Riemann-Roch Theorem - from the perspective of plane algeraic curves

David Gu

Computer Science Department
Stony Brook University

gu@cs.stonybrook.edu

September 24, 2023

Basic Concepts

Definition (Rings)

A ring is a set R equipped with two binary operations "$+$" and "$\cdot$" satisfying:

1. R is an Abelian group under "$+$";
2. "$\cdot$" is associate: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $\forall a, b, c \in R$, $\exists 1 \in R$, such that $a \cdot 1 = a$, $1 \cdot a = a$, $\forall a \in R$;
3. "$+$" is distributive with "$\cdot$":

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \quad \forall a, b, c \in R$$
$$(b + c) \cdot a = (b \cdot a) + (c \cdot a)$$

Definition (ideals)

A subset I of $(R, +, \cdot)$ is a left idea of R if

1. $(I, +)$ is a subgroup of $(R, +)$
2. $\forall r \in R, x \in I$, $rx \in I$

A subset I of $(R, +, \cdot)$ is a right ideal of R if

1. $(I, +)$ is a subgroup of $(R, +)$
2. $\forall r \in R, x \in I$, $xr \in I$

A two-sided idea is a left ideal that is also a right ideal.

Quotient Ring R/I

We first define $\sim$ on R as follows:

$$a \sim b \text{ iff } a - b \in I \quad \forall a, b \in R$$

Actually, $\sim$ is an equivalence relation, since

$$a \sim a, a \sim b \iff b \sim a, a \sim b \& b \sim c \implies a \sim c.$$

The equivalence class of $a \in R$ is

$$[a] = a + I := \{a + r : r \in I\}$$

Quotient Ring R/I

Definition (Quotient Ring)

R/I is the set of all equivalence classes,

$$R/I = \{[a] : a \in R\}$$

R/I becomes a ring under the addition and multiplication defined below:

$$\text{addtion:} \quad (a+I)+(b+I) = (a+b)+I$$

$$\text{multiplication:} \quad (a+I)\cdot(b+I) = ab+I$$

They are both well defined

$$a \sim a', b \sim b' \implies (a+b)+I = (a'+b')+I, \quad ab+I = a'b'+I$$

- "0" in R/I is $\bar{0} = 0 + I = I$;
- "1" in R/I is $\bar{1} = 1 + I$

Affine Varieties

Definition (Affine Varieties)

Suppose K is a field, $K[x_1, \dots, x_n]$ the polynomial ring in variables $x_1, x_2, \dots, x_n$,

1. For $n \in \mathbb{N}$, we call $\mathbb{A}^n := \mathbb{A}^n_K := K^n$ the affine n-space over K
2. For a subset $S \subset K[x_1, \dots, x_n]$ of polynomials, we call

$$V(S) := \{p \in \mathbb{A}^n : f(p) = 0 \ \forall f \in S\} \subset \mathbb{A}^n$$

   the the affine zero locus of S. Subsets of $\mathbb{A}^n$ of this form are called Affine varienties.

Affine Curves

Definition (Affine Curves)

1. An affine plane algebraic curve (over K) is a non-constant polynomial $F \in K[x, y]$ modulo units, i.e. modulo the equivalence relation $F \sim G$ if $F = \lambda G$ for some $\lambda \in K^*$. We call

$$V(F) := \{p \in \mathbb{A}^2 : F(p) = 0\}$$

   the set of points of F.

2. The degree of a curve is its degree as a polynomial.

3. A curve F is called irreducible if it is as a polynomial, and reducible otherwise. If $F = F_1^{a_1} \cdots F_k^{a_k}$ is the irreducible decomposition of F as a polynomial, we will also call this the irreducible decomposition of the curve F. The curves $F_1, \dots, F_k$ are then called the irreducible components of F and $a_1, \dots, a_k$ their multiplicities. A curve F is called reduced if all its irreducible components have multiplicity 1.

Plane Projective Curve

Projective Spaces

Field K is algebraically closed. F is a smooth and irreducible curve over K.

Definition (Projective Spaces)

For $n \in \mathbb{N}$, the projective n-space over K

$$\mathbb{P}^n = \{\text{1-dimensional linear subspaces of } K^{n+1}\}$$

$\mathbb{P}^n = (K^{n+1} \setminus \{0\})/\sim,$

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff x_i = \lambda y_i \quad \text{for some } \lambda \in K^* \text{and all } i$$

We denote the equivalence class of $(x_0, \dots, x_n)$ by $(x_0 : x_1 \dots x_n)$. We call $x_0, \dots, x_n$ the homogenous or projective coordinates of the point $(x_0 : x_1 \dots x_n)$.

Projective Spaces

$\mathbb{P}^n$ is the compactification of $\mathbb{A}^n$ ($\mathbb{A}^n := K^n$)

$$\mathbb{P}^n = \mathbb{S}^n / \sim \quad \mathbb{S}^n = \{(x_0, \dots, x_n) \in K^{n+1} : |x_0|^2 + \cdots |x_n|^2 = 1\}$$

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n) \iff x_i = -y_i$$

Example

$$\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$$
$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$$
$$\mathbb{P}^{n+1} = \mathbb{A}^{n+1} \cup \mathbb{P}^n$$

$[x_0 : x_1 : x_2] \in \mathbb{P}^2$, if $x_0 = 0$ and $(x_1, x_2) \neq (0, 0)$, then $[0 : x_1 : x_2] \in \mathbb{P}^1$; if $x_0 \neq 0$, $[1 : \frac{x_1}{x_0} : \frac{x_2}{x_0}] \in \mathbb{A}^2$. Hence $\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1$.

Projective Varieties

Let $f = \sum_{i_0+\cdots+i_n=d} a_{i_0\dots i_n} x_0^{i_0}\dots x_n^{i_n} \in K[x_0,\dots,x_n]$ be homogeneous of degree d.

1. f is not a well-defined function on $\mathbb{P}^n$. For example on $\mathbb{P}^1$, $f(x_0,x_1) = x_0 + x_1$, $[1:1] = [2:2]$, but $f(1,1) = 2 \neq f(2,2) = 4$. Its zero locus is well defined on $\mathbb{P}^n$, since

$$f(\lambda x_0,\dots,\lambda x_n) = 0 \iff f(x_0,\dots,x_n) = 0, \quad \forall \lambda \in K^*$$
$$f(\lambda x_0,\dots,\lambda x_n) = \lambda^d f(x_0,\dots,x_n)$$

2. If g is another homogenous polynomial of degree d

$$\frac{f(\lambda x_0,\dots,\lambda x_n)}{g(\lambda x_0,\dots,\lambda x_n)} = \frac{\lambda^d f(x_0,\dots,x_n)}{\lambda^d g(x_0,\dots,x_n)} = \frac{f(x_0,\dots,x_n)}{g(x_0,\dots,x_n)}$$

so $\frac{f}{g}$ is a well-defined function on the subset of $\mathbb{P}^n$ where g does not vanish.

Projective Varieties

Definition (Projective Varieties)

$\forall S \subset K[x_0, \dots, x_n]$ of homogeneous polynomials, we call

$$V(S) := \{p \in \mathbb{P}^n : f(p) = 0 \text{ for all } f \in S\} \subset \mathbb{P}^n$$

the (projective) zero locus of S. Subsets of $\mathbb{P}^n$ that of this form are called (projective) varieties.

Plane Projective Curve

Definition (Plane Projective Curve)

A (Projective plane algebraic) curve (over K) is a non-constant homogenous polynomial $F[x, y, z]$ modulo units (K^*). We call

$$V(F) = \{p \in \mathbb{P}^2 : F(p) = 0\}$$

its set of points.

Rational Function and Regular Function

Local ring of $\mathbb{A}^2$

Definition (Local ring of $\mathbb{A}^2$)

Let $p \in \mathbb{A}^2$ be a point.

1. The local ring of $\mathbb{A}^2$ at p is defined as
$$\mathcal{O}_p := \mathcal{O}_{\mathbb{A}^2,p} := \left\{ \frac{f}{g} : f,g \in K[x,y] \text{ with } g(p) \neq 0 \right\} \subset K(x,y).$$
2. It admits a well-defined ring homomorphism
$$\mathcal{O}_p \to K, \quad \frac{f}{g} \mapsto \frac{f(p)}{g(p)}$$
which we will call the evaluation map. Its kernel will be denoted by
$$I_p := I_{\mathbb{A}^2,p} := \left\{ \frac{f}{g} : f,g \in K[x,y] \text{ with } f(p) = 0 \text{ and } g(p) \neq 0 \right\} \subset \mathcal{O}_p.$$

The local ring $\mathcal{O}_p$ contains exactly one maximal ideal I_p.

$\mathbb{A}^2$ Intersection multiplicities

Definition (Intersection multiplicities)

Let $p \in \mathbb{A}^2$ and two curves (or polynomials) F and G we define the intersection multiplicity of F and G at p to be

$$\mu_p(F, G) := \dim \mathcal{O}_p / \langle F, G \rangle \quad \in \mathbb{N} \cup \{\infty\}.$$

$\mathbb{A}^2$ Intersection Multiplicity

Lemma

Let $p \in \mathbb{A}^2$, F and G be two curves (or polynomials). We have

1. $\mu_p(F,G) \geq 1$ *if and only if* $p \in F \cap G$;
2. $\mu_p(F,G) = 1$ *of and only if* $\langle F, G \rangle = I_p$ *in* $\mathcal{O}_p$.

Proof.

Assume first that $F(p) \neq 0$, then F is a unit in $\mathcal{O}_p$, and thus $\langle F, G \rangle = \mathcal{O}_p$, i.e. $\mu_p(F,G) = 0$. We then have $p \in F$ and $F \in I_p$. Similarly, $p \in G$. So we may now assume that $F(p) = G(p) = 0$, i.e. $p \in F \cap G$. Then the evaluatioin map at p induces a well-defined and surjective map $\mathcal{O}_p / \langle F, G \rangle \to K$. It follows that $\mu_p(F,G) \geq 1$, proving (a) is this case. More over, we have $\mu_p(F,G) = 1$ if and only if this map is an isomorphism i.e. if and only if $\langle F, G \rangle$ is exactly the kernel I_p of the evaluation map. □

$\mathbb{A}^2$ Affine coordinate rings

Definition (Affine Coordinate Rings)

Let F be a smooth an irreducible affine curve over algebraically closed field K, we all

$$A(F) := K[x, y]/\langle F \rangle$$

the affine coordinate ring of F.

Algebraic properties of $A(F)$:

1. As the curve F is assumed to be irreducible, the coordinate ring $A(F)$ is an integral domain: if $fg = 0 \in A(F)$, this means $F|fg$, hence $F|f$ or $F|g$, which means that $f = 0$ or $g = 0$ in $A(F)$.
2. The affine coordinate ring $A(F)$ is in general not a unique factorization domain.

$\mathbb{A}^2$ Rational functions and local rings

Definition (Rational functions and local rings)

Let F be a smooth an irreducible affine curve over algebraically closed field K,

1. The quotient field
$$K(F) := \left\{ \frac{f}{g} : f, g, \in A(F) \text{ with } g \neq 0 \right\}$$
of the coordinate ring is called the field of rational functions on F.
2. A rational function $\varphi K(F)$ is called regular at a point $p \in F$ if it can be written as $\varphi = \frac{f}{g}$ with $f, g \in A(F)$ and $g(p) \neq 0$. The regular function at p form a subring of $K(F)$ containing $A(F)$ denoted by
$$\mathcal{O}_{F,p} := \left\{ \frac{f}{g} : f, g \in A(F) \text{ with } g(p) \neq 0 \right\} \subset K(F)$$
This ring of regular functions at p is called the local ring of F at p.

Definition (Rational functions and local rings)

Let F be a smooth an irreducible affine curve over algebraically closed field K,

3. There is a well-defined evaluation map

$$\mathcal{O}_{F,p} \to K, \frac{f}{g} \mapsto \frac{f(p)}{g(p)}$$

which we will simply write as $\varphi \to \varphi(p)$ for $\varphi \in \mathcal{O}_{F,p}$, and whose kernel is

$$I_{F,p} := \left\{ \frac{f}{g} : f, g \in A(F) \text{ with } f(p) = 0 \text{ and } g(p) \neq 0 \right\}.$$

The local ring $\mathcal{O}_{F,p}$ contains exactly one maximal ideal $I_{F,p}$.

$\mathbb{A}^2$ Multiplicity for polynomial

Let p be a point on an affine curve F.

1. For a polynomial function $f \in A(F)$ we define its multiplicity at p to be
$$\mu_p(f) := \mu_p(F, f) = \dim \mathcal{O}_{\mathbb{A}^2, p} / \langle F, f \rangle \quad \in \mathbb{N} \cup \{\infty\}$$
Noe that this is well-defined since $f = g \in A(F)$ implies $g = f + hF$ for some polynomial h, then $\mu_p(F, f) = \mu_p(F, f + hF) = \mu_p(F, g)$. This multiplicity is ∞ if and only if f and F have a common component through p, i.e. (since F is irreducible) if and only if $f = 0 \in A(F)$.

$\mathbb{A}^2$ Multiplicity for rational

Let p be a point on an affine curve F.

2. For a rational function $\varphi = \frac{f}{g} \in K(F)$ we define its multiplicity at p to be
$$\mu_p(\varphi) := \mu_p(f) - \mu_p(g), \quad \in \mathbb{Z} \cup \{\infty\}$$
Again this is well-defined: As $g \neq 0 \in A(F)$ we have $\mu(g) < \infty$ and if $\frac{f}{g} = \frac{f'}{g'} \in A(F)$ then $fg' = gf' \in A(F)$, so that
$$\mu_p(f) - \mu_p(g) = \mu_p(f') = \mu_p(g')$$
by the additivity of multiplicities of polynomial functions. Moreover, the multiplicity $\mu_p(\varphi)$ is ∞ if and only if $\mu_p(f)$ is ∞, i.e. if and only if $f = 0$, and thus $\varphi = 0$.
3. The additivity of multiplicities extends to rational functions as well: for $\varphi = \frac{f}{g}$ and $\psi = \frac{f'}{g'}$ in $K(F)$ we have
$$\begin{aligned}\mu_p(\varphi\psi) &= \mu_p\left(\frac{ff'}{gg'}\right) = \mu_p(ff') - \mu_p(gg') \\ &= \mu_p(f) + \mu_p(f') - \mu_p(g) - \mu_p(g') = \mu_p(\varphi) + \mu_p(\psi)\end{aligned}$$

$\mathbb{A}^2$ Zeros and Poles

Definition (Zeros and Poles)

If a polynomial or rational function has multiplicity $n > 0$ at p we say that it has a zero of order n at p; if $n < 0$ we say that it has a pole of order of $-n$ at p.

$\mathbb{A}^2$ Discrete valuation ring

Lemma ($\mathcal{O}_{F,p}$ is a discrete valuation ring I)

Let p be a point on an affine curve F.

1. *The ideal $I_{F,p}$ is principal, i.e. it can written as $I_{F,p} = \langle t \rangle$ for some $t \in \mathcal{O}_{F,p}$ (which is unique up to units). We call t a local coordinate for F at p.*

Proof.

Let t be aline through p which is not the tangent T_pF, so t transversely intersects F at p, $\mu_p(t) = 1$. As t vanishes at p, we have $t \in I_{F,p}$, and thus

$$1 = \mu_p(t) = \dim \mathcal{O}_{F,p}/\langle t \rangle \geq \dim \mathcal{O}_{F,p}/I_{F,p} \geq 1,$$

where the last inequality holdes as the constant function 1 is a non-zero element of $\mathcal{O}_{F,p}/I_{F,p}$. Thus $I_{F,p} = \langle t \rangle$. □

$\mathbb{A}^2$ Discrete valuation ring

Lemma ($\mathcal{O}_{F,p}$ is a discrete valuation ring II)

Let p be a point on an affine curve F.

2. *Given a local coordinate t for F at p, every non-zero rational function $\varphi \in K(F)^*$ can be written uniquely as $\varphi = ct^n$ for a unit $c \in \mathcal{O}_{F,p}$ and $n \in \mathbb{Z}$, namely for $n = \mu_p(\varphi)$. In particular, we have $\varphi \in \mathcal{O}_{F,p}$ if and only if $\mu_p(\varphi) \geq 0$, i.e. φ does not have a pole at p.*

$\mathbb{P}^2$ Discrete valuation ring Rational Function

Definition (Homogenous Coordinate Rings)

Let F be a projective curve.

1. The homogenous coordinate ring of F:

$$S(F) := K[x, y, z]/\langle F \rangle$$

2. A non-zero element $f \in S(F)$ is called homogenous of degree d, if it can be represented by a homogenous polynomial of degree d in $K[x, y, z]$. The vector space of these elements, together with 0, will be denoted as $S_d(F)$.

$\mathbb{P}^2$ Rational Function and Local Rings

Definition (Field of Rational Functions)

Let F be a projective curve. The field of rational functions of F

$$K(F) := \left\{ \frac{f}{g} : f, g \in S_d(F) \text{ for some } d \in \mathbb{N}, \; g \neq 0 \right\}$$

$\varphi \in K(F)$ is regular at a point $p \in F$, if $\varphi = \frac{f}{g}$ with $f, g \in S(F)$ homogeneous of the same degree and $g(p) \neq 0$. The regular functions at p form a subring of $K(F)$:

$$\mathcal{O}_{F,p} := \left\{ \frac{f}{g} \in K(F) : g(p) \neq 0 \right\}$$

called the local ring of F at p, and they admit an evaluation map $\mathcal{O}_{F,P} \to K$, $\varphi \mapsto \varphi(p)$ with kernel

$$I_{F,p} := \{\varphi \in \mathcal{O}_{F,p} : \varphi((p) = 0\}$$

Multiplicities of Rational Functions

Let $p \in F$

1. For $f \in S(F)$ homogenous, the multiplicity at p is defined as

$$\mu_p(f) := \mu_p(F, f) := \dim \mathcal{O}_{\mathbb{P}^2, p}/\langle F, f \rangle \in \mathbb{N} \cup \{\infty\}$$

2. for $\varphi = \frac{f}{g} \in K(F)$, the multiplicity at p is defined as

$$\mu_p(\varphi) = \mu_p(f) - \mu_p(g)$$

$\mathbb{P}^2$ Intersection Multiplicity

Lemma

For any three projective plane algebraic curves F, G, H,
$\mu_p(F, G) = \mu_p(F, G + FH)$.

Proof.

$$
\begin{aligned}
\mu_p(F, G) &= \dim\, \mathcal{O}_{\mathbb{P}^2,p}/\langle F, G\rangle \\
\mu_p(F, G + FH) &= \dim\, \mathcal{O}_{\mathbb{P}^2,p}/\langle F, G + FH\rangle \\
\langle F, G\rangle &= \langle F, G + FH\rangle \\
\mu_p(F, G) &= \mu_p(F, G + FH)
\end{aligned}
$$

□

$\mathbb{P}^2$ Intersection Multiplicity

Lemma

For any three projective plane algebraic curves F, G, H,
$\mu_p(F, GH) = \mu_p(F, G) + \mu_p(F, H)$.

Lemma

$\mu_p(F, G) \geq 1$ *iff* $p \in F \cap G$.

Lemma

$\mu_p(F, G) = 1$ *iff* $\langle F, G \rangle = I_p$, *where*

$$I_p = \left\{ \frac{f}{g} : f(p) = 0, g(p) \neq 0 \right\}$$

Example: compute $\mu_{(0,0)}(y^2 - x^3, y^3 - x^2)$

$\mathbb{P}^2$ Additivity of Multiplicities

Additivity of multiplicities:

1. For $f, g \in S(F)$: $\mu_p(fg) = \mu_p(f) + \mu_p(g)$

$$\begin{aligned} \mu_p(fg) &= \mu_p(F, fg) \\ &= \mu_p(F, f) + \mu_p(F, g) \\ &= \mu_p(f) + \mu_p(g) \end{aligned}$$

2. For $\varphi = \frac{f}{g}, \psi = \frac{f'}{g'} \in K(F)$: $\mu_p(\varphi\psi) = \mu_p(\varphi) + \mu_p(\psi)$

$$\begin{aligned} \mu_p(\varphi\psi) = \mu_p\left(\frac{ff'}{gg'}\right) &= \mu_p(ff') - \mu_p(gg') \\ &= \mu_p(f) + \mu_p(f') - \mu_p(g) - \mu_p(g') \\ &= \mu_p(\varphi) + \mu_p(\psi) \end{aligned}$$

Bézout's Theorem

Theorem (Bézout's Theorem)

Let F and G be projective curves without common component over an infinite field K. Then

$$\sum_{p \in F \cap G} \mu_p(F,G) \leq degF \cdot degG.$$

If K is algebraicly closed, then equality holds.

Divisor

Divisor

Definition (Divisors)

1. A divisor on F is a formal finite linear combination $a_1 p_1 + \cdots + a_n p_n$ ($p_1, \ldots, p_n \in F$, $a_1, \ldots, a_n \in \mathbb{Z}$ for some $n \in \mathbb{N}$) under pointwise addition of the coefficients the divisors on F form an Abelian group, we denote it by $\mathrm{Div}F$.
2. effective divisor: $D \geq 0$ if $a_i \geq 0$ for all i. Written $D_2 \geq D_1$ or $D_1 \leq D_2$ if $D_2 - D_1$ is effective. In other words, $D_2 \geq D_1$ iff the coefficient of any point in D_2 is greater than or equal to the coefficient of this point in D_1.
3. the degree of a divisor $D = a_1 p_1 + \cdots + a_n p_n$:
$$\deg D := a_1 + \cdots + a_n \in \mathbb{Z}$$
$\deg : \mathrm{Div}F \to \mathbb{Z}$ is a group homomorphism with kernel
$$\mathrm{Div}^0 F := \{D \in \mathrm{Div}F : \deg D = 0\}$$

Divisors from polynomials and rational functions

1. For $f \in S(F) \setminus \{0\}$, the divisor of f

$$\mathrm{div} f := \sum_{p \in F} \mu_p(f) \cdot p \in \mathrm{Div} F$$

   $\mathrm{div} f$ is effective, it contains the data of zeros of f together with their multiplicities. (It is a well-defined divisor since $V(F, f)$ is finite, $\deg F \cdot \deg f$)

2. For $\varphi \in K(F)^*$, the divisor of φ $\mathrm{div}\varphi := \sum_{p \in F} \mu_p(\varphi) \cdot p \in \mathrm{Div} F$. $\mathrm{div}\varphi$ is not effective: it encodes the zeros and poles of φ together with their multiplicities. $\varphi = \frac{f}{g} \in K(F)^*$, $\mathrm{div}\varphi = \mathrm{div} f - \mathrm{div} g$.

$$\begin{aligned} \mathrm{div}\varphi &= \sum_{p \in F} \mu_p(\varphi) p = \sum_{p \in F} \mu_p\left(\frac{f}{g}\right) p = \sum_{p \in F} (\mu_p(f) - \mu_p(g)) p \\ &= \sum_{p \in F} \mu_p(f) p - \sum_{p \in F} \mu_p(g) p = \mathrm{div} f - \mathrm{div} g \end{aligned}$$

Additivity of multiplicities for Divisors

1. For $f, g \in S(F) \setminus \{0\}$ homogeneous,

$$\text{div}(fg) := \sum_{p \in F} \mu_p(fg) \cdot p = \sum_{p \in F} \mu_p(f) \cdot p + \sum_{p \in F} \mu_p(g) \cdot p = \text{div} f + \text{div} g$$

2. $\forall \varphi, \psi \in K(F)^*$, $\text{div}(\varphi\psi) = \text{div}\varphi + \text{div}\psi$, hence $\text{div} : K(F)^* \to \text{Div} F$ is a group homomorphism.

Bézout's Theorem for Divisors

1. For $f \in S(F) \setminus \{0\}$ homogeneous,
$$\deg\, \mathrm{div}(f) = \sum_{p \in F} \mu_p(f) = \sum_{p \in F} \mu_p(F, f) = \deg F \cdot \deg f$$
2. For $\varphi = \frac{f}{g} \in K(F)^*$, f, g nonzero and homogeneous of the same degree
$$\deg\, \mathrm{div}\varphi = \deg\, \mathrm{div} f - \deg\, \mathrm{div} g = \deg F \cdot \deg f - \deg F \cdot \deg g = 0$$
the number of zeros of φ equals the number of poles of φ. The image of $\mathrm{div} : K(F)^* \to \mathrm{Div} F$ lies in $\mathrm{Div}^0 F$.

Noether's Theorem for Divisors

Theorem (Noether)

Let F be a projective curve and let $g, h \in S(F)$ homogenous with $div(g) \leq div(f)$ ($\forall p \in F$, $\mu_p(g) \leq \mu_p(h)$), then $\exists b \in S(F)$ homogenous (of degree $deg(h) - deg(g)$) such that $h = bg$ in $S(F)$, and thus $divh = divb + divg$.

Noether's Theorem for Divisors

Corollary (Global regular functions on projective curves)

Let F be a projective curve. Then

$$\bigcap_{p \in F} \mathcal{O}_{F,p} = K \subset K(F),$$

i.e. the only rational functions that are everywhere regular on F are constants.

Proof.

Suppose $\varphi \in \cap_{p\in F}\mathcal{O}_{F,p}$, $\varphi = \frac{f}{g}$, then for each $p \in F$, $\varphi \in \mathcal{O}_{F,p}$, $\mu_p(\varphi) = \mu_p(f) - \mu_p(g) \geq 0$ so $\text{div} f \geq \text{div} g$. By Noether's theorem, $\exists b$ with degree $\deg f - \deg g = 0$, so b is a constant, such that $f = bg$. Hence $\varphi = b$, $\cap_{p\in F}\mathcal{O}_{F,p} = K \subset K(F)$. $\square$

Divisor Classes and Picard Groups

Let F be a projective curve

1. Divisor D is called principal if $D = \mathrm{div}\varphi$ for some $\varphi \in K(F)^*$,

$$\mathrm{Prim}F := \{\mathrm{div}\varphi : \varphi \in K(F)^*\}$$

   $\mathrm{Prim}F \subset \mathrm{Div}F$ since $\mathrm{Prim}F$ is the image of group homomorphism $\mathrm{div} : K(F)^* \to \mathrm{Div}F$. Also $\mathrm{Prim}F \subset \mathrm{Div}^0 F$

2. $\mathrm{Pic}F := \mathrm{Div}F/\mathrm{Prim}F$ is called the Picard group on F. D_1 and D_2 are said to be linearly equivalent, witten $D_1 \sim D_2$, if D_1 and D_2 defining the same element in $\mathrm{Pic}F$, namely with $D_1 - D_2 = \mathrm{div}\varphi$ for $\varphi \in K(F)^*$. $\mathrm{Pic}^0 F := \mathrm{Div}^0 F/\mathrm{Prim}F$, which is a subgroup of $\mathrm{Pic}F$.

Riemann-Roch

$L(D)$ and $l(D)$

Let F be a projective curve and D a divisor on F, we set

$$L(D) := \{\varphi \in K(F)^* : \mathrm{div}\varphi + D \geq 0\} \cup \{0\}$$

$D = \sum_{p \in F} a_p \cdot p$, $\mathrm{div}\varphi + D \geq 0$ implies $\mu_p(\varphi) \geq -a_p$. Hence, except for the zero function, $L(D)$ consists by construction of all rational functions $\varphi \in K(F)^*$ that are just regular at all points of F, except that

1. φ may have a pole of order at most a_p at p for all $a_p > 0$;
2. φ must have a zero of order at least $-a_p$ at p for all p with $a_p < 0$.

$L(D)$ and $l(D)$

Lemma

$L(D)$ is a vector space over K.

Proof.

$\forall \lambda \in K$, $\varphi, \psi \in L(D)$, i.e. $\mu_p(\varphi) \geq -a_p$, $\mu_p(\psi) \geq -a_p$, $\forall p \in F$, we have

$$\mu_p(\varphi + \psi) \geq \min(\mu_p(\varphi), \mu_p(\psi)) \geq -a_p$$
$$\mu_p(\lambda\varphi) = \mu_p(\varphi) \geq -a_p$$

thus $\varphi + \psi \in L(D)$, $\lambda\varphi \in L(D)$. $\square$

Define $l(D) := \dim L(D) \in \mathbb{N} \cup \{\infty\}$.

$L(D)$ and $l(D)$

Example $D = 0$

$$L(D) = \{\varphi \in K(F)^* : \text{div}\varphi \geq 0\} = \{\text{global regular function on } F\} = K$$

so $l(D) = 1$.

Example $\deg D < 0$

$L(D) = \{0\}$, $l(D) = 0$. If $\exists 0 \neq \varphi \in L(D)$, $\text{div}\varphi + D \geq 0$, so $\deg\text{div}\varphi + \deg D \geq 0$, i.e. $0 + \deg D \geq 0$, which contradicts to $\deg D < 0$.

Remark

(a) If $D \leq D'$ then $L(D) \subset L(D')$, hence $l(D) \leq l(D')$. since

$$\forall \varphi \in L(D), \text{div}\varphi + D \geq 0 \implies \text{div}\varphi + D' \geq \text{div}\varphi + D \geq 0.$$

(b) If $D \sim D'$, then $L(D) \cong L(D')$, $l(D) = l(D')$.

Proof.

$D - D' = \text{div}\psi$ for $\psi \in K(F)^*$. $L(D) \to L(D')$, $\varphi \mapsto \psi\varphi$ is an isomorphism of vector spaces, since

$$\text{div}\varphi + D \geq 0 \iff \text{div}(\psi\varphi) + D' = \text{div}\psi + D' + \text{div}\varphi \geq 0.$$

□

$l(D+p)$ and $l(D)$

Lemma

Let D be a divisor on a projective curve F.
(a). $\forall p \in F$, we have $l(D+p) = l(D)$ or $l(D+p) = l(D)+1$.
(b). For any divisors $D \leq D'$, we have $l(D) \leq l(D') \leq l(D) + deg(D' - D)$

Proof.

a. As $D \leq D+p \implies L(D) \subset L(D+p) \implies l(D) \leq l(D+p)$. Now let a_p be the coefficient of p in D, so that $a_p + 1$ is the coefficient of p in $D+p$. Consider the linear map

$$\Phi : L(D+p) \to K, \quad \varphi \mapsto (t^{a_p+1}\varphi)(p),$$

where t is a local coordinate around p. Since $\varphi \in L(D+p) \setminus \{0\}$, we have

$$\mu_p(t^{a_p+1}\varphi) = \mu_p(\varphi) + a_p + 1 \geq 0 \quad (*)$$

$\square$

$l(D+p)$ and $l(D)$

continued.

The kernel of Φ consists exactly of the rational functions for which $t^{a_p+1}\varphi$ has a zero at p, i.e. for which we have a strict inequality in $(*)$. As this is equivalent to $\mu_p(\varphi)+a_p \geq 0$, and thus to $\mathrm{div}\varphi + D \geq 0$, we conclude that $\ker\Phi = L(D)$. Hence

$$L(D+p)/L(D) \cong \mathrm{Img}\Phi \subset K,$$

if $\mathrm{Img}\Phi = \{0\}$, then $l(D+p) = l(D)$; else $\mathrm{Img}\Phi = K$,
$l(D+p) = l(D)+1$.
b. Since D' is obtained from D by adding $\deg(D'-D)$ points, (b) follows from (a) by induction on $\deg(D'-D)$. □

Divisor

Corollary

For any divisor D with deg $D > 0$ on a projective curve F, we have

$$l(D) \leq degD + 1 \tag{1}$$

In particular, the number $l(D)$ is always finite.

Proof.

Let $n = \deg D + 1$, choose $p \in F$, then
$\deg(D - np) = \deg D - n = -1 < 0$, so $l(D - np) = 0$. $D \geq D - np$, so
$l(D) \leq l(D - np) + \deg(np) = 0 + n = \deg D + 1$. $\square$

Remark

Definition (Algebraic degree - genus formula)

The algebraic genus of a projective plane curve F of degree d is $g = \binom{d-1}{2}$.

Remark

Lemma

Let F be a projective curve of degree d: without loss of generaliztiy we assume $F \neq z$. We denote the vector space of homogenous polynomials in x, y, z of degree n by $K[x, y, z]_n$. Then $\forall n \geq d$, for $D := ndivz$ ($D = divz^n$), we have $l(D) = degD + 1 - \binom{d-1}{2}$.

Proof.

We first show the following is an exact sequence of vector spaces

$$0 \to K[x, y, z]_{n-d} \xrightarrow{\varphi} K[x, y, z]_n \xrightarrow{\psi} L(D) \to 0, \quad (*)$$

where $\varphi(f) = fF$, $\forall f \in K[x, y, z]_{n-d}$; $\psi(g) = \frac{g}{z^n}$, $\forall g \in K[x, y, z]_n$.

1. $\text{Ker}\varphi = \{f \in K[x, y, z]_{n-d} | fF = 0 \text{ in } K[x, y, z]_n\} = \{0\}$

$\square$

Remark

Continued.

2. $\text{Img}\psi = \{\frac{g}{z^n} | g \in K[x,y,z]_n\}$

$$\left(\frac{g}{z^n}\right) + D = (g) - (z^n) + (z^n) = (g) \geq 0 \implies \text{img}\psi \subset L(D).$$

$\forall \frac{h_1}{h_2} \in L(D)$, h_1, h_2 are homogenous of the same degree

$$\text{div}\frac{h_1}{h_2} + D = \text{div}\frac{h_1}{h_2} + \text{div}z^n = \text{div}\frac{h_1}{h_2}z^n \geq 0,$$

i.e. $\text{div}h_1 z^n - \text{div}h_2 \geq 0$, by Noether's Theorem, $\exists g$ homogenous of degree $\deg(h_1 z^n) - \deg h_2 = n$, s.t. $h_1 z^n = g h_2$, i.e. $\frac{h_1}{h_2} = \frac{g}{z^n}$. Hence $L(D) \subset \text{Img}\psi$, then $L(D) = \text{Img}\psi$. □

Remark

Continued.

$$3.\quad \mathrm{Img}\varphi = \{fF \in K[x,y,z]_n | f \in K[x,y,z]_{n-d}\}$$
$$\mathrm{Ker}\psi = \{g \in K[x,y,z]_n | \frac{g}{z^n} = 0 \text{ in } L(D)\}$$

$\forall f \in K[x,y,z]_{n-d}$ $fF = 0$ in $S(F)$, so $\frac{fF}{z^n} = 0$ in $K(F)^*$, hence $\frac{fF}{z^n} = 0$ in $L(D)$, $fF \in \mathrm{Ker}\psi$, then $\mathrm{Img}\varphi \subset \mathrm{Ker}\psi$.
$\forall g \in K[x,y,z]_n$ with $\frac{g}{z^n} = 0$ in $L(D)$, $\frac{g}{z^n} = 0$ in $K(F)^*$. Since F is irreducible and $F \neq z$, we must have $F|g$. So $g \in \mathrm{Img}\psi$, $\mathrm{Img}\psi \subset \mathrm{Ker}\psi$.
Hence $\mathrm{Img}\varphi = \mathrm{Ker}\psi$. □

Remark

Continued.

By 1,2,3, $(*)$ is an exact sequence of vector spaces

$$
\begin{aligned}
l(D) &= \dim K[x,y,z]_n - \dim K[x,y,z]_{n-d} \\
&= \frac{(n+1)(n+2)}{2} - \frac{(n-d+1)(n-d+2)}{2} \\
&= \frac{(n+1)(n+2)}{2} - \frac{(n+1)(n+2) - d(2n+3) + d^2}{2} \\
&= nd + \frac{3d - d^2}{2}
\end{aligned}
$$

$$
\deg D = \deg \operatorname{div} z^n = \deg z^n \cdot \deg F = nd.
$$

Therefore

$$
l(D) = nd + \frac{3d - d^2}{2} = \deg D + 1 - \frac{d^2 - 3d + 2}{2} = \deg D + 1 - g.
$$

Theorem (Riemann's Theorem)

There is a unique smallest integer s, depending only on F, such that $l(D) \geq degD + 1 - s$, for any divisor D, $s = \binom{d-1}{2} = g$.

Proof.

Since we have $l(D) = \deg D + 1 - g$ for $D = \text{div} z^n$, we only have to show

$$l(D) \geq \deg D + 1 - g \quad (*)$$

holds $\forall D$. □

Riemann's Theorem

Proof.

Note first:

1. If $(*)$ holds for D and $D' \sim D$, then $(*)$ holds for D'. Since $l(D) = l(D')$, $\deg D = \deg D'$,
$l(D) \geq \deg D + (1-g) \implies l(D') \geq \deg D' + (1-g)$;
2. If $(*)$ holds for D, then it also holds for any divisor $D' \leq D$:

$$\begin{aligned} l(D') &\geq l(D) - \deg(D - D') \quad \text{similar as Eqn.(1)} \\ &\geq \deg D + (1-g) - \deg(D - D') \\ &= \deg D' + (1-g). \end{aligned}$$

□

Riemann's Theorem

continued.

Now let D be any divisor on F, then we can write

$$D = p_1 + p_2 + \cdots + p_n - E,$$

where E is effective. Since the points are allowed to allowed to appear in E, we may assume $n \geq d$. For every $i = 1, 2, \cdots, n$,

$$\operatorname{div}(l_i) = p_i + q_{i_1} + \cdots + q_{i_{d-1}},$$

for some $q_{i_1}, \cdots, q_{i_{d-1}} \in F$. $\square$

continued.

Then the divisor $D' := D + \mathrm{div}\frac{z^n}{l_1 \cdots l_n} \sim D$, and

$$
\begin{aligned}
D' &= p_1 + \cdots + p_n - E + \mathrm{div} z^n - \sum_{i=1}^{n} \mathrm{div} l_i \\
&= p_1 + \cdots + p_n - E + \mathrm{div} z^n - \sum_{i=1}^{n} (p_i + q_{i_1} + \cdots q_{i_{d-1}}) \\
&\leq p_1 + \cdots + p_n - E + \mathrm{div} z^n - p_1 - \cdots - p_n \\
&= \mathrm{div} z^n - E \\
&\leq \mathrm{div} z^n
\end{aligned}
$$

since $(*)$ holds for $\mathrm{div} z^n$, so it holds for D' by (2), and thus for D by (1). $\square$

Divisor

Summarizing,

$$\boxed{\deg D + 1 - g \leq l(D) \leq \deg D + 1} \tag{2}$$

for every divisor D with $\deg D \geq 0$ on a projective curve F of genus g.

Canonical Divisor

Definition (Canonical Divisor)

Let F be a projective curve of degree d. For any line $l(\neq F)$, we call

$$K_F := (d-3)\ \mathrm{div}\ l \in \mathrm{Pic}F$$

the canonical divisor (class) of F.

Note that K_F is well-defined, since for another line l', $\mathrm{div}l \sim \mathrm{div}l'$, as $\mathrm{div}\frac{l}{l'} \in \mathrm{Prim}F$.

Canonical Divisor

Lemma (Degree of canonical divisor)

For a projective curve F of genus g, we have $\deg K_F = 2g - 2$.

Proof.

$$\deg K_F = \deg (d-3)\mathrm{div} l = (d-3)\deg\,\mathrm{div} l = (d-3)\deg F \cdot \deg l$$
$$= (d-3)d = 2 \cdot \frac{(d-1)(d-2)}{2} - 2 = 2g - 2.$$

□

Canonical Divisor

Lemma

$\forall p \in F$, *we have* $l(K_F + p) = l(K_F)$.

Proof.

If $d = \deg F \leq 2$, then $g = 0$, $\deg K_F = 2g - 2 = -2 < 0$, $\deg(K_F + p) = -1 < 0$, so $l(K_F) = l(K_F + p) = 0$.
If $d \geq 3$:
Choose any line l through p, that is not the tangent $T_p F$. The divisor $\mathrm{div}(l) - p$ is then effective and doesn't contain p. $K_F = (d-3)\mathrm{div}(l)$. We want to show $L(K_F + p) = L(K_F)$. Clearly $K_F < K_F + p \implies L(K_F) \subset L(K_F + p)$, we only have to show $L(K_F + p) \subset L(K_F)$. □

Canonical Divisor

Continued.

Let $\varphi = \frac{f}{g} \in L(K_F + p)$ and $\varphi \neq 0$, then

$$\begin{aligned} \mathrm{div}(\varphi) + K_F + p &\geq 0 \\ \mathrm{div}(f) - \mathrm{div}(g) + (d-3)\mathrm{div}(l) + p &\geq 0 \\ (1) \quad \mathrm{div}(fl^{d-2}) \geq \mathrm{div}(g) + \mathrm{div}(l) - p &\geq \mathrm{div}(g) \quad (\mathrm{div}(l) \geq p) \end{aligned}$$

By Noether's Theorem, there is a homogeneous polynomial h of degree $\deg(fl^{d-2}) - \deg(g) = \deg(l^{d-2}) = d-2$ with $fl^{d-2} = gh$,

$$\begin{aligned} \mathrm{div}(h) &= \mathrm{div}(fl^{d-2}) - \mathrm{div}(g) \\ &\geq \mathrm{div}(g) + \mathrm{div}(l) - p - \mathrm{div}(g) \\ &= \mathrm{div}(l) - p \quad \text{by } (1) \end{aligned}$$

hence

$$(**) \quad \mathrm{div}(h) = \mathrm{div}(fl^{d-2}) - \mathrm{div}(g) \geq \mathrm{div}(l) - p$$

Continued.

Then $\forall Q \neq p$, $\mu_Q(h) \geq \mu_Q(l)$, hence $\langle F, h\rangle \subset \langle F, l\rangle$ in $\mathcal{O}_{P^2,Q}$.

$$\mu_Q(h) = \mu_Q(F,h) = \dim \mathcal{O}_{P^2,Q}/\langle F, h\rangle$$
$$\mu_Q(l) = \mu_Q(F,l) = \dim \mathcal{O}_{P^2,Q}/\langle F, l\rangle$$

hence

$$\langle F, h\rangle \subset \langle F, l\rangle \iff \mu_Q(h) \geq \mu_Q(l) \quad \text{in } \mathcal{O}_{P^2,Q}$$

So $h \in \langle F, l\rangle$ in $\mathcal{O}_{P^2,Q}$, so $\langle l, h\rangle \subset \langle F, l\rangle$, hence $\mu_Q(l,h) \geq \mu_Q(F,l)$, $\forall Q \neq p$. Then

$$\sum_{Q\neq p} \mu_Q(l,h) \geq \sum_{Q\neq p} \mu_Q(F,l) = \deg(\mathrm{div}(l) - p) = d - 1$$
$$\sum_{Q\neq p} \mu_Q(l,h) = \deg(l)\cdot\deg(h) = 1\cdot(d-2)$$

Continued.

By Bézout's Theorem, h must contain l as a factor. Hence $\text{div}(h) \geq \text{div}(l)$, by (**)

$$\text{div}(fl^{d-2}) - \text{div}(g) = \text{div}(h) \geq \text{div}(l)$$

$$\text{div}(f) - \text{div}(g) + \text{div}(l^{d-3}) = \text{div}(\varphi) + K_F \geq 0$$

so $\varphi \in L(K_F)$. $\square$

Riemann-Roch

Lemma

Let F be a projective curve of genus g, then

$$l(D) - l(K_F - D) \geq degD + (1-g) \tag{3}$$

for all divisors D on F.

Proof.

We prove it by descending induction on $\deg(D)$.
1. $\deg(D) > 2g-2$,
$\deg(K_F - D) = (2g-2) - \deg(D) < 0 \implies l(K_F - D) = 0$. Hence by Eqn. (2)

$$l(D) - l(K_F - D) = l(D) \geq \deg(D) + (1-g)$$

$\square$

Continued.

2.For the induction step, assume that the statement holds for a divisor D. we want to show it holds for $D-p$, $\forall p \in F$.

$$\begin{aligned} l(D-p) - l(K_F - D + p) &\geq (l(D)-1) - (l(K_F - D)+1) \quad (\star) \\ &= l(D) - l(K_F - D) - 2 \\ &\geq \deg(D) + (1-g) - 2 \quad \text{by assumption on } D \\ &= \deg(D) - g - 1 \\ &= \deg(D-p) - g \end{aligned}$$

We only have to show $(\star) is strict (thus$ LHS$\geq \deg(D-p) - g + 1)$. Namely,

$$l(D-p) = l(D) - 1, \quad l(K_F - D + p) = l(K_F - D) + 1$$

cannot be true simultaneously. □

Riemann-Roch

Continued.

Otherwise, assume

$$l(D-p) = l(D) - 1 \text{ and } l(K_F - D + p) = l(K_F - D) + 1$$

namely

$$L(D-p) \subsetneq L(D) \text{ and } l(K_F - D) \subsetneq L(K_F - D + p)$$

$\exists$ rational functions

$$\varphi \in L(D) \setminus L(D-p) \implies \text{div}(\varphi) + D \geq 0 \text{ with "=" at p}$$

$$\psi \in L(K_F - D + p) \setminus L(K_F - D)$$

$$\implies \text{div}(\psi) + K_F - D + p \geq 0 \text{ with "=" at p}$$

$\square$

Continued.

$$\mathrm{div}(\varphi\psi) + K_F + p = (\mathrm{div}(\varphi) + D) + (\mathrm{div}(\psi) + K_F - D + p) \geq 0$$

with "=" at p.

therefore

$$\varphi\psi \in L(K_F + p) \setminus L(K_F)$$

contradiction (since $L(K_F + p) = L(K_F)$). □

Riemann-Roch

Theorem (Riemann-Roch)

Let F be a projective curve of genus g, then

$$l(D) - l(K_F - D) = degD + (1 - g)$$

for all divisors D on F.

Riemann-Roch

Proof.

By Eqn. (3),

$$\begin{aligned} l(D) - l(K_F - D) &\geq \deg D + (1-g) \quad (a) \\ l(K_F - D) - l(K_F - (K_F - D)) &\geq \deg(K_F - D) + (1-g) \\ l(K_F - D) - l(D) &\geq \deg(K_F) - \deg(D) + (1-g) \\ &= (2g-2) - \deg(D) + (1-g) \\ &= (g-1) - \deg(D) \\ l(D) - l(K_F - D) &\leq \deg(D) + (1-g) \quad (b) \end{aligned}$$

By (a),(b), $l(D) - l(K_F - D) = \deg(D) + (1-g)$. □