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: $(\phi\psi)(P) = \phi(\psi(P))$)
- $\mathrm{Aut}(E)$ = invertible elts of $\mathrm{End}(E)$
- $\mathrm{Hom}_K(E_1, E_2)$, $\mathrm{End}_K(E)$, $\mathrm{Aut}_K(E)$.

ex $[m] : E \to E$ $\qquad [m] \in \mathrm{End}(E)$

$P \mapsto m \cdot P = P + \cdots + P$, $m > 0$

If $m < 0$, $[m]\cdot P = [-m]\cdot(-P) = \underbrace{(-P)+(-P)+\cdots+(-P)}_{m \text{ times.}}$

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

$[i] : (x, y) \mapsto (-x, iy)$ $\qquad [i] \in \mathrm{End}(E)$.

Prop 4.2 (a) $[m]$ is non-constant (on $E(\bar{k})$) for all $m \neq 0$. $m \in \mathbb{Z}$.

(b) $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.

(c) $\mathrm{End}(E)$ is a ring of char $= 0$ with no zero divisors (not necessarily commutative!).

Pf. Let p be a prime.

(a) Using explicit addition formulas, find $x([p]Q)$, $y([p]Q)$ and thus find $Q \in E(\bar{k})$ of order p for any prime p.

(b) Suppose $\phi \in \mathrm{Hom}(E_1, E_2)$, $m \in \mathbb{Z}$ $\quad m \cdot \phi := [m] \circ \phi$

$$[m] \circ \phi = [0] \Rightarrow \deg[m] \cdot \deg\phi = 0 \rightarrow \begin{cases} \deg[m] = 0 \Rightarrow m = 0. \\ \text{or } \deg\phi = 0 \rightarrow \phi = [0]. \end{cases}$$

$\Rightarrow \mathrm{Hom}(E_1, E_2)$ is torsion free as a $\mathbb{Z}$-module.

(c) From (b), $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is of char 0.

If $\phi \circ \psi = [0]$ then $\deg\phi \cdot \deg\psi = 0 \Rightarrow \begin{cases} \deg\phi = 0 \Rightarrow \phi = [0] \\ \deg\psi = 0 \Rightarrow \psi = [0] \end{cases}$ $\mathrm{End}(E)$ is an int. domain. ▨ □

DEF. $E[m] = \{ P \in E : [m]P = \mathcal{O} \} = E(\bar{K})[m]$

$m \geq 2$. $\quad$ $P \in E(\bar{K})$

$E(K)[m] = \{ P \in E(K) : [m]P = \mathcal{O} \} \subseteq E[m]$.

$E_{TORS} = \bigcup_{m=1}^{\infty} E[m]$

DEF. (NOTE: $[\cdot] : \mathbb{Z} \longrightarrow End(E)$ is an injection)

$m \longmapsto [m]$ $\quad$ $(\mathbb{Z} \subseteq End(E))$

If $\mathbb{Z} \subsetneq End(E)$, then we say that E has complex multiplication or that E has CM.

ex $E : y^2 = x^3 - x$ $\quad$ $End(E) \supsetneq \{ [m] : m \in \mathbb{Z} \}$

$[i] : (x,y) \mapsto (-x, iy)$ $\quad$ $[i]$ $\quad$ $[a] + [i]\cdot[b] \longleftrightarrow a + bi$

$\rightsquigarrow End(E) \cong \mathbb{Z}[i]$

(E has CM by $\mathbb{Z}[i]$.)

ISOGENIES (CONTINUED)

NOTE: $[m] : E \to E$ non-constant.

$$[m]([x,y,z]) = [f(x,y,z), g(x,y,z), h(x,y,z)] \stackrel{?}{=} [0,1,0].$$

THM 4.10 Let $\phi : E_1 \to E_2$ be a non-zero separable isogeny.

(a) (non-sep)

(b) The map

$$\begin{aligned} \ker\phi &\xrightarrow{\cong} \mathrm{Aut}\left(\bar{K}(E_1)/\phi^*\bar{K}(E_2)\right) \\ T &\longmapsto \tau_T^* \end{aligned}$$

is an isomorphism

where $\tau_T : E_1 \to E_1$

$$P \longmapsto P+T$$

(c) ϕ is unramified, $\#\ker\phi = \deg\phi$, and

$$\bar{K}(E_1)/\phi^*\bar{K}(E_2) \text{ is Galois.}$$

(c) $\#\ker\phi = \deg\phi$.

Recall: $\#\phi^{-1}(Q) = \deg\phi$ for almost all $Q \in E_2$.

Suppose Q s.t. $\#\phi^{-1}(Q) = \deg\phi$
and let $Q' \in E_2$. Then, let $T \in E_2$ s.t. $Q+T=Q'$
and let $\phi^{-1}(T) = P$.

Then if $\phi(S) = Q$ then $\phi(S+P) = Q + T = Q'$

Thus, $\deg\phi \geq \#\phi^{-1}(Q') \geq \#\{S+P : S \in \phi^{-1}(Q)\} = \#\phi^{-1}(Q) = \deg\phi$

$S+P = S'+P \Rightarrow S=S'$

$\Rightarrow \#\phi^{-1}(Q') = \deg\phi$. ✓

$\Longrightarrow \#\phi^{-1}(Q) = \deg\phi \ \ \forall Q \in E_2 \Rightarrow \phi$ is unramified.

- By (b) $\#\mathrm{Aut}\left(\overline{k}(E_1)/\phi^*\overline{k}(E_2)\right) = \#\ker\phi = \deg\phi = \left[\overline{k}(E_1)/\phi^*\overline{k}(E_2)\right]$

$\Rightarrow$ Galois! ▨

COR 4.11 Let $\phi : E_1 \to E_2$, $\psi : E_1 \to E_3$ be (sep) isogenies.

If $\ker\phi \subseteq \ker\psi$ then $\exists!$ (isogeny) $\lambda : E_2 \to E_3$ s.t. $\psi = \lambda \circ \phi$.

Pf. $\ker\phi \subseteq \ker\psi \Rightarrow \psi^*\bar{K}(E_3) \subseteq \phi^*\bar{K}(E_2) \subseteq \bar{K}(E_1)$

$\Rightarrow \exists!\ \lambda : E_2 \to E_3$ s.t. $\phi^*(\lambda^*(\bar{K}(E_3))) = \psi^*\bar{K}(E_3)$

$\Rightarrow \lambda \circ \phi = \psi$. Moreover $\lambda(O) = \lambda(\phi(O)) = \psi(O) = O$.

PROP 4.12. Let E be an ell. curve, and let Φ be a fin. subgp of E.

Then $\exists!\ E'$, $\phi : E \to E'$ isogeny s.t. $\ker\phi = \Phi$. (NOTATION: $E' = E/\Phi$, $E \to E/\Phi$)

Sketch Pf $T \in \Phi \rightsquigarrow \tau_T : E \to E$, $P \mapsto P+T$ $\rightsquigarrow \tau_T^*$ automorphism of $\bar{K}(E)$.

$\bar{K}(E)^{\Phi}$ fixed field by $\{\tau_T^*\}$, $\Phi = \mathrm{Gal}(\bar{K}(E)/\bar{K}(E)^{\Phi})$ — trans deg 1 fin fields.

$\Rightarrow \exists\, C, \phi$ $\phi : E \to C$ s.t. $\phi^*\bar{K}(C) = \bar{K}(E)^{\Phi}$

Last step: use Hurwitz formula to prove that genus of C is 1. ▨

Q $\phi : E \to E$ is a morphism, $\phi(O) = O$ $\Rightarrow$ gp hom.

(isogeny.)

Suppose $E(\bar{k}) \to E(\bar{k})$ is a gp hom. ... is this a rational map?

DEF. An abelian gp D is called divisible if the map $x \mapsto nx$ is surjective $\forall n \geq 1$.

COR. (of Zorn's Lemma) Let D be a divisible gp. If A is any abelian gp and $B \subseteq A$ is any subgp., then any homomorphism $f : B \to D$ can be extended to a hom. $\hat{f} : A \to D$.

APPLICATION: Take $A = D = E(\bar{k})$, let P, Q be two lin. indep. pts on $E(\bar{k})$ of infinite order ($nP \neq mQ$ for any $n, m \in \mathbb{Z}$).

Consider $B = \langle P, Q \rangle$ and $f : B \to E(\bar{k})$
$aP + bQ \mapsto aP \quad \forall a, b \in \mathbb{Z}$ $\left(\begin{matrix} P \mapsto P \\ Q \mapsto O \end{matrix}\right)$

Then COR $\Rightarrow$ $\hat{f} : E(\bar{k}) \to E(\bar{k})$ extends f., a gp. hom.

But $\hat{f}$ is non-constant ($\hat{f}(P) = P$), AND $\ker \hat{f} \supseteq \langle Q \rangle$ is infinite!

THUS $\hat{f}$ CANNOT BE AN ISOGENY B/C $\#\ker \hat{f} = \infty$!!

Remark. A cyclic isogeny is an isogeny $\phi : E \to E_1$ s.t. $\ker \phi$ is cyclic.

An isogeny is K-rational if ϕ / K.

Cyclic rational isogenies for elliptic curves $/\mathbb{Q}$ are completely classified.

ex $E/\mathbb{Q}$ w/ a 3-isogeny $\iff \exists\, t \in \mathbb{Q}^{\neq 0}$ s.t. $j(E) = \dfrac{(t+27)(t+3)^3}{t}$

... 5-isogeny $\iff \exists\, t \in \mathbb{Q}^{\neq 0,*}$ s.t. $j(E) = \dfrac{(t^2+10t+5)^3}{t}$

$\vdots$

... 27-isogeny $\iff j(E) = -2^{15} \cdot 3 \cdot 5^3$.

DEGREES:

$2 - 10, 12, 13, 16, 18, 25$, $11, 14, 15, 17, 19, 21, 27, 37, 43, 67, 163$, other

inf. many j's | $0 <$ fin. many j's | no j's.

THE DUAL ISOGENY

PREVIOUSLY... **COR 4.11** Let $\phi: E_1 \to E_2$, $\psi: E_1 \to E_3$ be sep. (non-c.) isogenies s.t. $\ker\phi \subseteq \ker\psi$. Then $\exists!$ isogeny $\lambda: E_2 \to E_3$ s.t. $\psi = \lambda \circ \phi$.

ex $E_1 : y^2 = x^3 + ax^2 + bx$, $E_2 : Y^2 = X^3 - 2aX + (a^2 - 4b)X$

$\phi : E_1 \longrightarrow E_2$, $(x,y) \longmapsto \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\right)$ "r"

$\hat{\phi} : E_2 \longrightarrow E_1$, $(X,Y) \longmapsto \left(\frac{Y^2}{4X^2}, \frac{Y(r-X^2)}{8X^2}\right)$

s.t. $\phi \circ \hat{\phi} = [2]$ and $\hat{\phi} \circ \phi = [2]$.

Let $\phi: E_1 \to E_2$ an isogeny. (unramified!)

$\phi^* : \mathrm{Div}(E_2) \to \mathrm{Div}(E_1)$

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

$\rightsquigarrow \phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_2)$

- $\deg \phi^* D = (\deg \phi) \cdot (\deg D)$

  $\mathrm{Div}^0(E_2) \to \mathrm{Div}^0(E_1)$

- $\phi^*(\mathrm{div}\, g) = \mathrm{div}(\phi^* g)$

  $\mathrm{Princ}(E_2) \to \mathrm{Princ}(E_1)$

Induces $\phi^*: \mathrm{Pic}^0(E_2) \longrightarrow \mathrm{Pic}^0(E_1)$

$$[(Q)] \longmapsto \left[\sum_{P \in \phi^{-1}(Q)} (P)\right]$$

NOTE.

If P' also $\phi(P') = Q$ then $P' = P + T$ w/ $T \in \ker \phi$ and $\phi(T) = O$

$$[\deg\phi](P') = [\deg\phi](P+T) = [\deg\phi]P + [\deg\phi]T = [\deg\phi]P$$

Recall: $\kappa_i : E_i \cong \mathrm{Pic}^0(E_i)$ $i = 1, 2$

$$P \longmapsto [(P) - (O)]$$

Get: $E_2 \xrightarrow{\kappa_2} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{\kappa_1^{-1}} E_1$, with $\hat{\phi}$ the composite $E_2 \to E_1$.

$\#\ker\phi = \#\phi^{-1}(O)$

$\#\phi^{-1}(Q) = [\deg\phi]\,\#\phi^{-1}(O)$

Let $Q \in E_2$, let $P \in E_1$ s.t. $\phi(P) = Q$. Then

$$Q \xmapsto{\kappa_2} (Q) - (O) \xmapsto{\phi^*} \sum_{S \in \phi^{-1}(Q)} (S) - \sum_{T \in \phi^{-1}(O)} (T) = \sum_{S \in \phi^{-1}(Q)} (S) - (O) - \sum_{T \in \phi^{-1}(O)} (T) - (O)$$

$$\longmapsto \sum_{S \in \phi^{-1}(Q)} S - \sum_{T \in \phi^{-1}(O)} T = \sum_{T \in \phi^{-1}(O)} P + T - \sum_{T \in \phi^{-1}(O)} T = \sum_{T \in \phi^{-1}(O)} P = [\#\phi^{-1}(O)] \cdot P = [\deg\phi] \cdot P$$

if $\phi(P) = Q$, then $\phi(P+T) = Q$, i.e. $\phi(P) + \phi(T)$

if $T \in \ker\phi = \phi^{-1}(O)$

$$E_2 \xrightarrow{k_2} \mathrm{Pic}^0(E_2) \xrightarrow{\phi^*} \mathrm{Pic}^0(E_1) \xrightarrow{k_1^{-1}} E_1$$

$$Q \longmapsto [\deg\phi]\cdot P$$

in the video I made a mistake and said $P \longmapsto [\deg\phi](P)$ but $Q \longmapsto [\deg\phi](P)$ is NOT clearly an isogeny. The proof below shows it is an isogeny!

THM 6.1 Let $\phi: E_1 \to E_2$ be an isogeny of degree $m \geq 1$. (separable)

(a) $\exists!$ isogeny $\hat{\phi}: E_2 \longrightarrow E_1$ s.t. $\hat{\phi}\circ\phi = [m] = [\deg\phi]$.

(b) As a gp hom. $\hat{\phi} = k_1^{-1}\circ\phi^*\circ k_2$.

Pf. (a) Uniqueness. $\hat{\phi}, \hat{\phi}'$ are such that $\hat{\phi}\circ\phi = [m] = \hat{\phi}'\circ\phi$

$$\to (\hat{\phi} - \hat{\phi}')\circ\phi = [m] - [m] = [0]$$

Since ϕ is non-constant, $\hat{\phi} - \hat{\phi}'$ must be constant $\Rightarrow \hat{\phi} = \hat{\phi}'$.

- $\#\ker\phi = \deg\phi = m$, so $\ker\phi \subseteq \ker[m] \Rightarrow \exists!$ isogeny $\hat{\phi}: E_2 \to E_1$ s.t. $\hat{\phi}\circ\phi = [m]$, and $\to \hat{\phi} = k_1^{-1}\circ\phi^*\circ k_2$

$$\hat{\phi}(Q) = \hat{\phi}(\phi(P)) = [m]P = [\deg\phi]P = (k_1^{-1}\circ\phi^*\circ k_2)(Q)$$ ▨

DEF. Let $\phi : E_1 \to E_2$ be an isogeny.
The isogeny $\hat{\phi} : E_2 \to E_1$ s.t. $\hat{\phi} \circ \phi = [m]$
is called the dual isogeny.

THM 6.2. $\phi : E_1 \to E_2$, $\deg \phi = m$

(a) $\hat{\phi} \circ \phi = [m]_{E_1}$, $\phi \circ \hat{\phi} = [m]_{E_2}$

(b) $\lambda : E_2 \to E_3$ isog. then $\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}$

(c) $\psi : E_1 \to E_2$ isog. then $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$

(d) $\forall m \in \mathbb{Z}$ $\widehat{[m]} = [m]$, $\deg [m] = m^2$

Clear $m=0$, $m=1$

Induction on m:

$\widehat{[m+1]} = \widehat{[m]} + \widehat{[1]}$

$= [m] + [1] = [m+1]$

and $d = \deg [m]$

$[d] = \widehat{[m]} \circ [m] = [m] \circ [m]$

$= [m^2]$

$\Rightarrow d = m^2$.

(e) $\deg \hat{\phi} = \deg \phi$

(f) $\hat{\hat{\phi}} = \phi$.

Cor • $\#E[m] = m^2$

• If $\mathrm{char}(k) = 0$ (or if $\gcd(\mathrm{char}(k), m) = 1$) then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

$$\| \quad E(\overline{k})[m]$$

• If $\mathrm{char}(k) = p$ then either $\begin{cases} E[p^e] \cong \{0\} & \forall e = 1,2,3\ldots \\ E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} & \forall e \geq 1. \end{cases}$

Pf • $\#E[m] = \#\ker[m] = \deg[m] = m^2$.

• $\#E[m] = m^2$ and $d \mid m$, then $\#E[d] = d^2$ and $E[d] \subseteq E[m]$.

$E[m]$ is a finite ab gp:

- $\#E[m] = m^2$
- $\#E[d] = d^2$ for any $d \mid m$
- $P \in E[m]$, $\mathrm{ord}(P) \mid m$.

$\Rightarrow E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

exercise in gp. theory.

ex p prime

$\#E[p] = p^2$

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ ✓

$\mathbb{Z}/p^2\mathbb{Z}$ ← cannot be $\cdot$ elts of order p^2!

✓