Thm The group hom. $\mathbb{Z} \longrightarrow \mathrm{End}(E)$ is
$m \longmapsto [m]$

injective.

Pf Assume $[m] = 0$, $m \neq 0$.

$m \mid 2^k(2^\ell - 1)$ for some $k \geq 0$, $\ell \geq 1$.

We've shown that $\deg([2]) = 4$.

$\Rightarrow \deg([2^\ell]) = 4^\ell \neq 1$

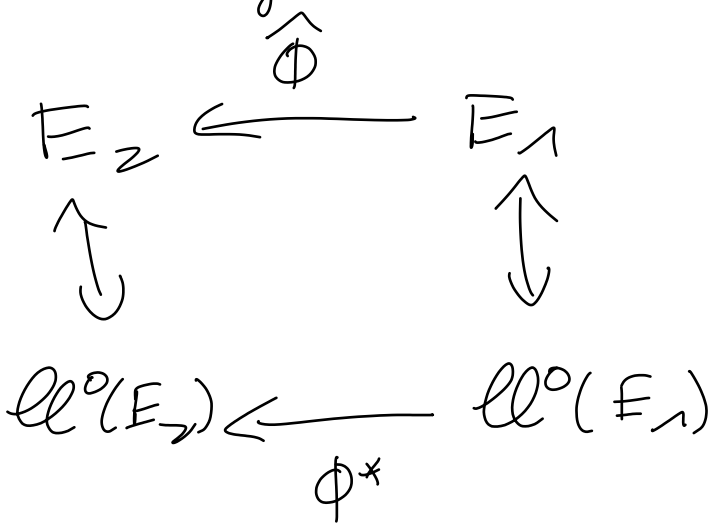
$\Rightarrow [2^\ell] \neq [1] \Rightarrow [2^\ell - 1] \neq 0$

The morphisms $[2]$ and $[2^\ell - 1]$ are nonconstant (= dominant = surjective).

$\Rightarrow [2^k(2^\ell - 1)] \neq 0 \Rightarrow [m] \neq 0$.

□

Def The *dual isogeny* $\hat{\phi}$ of $\phi \neq 0$ is the map given by the following commutative diagram:



The dual of $\phi = 0$ is $\hat{\phi} = 0$.

Ex $\widehat{id} = id$

Rmk $\hat{\phi}$ is a group hom. because ϕ^* is.

But we need to prove it's a morphism!

Rmk $\widehat{\phi_1 \circ \phi_2} = \hat{\phi}_2 \circ \hat{\phi}_1$

Rmk $\phi \circ \hat{\phi} = [\deg(\phi)]$, where we let $\deg(\phi) = 0$ if $\phi = 0$.

Pf $\phi(\phi^*(D)) = \deg(\phi) \cdot D$ □

Rmk $\hat{\phi} \circ \phi = [\deg(\phi)]$

Pf Let $P \in E_1$.

$$\begin{array}{ccc} \hat{\phi}(\phi(P)) & \longleftarrow & \phi(P) \\ \downarrow & & \downarrow \\ \sum_{P' \in \phi^{-1}(\phi(P))} [P'] - \sum_{T \in \phi^{-1}(0)} [T] & \longleftarrow & [\phi(P)] - [0] \end{array}$$

ϕ is unramified, so all multiplicities are 1

$$\Rightarrow \hat{\phi}(\phi(P)) = \sum_{P' \in \phi^{-1}(\phi(P))} P' - \sum_{T \in \phi^{-1}(0)} T$$

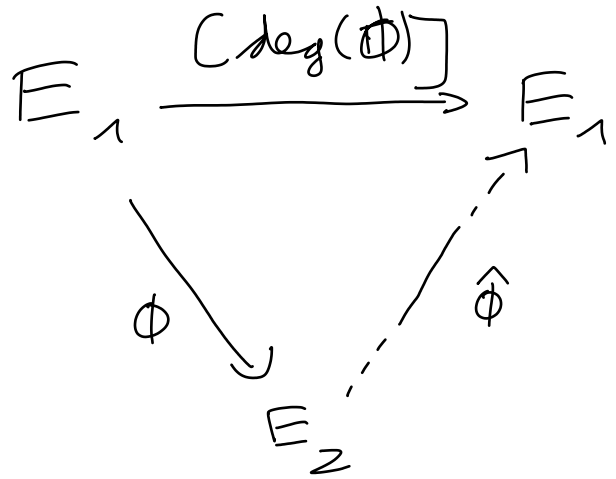
$$= \sum_{T \in \ker(\phi)} ((P+T) - T)$$

$$= \deg(\phi) \cdot P.$$

□

Thm $\hat{\phi}$ is a morphism (and therefore an isogeny).

Pf Assume $\phi \neq 0$.



Since $|\ker(\phi)| = \deg(\phi)$, every element of $\ker(\phi)$ is $\deg(\phi)$ torsion.

$\Rightarrow \ker(\phi) \subseteq \ker([\deg(\phi)])$

$\Rightarrow$ There is a morphism $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [\deg(\phi)]$.

Since $\hat{\phi} \circ \phi = [\deg(\phi)]$ and ϕ is surjective, we have $\hat{\phi} = \hat{\phi}$. □

Def Elliptic curves E_1, E_2 are isomorphic if there is an isogeny $\phi : E_1 \to E_2$ which is an isomorphism (i.e. has degree 1).

They are isogenous if there is a nonconstant isogeny $\phi : E_1 \to E_2$. (symmetry follows from existence of $\hat{\phi}$.)

Thm $\widehat{\phi_1+\phi_2} = \hat{\phi}_1+\hat{\phi}_2$ for any isogenies $\phi_1, \phi_2 : E_1 \to E_2$.

Pf (For more details, see Thm III. 6.2 in Silverman, or Exercise 3.31 in Silverman).

For any $P \in E_1$,

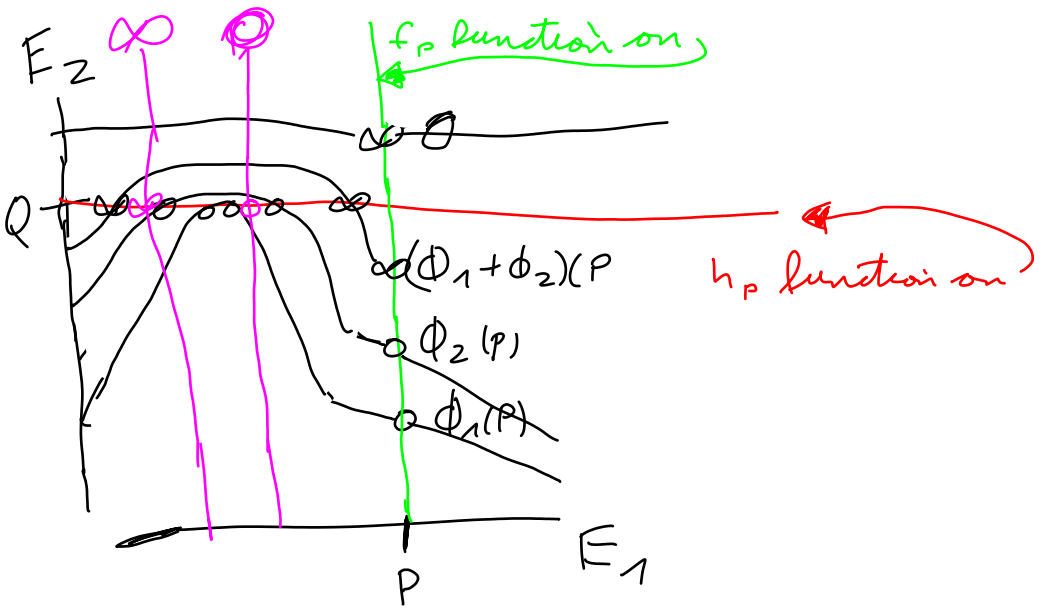
$(\phi_1+\phi_2)(P) = \phi_1(P)+\phi_2(P)$ in E_2 means that there is a rational function $f_P \in K(E_2)^\times$ such that

$$\left([\phi_1(P)]-[O]\right)+\left([\phi_2(P)]-(O]\right)-\left([(\phi_1+\phi_2)(P)]-[O]\right)$$
$$= \operatorname{div}(f_P).$$

We take f_P = quotient of two homogeneous degree 1 pol. with roots at

$\phi_1(P), \phi_2(P), -(\phi_1(P)+\phi_2(P))$
and at
$\phi_1(P)+\phi_2(P), -(\phi_1(P)+\phi_2(P)), O$.
respectively

The coefficients of the rational function f_P are rational functions in the coordinates of P (at all points P where they are defined).



$\rightsquigarrow$ We get a rational function g on $E_1 \times E_2$ with $g(P, Q) = f_P(Q)$ whenever both sides are defined.

For almost all $Q \in E_2$ (those not on a "horizontal" zero or pole of g), we get a rational function $h_Q \in K(E_1)^\times$, with $g(P, Q) = h_Q(P)$ whenever both sides are defined.

$$\operatorname{div}(h_Q) = \phi_1^*(Q) + \phi_2^*(Q) - (\phi_1+\phi_2)^*(Q) + D$$

for some fixed divisor $D \in \operatorname{Div}(E_1)$ independent of Q (corresponding to "vertical" zeros and poles of g).

$\Rightarrow \phi_1^*(Q) + \phi_2^*(Q) - (\phi_1+\phi_2)^*(Q) = -D$ in $\mathrm{Pic}(E_1)$
for almost all $Q \in E_2$

$\Rightarrow \underbrace{\widehat{\phi_1}(Q) + \widehat{\phi_2}(Q) - \widehat{\phi_1+\phi_2}(Q)}_{\text{morphism in } Q} = R$ for almost all $Q \in E_2$ and some fixed $R \in E_1$

$\Rightarrow \widehat{\phi_1}(Q) + \widehat{\phi_2}(Q) - \widehat{\phi_1+\phi_2}(Q) = R$ for all $Q \in E_2$.
$\uparrow$ continuity

For $Q = 0$, LHS $= 0$. $\Rightarrow R = 0$
$\Rightarrow \widehat{\phi_1}(Q) + \widehat{\phi_2}(Q) = \widehat{\phi_1+\phi_2}(Q)$ for all $Q \in E_2$.

□

Lem $\widehat{[m]} = [m]$

Pf Induction over $|m|$. □

Lem $\deg([m]) = m^2$.
In other words, $\#E[m] = m^2$.

(including all points with coordinates in $\bar{k}$)

Pf $\widehat{[m]} \circ [m] = [\deg([m])]$.
$\|$
$[m^2]$
Use that $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ is injective. □

Cor $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$.

Pf HW.

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

Pf Assume $\phi \neq 0$.

$$\hat{\phi} \circ \phi = [\deg(\phi)]$$

$$\Rightarrow \deg(\hat{\phi}) \deg(\phi) = \deg(\phi)^2$$

$$\Rightarrow \deg(\hat{\phi}) = \deg(\phi).$$ □

Thm $\hat{\hat{\phi}} = \phi$

Pf $\hat{\hat{\phi}} \circ \hat{\phi} = [\deg(\hat{\phi})] = [\deg(\phi)] = \phi \circ \hat{\phi}$.

If $\phi \neq 0$, then $\hat{\phi} \neq 0$, so $\hat{\phi}$ is surjective.

$$\Rightarrow \hat{\hat{\phi}} = \phi.$$ □

Thm $\deg : \mathrm{End}(E) \longrightarrow \mathbb{Z}$ is a positive definite quadratic form.

In other words, the following is bilinear:

$$\langle \cdot, \cdot \rangle : \mathrm{End}(E) \times \mathrm{End}(E) \longrightarrow \mathbb{Z}$$

$$(\phi_1, \phi_2) \longmapsto \frac{1}{2}(\deg(\phi_1 + \phi_2) - \deg(\phi_1) - \deg(\phi_2))$$

Pf $[\deg(\phi_1 + \phi_2) - \deg(\phi_1) - \deg(\phi_2)] = \widehat{\phi_1 + \phi_2} \circ (\phi_1 + \phi_2) - \hat{\phi}_1 \circ \phi_1 - \hat{\phi}_2 \circ \phi_2$

$= \hat{\phi}_1 \circ \phi_2 + \hat{\phi}_2 \circ \phi_1$, which is linear in ϕ_1, ϕ_2. □