ISOGENIES

DEF. Let E_1, E_2 be elliptic curves. A morphism

$$\phi : E_1 \longrightarrow E_2 \quad \text{w/} \quad \phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$$ is called an isogeny.

If $\phi(E_1) \neq \{\mathcal{O}_{E_2}\}$ we say that E_1 and E_2 are isogenous.

ex $[0] : E_1 \longrightarrow E_2$

$P \longmapsto \mathcal{O}_{E_2}$

$[m] : E_1 \longrightarrow E_1$

$P \longmapsto [m]P = \underbrace{P+P+\cdots+P}_{m \text{ times}}$ for $m \geq 1$.

THM $E \times E \longrightarrow E$ is a morphism

$(P, Q) \longmapsto P+Q$

$E \longrightarrow E$ is a morphism

$P \longmapsto -P$

ex $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : y^2 = x^3 - 2ax + \underbrace{(a^2-4b)}_{r}x$

$\phi : E_1 \longrightarrow E_2$

$(x,y) \longmapsto \left(\frac{y^2}{x^2} , \frac{y(b-x^2)}{x^2} \right)$

$\hat{\phi} : E_2 \longrightarrow E_1$

$(X,Y) \longmapsto \left(\frac{Y^2}{4X^2} , \frac{Y(r-X^2)}{8X^2} \right)$

(a 2-isogeny)

$\phi \circ \hat{\phi} = [2] : E_2 \to E_2$

$\hat{\phi} \circ \phi = [2] : E_1 \to E_1$

DEF. ϕ is an isogeny, $\phi : E_1 \to E_2$, $\deg \phi = [\bar{K}(E_1) : \phi^* \bar{K}(E_2)]$

$\deg [0] = 0$.

THM. Let $\phi : E_1 \to E_2$ be an isogeny.

Then $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.

Pf. If $\phi = [0]$, clear. Otherwise ϕ is a finite map.

and let $\phi_* : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2)$

$$\text{class of } \sum n_i \cdot (P_i) \longmapsto \text{class of } \sum n_i (\phi(P_i))$$

Recall: $\mathrm{Pic}^0(E_i) \cong E_i$

(NOTE: ϕ_* is well-defined : $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$)

$$\begin{array}{ccc} E_1 & \cong & \mathrm{Pic}^0(E_1) \\ \phi \downarrow & \circlearrowright & \downarrow \phi_* \\ E_2 & \cong & \mathrm{Pic}^0(E_2) \end{array}$$

The diagram commutes:

$$\begin{array}{ccc} P & \longmapsto & [(P) - (O)] \\ \downarrow & & \downarrow \\ \phi(P) & & [(\phi(P)) - (\phi(O))] \\ & \searrow & \\ & & [(\phi(P)) - (O)] \end{array}$$

$$\begin{array}{ccc} E_1 & \cong & \mathrm{Pic}^0(E_1) \\ \phi \downarrow & \circlearrowright & \downarrow \phi_* \\ E_2 & \cong & \mathrm{Pic}^0(E_2) \end{array}$$

$$P+Q \longmapsto (P+Q)-(\mathcal{O}) \sim (P)-(\mathcal{O})+(Q)-(\mathcal{O})$$

$$(P+Q)-(P)-(Q)+(\mathcal{O}) = \mathrm{div}(\ell/v) \sim 0$$

$$\Rightarrow (P+Q)-(\mathcal{O}) \sim (P)-(\mathcal{O})+(Q)-(\mathcal{O})$$

$$\begin{array}{ccc} \phi(P+Q) & \xrightarrow{\cong} & (\phi(P+Q))-(\mathcal{O}) \sim (\phi(P))-(\mathcal{O})+(\phi(Q))-(\mathcal{O}) \\ \| & & \\ \phi(P)+\phi(Q) & & \end{array}$$

Cor. $\phi : E_1 \to E_2$ a non-const. isogeny. Then $\ker\phi = \phi^{-1}(\mathcal{O})$ is a finite subgp of E_1. In particular $\#\ker\phi \le \deg\phi$.

Pf. $\sum_{P \in \phi^{-1}(\mathcal{O})} e_\phi(P) = \deg\phi \quad \Rightarrow \#\phi^{-1}(\mathcal{O}) \le \deg\phi.$ ∎

DEF. Let E_1, E_2 be ell. curves over K.

- $\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\}$ ($\mathrm{Hom}(E_1,E_2)$ is a gp under addition: $(\phi+\psi)(P) = \phi(P)+\psi(P)$)
- $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ ($\mathrm{End}(E)$ is a ring under $+$, $\circ$ composition: $(\phi\psi)(P) = \phi(\psi(P))$)
- $\mathrm{Aut}(E)$