2.8 Endomorphisms

Rong-Jaye Chen

Department of Computer Science, National Chiao Tung University

ECC 2008

Outline

Definition of endomorphism

- Define Endomorphism of E:

$$\text{homomorphism } \alpha : E(\overline{K}) \rightarrow E(\overline{K})$$

$$\alpha \text{ is given by rational functions}$$

i.e.

1. $\alpha(x, y) = (R_1(x, y), R_2(x, y))$
   with rational functions (quotients of polynomials) $R_1(x, y)$, $R_2(x, y)$
   with coefficients in $\overline{K}$, $\forall(x, y) \in E(\overline{K})$

2. $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$

Example

Example

$E: \quad y^2 = x^3 + Ax + B$, $\alpha(P) = 2P$

Then α is a homomorphism and $\alpha(x, y) = (R_1(x, y), R_2(x, y))$, where

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x$$

$$R_2(x, y) = \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y$$

$\therefore \alpha$ is an endomorphism of E.

Transformation of rational functions

- Rewrite

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y} \qquad \left(\times \frac{p_3(x) - p_4(x)y}{p_3(x) - p_4(x)y} \right)$$

$$\rightarrow R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)} \qquad (2.10)$$

- Since $\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y)$
  $\rightarrow R_1(x,-y) = R_1(x,y)$ and $R_2(x,-y) = -R_2(x,y)$
- If R_1 is written in the form (2.10), then $q_2(x) = 0$
- If R_2 is written in the form (2.10), then $q_1(x) = 0$

Transformation of rational functions (Continue)

- So we assume

$$\alpha(x, y) = (r_1(x), r_2(x)y) \quad \text{with rational } r_1(x),\ r_2(x)$$

  write $r_1(x) = p(x)/q(x)$

- If $q(x) = 0$ for some (x, y) , then assume $\alpha(x, y) = \infty$
- If $q(x) \neq 0$, then $r_2(x)$ is defined. (Ex.2.14)

Definition

- Define degree of endomorphism α :

$$\deg(\alpha) = \max\{\deg(\,p(x)\,), \deg(\,q(x)\,)\}$$

$$\text{If } \alpha = 0 \;\rightarrow\; \deg(0) = 0$$

- Define $\alpha \neq 0$ is a separable endomorphism :

If $r_1'(x) \neq 0 \quad \Leftrightarrow$ at least one of $p'(x)$ and $q'(x)$ is not zero

Example 2.5

Example

Endomorphism $\alpha(P) = 2P$ (char. $\neq$ 2,3):

$$R_1(x, y) = (\frac{3x^2 + A}{2y})^2 - 2x$$

$$\rightarrow \quad r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

$\deg(\alpha) = 4$, and α is separable. ($\because q'(x) = 4(3x^2 + A)$ is not zero, including in char. 3, since if $A = 0$, then $x^3 + B$ has multiple roots!)

Example 2.6

Example

In char. 2 (By Section 2.7), $\alpha(P) = 2P$ in $y^2 + xy = x^3 + a_2x^2 + a_6$

$$\alpha(x, y) = (r_1(x), R_2(x, y))$$

$$r_1(x) = \frac{x^4 + a_6}{x^2} \qquad \therefore \deg(\alpha) = 4$$

$$p'(x) = 4x^3 = 0, \quad q'(x) = 2x = 0 \qquad \therefore \alpha \text{ is not separable}$$

In general, E/K, $char.(K) = p$, endomorphism $\alpha(Q) = pQ$
$\rightarrow \deg(\alpha) = p^2$, α is not separable.
(See Proposition 2.27)

Frobenius map

- Define Frobeius map:

$$E/\mathbb{F}_q : \quad \phi_q(x, y) = (x^q, y^q)$$

- Lemma 2.19:
  Let E be defined over $\mathbb{F}_q$. Then ϕ_q is an endomorphism of E of degree q, and ϕ_q is not separable

Proposition 2.20

Proposition 2.20

Let $\alpha \neq 0$ *be a separable endomorphism of an elliptic curve* E*. Then*

$$\deg \alpha = \#Ker(\alpha),$$

where $Ker(\alpha)$ *is the kernel of the homomorphism* $\alpha : E(\overline{K}) \to E(\overline{K})$*.*
If $\alpha \neq 0$ *is not separable, then*

$$\deg \alpha > \#Ker(\alpha).$$

Proof

- Write $\alpha(x,y) = (r_1(x), yr_2(x))$ with $r_1(x) = p(x)/q(x)$

  If α is separable, then $r_1' \neq 0$ so $p'q - pq'$ is not the zero polynomial.

  Let S be the set of $x \in \overline{K}$ such that $(pq' - p'q)(x)q(x) = 0$

  Let $(a,b) \in E(\overline{K})$, satisfying

  1. $a \neq 0$, $b \neq 0$, $(a,b) \neq \infty$
  2. $\deg(p(x) - aq(x)) = \max\{\deg(p), \deg(q)\} = \deg(\alpha)$
  3. $a \notin r_1(S)$
  4. $(a,b) \in \alpha(E(\overline{K}))$

  $\because pq' - p'q$ is not zero polynomial, $\therefore S$ is a finite set.

Proof - continue

- Given $(a, b) \in E(\overline{K})$
  We claim exactly $\deg(\alpha)$ points $(x_1, y_1) \in E(\overline{K})$ such that $\alpha(x_1, y_1) = (a, b)$.

  For such a point,

  $$\frac{p(x_1)}{q(x_1)} = a, \quad y_1 r_2(x_1) = b$$

  Since $(a, b) \neq \infty$, $\therefore q(x_1) \neq 0$, $r_2(x_1)$ is defined.

  $$\therefore y_1 = \frac{b}{r_2(x_1)} \quad \text{so we only need to count values of } x_1$$

  By assumption (2), $p(x) - aq(x) = 0$ has $\deg(\alpha)$ roots, counting multiplicities.

Proof - continue

- Suppose x_0 is a multiple root. Then

$$p(x_0) - aq(x_0) = 0 \quad \text{and} \quad p'(x_0) - aq'(x_0) = 0$$

multiplying $p = aq$ and $aq' = p'$ yields

$$ap(x_0)q'(x_0) = ap'(x_0)q(x_0)$$

$\because a \neq 0 \quad \rightarrow \quad x_0$ is a root of $pq' - p'q$
so $x_0 \in S$.
Therefore, $a = r_1(x_0) \in r_1(S)$, contrary to assumption (3).
$\therefore p - aq$ has no multiple roots, and therefore has $\deg(\alpha)$ distinct roots.
$\because$ there are exactly $\deg(\alpha)$ points with $\alpha(x_1, y_1) = (a, b)$, the kernel of α has $\deg(\alpha)$ elements.

- If α is not separable, trivial now.

Theorem 2.21

Theorem 2.21

Let E be an elliptic curve defined over a field K. Let $\alpha \neq 0$ be an endomorphism of E.
Then $\alpha : E(\overline{K}) \to E(\overline{K})$ is surjective.

Proof:

- Let $(a, b) \in E(\overline{K})$.
  Since $\alpha(\infty) = \infty$, we may assume that $(a, b) \neq \infty$
  Let $r_1(x) = p(x)/q(x)$
  Consider two cases:
  1. $p(x) - aq(x)$ is not constant polynomial
  2. $p(x) - aq(x)$ is constant polynomial

Proof - continue

- If $p(x) - aq(x)$ is not constant polynomial, then it has a root x_0.
  Choose $y_0 \in \overline{K}$ to be either square root of $x_0^3 + Ax_0 + B$.
  Then $\alpha(x_0, y_0)$ is defined and equals (a, b') for some b'.
  Since $b'^2 = a^3 + Aa + B = b^2 \quad \rightarrow \quad b' = \pm b$
  If $b' = b$, we're done.
  If $b' = -b$, then $\alpha(x_0, -y_0) = (a, -b') = (a, b)$
- If $p(x) - aq(x)$ is constant polynomial.
  $\rightarrow$ see Textbook p: 51

Lemma 2.23

Lemma 2.23

Let E be the elliptic curve $y^2 = x^3 + Ax + B$ *. Fix a point* (u, v) *on* E *. Write*

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

where $f(x, y)$ *and* $g(x, y)$ *are rational functions of x, y (the coefficients depend on* (u, v) *). Then*

$$\frac{\frac{d}{dx} f(x, y)}{g(x, y)} = \frac{1}{y}.$$

NB. $\frac{d}{dx} f(x, y) = f_x(x, y) + f_y(x, y)y'$

Lemma 2.25

Lemma 2.25

Let $\alpha_1, \alpha_2, \alpha_3$ *be nonzero endomorphisms of an elliptic curve* E *with* $\alpha_1 + \alpha_2 = \alpha_3$ *. Write*

$$\alpha_j(x, y) = (R_{\alpha_j}(x), yS_{\alpha_j}(x)).$$

Suppose there are constants $c_{\alpha_1}, c_{\alpha_2}$ *such that*

$$\frac{R'_{\alpha_1}(x)}{S_{\alpha_1}(x)} = c_{\alpha_1}, \ \frac{R'_{\alpha_2}(x)}{S_{\alpha_2}(x)} = c_{\alpha_2}.$$

Then

$$\frac{R'_{\alpha_3}(x)}{S_{\alpha_3}(x)} = c_{\alpha_1} + c_{\alpha_2}$$

Proposition 2.27

Proposition 2.27

Let E be an elliptic curve defined over a field K , and let n be a nonzero integer. Suppose that multiplication by n on E is given by

$$n(x,y) = (R_n(x), yS_n(x))$$

for all $(x,y) \in E(\overline{K})$, where R_n and S_n are rational functions. Then

$$\frac{R_n'(x)}{S_n(x)} = n.$$

Therefore, multiplication by n is separable if and only if n is not a multiple of $char(K)$.

Proposition 2.28

Proposition 2.28

Let E be an elliptic curve defined over $\mathbb{F}_q$, where q is a power of the prime p .
Let r and s be integers, not both 0. The endomorphism $r\phi_q + s$ is separable if and only if $p \nmid s$

Proof:

- Write the multiplication by r endomorphism as

$$r(x, y) = (R_r(x), yS_r(x)).$$

Then

$$(R_{r\phi_q}(x), yS_{r\phi_q}(x)) = (r\phi_q)(x, y) = (R_r^q(x), y^q S_r^q(x))$$

$$= \left(R_r^q(x), y(x^3 + Ax + B)^{(q-1)/2} S_r^q(x)\right).$$

Proof - continue

- Therefore,

$$c_{r\phi_q} = R'_{r\phi_q}/S_{r\phi_q} = qR_r^{q-1}R'_r/S_{r\phi_q} = 0.$$

Also, $c_s = R'_s/S_s = s$ by Proposition 2.27. By Lemma 2.25,

$$R'_{r\phi_q+s}/S_{r\phi_q+s} = c_{r\phi_q+s} = c_{r\phi_q} + c_s = 0 + s = s.$$

Therefore, $R'_{r\phi_q+s} \neq 0$ if and only if $p \nmid s$.