

ISOGENIES

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

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

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

ex $[0]: E_1 \rightarrow E_2$
 $P \mapsto \mathcal{O}_{E_2}$

$$[m]: E_1 \rightarrow E_1$$

$$P \mapsto [m]P = \underbrace{P + P + \dots + P}_{m \text{ times}}$$

for $m \geq 1$.

THM

$E \times E \rightarrow E$ is a morphism

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

$$E \rightarrow E$$

$$P \mapsto -P$$

is a morphism

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

$$\phi: E_1 \longrightarrow E_2$$

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

(a 2-isogeny)

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

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

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

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

DEF. ϕ is an isogeny, $\deg \phi = [\bar{K}(E_1) : \phi^* \bar{K}(E_2)]$
 $\phi: E_1 \rightarrow E_2$
 $\deg [0] = 0.$

THM. Let $\phi: E_1 \rightarrow E_2$ 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.

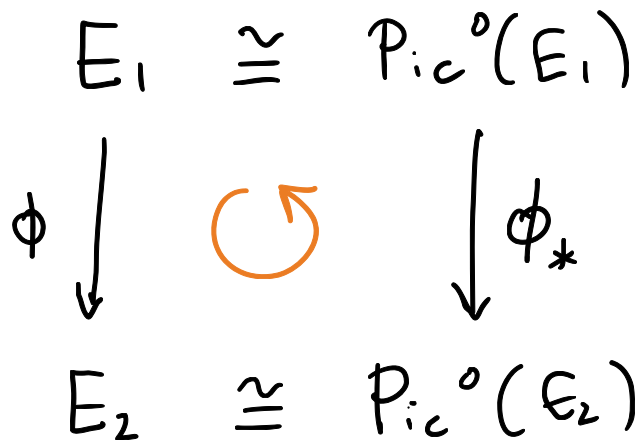
and let $\phi_*: \text{Pic}^0(E_1) \rightarrow \text{Pic}^0(E_2)$

class of $\sum n_i \cdot (P_i) \mapsto$ class of $\sum n_i (\phi(P_i))$

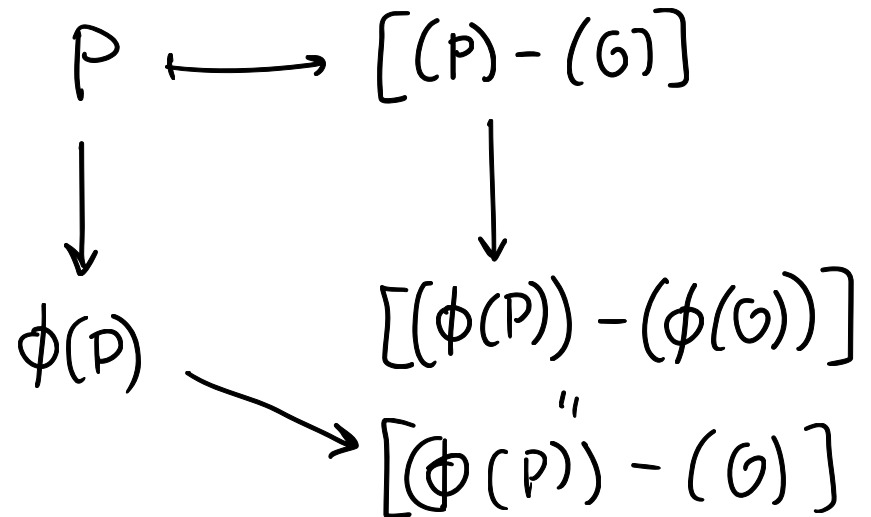
Recall:

$\text{Pic}^0(E_i) \cong E_i$

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



The diagram commutes:



$$E_1 \cong \text{Pic}^0(E_1)$$

$$\phi \downarrow \quad \hookrightarrow \quad \downarrow \phi_*$$

$$E_2 \cong \text{Pic}^0(E_2)$$

$$P+Q \mapsto (P+Q)-(0) \sim (P)-(0) + (Q)-(0)$$

$$(P+Q)-(P)-(Q)+(0) = \text{div}\left(\frac{f}{g}\right) \sim 0$$

$$\Rightarrow (P+Q)-(0) \sim (P)-(0) + (Q)-(0)$$

$$\phi(P+Q) \xrightarrow{\cong} (\phi(P+Q))-(0) \sim (\phi(P))-(0) + (\phi(Q))-(0)$$

$$\parallel$$

$$\phi(P) + \phi(Q)$$

Cor. $\phi: E_1 \rightarrow E_2$ an $\sqrt{\text{non-d.}}$ isogeny. Then $\ker \phi = \phi^{-1}(0)$ is a finite subgroup of E_1 .
 In particular $\#\ker \phi \leq \deg \phi$.

Pr. $\sum_{P \in \phi^{-1}(0)} e_\phi(P) = \deg \phi \Rightarrow \#\phi^{-1}(0) \leq \deg \phi$ \square

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

- $\text{Hom}(E_1, E_2) = \{ \text{isogenies } : E_1 \rightarrow E_2 \}$ $\left(\begin{array}{l} \text{Hom}(E_1, E_2) \text{ is a gp under} \\ \text{addition: } (\phi + \psi)(P) = \phi(P) + \psi(P) \end{array} \right)$
- $\text{End}(E) = \text{Hom}(E, E)$ $\left(\begin{array}{l} \text{End}(E) \text{ is a ring under } +, \circ \text{ composition} \\ (\phi \psi)(P) = \phi(\psi(P)) \end{array} \right)$
- $\text{Aut}(E)$

