11.1 Divisors

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008

Outline

Definitions - (1)

- E/K , $P \in E(\overline{K})$, $[P]$: a formal symbol of P

(1) Definition
A divisor D on E is a finite linear combination of the formal symbols with integer coefficients:

$$D = \sum_j a_j [P_j], \quad a_j \in \mathbb{Z}$$

(2) Definition
$Div(E)$: group of divisors in (1)

(3) Define degree and sum of a divisor

$$\deg\left(\sum_j a_j [P_j]\right) = \sum_j a_j \in \mathbb{Z}$$
$$sum\left(\sum_j a_j [P_j]\right) = \sum_j a_j P_j \in E(\overline{K})$$

Definitions - (2)

- (Continue):
  - (4) Definition
    $Div^0(E)$: subgroup of $Div(E)$

$$Div^0(E) = \{\text{divisors of degree } 0\}$$

  - (5) sum : $Div^0(E) \rightarrow E(\overline{K})$ is a surjective homomorphism. The surjectivity is because

$$sum([P] - [\infty]) = P$$

Functions on E - (1)

- $E/K : y^2 = x^3 + Ax + B$

  (1) Definition

  A function on E is a rational function

  $$f(x, y) \in \overline{K}(x, y)$$

  that is defined for at least one point in $E(\overline{K})$. (e.g. rational function $1/(y^2 - x^3 - Ax - B)$ is not allowed.)

  (2) Examples

  $E : y^2 = x^3 - x$

  $f(x, y) = x/y$ is defined at $(0, 0)$ on E !

  $$\because \quad \frac{x}{y} = \frac{y}{x^2 - 1} = 0 \quad \text{at } (0, 0)$$

  similarly,

  $$g(x, y) = \frac{y}{x} = \frac{x^2 - 1}{y} = \infty \quad \text{at } (0, 0)$$

Functions on E - (2)

- (Continue):
  - (3) Any function can always be transformed in this manner so as to obtain an expression that is not $0/0$ and hence gives an uniquely value in $\overline{K} \cup \{\infty\}$
  - (4) Definition
    A function f has a zero at P if $f(P) = 0$
    A function f has a pole at P if $f(P) = \infty$

Order of f at P - (1)

(1) Definition

For each P , $\exists$ a function u_P (a uniformizer at P) with $u_P(P) = 0$ and such that every function $f(x, y)$ can be written in

$$f = u_P^r g, \quad \text{with} \quad r \in \mathbb{Z} \text{ and } g(P) \neq 0, \infty$$
$$r \triangleq ord_P(f) \ : \text{ order of } f \text{ at } P$$

(2) Example

$y^2 = x^3 - x$, $u_{(0,0)}(x, y) = y$ a uniformizer at $(0, 0)$

$ord_{(0,0)}(x) =$?

$$\because x = y^2 \frac{1}{x^2 - 1} \quad \therefore ord_{(0,0)}(x) = 2$$

and $ord_{(0,0)}(x/y) = 1$

Order of f at P - (2)

(3) For $P = (x_0, y_0)$, uniformizer u_P can be taken from the equation of a line that passes through P but is not tangent to E .
A natural choice is $u_P = x - x_0$ when $y_0 \neq 0$ and $u_P = y$ when $y_0 = 0$

Examples

$y^2 = x^3 + 72, \quad P = (-2, 8), \quad u_P(x, y) = x + 2$

1. $f(x, y) = x + y - 6, \quad f(P) = 0$
   $y^2 = x^3 + 72 \rightarrow (y + 8)(y - 8) = (x + 2)^3 - 6(x + 2)^2 + 12(x + 2)$

   $$\therefore \ f(x, y) = (x+2)+(y-8) = (x+2)\left(1 + \frac{(x + 2)^2 - 6(x + 2) + 12}{y + 8}\right)$$

   so $ord_P(f) = 1$

Order of f at P - (3)

(3) Example (continue):

2. $t(x, y) = \frac{3}{4}(x+2) - y + 8$
   (come from the tangent line to E at P)

$$\begin{aligned} t(x, y) &= (x+2)\left(\tfrac{3}{4} - \tfrac{(x+2)^2 - 6(x+2) + 12}{y+8}\right) \\ &= \tfrac{(x+2)}{4(y+8)}\left(-4(x+2)^2 + 24(x+2) + 3(y-8)\right) \\ &= \tfrac{(x+2)^2}{4(y+8)}\left(-4(x+2) + 24 + 3\tfrac{(x+2)^2 - 6(x+2) + 12}{y+8}\right) \end{aligned}$$

$\therefore\ ord_P(t) = 2$

Order of f at P - (4)

(4) The point at ∞ is a little harder to deal with.

$$y^2 = x^3 + Ax + B \quad \text{a uniformizer at } \infty \text{ is } u_\infty = x/y$$

Let's compute $ord_\infty(x)$ and $ord_\infty(y)$

$$\left(\frac{x}{y}\right)^2 = x^{-1}\left(1 + \frac{A}{x^2} + \frac{B}{x^3}\right)^{-1}$$
$$\rightarrow\ x = \left(\frac{x}{y}\right)^{-2}\left(1 + \frac{A}{x^2} + \frac{B}{x^3}\right)^{-1} \quad \therefore\ ord_\infty(x) = -2$$
$$\rightarrow\ y = x\left(\frac{y}{x}\right) = \left(\frac{x}{y}\right)^{-3}\left(1 + \frac{A}{x^2} + \frac{B}{x^3}\right)^{-1} \quad \therefore\ ord_\infty(y) = -3$$

Divisor of f - (1)

(1) Definition

f is a function on E , $f \neq 0$

the divisor of f

$$div(f) \triangleq \sum_{P \in E(\overline{K})} ord_P(f)[P] \in Div(E)$$

(2) Proposition 11.1

$f \neq 0$ is a function on E . Then

1. f has only finitely many zeros and poles
2. $\deg(div(f)) = 0$
3. If f has no zero or pole (so $div(f) = 0$), then f is a constant.

(3) Definition

A divisor D is a principal divisor if it is the divisor of a function.

i.e. $D = div(f)$, for some f

Divisor of f - (2)

(4) Suppose P_1, P_2, P_3 are 3 points on E that lie on the line $ax + by + c = 0$
Then $f(x, y) = ax + by + c$ has zeros at P_1, P_2, P_3 . If $b \neq 0$ then f has a triple pole at ∞ .
Therefore

$$div(ax + by + c) = [P_1] + [P_2] + [P_3] - 3[\infty]$$

The line through $P_3 = (x_3, y_3)$ and $-P_3$ is $x - x_3 = 0$.

$$div(x - x_3) = [P_3] + [-P_3] - 2[\infty]$$

Divisor of f - (3)

(4) (Continue)
Therefore,

$$div\left(\frac{ax+by+c}{x-x_3}\right) = div(ax+by+c) - div(x-x_3)$$

$$= [P_1] + [P_2] - [-P_3] - [\infty]$$

Since $P_1 + P_2 = -P_3$ on E . So

$$[P_1] + [P_2] = [P_1 + P_2] + [\infty] + div\left(\frac{ax+by+c}{x-x_3}\right)$$

Theorem 11.2 and Corollary 11.4

Theorem 11.2

D : divisor on E with $\deg(D) = 0$

$\rightarrow$ *$\exists\ f$ on E with $div(f) = D$ if and only if $sum(D) = \infty$*

Corollary 11.4

The map

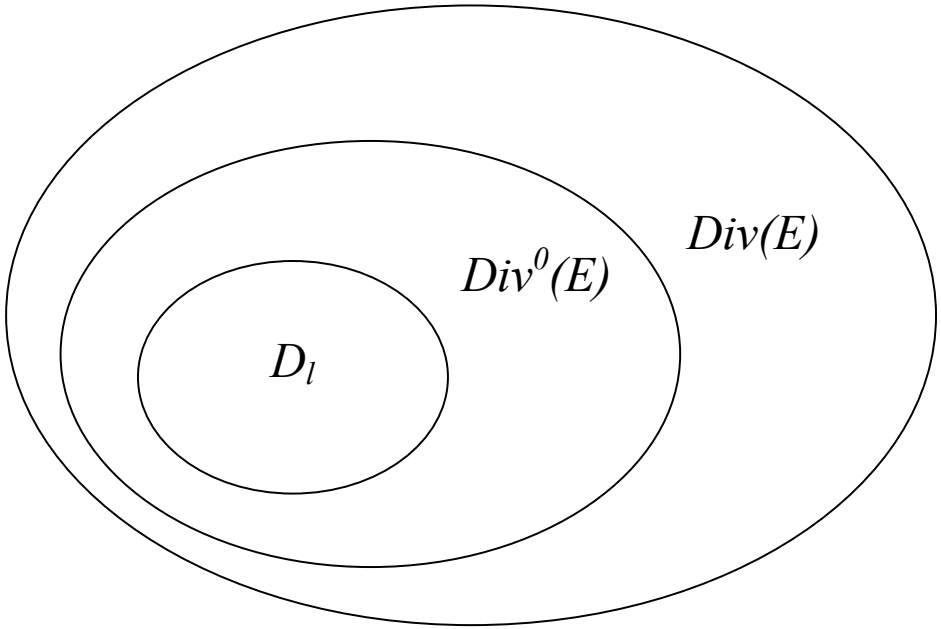
$$sum : Div^0(E)/(principaldivisors) \rightarrow E(\overline{K})$$

is an isomorphism of groups

Proof:

- $\because\ sum([P] - [\infty]) = P$ $\quad\quad$ $\therefore$ surjective
  The theorem says that the kernel is exactly the principal divisors.

Group relation of $Div(E)$, $Div^0(E)$, D_l



D_l : principal divisors on E

Example 11.4 - (1)

- $E/F_{11} : y^2 = x^3 + 4x$,
  $D = [(0,\ 0)] + [(2,\ 4)] + [(4,\ 5)] + [(6,\ 3)] - 4[\infty]$
  $\because\ \deg(D) = 0, \quad sum(D) = \infty$
  By theorem, D is a divisor of a function.
  Let's find the function.

  (1) The line through $(0,\ 0)$, $(2,\ 4)$ is $y - 2x = 0$.
  It is tangent to E at $(2,\ 4)$, so
  $div(y - 2x) = [(0,\ 0)] + 2[(2,\ 4)] - 3[\infty]$

  (2) The vertical line through $(2,\ 4)$ is $x - 2 = 0$,
  $div(x - 2) = [(2,\ 4)] + [(2,\ -4)] - 2[\infty]$

$$\therefore\ D = [(2, -4)] + div\left(\frac{y - 2x}{x - 2}\right) + [(4,\ 5)] + [(6,\ 3)] - 3[\infty]$$

Example 11.4 - (2)

- (Continue):
  (3) Similarly,

$$[(4,\,5)] + [(6,\,3)] = [(2,\,4)] + [\infty] + div\left(\frac{y+x+2}{x-2}\right)$$

$$\rightarrow\ D = [(2,\,-4)] + div\left(\frac{y-2x}{x-2}\right) + [(2,\,4)] + div\left(\frac{y+x+2}{x-2}\right) - 2[\infty]$$

$$\rightarrow\ D = div(x-2) + div\left(\frac{y-2x}{x-2}\right) + div\left(\frac{y+x+2}{x-2}\right)$$

$$= div\left(\frac{(y-2x)(y+x+2)}{x-2}\right)$$

(4) $(y-2x)(y+x+2) = y^2 - xy - 2x^2 + 2y - 4x$
$= x^3 - xy - 2x^2 + 2y$ (Since $y^2 = x^3 + 4x$)
$= (x-2)(x^2-y)$

$\therefore\ D = div(x^2 - y)$