)$$ □

When X is a variety, the $\mathcal{O}$-module Ω_X of differentials on X is defined using the standard procedure: If $X' = \operatorname{Spec} A$ is an affine open, the A-module of sections of Ω_X on X' is Ω_A.

omegafunct **8.5.6. Proposition.** *For any variety Y, Ω_Y is a finite $\mathcal{O}_Y$-module. If Y is a smooth curve, Ω_Y is an invertible $\mathcal{O}_Y$-module.*

proof. The coherence property, the sheaf property, and the fact that Ω_Y is a finite module, all follow from Proposition 8.5.4. Suppose that Y is a smooth curve. We apply Proposition 8.4.2. There is an affine open subset $Y' = \operatorname{Spec} B'$ that is a localization of a plane curve $\{F(x,y) = 0\}$. We replace Y by this affine curve. Let R denote the polynomial ring $\mathbb{C}[x,y]$. Then Ω_Y is obtained from the free B-module with basis dx, dy by introducing the relation $F_x dx + F_y dy = 0$. Since Y' is smooth, at least one of the partial derivatives F_x or F_y is nonzero at any given point, and then $\Omega_{Y'}$ will be freely generated by dx or dy, locally. □

dygenerates **8.5.7. Lemma.** *Let $Y \xrightarrow{\pi} X$ be a map from a smooth curve to $X = \mathbb{P}^1$. Every point p of X has an open neighborhood X' such that the restriction of Ω_Y to $Y' = \pi^{-1}(X')$ is generated as $\mathcal{O}_Y$-module by a single differential dy.*

proof. We apply Proposition 8.4.2. We may assume that $Y' = \operatorname{Spec} B'$ is a localization of an algebra of the form $B_0 = \mathbb{C}[x,y]/(F)$. Let p be a point of X'. Then Ω_B is generated by dx and dy, with the relation $dF = F_x dx + F_y dy = 0$. Because Y' is smooth, the partial derivatives F_x and F_y cannot both be zero at any of its points, and if $F_y \neq 0$ at a point q, then dy generates Ω_B locally. If $F_y = 0$ at some point q that lies over p, then $F_x \neq 0$ there. In that case, we replace y by $y + cx$ for generic $c \in \mathbb{C}$. □

8.6 Trace

tracediff The next sections present an adaptation of Grothendieck's proof of duality to Riemann-Roch for curves. The proof prceeds by analyzing a projection from a curve to $\mathbb{P}^1$. Its most interesting part is a subtle fact, that there is a trace map for differentials analogous to the trace map for functions.

tracefn **(8.6.1) trace of a function, revisited**

Let $Y \xrightarrow{\pi} X$ be a finite morphism from a smooth projective curve Y to $X = \mathbb{P}^1$ as before, and let K and F be the function fields of X and Y, respectively. So K is a finite field extension of the rational function field $F = \mathbb{C}(x)$, and the degree n of the extension is equal to the degree of Y over X.

We denote the *trace map* for functions, which carries K to F, by tr. The trace of an element g of K was defined before (4.3.6), as the trace of the operator of multiplication by g on the F-vector space K.

The trace carries regular functions to regular functions: If $X' = \operatorname{Spec} A$ is an affine open subset of X whose inverse image is $Y' = \operatorname{Spec} B$, the trace of an element of B will be in A (4.3.4).

One can describe the trace analytically as a sum over the sheets of the covering $Y \to X$. Let p be a point of X that isn't a branch point for the covering. There will be n points in the fibre over p, say $q_1, ..., q_n$. If U is a small neighborhood of p in the classical topology, its inverse image $V = \pi^{-1}U$ will consist of disjoint neighborhoods V_i of q_i, each of which maps bijectively to U, and the ring of analytic functions on V_i will be isomorphic to the ring R of analytic functions on U.

This allows us to identify the ring of analytic functions on V with the direct sum of n copies of R. If a rational function g on Y is regular on V, its restriction to V can be written as $g = g_1 \oplus \cdots \oplus g_n$, with g_i in R. The matrix of left multiplication by g on $R \times \cdots \times R$ is the diagonal matrix with entries g_i. Therefore the trace of g is

trsum (8.6.2)
$$\operatorname{tr}(g) = g_1 + \cdots + g_n$$

tracesum **8.6.3. Lemma.** *With $Y \xrightarrow{\pi} X$ as above, let p be a point of X, possibly a branch point, and let $q_1, ..., q_k$ be the fibre over p. Let e_i be the ramification index at q_i. If g is a rational function on Y that is regular at the points $q_1, ..., q_k$, the value of the trace $\operatorname{tr}(g)$ at p is*

$$[\operatorname{tr}(g)](p) = \sum e_i g(q_i)$$

proof. When p is not a branch point, we will have $e_i = 1$ for all i and $k = n$. In this case, the lemma simply restates (8.6.2). It follows by continuity for any point p because, as a point p' of X approaches p, e_i points of the fibre over p' approach q_i. □

The next proposition is essential for what follows.

smallpole **8.6.4. Proposition.** *With notation as above, let g be a rational function on Y, and suppose that for $i = 1, ..., k$, g a pole of order at most $e_i - 1$ at the point q_i. Then $\mathrm{tr}(g)$ is a regular function on X at p.*

proof. Say that p is the point $x = 0$ of X. Let $h = xg$. Since x has a zero of order e_i at q_1 and g has a pole of order at most $e_i - 1$, h is a regular function at q_i, and $h(q_i) = 0$. Therefore the trace of h is regular at p. The previous lemma shows that $\mathrm{tr}(h)$ vanishes at p. Therefore $\mathrm{tr}(h)/x$ is a regular function at p. On the other hand, since tr is $\mathcal{O}_X$-linear, $\mathrm{tr}(h) = x\,\mathrm{tr}(g)$. Therefore $\mathrm{tr}(g)$ is also regular at p. □

For example, when Y is the locus $y^e = x$, multiplication by $\zeta = e^{2\pi i/e}$ permutes the sheets of Y over X. The trace of y^k is

sumzeta (8.6.5)
$$\sum_i \zeta^{ki} y^k$$

The trace is zero unless $k \equiv 0$ modulo e.

traced **(8.6.6) trace of a differential**

Let $Y \to X$ denote a map of a smooth projective curve Y to $\mathbb{P}^1$ as before, and let K and F denote the function fields of Y and X, respectively. The trace for differentials, which we are about to define, will be denoted by τ. We first define this trace for differentials of the function field K. Because the $\mathcal{O}_Y$-module Ω_Y is invertible, the module Ω_K of K-differentials is a free K-module of rank one (see (8.5.4) **(ii)**). Any nonzero differential will form a K-basis. So one can write an element α of Ω_K uniquely in the form

$$\alpha = g\,dx$$

where x is the coordinate variable in X and g is an element of K. The trace τ is defined by

deftrdif (8.6.7)
$$\tau(g\,dx) = \mathrm{tr}(g)dx$$

where $\mathrm{tr}(g)$ is the trace of the function g. Thus τ is an F-linear map $\Omega_K \to \Omega_F$.

regdiff **8.6.8. Definition.** A differential α of Ω_K is *regular* at a point q of Y if there is an affine open neighborhood $Y' = \mathrm{Spec}\,B$ of q such that α is an element of Ω_B.

tracereg **8.6.9. Proposition.** *Let p be a point of X and let $q_1, ..., q_k$ be the points of Y that lie over p. If a differential α on Y is regular at the points $q_1, ..., q_k$, its trace $\tau(\alpha)$ is regular at p.*

proof. We write $\alpha = gdx$, where g is a rational function on Y, an element of K. So $\tau(\alpha) = \mathrm{tr}(g)dx$, and we want to show that $\mathrm{tr}(g)$ is a regular function at p. According to Proposition 8.6.4, it suffices to show that g has poles of orders at most $e_i - 1$ at the points q_i. We drop the subscript i. Let q be a point that lies over p. We use notation as in (8.4.2), arranging coordinates so that p is the point $x = 0$ and q is the point $y = 0$ of $\mathrm{Spec}\,B'$.

Let v be the valuation of K associated to q, and suppose that $\mathrm{v}(x) = e$. So e is the ramification index of the covering $Y \to X$ at q. Then $x = uy^e$, where u is a unit of the valuation ring R. Working analytically,

dx (8.6.10)
$$dx = y^e du + ey^{e-1}udy = \big(y^e \frac{du}{dy} + ey^{e-1}u\big)dy$$

Since u is a regular function, its derivative $\frac{du}{dy}$ is analytic. The formula shows that dx has a pole of order $e-1$. Therfore, if α is regular at q, then g will have a pole of order at most $e - 1$ at q. □

For example, if $x = y^e$, then $dx = ey^{e-1}dy$.

omegaYandX **8.6.11. Corollary.** *The trace map (8.6.7) defines a homomorphism of $\mathcal{O}_X$-modules $\Omega_Y \xrightarrow{\tau} \Omega_X$.* □

We define a map The map

defeps (8.6.12)
$$\Omega_Y \xrightarrow{\epsilon} \underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{O}_Y, \Omega_X)$$

by sending a differential α to the map $\mathcal{O}_Y \xrightarrow{\epsilon_\alpha} \Omega_X$ defined by

$$\epsilon_\alpha(g) = \tau(g\alpha)$$

traceisom **8.6.13. Theorem.** *The map (8.6.12) is an isomorphism of $\mathcal{O}_Y$-modules.*

proof. Let $\mathcal{H} = \underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{O}_Y, \Omega_X)$. As explained in Section **??**, the structure of $\mathcal{O}_Y$-module on $\mathcal{H}$ is given by the right $\mathcal{O}_Y$-module structure on $\mathcal{O}_Y$. We verify that the map $\Omega_Y \xrightarrow{\epsilon} \mathcal{H}$ is $\mathcal{O}_Y$-linear. Let α be a regular differential on the inverse image Y' of an open subset X' of X, and let h be a regular function on Y'. We must show that $(\epsilon_\alpha)h = \epsilon_{(\alpha h)}$. By definition,

$$(\epsilon_\alpha)h(g) = \epsilon_\alpha(gh)\,\tau(gh\alpha) = \tau(g(\alpha h)) = \epsilon_{(\alpha h)}(g)$$

Thus ϵ is a homomorphism of $\mathcal{O}_Y$-modules. We also know that Ω_Y is an invertible $\mathcal{O}_Y$-module. To show that $\mathcal{H}$ is invertible, we note that it is torsion-free. So it is enough to show that it has rank one as $\mathcal{O}_Y$-module. This is true because, as $\mathcal{O}_X$-module, it has the same rank as $\mathcal{O}_Y$.

Since the map ϵ is nonzero, it is injective. Now suppose given a nonzero and therefore injective map $\mathcal{L}_1 \to \mathcal{L}_2$ of invertible modules. We tensor with the dual $\mathcal{L}_2^*$, obtaining an injective map $\mathcal{M} \to \mathcal{O}$, where $\mathcal{M} = \mathcal{L}_2^* \otimes_{\mathcal{O}} \mathcal{L}_1$. Then $\mathcal{M}$ is an ideal of $\mathcal{O}$. It is isomorphic to $\mathcal{O}(-D)$ for some effective divisor D. Tensoring back, $\mathcal{L}_2 \approx \mathcal{L}_1(D)$.

Going back to our situation, we now have $\mathcal{H} \approx \Omega_Y(D)$ for some effective divisor D. To show that ϵ is an idomorphism, we show that $D = 0$, and to do this, we show that, with $q_1, ..., q_k$ lying over p as before, there is a differential α on Y with a simple pole at one of the points, say q_1, that is regular at the points $q_2, ..., q_k$, and whose $\tau(\alpha)$ isn't a regular differential at p. Then the coefficient of q_1 in D must be zero.

The first try is the logarithmic differential $\alpha = dx/x$, viewed as a differential on Y. Its trace is ndx/x, which is not regular at p. But because α isn't regular at the points $q_2, ..., q_k$, we write this differential as a sum. The power $\mathfrak{m}_1^N$ and the product of the powers $\mathfrak{m}_2^N \cdots \mathfrak{m}_k^N$ are comaximal. So we can write $1 = g_1 + g_2$ with $g_1 \in \mathfrak{m}_1^N$ and $g_2 \in \mathfrak{m}_2^N \cdots \mathfrak{m}_k^N$. The trace $\mathrm{tr}(g_2)$ is a regular function at p, whose value $e_1 g_2(q_1)$ at p is nonzero. If N is large, $g_2\alpha$ has a pole at q_1, is regular at $q_2, ..., q_k$, and its trace is $n\,\tau(g_2)dx/x$, which has a pole at p. □

8.7 Riemann-Roch

rroch

Let X be a smooth projective curve, and let $\mathcal{M}$ be a locally free $\mathcal{O}_X$-module. We denote the module $\underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{M}, \Omega_X)$ by $\mathcal{M}^D$. This module is the *Serre dual* of $\mathcal{M}$. Since Ω_X is invertible, the Serre dual $\mathcal{M}^D$ will be locally free, and it will have the same rank as $\mathcal{M}$. Moreover, the canonical map $\mathcal{M} \to (\mathcal{M}^D)^D$ will be an isomorphism. This follows from the discussion of **8.1.6** because $\mathcal{M}$ and $\mathcal{L}$ are locally free. It also follows that $\mathcal{O}_X^D = \Omega_X$ and $\Omega_X^D = \mathcal{O}_X$.

dualcohom **8.7.1. Riemann-Roch Theorem (version 2).** *Let X be a smooth projective curve, let $\mathcal{M}$ be a locally free $\mathcal{O}_X$-module, and let $\mathcal{M}^D$ be its Serre dual. Then* $\dim H^1(X, \mathcal{M}) = \dim H^0(X, \mathcal{M}^D)$*, and* $\dim H^0(X, \mathcal{M}) = \dim H^1(X, \mathcal{M}^D)$.

Since $\mathcal{M}$ and $\mathcal{M}^{DD}$ are isomorphic, the two assertions of the theorem are equivalent.

A more precise version of this theorem states that the vector spaces $H^1(X, \mathcal{M})$ and $H^0(X, \mathcal{M}^D)$ are dual spaces. We omit the proof. The fact that the dimensions of these spaces are equal is enough for nearly every application. And of course, any complex vector spaces V and W whose dimensions are equal can be made into dual spaces by the choice of a nondegenerate bilinear form $V \times W \to \mathbb{C}$. The precise duality is useful only when one needs to analyze the cohomology map corresponding to a homomorphism $\mathcal{M} \to \mathcal{N}$.

Our plan is to prove the theorem 8.7.1 directly for the case of the projective line. The structure of locally free modules on $\mathbb{P}^1$ is very simple, so this will be easy. We will deduce it for an arbitrary smooth projective curve Y by projection to $\mathbb{P}^1$.

We discuss the projection to $\mathbb{P}^1$ first. Let Y be a smooth projective curve, let $Y \xrightarrow{\pi} X = \mathbb{P}^1$ be a finite morphism, and let $\mathcal{M}$ be a locally free $\mathcal{O}_Y$-module. The Serre dual of $\mathcal{M}$ was defined above. It is

$$\mathcal{M}_1^D = \underline{\mathrm{Hom}}_{\mathcal{O}_Y}(\mathcal{M}, \Omega_Y)$$

However, we can also view $\mathcal{M}$ as a locally free $\mathcal{O}_X$-module by taking its direct image, which we are denoting by $\mathcal{M}$ too. Then we can form the Serre dual on X:

$$\mathcal{M}_2^D = \underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{M}, \Omega_X)$$

abouthom **8.7.2. Lemma.** *When regarded as an $\mathcal{O}_X$-module, the Serre dual $\mathcal{M}_1^D$ is canonically isomorphic to $\mathcal{M}_2^D$.*

proof. We map $\underline{\mathrm{Hom}}_{\mathcal{O}_Y}(\mathcal{M}, \Omega_Y)$ to $\underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{M}, \Omega_X)$ by composition with the trace map for differentials. If $\mathcal{M} \xrightarrow{\varphi} \Omega_Y$ is an $\mathcal{O}_Y$-homomorphism, its image $\tau \circ \varphi$ is an $\mathcal{O}_X$-homomorphism $\mathcal{M} \to \Omega_X$. This gives us a functorial map $\mathcal{M}_1^D \xrightarrow{\tau} \mathcal{M}_2^D$. It suffices to prove that the map is an isomorphism on an affine open covering of X. Then since $\mathcal{M}$ is locally free, it suffices to prove that the map is an isomorphism when $\mathcal{M}$ is the structure sheaf $\mathcal{O}_Y$. In that case, the functorial map is the trace map $\underline{\mathrm{Hom}}_{\mathcal{O}_Y}(\mathcal{O}_Y, \Omega_Y) \xrightarrow{\tau} \underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{O}_Y, \Omega_X)$. The fact that this map is an isomorphism is Theorem 8.6.13. □

We now drop the subscripts from $\mathcal{M}^D$.

dualitymaps **8.7.3. Corollary.** *Let $Y \xrightarrow{\pi} X$ be a finite morphism of projective curves, and let $\mathcal{M}$ be a locally free $\mathcal{O}_Y$-module. Then $H^q(Y, \mathcal{M}) \approx H^q(X, \mathcal{M})$ and $H^q(Y, \mathcal{M}^D) \approx H^q(X, \mathcal{M}^D)$.*

See Lemma 7.4.17. □

This corollary shows that it suffices to prove Theorem 8.7.1 for the case that $Y = \mathbb{P}^1$.

dualityfor pone

(8.7.4) Riemann-Roch for the projective line

Here X denotes the projective line $\mathbb{P}^1$. We apply the theorem of Birkhoff and Grothendieck: Every locally free $\mathcal{O}_X$-module $\mathcal{M}$ is a direct sum of twisting sheaves. Thus it suffices to verify the Riemann-Roch Theorem for the twisting sheaves $\mathcal{O}_X(n)$.

omegapone **8.7.5. Lemma.** *The module Ω_X on X is isomorphic to the twisting sheaf $\mathcal{O}_X(-2)$.*

proof. On the standard open set $\mathbb{U}^0 = \operatorname{Spec} \mathbb{C}[x]$, the module of differentials is generated by dx. Let $z = x^{-1}$ be the coordinate of X on $\mathbb{U}^1$. Then $dx = d(z^{-1}) = -z^{-2}dz$ describes the differential dx on $\mathbb{U}^1$. It has a pole of order 2 at the point p_∞ at infinity. So dx is a section of $\Omega_X(2p_\infty)$. This section is nowhere zero, and defines isomorphisms $\mathcal{O}_X \approx \Omega_X(2p_\infty)$ and $\Omega_X \approx \mathcal{O}_X(-2p_\infty) \approx \mathcal{O}_X(-2)$. □

The Serre dual of $\mathcal{O}_X(n)$ is then $\underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{O}_X(n), \Omega_X) \approx \underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{O}_X(n), \mathcal{O}_X(-2))$. Now, for any $\mathcal{O}$-modules $\mathcal{M}$ and $\mathcal{N}$ on $\mathbb{P}^d$, $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M}, \mathcal{N})$ is canonically isomorphic to $\underline{\mathrm{Hom}}_{\mathcal{O}}(\mathcal{M}(r), \mathcal{N}(r))$. Given a homomorphism $\mathcal{M} \xrightarrow{\varphi} \mathcal{N}$, the corresponding homomorphism $\mathcal{M} \otimes_{\mathcal{O}} \mathcal{O}(r) \to \mathcal{N} \otimes_{\mathcal{O}} \mathcal{O}(r)$ is $\varphi \otimes id$. Tensoring with $\mathcal{O}(-n)$, we find that

$$\mathcal{O}_X(n)^D \approx \underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{O}_X(n), \mathcal{O}_X(-2)) \approx \underline{\mathrm{Hom}}_{\mathcal{O}_X}(\mathcal{O}_X, \mathcal{O}_X(-2-n)) \approx \mathcal{O}_X(-2-n)$$

To prove Riemann-Roch for $X = \mathbb{P}^1$, we must show that

$$\dim H^0(X, \mathcal{O}(n)) = \dim H^1(X, \mathcal{O}(-2-n)) \quad \text{and} \quad \dim H^1(X, \mathcal{O}(n)) = \dim H^0(X, \mathcal{O}(-2-n))$$

This follows from the computation of cohomology on projective space (see Theorem 7.5.4). □

8.8 Genus

genussm-curve

There are three closely related numbers associated to a smooth projective curve Y. The first two are its topological *genus* g, and its *arithmetic genus* $p_a = \dim H^1(Y, \mathcal{O}_Y)$. The topological genus is defined, because Y is connected. The third number is the degree δ of the module of differentials Ω_Y, which is the difference $z - p$ of the numbers of zeros and of poles of a differential (see (8.3.6)).

genusgenus **8.8.1. Theorem.** *Let Y be a smooth projective curve.*
(i) *The topological genus and the arithmetic genus of Y are equal: $g = p_a$.*
(ii) *The degree of the module Ω_Y of differentials on Y is $\delta = 2g-2 = 2p_a - 2$.*

Since Ω_Y is invertible, it is isomorphic to a module of the form $\mathcal{O}_Y(K)$ for a divisor K of degree $2g-2$, called a *canonical divisor*. However, the canonical divisor K is determined only up to linear equivalence (see Proposition 8.2.3 **(iii)**). Using the canonical divisor, one can write the Riemann-Roch Theorem for $\mathcal{O}(D)$ in the form

RROD **8.8.2. Corollary.** *Let K be a canonical divisor on a smooth projective curve Y, and let D be another divisor. Then* $\dim H^0(Y, \mathcal{O}(D)) = \dim H^1(Y, \mathcal{O}(K-D))$ *and* $\dim H^0(Y, \mathcal{O}(K-D)) = \dim H^1(Y, \mathcal{O}(D))$. □

proof of the theorem. **(ii)** Riemann-Roch tells us that $\dim H^0(Y, \Omega_Y) = \dim H^1(Y, \mathcal{O}_Y) = p_a$ and that $\dim H^1(Y, \Omega_Y) = \dim H^0(Y, \mathcal{O}_Y) = 1$ (see (8.7.1). So $\chi(\Omega_Y) = p_a - 1$. Since we also know that $\chi(\Omega_Y) = \delta + 1 - p_a$ (8.3.6), $\delta = 2p_a - 2$, as expected.

(i) We choose a map $Y \xrightarrow{\pi} X$ to the projective line. The topological Euler characteristic of Y can be computed in terms of the branching data for the covering Y over X. It is

$$2 - 2g = e(Y) = ne(X) - \sum(e_i - 1) = 2n - \sum(e_i - 1)$$

Next, we determine the degree of Ω_Y by computng the divisor of the differential dx on Y. Let q be a point of Y with ramification index e, possibly $e = 1$. We choose coordinates so that its image p in X is the point $x = 0$, and that the point at infinity is not a branch point. Then if y is a local generator for the maximal ideal $\mathfrak{m}_q$, we will have $x = uy^e$, and dx has a zero of order $e-1$ at q (8.6.10).

On X, dx has a pole of order 2 at ∞. Then if n is the degree of Y over X, there will be n points on Y at which dx has a pole of order 2. The degree of Ω_Y is therefore

$$\delta = \#\{zeros\} - \#\{poles\} = \sum(e_i - 1) - 2n = -e(Y) = 2g - 2$$

Thus $\delta = 2p_a - 2 = 2g - 2$, and $p_a = g$. □

The next corollary follows by duality from Corollary 8.3.5 **(v)** and **(vi)**.

Honezero **8.8.3. Corollary.** *Let D be a divisor on a smooth projective curve Y of genus g.*
(i) *If* $\deg\, D > 2g-2$ *then* $H^1(Y, \mathcal{O}(D)) = 0$.
(ii) *If* $\deg\, D \le g-2$, *then* $H^1(Y, \mathcal{O}(D)) \neq 0$. □

8.9 Curves of Genus Zero or One

lowgenus The next proposition will be convenient for use in this section. It is an example of the general principle that a finite sequence of computations done in a localization can be made in a simple localization.

pointsinfibre **8.9.1. Proposition.** *Let $Y \xrightarrow{u} X$ be a morphism of varieties whose image contains a nonempty open subset of X, and let K and L be the function fields of X and Y, respectively. Suppose that L is a finite extension of K of degree n. Then there are open subsets $X' \subset X$ and $Y' = u^{-1}X' \subset Y$ such that all fibres of Y' over X' have order n.*

proof. We may replace X and Y by arbitrary nonempty open subsets, and we may do this finitely often. Thus we may assume that X and Y are affine, say $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$. The fraction fields of A and B will be K and L, respectively. Let $B \otimes_A K = BS^{-1}$, where S is the multiplicative system of nonzero elements of A. Since L is a finite extension of K and $B \otimes_A K \subset L$, $B \otimes_A K$ is a field. It is therefore equal to L. This means that every element of L can be written as a fraction b/s, with $b \in B$ and $s \in A$.

The extension L of K can be generated by one element β. Let $f(y)$ be the monic irreducible polynomial for β over K, so that $L = K[\beta] = K[y]/(f)$. Localizing, we may assume that the coefficients of f are in A, and that β is in B. Let $B_0 = A[\beta] = A[y]/(f)$. Then $B_0 \subset B$.

Let $b_1, ..., b_k$ be generators for the finite-type algebra B. They are in $L = K[\beta]$, and therefore in a simple localization of $A[\beta] = B_0$ by an element s of A. Localizing again, we may assume that they are elements of B_0. Then $B_0 = B$. We keep the notation $X = \operatorname{Spec} A$ and $Y = \operatorname{Spec} B$ for these localized varieties.

Say that $f(y) = y^n + a_{n-1}y^{n-1} + \cdots + a_0$, and let p be a point of X. The fibre of Y over the point p is the set of roots of the polynomial $\overline{f}(y) = y^n + \overline{a}_{n-1}y^{n-1} + \cdots + \overline{a}_0$, where $\overline{a}_i = a_i(p)$. There will be n points in the fibre, provided that the discriminant of $\overline{f}$ isn't zero. Since f is a polynomial with coefficients in the field K, its discriminant isn't identically zero (Proposition **??**). When we localize by inverting this discriminant, all fibres will have order n. □

genuszero **(8.9.2)** **curves of genus zero**

Let Y be a smooth projective curve of genus $g = 0$. So $H^1(Y, \mathcal{O}_Y) = 0$. Let p be a point of Y. The exact sequence

$$0 \to \mathcal{O}_Y \to \mathcal{O}_Y(p) \to \epsilon \to 0$$

gives us an exact cohomology sequence

$$0 \to H^0(Y, \mathcal{O}_Y) \to H^0(Y, \mathcal{O}_Y(p)) \to H^0(Y, \epsilon) \to 0$$

because $H^1(Y, \mathcal{O}_Y) = 0$. Therefore $\dim H^0(Y, \mathcal{O}_Y(p)) = 2$. We choose a basis $(x, 1)$ for $H^0(Y, \mathcal{O}_Y(p))$, 1 being the constant function. This basis defines a point with values in the function field K, and therefore a morphism $Y \xrightarrow{\varphi} \mathbb{P}^1$. Because x has just one pole of order 1, it takes every value exactly once. Therefore φ is bijective. It is a map of degree 1. The function fields F of $\mathbb{P}^1$ and K of Y are isomorphic. The embedding of Y into a projective space $\mathbb{P}^r$ that we assume given defines a point of $\mathbb{P}^r$ with values in K, which gives us a point with values in the isomorphic field F. The point with values in F defines a morphism $\mathbb{P}^1 \to \mathbb{P}^r$ that inverts φ. So φ is an isomorphism.

gzero **8.9.3. Corollary.** *Every curve of genus zero is isomorphic to the projective line* $\mathbb{P}^1$. □

genusone **(8.9.4)** **curves of genus one**

Let Y be a smooth projective curve of genus 1. Riemann-Roch tells us that

$$\chi(\mathcal{O}(D)) = \deg\, D$$

. The degree of a canonical divisor K is $2g - 2 = 0$. Since $\dim H^0(Y, \mathcal{O}(K)) = \dim H^1(Y, \mathcal{O}) = 1$, $\mathcal{O}(K)$ has a nonzero global section. This section cannot vanish anywhere, so it defines an isomorphism $\mathcal{O} \to \mathcal{O}(K)$. The module of differentials is free.

Let p be a point of Y. Then $K - rp$ has negative degree. Therefore $\dim H^0(Y, \mathcal{O}(K - rp)) = \dim H^1(Y, \mathcal{O}(rp)) = 0$

- If $r \geq 1$, then $\dim H^0(Y, \mathcal{O}_Y(rp)) = r$ and $H^1(Y, \mathcal{O}_Y(rp)) = 0$.

  (It isn't difficult to derive this conclusion from version 1 of the Riemann-Roch Theorem.)

The basis (1) for $H^0(Y, \mathcal{O}_Y)$ is also a basis for $H^0(Y, \mathcal{O}_Y(p))$. We choose a basis $(x, 1)$ for $H^1(Y, \mathcal{O}_Y(2p))$, which has dimension 2. Next, we choose a basis $(1, y)$ for $H^1(Y, \mathcal{O}_Y(3p))$. So x and y are functions with poles of orders 2 and 3, respectively, at p, and no other poles. Having done this, $(x, y, 1)$ determines a point of $\mathbb{P}^2$ with values in K, and a morphism $Y \to \mathbb{P}^2$ that sends a point $q \neq p$ to $(x(q), y(q), 1)$.

To determine the image of p, we multiply by y^{-1} to normalize the third coordinate to 1, obtaining the equivalent vector $(y^{-1}, xy^{-1}, 1)$. The rational function xy^{-1} has a simple zero at p and y^{-1} has a zero of order 3. Evaluating at p, we see that the image of p is the point $(0, 1, 0)$.

Let ℓ be the line $\{ax + by + cz = 0\}$ in $\mathbb{P}^2$, with $b \neq 0$. On Y, $ax + by + c$ is a function with a pole of order 3 at p and no other pole. It takes the value 0 three times, counted with multiplicity. This means that ℓ meets the image of Y in three points. The image of φ is a cubic curve in the plane, so there must be a cubic relation among the functions $x, y, 1$.

To find this cubic relation, we determine bases for the space $H^0(Y, \mathcal{O}_Y(rp))$, when $r = 4, 5, 6$. The dimension of that space is r. Setting $r = 4$, we note that x^2 has a pole of order 4 at p. It is not a combination of $x, y, 1$, which have poles orders ≤ 3. Therefore $(1, x, y, x^2)$ is a basis for $H^0(Y, \mathcal{O}_Y(4p))$. Continuing, $(1, x, y, x^2, xy)$ is a basis for $H^0(Y, \mathcal{O}_Y(5p))$. But there are two monomials in x, y with pole of orders 6, namely x^3 and y^2. Since $\dim H^0(Y, \mathcal{O}_Y(6p)) = 6$, there is a linear relation among the seven monomials $1, x, y, x^2, xy, x^3, y^2$. This gives us a cubic equation satisfied by the image Y'.

The cubic relation has the form

$$cy^2 + (a_1x + a_3)y + (a_0x^3 + a_2x^2 + a_4x + a_6) = 0.$$

The coefficients of y^2 and x^3 aren't zero, so we may assume that $c = 1$. We "complete the square", adding a combination of 1 and x to y to eliminate the linear term in y from this relation. Then we replace x by a combination of $1, x$ to eliminate the quadratic term in x and to normalize a_0 to 1. Bringing the terms in x to the other side of the equation, we are left with a cubic relation

$$y^2 = x^3 + a_4x + a_6.$$

The coefficients a_4 and a_6 will have changed, of course.

The image of Y is the cubic plane curve Y' defined by the homogenized equation $y^2z = x^3 + a_4xz^2 + a_6z^3$.

As it happens, the genus of a cubic curve in $\mathbb{P}^2$ is equal to 1 (see Section **??**). Using this fact, one can show that Y maps isomorphically to Y'.

Summing up, every curve of genus 1 is isomorphic to a cubic curve in $\mathbb{P}^2$.

genusone-froup

(8.9.5) the group law on a curve of genus 1

A smooth curve Y of genus 1, an *elliptic curve* has a group law that is uniquely determined, once one chooses a point to be the identity element.

We choose a point of Y and label it o. We'll write the group law that is to be defined additively, using the symbol $p \oplus q$ for the sum. We do this to distinguish the sum $p \oplus q$, which is a point of Y, from the divisor $p + q$.

Let p and q be points of Y. To define $p \oplus q$, we compute the cohomology of $\mathcal{O}_Y(p+q-o)$. Riemann-Roch shows that $\dim H^0(Y, \mathcal{O}_Y(p + q - o)) = 1$ and that $H^1(Y, \mathcal{O}_Y(p + q - o)) = 0$. There is a nonzero function f, unique up to scalar factor, with simple poles at p and q and a zero at o. This function has exactly one other zero. That zero is defined to be the sum $s = p \oplus q$ in the group.

In terms of linearly equivalent divisors, s is the unique point such that the divisor s is linearly equivalent to $p + q - o$, or such that $p + q$ and $o + s$ are linearly equivalent. Note that this is a commutative law of composition on Y. Let'sdenote linear equivalence by the symbol $\sim$. So $D \sim E$ mreans that $D - E$ is the divisor of a function. To verify the associative law, we let p, q, r be points of Y. Then $(p \oplus q) \oplus r$ is obtained this way: We let $s = p \oplus q$, so that $s \sim p + q - o$. Then we let $t = s \oplus r$, so that $t \sim s + r - o$. Combining, $t \sim p + q - o + r - o = p + q + r - 2o$. This determines the point t, and computation of $p \oplus (q \oplus s)$ leads to the same answer.

Finally, we check that a point p has an inverse by solving the equation $p \oplus q = o$ for q. We need q so that $o \sim p + q - o$, or that $q \sim 2o - p$. As before, one finds that $\dim H^0(Y, \mathcal{O}_Y(2o - p)) = 1$, so there is a unique solution for q.