Divisors on algebraic curves

Silverman, *Arithmetic of Elliptic Curves*, Chapter II

Alec Sun

July 27, 2020

Notation

Here C denotes a curve and $P \in C$ is a point of C.

C/K	C is defined over K.
$\bar{K}(C)$	the function field of C over $\bar{K}$.
$K(C)$	the function field of C over K.
$\bar{K}[C]_P$	the local ring of C at P.
M_P	the maximal ideal of $\bar{K}[C]_P$.

Algebraic curves

Recall from algebraic geometry:

- Let C be a curve and $P \in C$ a smooth point. Then $\bar{K}[C]_P$ is a DVR with valuation $\text{ord}_P(f) = \sup\{d \in \mathbb{Z} : f \in M_P^d\}$.
- This extends to $\text{ord}_P : \bar{K}(C) \to \mathbb{Z} \cup \infty$ by $\text{ord}_P(f/g) = \text{ord}_P(f) - \text{ord}_P(g)$.
- A *uniformizer* for C at P is a function $t \in \bar{K}(C)$ with $\text{ord}_P(t) = 1 \implies M_P = (t)$.

Definition

- $\text{ord}_P(f) > 0 \implies f$ has a *zero* at P.
- $\text{ord}_P(f) < 0 \implies f$ has a *pole* at P.

Maps between curves

Proposition

Let C be a smooth curve and $f \in \bar{K}(C)$ with $f \neq 0$. Then there are finitely many points of C at which f has a pole or zero.

Proposition

Let C be a curve and $V \subset \mathbb{P}^N$ a variety. If $P \in C$ is a smooth point and $\phi : C \to V$ is a rational map, then ϕ is regular at P.

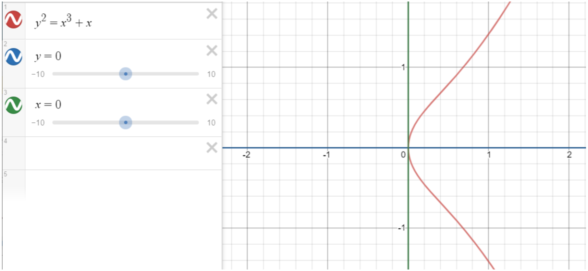
Theorem

A morphism of curves $\phi : C_1 \to C_2$ is either constant or surjective.

Order functions

Example

- $C : y^2 = x^3 + x,\ P = (0,0),\ M_P/M_P^2 = (y)$
- $\mathrm{ord}_P(y) = 1,\ \mathrm{ord}_P(x) = 2$



Maps of function fields

Let C_1/K and C_2/K be curves. If $\phi : C_1 \to C_2$ is a non-constant rational map, there is an injective map of function fields

$$\phi^* : K(C_2) \to K(C_1)$$
$$\phi^* f = f \circ \phi.$$

Definition

If ϕ is constant, define $\deg \phi = 0$, otherwise define

$$\deg \phi = [K(C_1) : \phi^* K(C_2)] .$$

Ramification index

Definition

Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves, and let $P \in C_1$. The *ramification index* is $e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)})$ where $t_{\phi(P)} \in K(C_2)$ is a uniformizer at $\phi(P)$.

Definition

Note that $e_\phi(P) \geq 1$ since $t_{\phi(P)} \in M_{\phi(P)}$. Say that ϕ is *unramified* at P if $e_\phi(P) = 1$.

Ramification index

Proposition

1. *For every $Q \in C_2$,*

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

2. *For all but finitely many $Q \in C_2$,*

$$\#\{\phi^{-1}(Q)\} = \deg(\phi) \iff e_\phi(P) = 1, \forall P \in \phi^{-1}(Q).$$

Remark

This is analogous to $\sum e_i f_i = [K : \mathbb{Q}]$ in algebraic number theory.

Divisors on curves

Definition

A divisor $D \in \mathrm{Div}(C)$ is a formal sum

$$D = \sum_{P \in C} n_P (P), \quad n_P \in \mathbb{Z}, n_P = 0 \text{ for all but finitely many } P.$$

$$\deg D = \sum_{P \in C} n_P$$

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : \deg D = 0\}$$

If C is smooth and $f \in \bar{K}(C)^*$, define a *principal* divisor

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Degree of principal divisors

Proposition

1. $\operatorname{div}(f) = 0 \iff f \in \bar{K}^*$.
2. *If C is a smooth curve and $f \in \bar{K}(C)^*$, then* $\deg(\operatorname{div}(f)) = 0$.

Example

On $\mathbb{P}^1$, every divisor

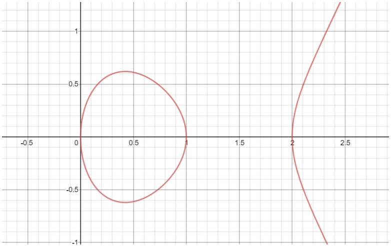
$$D = \sum_P n_P(P) = \operatorname{div}\left(\prod_{P\in\mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}\right), \quad P = [\alpha_P, \beta_P]$$

of degree 0 is principal.

Divisor example

Example

- $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$ for e_1, e_2, e_3 pairwise distinct. Define $P_i = (e_i, 0) \in C$ for $i = 1, 2, 3$.
- $\text{div}(x - e_i) = 2(P_i) - 2(P_\infty)$,
  $\text{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$



Maps of divisor groups

Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. Recall that $\phi^* : \bar{K}(C_2) \to \bar{K}(C_1)$.

Definition

Similarly, define

$$\phi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$$
$$(Q) \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)(P).$$

Proposition

Let $\phi : C_1 \to C_2$ be a non-constant map of smooth curves. Then for all $D \in \mathrm{Div}(C_2)$, $\deg(\phi^* D) = (\deg \phi)(\deg D)$.

Degree of divisor of rational function is 0

Example 2.2. Let C/K be a smooth curve and let $f \in K(C)$ be a function. Then f defines a rational map, which we also denote by f,

$$f : C \longrightarrow \mathbb{P}^1, \qquad P \longmapsto [f(P), 1].$$

From (II.2.1), this map is actually a morphism. It is given explicitly by

$$f(P) = \begin{cases} [f(P), 1] & \text{if } f \text{ is regular at } P, \\ [1, 0] & \text{if } f \text{ has a pole at } P. \end{cases}$$

Conversely, let

$$\phi : C \longrightarrow \mathbb{P}^1, \qquad \phi = [f, g],$$

be a rational map defined over K. Then either $g = 0$, in which case ϕ is the constant map $\phi = [1, 0]$, or else ϕ is the map corresponding to the function $f/g \in K(C)$. Denoting the former map by ∞, we thus have a one-to-one correspondence

$$K(C) \cup \{\infty\} \longleftrightarrow \{\text{maps } C \to \mathbb{P}^1 \text{ defined over } K\}.$$

We will often implicitly identify these two sets.

Degree of divisor of rational function is 0

Example

Let C be a smooth curve, $f \in \bar{K}(C)$ a non-constant function, and $f : C \to \mathbb{P}^1$ the corresponding map. Then from the definition of ramification, $\operatorname{div}(f) = f^*((0) - (\infty))$.

Corollary

For $f \in \bar{K}(C)$ a non-constant function, $f : C \to \mathbb{P}^1$ satisfies $\deg \operatorname{div}(f) = \deg f - \deg f = 0$.

Differentials

Definition

The space Ω_C of (meromorphic) differential forms on C is the $\bar{K}(C)$-vector space generated by symbols dx, $x \in \bar{K}(C)$, subject to:

1. $d(x+y) = dx + dy$
2. $d(xy) = x\,dy + y\,dx$
3. $da = 0$, $a \in \bar{K}$

Proposition

Ω_C is a 1-dimensional $\bar{K}(C)$-vector space.

Differentials

Proposition

Let $t \in \bar{K}(C)$ be a uniformizer at P.

1. *For every $\omega \in \Omega_C$ there exists a unique $g \in \bar{K}(C)$ with $\omega = g\,dt$. Denote g by ω/dt.*
2. *If $f \in \bar{K}(C)$ is regular at P then so is df/dt.*
3. *$\mathrm{ord}_P(\omega/dt)$ for $\omega \neq 0$ is independent of the choice of t, so we can denote by $\mathrm{ord}_P(\omega)$ the order of ω at P.*

Divisors of differentials

Definition

The divisor associated to $\omega \neq 0$ is

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P) \in \mathrm{Div}(C).$$

- If $\mathrm{ord}_P(\omega) \geq 0, \forall P \in C$, $\omega \in \Omega_C$ is *regular* or *holomorphic*.
- If $\mathrm{ord}_P(\omega) \leq 0, \forall P \in C$, $\omega \in \Omega_C$ is *non-vanishing*.

Divisors of differentials

Example

The function $t - \alpha$ on $\mathbb{P}^1$ is a uniformizer at $\alpha \in \bar{K}$ and the function $1/t$ is a uniformizer at $\infty \in \mathbb{P}^1$.
We have

$$\mathrm{ord}_\alpha(dt) = \mathrm{ord}_\alpha(d(t-\alpha)) = 0$$

$$\mathrm{ord}_\infty(dt) = \mathrm{ord}_\infty\left(-t^2\, d\left(\frac{1}{t}\right)\right) = -2$$

$$\mathrm{div}(dt) = -2(\infty).$$

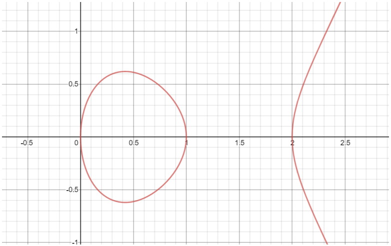
For any nonzero $\omega \in \Omega_{\mathbb{P}^1}$,

$$\deg \mathrm{div}(\omega) = \deg \mathrm{div}(dt) = -2 \implies \omega \text{ not holomorphic.}$$

Divisors of differentials

Example

- $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$
- $dx = d(x - e_i) = -x^2\, d(1/x)$
- $\operatorname{div}(dx) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$
- $\operatorname{div}(dx/y) = 0$ is holomorphic and non-vanishing.



Divisorial inequalities

Definition

- A divisor $D \geq 0$ is positive if $n_P \geq 0, \forall P \in C$.
- $D_1 \geq D_2$ denotes $D_1 - D_2 \geq 0$.

This notation is useful for describing poles and zeros.

Example

$$\text{div}(f) \geq (Q) \implies f \text{ is regular and has zero at } Q$$

$$\text{div}(f) \geq -n(P) \implies f \text{ is regular except for pole of order } \leq n \text{ at } P$$

Divisorial inequalities

Definition

For $D \in \mathrm{Div}(C)$ define

$$\mathcal{L}(D) = \left\{ f \in \bar{K}(C)^* : \mathrm{div}(f) \geq -D \right\} \cup \{0\}$$

$$\ell(D) = \dim_{\bar{K}} \mathcal{L}(D).$$

Proposition

- *If* $\deg D < 0$ *then* $\mathcal{L}(D) = \{0\}$.
- $\mathcal{L}(D)$ *is a finite-dimensional* $\bar{K}$*-vector space.*
- *If* $D' \in \mathrm{Div}(C)$ *is linearly equivalent to* D*, which means that* D' *and* D *differ by a principal divisor, then* $\mathcal{L}(D) \cong \mathcal{L}(D')$.

Canonical divisors

Recall that for any nonzero $\omega_1, \omega_2 \in \Omega_C$ we have $\omega_1 = f\omega_2$ for some $f \in \bar{K}(C)^*$.

Definition

Noting that

$$\mathrm{div}(\omega_1) = \mathrm{div}(f) + \mathrm{div}(\omega_2),$$

the image in $\mathrm{Pic}(C)$ of $\mathrm{div}(\omega)$ for any nonzero $\omega \in \Omega_C$ is well-defined. Denote by $\mathrm{div}(\omega) \in \mathrm{Div}(C)$ a *canonical divisor*.

Holomorphic forms

Let $K_C = \mathrm{div}(\omega) \in \mathrm{Div}(C)$ be a canonical divisor on C. For $f \in \bar{K}(C)^*$,

$$f \in \mathcal{L}(K_C) \iff \mathrm{div}(f) \geq -\mathrm{div}(\omega) \iff \mathrm{div}(f\omega) \geq 0$$
$$\iff f\omega \text{ holomorphic}$$

Since $f\omega$, $f \in \bar{K}(C)^*$ ranges over all differentials on C,

$$\mathcal{L}(K_C) \cong \{\omega \in \Omega_C : \omega \text{ holomorphic}\}.$$

Remark

The dimension $\ell(K_C)$ of this space is an important invariant of C.

Riemann-Roch

This is a fundamental result in the algebraic geometry of curves.

Theorem (Riemann-Roch)

There is an integer $g \geq 0$, called the genus of C, such that for every divisor $D \in \mathrm{Div}(C)$ we have

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Corollary

- $\ell(K_C) = g$
- $\deg K_C = 2g - 2$
- $\deg D > 2g - 2 \implies \ell(D) = \deg D - g + 1$

Riemann-Roch

Example

Let $C = \mathbb{P}^1$. Since there are no holomorphic differentials on C, $g = \ell(K_C) = 0$. Note that $\deg K_C = 2g - 2$ is consistent with $\deg \operatorname{div}(\omega) = -2$. In general,

$$\ell(D) - \ell(-2(\infty) - D) = \deg D + 1.$$

Setting $D = n(\infty)$, $n \geq 0$ we see that $\ell(n(\infty)) = n + 1$.

Riemann-Roch

Example

- $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$
- Since $\text{div}(dx/y) = 0$, $K_C = 0 \implies g = \ell(K_C) = \ell(0) = 1$.
- $\ell(D) = \deg D$ for $\deg D \geq 1$.
  - If $P \in C$, then $\ell((P)) = 1$. Since $\bar{K} \subset \mathcal{L}((P))$, there are no functions on C having a single simple pole.
  - $\ell(n(P_\infty)) = n$
    - $\{1, x\}$ is a basis for $\mathcal{L}(2(P_\infty))$
    - $\{1, x, y\}$ is a basis for $\mathcal{L}(3(P_\infty))$
    - $\{1, x, y, x^2\}$ is a basis for $\mathcal{L}(4(P_\infty))$
    - The 7 functions $1, x, y, x^2, xy, x^3, y^2$ lie in dimension 6 space $\mathcal{L}(6(P_\infty))$ and hence are linearly dependent.
    - If genus is 1, then curve is plane cubic.