Lecture 5

Goal: To state Riemann–Roch theorem and derive equation for elliptic curve using Riemann–Roch theorem and view the group law on elliptic curve in the light of Riemann–Roch.

Let X be an algebraic curve.

(irreducible, non-singular)

Defn (Divisor) A **divisor** is a formal sum

$$\sum_{P \in X} n_P (P)$$

n_P's are 0 except finitely many

$n_P \in \mathbb{Z}$

Given two divisors, we can add them to obtain a new divisor.

$$D_1 = n_1P_1 + n_2P_2 + \cdots + n_rP_r$$

$$D_2 = m_1P_1 + m_2P_2 + \cdots + m_rP_r$$

$$D_1 + D_2 = (n_1+m_1)P_1 + (n_2+m_2)P_2 + \cdots + (n_r+m_r)P_r$$

The set of divisors form an abelian group.

Divisors ~~~~ degree of a divisor

$$\sum_{i=1}^{n} n_{P_i} P_i \qquad n_{P_1} + n_{P_2} + \cdots + n_{P_n} \in \mathbb{Z}$$

$$\left\{\begin{matrix}\text{Principal}\\ \text{divisors}\end{matrix}\right\} \subseteq \left\{\begin{matrix}\text{Set of all}\\ \text{degree 0}\\ \text{divisors}\end{matrix}\right\} \subseteq \left\{\begin{matrix}\text{Set of all}\\ \text{divisors}\end{matrix}\right\}$$

$\downarrow$

Subgroup

Suppose r is a rational function on X.

$\operatorname{div}(r)$ Zeroes of r $Z_1, \ldots, Z_t$

Poles of r $P_1, \ldots, P_s$

$$\operatorname{div}(r) = \operatorname{ord}_r(Z_1) Z_1 + \cdots + \operatorname{ord}_r(Z_t) Z_t + \operatorname{ord}_r(P_1) P_1 + \cdots + \operatorname{ord}_r(P_s) P_s$$

$$\deg(\operatorname{div} r) = 0$$

Defn: A <u>principal divisor</u> is a divisor of the form $\operatorname{div}(r)$ for some rational function r on X.

$$\{\text{Principal divisors}\} \subseteq \{\text{Set of all degree 0 divisors}\}$$

$\downarrow$

Sub group

We can define an equivalence relation on set of divisors.

$$D_1 \sim D_2 \iff D_1 = D_2 + \operatorname{div}(r)$$

for some rational fn r on X.

If $D_1 \sim D_2$, then $\deg(D_1) = \deg(D_2)$

$$\begin{aligned}\deg(D_1) &= \deg(D_2 + \operatorname{div}(r)) \\ &= \deg(D_2) + \deg(\operatorname{div}(r)) \\ &= \deg(D_2)\end{aligned}$$

Lemma: The set of all principal divisors form a subgroup of set of all degree 0 divisors.

Pf: 1) $\operatorname{div}(r) + \operatorname{div}(r') = \operatorname{div}(rr')$

2) Take a constant function (non-zero)

λ

$$\text{div}(\lambda) + \text{div}(r) = \text{div}(r)$$

3) r, then take $r' = 1/r$

$$\text{div}(r') + \text{div}(r) = 0$$

Towards Riemann-Roch theorem

Let D be a divisor on X.

$$L(D) = \{0\} \cup \{ \text{rational fns } r \text{ on } X \text{ s.t. } \text{div}(r) + D \geq 0 \}$$

Propn: $L(D)$ is a vector space over $\mathbb{R}$.

Pf: Exercise!

Aside: (On vector Spaces)

Example: Think of $\mathbb{R}^n$ over $\mathbb{R}$

We can add two elements

Scalar multiplication

$r(x_1, \ldots, x_n) = (rx_1, \ldots, rx_n)$

A vector space V over a field F is a set that is equipped with $(+)$ addition & scalar multiplication

1) $(V, +)$ is an abelian group.

2) $(c_1 c_2) v = c_1 (c_2 v)$ $\quad c_1, c_2 \in F$

$c_1 c_2$: Multiplication in field

$c_2 v$: Scalar multiplication

3) Suppose $1 \in F$ is the multiplicative identity

$$1(v) = v$$

4) Distributive relations

$$(c_1 + c_2) v = c_1 v + c_2 v \qquad c_1, c_2, c \in F \quad v, w \in V$$

$c_1 + c_2$: Addition in field

$c_1 v + c_2 v$: Vector addition

$$c(v + w) = cv + cw$$

Basis Example: $\mathbb{R}^n$ over $\mathbb{R}$

$$e_1 = (1, 0, 0, \ldots 0)$$
$$e_2 = (0, 1, 0, \ldots, 0)$$
$$\vdots$$
$$e_n = (0, 0, 0, \ldots, 1)$$

$$(x_1, x_2, \ldots, x_n) = \underbrace{x_1 e_1 + x_2 e_2 + \cdots + x_n e_n}$$

↳ Spanning — Linear Combination

Suppose

$$c_1 e_1 + c_2 e_2 + \cdots + c_n e_n = 0$$

$$(c_1, c_2, \ldots, c_n) = (0, 0, \ldots, 0)$$

$$\Rightarrow c_i = 0$$

Linear independence

Thm: Every vector space has a basis.

$L(D)$ has a basis, $\dim(L(D)) =: \ell(D)$

Defn (Canonical divisor) It is a divisor of the form $\operatorname{div}(w)$, w is a non-zero differential on X.

$f(x,y)$

$\hookrightarrow \dfrac{\partial f}{\partial x}\,dx + \dfrac{\partial f}{\partial y}\,dy$

dx, dy $\downarrow$ differentials

Riemann-Roch Thm For any divisor D on X,

$$\boxed{l(D) = \deg(D) - g + 1 + l(\operatorname{div}(w) - D)}$$

$g \downarrow$ genus (X)

Remarks: (How do we define genus?)

(Riemann's Thm) Given X, $\exists\, g \in \mathbb{Z}$ s.t

$$\ell(D) \geq \deg(D) + 1 - g$$

for all divisors D on X.

Suppose $g' > g$

$$-g' < -g$$

$$\deg(D) + 1 - g' < \deg(D) + 1 - g \leq \ell(D)$$

The smallest such g is called genus of X. (Geometric genus)

Arithmetic genus (via Hilbert polynomials)

for a curve, geometric genus = arithmetic genus.

(RR) $\ell(D) = \deg(D) - g + 1 + \ell(\mathrm{div}(w) - D)$

Some useful corollaries:

1) Set $D = 0$

$$L(0) = \{0\} \cup \{ r \mid \operatorname{div}(r) \geq 0 \}$$

$$= \{0\} \cup \{k^\times\} = k$$

$$\dim_k (L(0)) = 1 = \ell(0)$$

$$1 = -g + 1 + \ell(\operatorname{div}(w))$$

$$\boxed{\ell(\operatorname{div}(w)) = g}$$

2) Set $D = \operatorname{div}(w)$

$$g = \deg(D) - g + 2$$

$$\boxed{\deg(\operatorname{div}(w)) = 2g - 2}$$

Equation for elliptic curve

Defn: (Elliptic Curve) It is a non-singular, projective curve of genus 1, with a point defined over base field.

E genus 1

$P \in E$

$P, 2P, 3P, \ldots nP$

$$\ell(nP) = \deg(nP) + \ell(\underbrace{\text{div}(w) - D}_{\text{II}})$$

$$L(\text{div}(w) - D) = \{0\} \cup \{r \mid \text{div}\, r + \text{div}\, w - D \geq 0\}$$

$$= \{0\}$$

$$\ell(nP) = n$$

$\ell(P)$ Basis for $L(P) = \{1\}$

$\ell(2P)$ Basis ——— $= \{1, x\}$

$$L(aP) = \{0\} \cup \{ r \mid \operatorname{div}(r) + aP \geq 0 \}$$

$$\downarrow$$

$$\operatorname{div}(r) \geq -aP$$

x has a pole at P of order 2

$\ell(3P)$ Basis $\{1, x, y\}$

y has a pole at P of order 3

$\ell(4P)$ Basis $\{1, x, y, x^2\}$

$\ell(5P)$ —— $\{1, x, y, x^2, xy\}$

$\ell(6P)$ —— $\{1, x, y, x^2, xy, y^2, x^3\}$

both are candidates

The set $\{1, x, y, x^2, xy, x^3, y^2\}$

$$y^2 + a_5 xy + a_3 y = x^3 + a_4 x^2 + a_2 x + a_0$$

→ By change of variables we can simplify the above equation to

$$y^2 = x^3 + ax + b \qquad \Delta \neq 0$$

$\Delta = 4a^3 + 27b^2$

Weierstrass form of an elliptic curve

Reference:

1) Hartshorne, Algebraic Geometry

2) Algebraic Curves by Fulton