RIEMANN-ROCH FOR NONSINGULAR COMPLETE CURVES

ISABEL LONGBOTTOM

1. Introduction

We state and prove a generalisation of the Riemann-Roch theorem, for 1-dimensional (nonsingular, complete) curves over any field, not necessarily algebraically closed. Notably, we are interested in finite fields. The chief difficulties present in doing this are: first, to determine for what kinds of 1-dimensional curves will such a generalisation make sense; second, defining the genus of such a curve since we may not have a topological genus; third, finding an analogue of the sheaf of holomorphic 1-forms which has the properties of Serre duality, in the situation where the curve is not analytic.

We begin by defining the curves we will be working with algebraically, and developing a notion of functions and divisors on such a curve. We then progress to proving a version of Riemann-Roch without Serre duality, and defining the genus of a curve. Finally, we prove the existence of a canonical class in the Picard group which coincides with the usual sheaf of holomorphic 1-forms over the base field $\mathbb{C}$, and for which Serre duality holds in generality.

Throughout our discussion, we highlight the analogies with the case where the base field is $\mathbb{C}$. It is assumed that the reader is familiar with the development of the same theory in this special case, where the curve in question is a compact Riemann surface.

2. Nonsingular Complete Curves

From a modern algebraic geometry perspective, a nonsingular complete curve is an integral scheme of dimension 1, all of whose local rings are regular, and which is proper over a base field k. Such a curve is projective with one non-closed point, and its Zariski topology is the cofinite topology on the closed points. We give a different — but equivalent — definition to allow us to work more concretely without building up the language of schemes.

Definition 2.1. A *valuation* on a field L is a map $v : L^* \to \mathbb{Z}$ satisfying

(a) $v(xy) = v(x) + v(y)$
(b) $v(x + y) \geq \min\{v(x), v(y)\}$

for every $x, y \in L^*$. We extend v to a map on L by setting $v(0) = \infty$. Given a field extension L/k, a valuation of L is *trivial on* k if $v(k^*) = 0$. Let $\mathcal{V}(L/k)$ be the set of surjective valuations of L which are trivial on k.

As a first example, the trivial homomorphism $v = 0$ is a valuation. To construct more interesting valuations, one can consider the valuation at a maximal ideal in a Dedekind domain. Recall that a Dedekind domain is a Noetherian ring with Krull dimension 1, such that the localisation at any maximal ideal is a local principal ideal domain. In particular, every nonzero prime ideal is maximal and every ideal can be uniquely factorised as a product of prime ideals.

Example 2.2. Let B be a Dedekind domain, and $\mathfrak{p} \subset B$ a nonzero prime ideal. We define a valuation $v_\mathfrak{p} : \mathrm{Frac}(B)^* \to \mathbb{Z}$ as follows. Given $x \in B \setminus \{0\}$, the ideal (x) factors as some product of prime ideals of B. Let $v_\mathfrak{p}(x)$ be the exponent of $\mathfrak{p}$ in this factorisation, which is a nonnegative integer. Then for an element $x/y \in \mathrm{Frac}(B)^*$, we define

$$v_\mathfrak{p}(x/y) = v_\mathfrak{p}(x) - v_\mathfrak{p}(y).$$

This is well-defined because if we choose a different representative $x'/y' = x/y$ then $x'y = xy'$, so $v_\mathfrak{p}(x') + v_\mathfrak{p}(y) = v_\mathfrak{p}(x) + v_\mathfrak{p}(y')$. Also, this valuation is surjective, since by uniqueness of prime factorisation we have $\mathfrak{p}^n \setminus \mathfrak{p}^{n+1}$ nonempty for any positive integer n. Note that $v_\mathfrak{p}(x) \geq 0$ if $x \in B$, and if $v_\mathfrak{p}(x) = 0$ then $x \notin \mathfrak{p}$. This motivates our next definition.

Definition 2.3. Let v be a non-trivial valuation of a field L. Define

$$\mathcal{O}_v = \{x \in L^* \mid v(x) \geq 0\} \sqcup \{0\}, \qquad \text{and} \qquad \mathcal{M}_v = \{x \in L^* \mid v(x) > 0\} \sqcup \{0\}.$$

One can show that $\mathcal{O}_v$ is a local principal ideal domain and $\mathcal{M}_v$ is its unique maximal ideal. Let $k_v := \mathcal{O}_v/\mathcal{M}_v$ be the residue field.

For us, a complete nonsingular curve will have as its points the elements of $\mathcal{V}(L/k)$, endowed with the cofinite topology. These correspond to the closed points in the usual scheme definition.

Definition 2.4. Fix a base field k. A *function field* L/k is a field extension of transcendence degree 1, such that every element of L which is algebraic over k lies in k itself. That is, k is algebraically closed in L.

Definition 2.5. Let k be a field. A *nonsingular complete curve* X/k *over* k is the set $\mathcal{V}(k(X)/k)$ endowed with the cofinite topology, where $k(X)$ is a field of transcendence degree 1 over k. Then $k(X)$ is the field of *rational functions* on X.

We think of the space geometrically, so an element p of X is called a *point*, and the corresponding valuation is denoted v_P. Think of $\mathcal{O}_p := \mathcal{O}_{v_P}$ as the functions defined at p, and $\mathcal{M}_p := \mathcal{M}_{v_p}$ as the functions vanishing at p. An element $\alpha \in k(X) \setminus \mathcal{O}_p$ is a rational function with a pole at p. The integer $v_p(\alpha)$ is the *order of vanishing* of α at p, and is negative when α has a pole at p.

The *domain* of a function $\alpha \in k(X)$ is the set of points p where α doesn't have a pole. For an open set $U \subset X$ let $\mathcal{O}_X(U) = \bigcap_{p\in U} \mathcal{O}_p$. This is the set of functions defined everywhere on U. Then $\mathcal{O}_X$ is a sheaf on X, called the structure sheaf, whose stalks are regular, given by $\mathcal{O}_p$. A *global section* is an element of $\mathcal{O}_X(X)$, that is a rational function defined everywhere on X.

We will require the additional hypothesis that $\mathcal{O}_X(X) = k$, that so the only globally-defined functions are the constants. This condition ensures that L/k is a function field[1].

Complete nonsingular curves will be our main object of study. Before discussing line bundles on these spaces in the next section, we would like to develop the analogy between such spaces and compact Riemann surfaces. As an easy first observation, every nonsingular complete curve has dimension 1, just as a Riemann surface is a 1-dimensional complex manifold.

A rational function on a nonsingular complete curve is the same animal as a meromorphic function on a compact Riemann surface. Its domain is an open set, whose complement is finite and in particular discrete. The global sections are the equivalent of holomorphic functions, since these are precisely the rational functions which are defined everywhere. By assumption, the only holomorphic functions are the constants, that is elements of the base field k. This hypothesis serves the same purpose as compactness for Riemann surfaces. One can also show that any rational function on a complete nonsingular curve must have the same number of zeroes as poles, counting multiplicity in a sense to be made precise in Section 3.

In fact, every Riemann surface can be realised as a complete nonsingular curve, in the sense that the meromorphic functions over any open set agree with those on the Riemann surface, although the analtic topology of the Riemann surface is of course much finer. This realisation even captures the structure of the group of line bundles (invertible sheaves) over the surface.

Example 2.6 ($\mathbb{P}^1(\mathbb{C})$ as a nonsingular complete curve)**.** Take the nonsingular complete curve X defined by $k(x)/k$, so $k(X) = k(x)$ is the transcendental field in one variable. We have a valuation v_∞ given by degree, so that $v_\infty(f/g) = \deg(g) - \deg(f)$ for two polynomials $f, g \in k[x]$. One can show that all the surjective valuations trivial on k except v_∞ are valuations at maximal ideals in the ring $k[x]$, so they correspond to irreducible monic polynomials $f \in k[x]$. In particular, if k is algebraically closed then all irreducible polynomials are linear, so X is in bijection with $k \sqcup \{\infty\}$.

When $k = \mathbb{C}$, this tells us that X is in bijection with the Riemann sphere. But we get much more than a bijection as sets. The field of rational functions is $k(x)$, consisting of global quotients of polynomials, and the meromorphic functions of the usual Riemann sphere have exactly this form. Moreover, if we exclude v_∞, then the points of X are in bijection with $\mathbb{C}$, and the set of globally defined functions is $\mathcal{O}_X(X \setminus \{\infty\}) = k[x]$. This is because a function defined at v_{x-z} must have nonnegative valuation there, meaning $x - z$ doesn't appear in the denominator. Hence the functions defined on $X \setminus \{\infty\}$ can have no linear factors in their denominator, so are polynomials.

We can realise an elliptic curve (over $\mathbb{C}$) in a similar way. Given an equation of the form $w^2 = f(z)$ defining the elliptic curve, where $f(z)$ is a monic cubic equation, we take the nonsingular complete curve X with rational functions $\mathrm{Frac}(\mathbb{C}[w, z]/(w^2 - f(z)))$. This simply encodes algebraically the fact that we want points (w, z) which are solutions to the equation $w^2 = f(z)$. This field has transcendence degree 1 over $\mathbb{C}$ because it is a finite extension of $\mathbb{C}(w)$. Points on X corresponding to maximal ideals $(w - c_0, z - c_1)$ of $\mathbb{C}[w, z]$ where $c_0^2 = f(c_1)$ form a dense open subset of X, whose complement is finite. One can think of the complement as the points needed to compactify the curve — these are the points lying in the projective closure of the points corresponding to maximal ideals.

From now on, the term *curve* refers to a nonsingular complete curve, to avoid carying these qualifiers around with us.

3. Divisors and the Picard Group

As in the case of Riemann surfaces, the group of divisors of a curve is the free abelian group on the points. We denote this group $\mathrm{Div}(X/k)$ or $\mathrm{Div}(L/k)$, where $L = k(X)$ is the field defining the curve X. This is also

[1]Any valuation trivial on k must be trivial on any element of L which is algebraic over k, so any element of L algebraic over k lies in $\mathcal{O}_X(X) = k$.

the free abelian group on the set of valuations $\mathcal{V}(L/k)$. We call a divisor *effective* if all its coefficients are nonnegative. We get a divisor corresponding to any rational function, which we call *principal*, and which has coefficients given by the order of the pole of the rational function at each point. However, defining the degree of a divisor is more complicated than in the Riemann surface case — points have an associated degree, coming from the degree of a particular field extension, and we need to weight our computation of the degree of a divisor by the degrees of the points with nonzero coefficients.

We obtain a principal divisor from a rational function in L^* via the following map, which sends each rational function to a finite sum of points by Proposition VII.4.11 in [1].

$$\begin{aligned} \mathrm{div} : L^* &\to \mathrm{Div}(L/k) = \mathrm{Div}(X/k) \\ f &\mapsto \mathrm{div}(f) := -\sum_{v \in \mathcal{V}(L/k)} v(f) x_v \end{aligned}$$

where $x_v \in X$ is the point corresponding to the valuation v.

It follows that $\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g)$, so this map is a group homomorphism. We now take the Picard group to be divisors modulo principal divisors, as in the case of a Riemann surface.

Definition 3.1. Let L/k be a field extension of transcendence degree 1. The *Picard group*, denoted $\mathrm{Pic}(L/k)$, is the quotient of the group of divisors by the subgroup of principal divisors. We call the quotient map $\mathrm{cl} : \mathrm{Div}(L/k) \to \mathrm{Pic}(L/k)$. We thus have the following exact sequence:

$$0 \to \cap_{v \in \mathcal{V}(L/k)} \mathcal{O}_v^* \to L^* \overset{\mathrm{div}}{\to} \mathrm{Div}(L/k) \overset{\mathrm{cl}}{\to} \mathrm{Pic}(L/k) \to 0. \tag{3.1}$$

Two divisors are called *linearly equivalent* if they are identified in the Picard group.

When we consider the curve X corresponding to a field extension L/k as in the previous definition, we have by hypothesis that the global sections are precisely k. So writing $\mathrm{Pic}(X/k) = \mathrm{Pic}(L/k)$ and $L = k(X)$, the above sequence becomes

$$0 \to k^* \to k(X)^* \overset{\mathrm{div}}{\to} \mathrm{Div}(X/k) \overset{\mathrm{cl}}{\to} \mathrm{Pic}(X/k) \to 0. \tag{3.2}$$

In the context of algebraic geometry, the Picard group of a space is usually defined to be the quotient of the group of *locally* principal divisors by the principal divisors, so that each equivalence class of divisors represents an isomorphism class of line bundles on the space. For nonsingular complete curves, every divisor is locally principal, so the definition we have given is equivalent to the usual one. Hence the Picard group of a curve is the group of line bundles. The map cl is a group homomorphism, with addition of divisors corresponding to tensoring line bundles.

We next consider degree. Over a Riemann surface, the degree of a divisor is taken to be the sum of the coefficients. We will need a more sophisticated definition when working over a field k which is not algebraically closed. We define the degree of a divisor which consists of a single point, and extend linearly.

Definition 3.2. Let $p \in X/k$ be a point in a curve. Let v be the valuation associated to p, with residue field $k_v = \mathcal{O}_v/\mathcal{M}_v$. Then k_v/k is a finite[2] extension of fields, and we define $\deg(p) = [k_v : k]$. More generally,

$$\deg\left(\sum_i a_i p_i\right) = \sum_i a_i \deg(p_i) = \sum_i a_i [k_{v_i} : k].$$

This definition agrees with the usual definition over a Riemann surface, since $\mathbb{C}$ is algebraically closed so it has no nontrivial finite extensions. We state a few useful facts about the divisor and Picard groups.

Theorem 3.3 ([1], Thm VII.7.9). *Let k be a field and X/k a curve. For any $\alpha \in k(X)^*$, we have* $\deg(\mathrm{div}(\alpha)) = 0$.

As in the case of Riemann surfaces, the divisor corresponding to any rational function has degree 0. In particular, any global section (which has no poles) has no zeroes, and therefore the divisor corresponding to any global section is trivial. This justifies why the first term in each of (3.1) and (3.2) is the kernel of the map div.

It also follows from Theorem 3.3 that the degree of an element of the Picard group is well-defined, since any two divisors in the same class differ by a principal divisor, which has degree 0. In fact, we obtain a group homomorphism

$$\deg : \mathrm{Pic}(X/k) \to \mathbb{Z}, \mathrm{cl}(D) \mapsto \deg(D)$$

which is nontrivial because $\mathrm{Div}(X/k)$ contains some nontrivial effective divisors. But a nontrivial map to $\mathbb{Z}$ has infinite image, and so the Picard group must be infinite. We prefer working with finite groups, which motivates the following definition.

[2]See Corollary 10.11 in [1].

Definition 3.4. Let X/k be a curve. Define $\mathrm{Div}^0(X/k)$ to be the kernel of the degree map on Div, and $\mathrm{Pic}^0(X/k)$ to be the kernel of the degree map on line bundles. So $\mathrm{Pic}^0(X/k)$ consists of all the degree zero classes of divisors. It follows that the following sequence is exact.

$$0 \to k^* \to k(X)^* \to \mathrm{Div}^0(X/k) \overset{\mathrm{cl}}{\to} \mathrm{Pic}^0(X/k) \to 0.$$

In particular, the degree 0 divisors surject onto the degree 0 line bundles. To conclude this section, we discuss a result specific to the case where k is a finite field. This is a corollary of Riemann-Roch, which we prove in the next section.

Theorem 3.5 ([1], Thm VII.7.13)**.** *Let k be a finite field and X/k a curve. Then $\mathrm{Pic}^0(X/k)$ is finite.*

Proof sketch. Let $d \in \mathbb{N}$ and $\mathrm{Pic}^d(X/k)$ be the divisor classes of degree d. This is one of the cosets of the kernel of the map deg, so in particular has the same cardinality as $\mathrm{Pic}^0(X/k)$. So it is enough to show $\mathrm{Pic}^d(X/k)$ is finite for some large enough d.

Consider the set of effective divisors of degree d, which we denote $\mathrm{Eff}^d(X/k)$, and the restriction of the class map

$$\mathrm{cl}^d : \mathrm{Eff}^d(X/k) \to \mathrm{Pic}^d(X/k).$$

It follows from Riemann-Roch that if d is large enough, then cl^d is surjective. See Remark 4.3. Hence it is enough to show that for large enough d, the set $\mathrm{Eff}^d(X/k)$ is finite.

But in fact, $\mathrm{Eff}^d(X/k)$ is finite for all positive d. An effective divisor D of degree d must have the form $\sum_i a_i \deg(p_i)$ for positive coeffients a_i, and so in particular must have all $|k_{v_i}| < \deg(p_i) \leq d$. We conclude the proof by noting that there are finitely many valuations $v \in \mathcal{V}(L/k)$ such that $|k_v| \leq d$, when k is a finite field. ☐

When k is a finite field, the number $|\mathrm{Pic}^0(X/k)|$ is called the *class number* of the field $k(X)/k$ or of the curve X.

4. Riemann-Roch and Genus

As in the case of Riemann surfaces, the Riemann-Roch theorem provides an answer to the question of when it is possible to find a rational function on a curve X/k with poles and zeroes as specified by a divisor. To make this precise, we need a notion of genus for a curve over any field k, where we do not necessarily have a definition of topological genus.

We have a natural partial order relation on $\mathrm{Div}(X/k)$, where $D' \geq D$ if each coefficient of D' is at least the corresponding coefficient of D. Then we define

$$H^0(D) = \{\alpha \in k(X) \mid \mathrm{div}(\alpha) \leq D\}.$$

In particular, for any nonzero $\alpha \in H^0(D)$ the divisor $D - \mathrm{div}(\alpha) \geq 0$ is effective. This means that if $H^0(D)$ contains at least one nonzero rational function, then $\mathrm{cl}(D)$ is represented by an effective divisor. As is the case for compact Riemann surfaces, it follows from the definitions that $H^0(D) = 0$ for a divisor D of negative degree.

We next consider the vector spaces

$$\mathcal{L}(D)_p = \{\alpha \in k(X) \mid v_p(\alpha) \geq -\mathrm{ord}_p(D)\}$$

for each point $p \in X$, where $\mathrm{ord}_p(D)$ is the coefficient of the point p in D. An element of $H^0(D)$ satisfies this inequality at every point $p \in X$, so is zero in the quotient $k(X)/\mathcal{L}(D)_p$, for every p. This motivates the following definition. Consider the map

$$\begin{aligned} \phi_D : k(X) &\to \bigoplus_{p \in X} (k(X)/\mathcal{L}(D)_p) \\ f &\mapsto \bigoplus_{p \in X} (f \mod \mathcal{L}(D)_p). \end{aligned}$$

Then the kernel of this map is $H^0(D)$, and to extend to an exact sequence we define $H^1(D)$ to be the cokernel. We get an exact sequence

$$0 \to H^0(D) \to k(X) \overset{\phi_D}{\to} \bigoplus_{p \in X} k(X)/\mathcal{L}(D)_p \to H^1(D) \to 0. \tag{4.1}$$

One can show that linearly equivalent divisors D, D' with $D' = D + \mathrm{div}(\alpha)$ satisfy $H^0(D) \cong H^0(D')$ and $H^1(D) \cong H^1(D')$, with the isomorphisms induced between the sequences (4.1) for D and D' by multiplication by α on $k(X)$. Hence these definitions make sense on the Picard group. Before discussing Riemann-Roch, we indulge a brief digression to relate (4.1) to sheaf cohomology of the corresponding element of the Picard group, $\mathrm{cl}(D)$.

On the Picard group, the groups $H^0(D)$ and $H^1(D)$ become the sheaf cohomology of the invertible sheaf corresponding to $\mathrm{cl}(D)$, which we denote $\mathcal{L}(D)$. These are the only nonzero cohomology groups, since X has dimension 1.

The invertible sheaf $\mathcal{L}(D)$ is defined on the open set $U \subset X$ by

$$\mathcal{L}(D)(U) = \{\alpha \in k(X) \mid v_p(\alpha) \geq -\operatorname{ord}_p(D) \ \forall\, p \in U\}$$

and the vector spaces $\mathcal{L}(D)_p$ we defined previously are the stalks of this sheaf. By comparing the two definitions, we can see that the global sections are

$$H^0(X, \mathcal{L}(D)) = \mathcal{L}(D)(X) = H^0(D).$$

Let C denote the constant sheaf on X, whose sections over any open set are $k(X)$. Then we have a short exact sequence

$$0 \to \mathcal{L}(D) \to C \to C/\mathcal{L}(D) \to 0$$

coming from the natural inclusion $\mathcal{L}(D) \hookrightarrow C$. The long exact sequence on cohomology induced from this simplifies to

$$0 \to H^0(X, \mathcal{L}(D)) \to k(X) \to H^0(X, C/\mathcal{L}(D)) \to H^1(X, \mathcal{L}(D)) \to 0 \tag{4.2}$$

after noting that $H^0(X, C) = k(X)$ and $H^1(X, C) = 0$. Then (4.1) and (4.2) are naturally isomorphic. One gets that both $H^0(D)$ and $H^1(D)$ are finite-dimensional k-vector spaces.

Definition 4.1. Let D be a divisor on a curve X/k. Then $h^0(D) := \dim H^0(D)$ and $h^1(D) := \dim H^1(D)$. The genus $g = g(X)$ of the curve X is defined to be $h^1(X, \mathcal{O}_X) = h^1(0)$.

We are now in a position to state the Riemann-Roch Theorem for nonsingular complete curves.

Theorem 4.2 (Riemann-Roch, see [1] Thm IX.3.8)**.** *Let X/k be a curve. Then for every divisor $D \in \mathrm{Div}(X/k)$,*

$$h^0(D) = \deg(D) + 1 - g(X) + h^1(D). \tag{4.3}$$

Remark 4.3. Since $h^1(D)$ is the dimension of a vector space, it is in particular nonnegative, so we obtain the inequality $h^0(D) \geq \deg(D) + 1 - g(X)$. This means that for any divisor D of large enough degree, the space $H^0(D)$ has positive dimension and must contain some nonzero rational function. But as mentioned previously, for such a rational function α the divisor $D - \mathrm{div}(\alpha)$ is effective and linearly equivalent to D, of the same degree as D. Hence the class map on effective divisors of degree d is surjective, for any $d \geq g(X)$.

Rearraging (4.3), we obtain that for any divisor D,

$$h^0(D) - h^1(D) - \deg(D) = 1 - g(X). \tag{4.4}$$

In particular, the left hand side is independent of the choice of divisor. In the special case where $D = 0$ is the trivial divisor, we have $h^0(0) = 1$, $g(X) = h^1(0)$ and $\deg(0) = 0$ by definition. So (4.4) holds for $D = 0$. Then it's enough to show that the LHS of (4.4) is independent of choice of D. The following proof is based on [2], Theorem IV.1.3.

Proof. Consider, for any point $p \in X$, the short exact sequence of sheaves on X/k

$$0 \to \mathcal{L}(D) \to \mathcal{L}(D + p) \to k_{v_p}(p) \to 0$$

where $k_{v_p}(p)$ is the skyscraper sheaf at the point p. Because sheaves on X have no higher cohomology, the Euler characteristic is given by $h^0 - h^1$ in each case. But Euler characteristic is additive on short exact sequences, so

$$h^0(D) - h^1(D) + \chi(k_{v_p}(p)) = h^0(D + p) - h^1(D + p).$$

Now the Euler characteristic of a skyscraper sheaf equals h^0, which in this case is $\dim_k(k_{v_p}) = \deg(p)$. Thus $\chi(D) + \deg(p) = \chi(D + p)$. We also have $\deg(D + p) = \deg(D) + \deg(p)$, and hence

$$\chi(D) - \deg(d) = \chi(D + p) - \deg(D + p)$$

so the LHS of (4.4) does not change when we add or subtract a point from the divisor D. But we can get from any divisor to any other by adding and subtracting a finite set of points, so (4.4) does not depend on the divisor D. □

5. Serre Duality and the Canonical Divisor

When X is a Riemann surface, the space $H^1(D)$ is not just a vector space — it can be realised as $H^0(X, \mathcal{K} \otimes \mathcal{L}(-D))^\vee$ where $\mathcal{K}$ is the sheaf of holomorphic 1-forms on X. Without the differential structure of a Riemann surface it is somewhat difficult to define the sheaf $\mathcal{K}$ directly for a general curve X. In this section we will construct a divisor $K \in \mathrm{Div}(X/k)$ having the property that $H^1(D)^\vee \cong H^0(K-D)$ for any divisor D. This gives a corresponding sheaf $\mathcal{L}(K)$ with the desired duality property. The invertible sheaf $\mathcal{L}(K)$ is the *canonical bundle* of the curve X, and as in the Riemann surface case it follows from Riemann-Roch that it must have degree $2g(X)-2$, and $h^0(K) = g(X)$.

Theorem 5.1 (Serre duality, [1] Thm IX.4.1)**.** *Let k be a field, and X/k a curve. There exists a divisor $K \in \mathrm{Div}(X/k)$ having the property that $H^1(D)^\vee \cong H^0(K-D)$ for every divisor D.*

Any such divisor K is called a *canonical divisor* of the curve X, and its class in $\mathrm{Pic}(X/k)$ is the *canonical divisor class.*

To prove Serre duality, we use the k-vector spaces $H^1(D)^\vee, D \in \mathrm{Div}(X)$ to define a $k(X)$-vector space J, the so-called space of differentials on X. To construct this space, we first need a few preliminary notions.

For two divisors D, E we define their *gcd* to be the divisor which has as its coefficients the minimum of the corresponding coefficients for D and E. Similarly, we define the *lcm* to be the pointwise maximum of the coefficients.

Whenever $E \leq D$, we get a corresponding map on cohomology $\phi_{E,D} : H^1(E) \to H^1(D)$ in a natural way. This induces a dual map $\phi_{E,D}^\vee : H^1(D)^\vee \to H^1(E)^\vee$. Moreover, for $\alpha \in k(X)^*$, there is an isomorphism $\phi_\alpha^D : H^1(D - \mathrm{div}(\alpha)) \xrightarrow{\sim} H^1(D)$ induced from multiplication by α, for any divisor D. This gives a dual isomorphism $(\phi_\alpha^D)^\vee : H^1(D)^\vee \xrightarrow{\sim} H^1(D - \mathrm{div}(\alpha))^\vee$.

We then consider the category whose objects are groups $H^1(D)^\vee$ for some divisor D, and whose morphisms are maps $\phi_{E,D}^\vee$ when $E \leq D$. In this category, *gcd* is a pullback and *lcm* is a pushout. Let J be the additive group that is obtained by taking the filtered colimit over this category. As a set J is a disjoint union of the groups $H^1(D)^\vee$, modulo the equivalence relation that elements $\lambda_1 \in H^1(D_1)$ and $\lambda_2 \in H^1(D_2)$ are equal whenever there exists some divisor C with $C \leq D_1, D_2$ such that

$$(\lambda_1 \circ \phi_{C,D_1} =)\phi_{C,D_1}^\vee(\lambda_1) = \phi_{C,D_2}^\vee(\lambda_2)(= \lambda_2 \circ \phi_{C,D_2}).$$

To add two elements $j_1, j_2 \in J$, pick a divisor corresponding to each so that $j_i \in H^1(D_i)^\vee$. Then for any divisor $C \leq D_1, D_2$ we set $j_1 + j_2 = j_1 \circ \phi_{C,D_1} + j_2 \circ \phi_{C,D_2}$. We could for example choose $C = gcd(D_1, D_2)$, but any choice of C gives a result equivalent in J.

Finally, J has a natural $k(X)$-vector space structure coming from the maps ϕ_α^D. Define $\alpha \cdot j$ to be the functional $\lambda \circ \phi_\alpha^D$, with $\lambda \in H^1(D)^\vee$ any representative for $j \in J$.

Lemma 5.2 ([1], Thm IX.4.5)**.** *J is a $k(X)$-vector space of dimension 1.*

Using the space J, we can construct the class in $\mathrm{Pic}(X/k)$ of the canonical divisor as follows.

Theorem 5.3 ([1], Thm IX.4.6)**.** *Let k be a field, X/k a curve. For any nonzero $j \in J$, there exists a divisor $K(j) \in \mathrm{Div}(X/k)$ satisfying:*

(i) j can be represented by $\lambda \in H^1(K(j))^\vee$;

(ii) $K(j)$ is maximal with this property, meaning that for any E satisfying (i), $K(j) \geq E$.

Moreover, for $\alpha \in k(X)^*$ we have $K(\alpha j) = K(j) + \mathrm{div}(\alpha)$, and the class $K(j)$ in $\mathrm{Pic}(X)$ is independent of choice of j. This is the canonical class of X.

Proof sketch. Let $j \in J$.

First, one shows that $h^1(0) \geq h^0(D)$ for any such divisor D, by showing that a basis for $H^0(D)$ gives rise to a linearly independent set in $H^1(0)^\vee$. Then by Riemann-Roch,

$$\deg(d) \leq h^0(D) + g - 1 \leq 2g - 1$$

since $h^1(0) = g$. Hence the divisors satisfying (i) are bounded in degree, so choose D to have maximal degree among such divisors.

Next, one shows that if D and E satisfy (i) then so must $gcd(D,E)$ and $lcm(D,E)$. But since D has maximal degree among divisors satisfying (i), and $\deg(lcm(D,E)) \geq \deg(D)$, we find that $D = lcm(D,E)$. In particular, $D \geq E$. Therefore D satisfies both (i) and (ii). Note that this argument shows there is a unique divisor of maximal degree satisfying (i).

Since $\lambda \in H^1(K(j))^\vee$ representing j gives a map $\alpha \cdot \lambda \in H^1(K(j) - \mathrm{div}(\alpha))^\vee$ representing αj by the $k(X)$-action, we have by (ii) that $K(\alpha j) \geq K(j) - \mathrm{div}(\alpha)$. Applying the same argument to α^{-1} gives equality.

Now since J has dimension 1, any two elements j, j' differ by scalar multiplication, giving $j' = \alpha j$. Hence $K(j') = K(j) - \mathrm{div}(\alpha)$ and so any two such divisors lie in the same class in $\mathrm{Pic}(X/k)$. This gives a well-defined canonical class, independent of j. ∎

Serre duality follows directly from this theorem, with any choice of $K = K(j)$.

Proof of Serre duality, Theorem 5.1. Let $D \in \mathrm{Div}(X)$, and fix nonzero $j \in J$. Set $K := K(j)$. We show that the map

$$\delta : H^0(D) \to \mathrm{Hom}_k(H^1(K-D), H^1(K))$$
$$\alpha \mapsto \phi_\alpha^K \circ \phi_{K-D,K-\mathrm{div}(\alpha)} \qquad \text{for } \alpha \neq 0$$

is an isomorphism. First, this is well-defined since for $\alpha \in H^0(D)$ we have $\mathrm{div}(\alpha) \leq D$ and so $K - \mathrm{div}(\alpha) \geq K - D$. Then we are simply taking the composition

$$H^1(K-D) \xrightarrow{\phi_{K-D,K-\mathrm{div}(\alpha)}} H^1(K-\mathrm{div}(\alpha)) \xrightarrow{\phi_\alpha^K} H^1(K)$$

Assuming for now that δ is an isomorphism, take $D = 0$. This gives

$$H^0(0) \xrightarrow{\sim} \mathrm{Hom}_k(H^1(K), H^1(K))$$

and so we conclude that $h^1(K) = 1$, because $h^0(0) = 1$. Now for any D, we can identify $\mathrm{Hom}_k(H^1(K-D), H^1(K))$ with $H^1(K-D)^\vee$. Explicitly, we do this by postcomposing with a fixed $\lambda \in H^1(K)^\vee$. Then setting $D = K - D'$, we have an isomorphism

$$H^0(K-D') \xrightarrow{\sim} \mathrm{Hom}_k(H^1(D'), H^1(K)) \cong H^1(D')^\vee$$

and so $H^0(K-D') \cong H^1(D')$ for every $D' \in \mathrm{Div}(X/k)$.

So it's enough to show that δ is an isomorphism. Let $\lambda \in H^1(K)$ represent j. For injectivity, suppose $\delta(\alpha) = 0$. If $\alpha \neq 0$, we have

$$0 = \lambda \circ \delta(\alpha) = \lambda \circ \phi_\alpha^K \circ \phi_{K-D,K-\mathrm{div}(\alpha)}$$

and by the equivalence relation on J, this means $\alpha \cdot j = \lambda \circ \phi_\alpha^K = 0$ in J. But this implies $\alpha = 0$, because j is nonzero.

For surjectivity, let $\psi \in \mathrm{Hom}_k(H^1(K-D), H^1(K))$ be nonzero, and then $\lambda \circ \psi \in H^1(K-D)^\vee$. Because J is 1-dimensional, there exists $\alpha \in k(X)^*$ with $\alpha\lambda = \lambda \circ \psi \in J$. We know $K - \mathrm{div}(\alpha)$ is the maximal divisor which represents $\alpha\lambda$, so we must have $K - D \leq K - \mathrm{div}(\alpha)$ because $K - D$ also represents $\alpha\lambda$. Hence $\alpha \in H^0(D)$, and moreover

$$\lambda \circ \psi = \lambda \circ \phi_\alpha^K \circ \phi_{K-D,K-\mathrm{div}(\alpha)}.$$

Thus $\psi = \delta(\alpha)$ lies in the image. □

We know already that for any canonical divisor K we must have $\deg(K) = 2g-2$ and $h^0(K) = g$. But in fact, these two properties fully characterise canonical divisors.

Lemma 5.4 ([1], Thm IX.5.10)**.** *Let X/k be a curve of genus g, and $D \in \mathrm{Div}(X/k)$ be such that* $\deg(D) = 2g-2$ *and $h^0(D) = g$. Then D is a canonical divisor.*

Proof. Let K be a canonical divisor, so $h^0(D) = \deg(D) + 1 - g + h^0(K-D)$. From the hypotheses, we must have $h^0(K-D) = 1$. Choose nonzero $\alpha \in h^0(K-D)$, so that $K - D - \mathrm{div}(\alpha) \geq 0$. The degrees of both sides are equal, so this must be an equality, and hence $K - D = \mathrm{div}(\alpha)$ is principal. So D lies in the canonical divisor class. □

6. References

[1] D. Lorenzini, *An invitation to arithmetic geometry*, vol. 9. American Mathematical Society, 1996.
[2] R. Hartshorne, *Algebraic geometry*, vol. 52. Springer Science & Business Media, 2013.
[3] R. Vakil, "The rising sea: foundations of algebraic geometry," *preprint*, 2017.