dual isogeny

Canonical name	DualIsogeny
Date of creation	2013-03-22 12:52:58
Last modified on	2013-03-22 12:52:58
Owner	mathcam (2727)
Last modified by	mathcam (2727)
Numerical id	9
Author	mathcam (2727)
Entry type	Definition
Classification	msc 14-00
Related topic	ArithmeticOfEllipticCurves

Given an isogeny $f : E \to E'$ of elliptic curves of degree n, the *dual isogeny* is an isogeny $\hat{f} : E' \to E$ of the same degree such that $f \circ \hat{f} = [n]$. Here $[n]$ denotes the multiplication-by-n isogeny $e \mapsto ne$ which has degree n^2.

Often only the existence of a dual isogeny is needed, but the construction is explicit as

$$E' \to \mathrm{Div}^0(E') \xrightarrow{f^*} \mathrm{Div}^0(E) \to E$$

where Div^0 is the group of divisors of degree 0. To do this, we need maps $E \to \mathrm{Div}^0(E)$ given by $P \mapsto P - O$ where O is the neutral point of E and $\mathrm{Div}^0(E) \to E$ given by $\sum n_P P \mapsto \sum n_P P$.

To see that $f \circ \hat{f} = [n]$, note that the original isogeny f can be written as a composite

$$E \to \mathrm{Div}^0(E) \xrightarrow{f_*} \mathrm{Div}^0(E') \to E'$$

and that since f is finite of degree n, $f_* f^*$ is multiplication by n on $\mathrm{Div}^0(E')$.

Alternatively, we can use the smaller Picard group Pic^0, a quotient of Div^0. The map $E \to \mathrm{Div}^0(E)$ descends to an isomorphism, $E \xrightarrow{\sim} \mathrm{Pic}^0(E)$. The dual isogeny is

$$E' \xrightarrow{\sim} \mathrm{Pic}^0(E') \xrightarrow{f^*} \mathrm{Pic}^0(E) \xrightarrow{\sim} E$$

Note that the relation $f \circ \hat{f} = [n]$ also implies the conjugate relation $\hat{f} \circ f = [n]$. Indeed, let $\phi = \hat{f} \circ f$. Then $\phi \circ \hat{f} = \hat{f} \circ [n] = [n] \circ \hat{f}$. But $\hat{f}$ is surjective, so we must have $\phi = [n]$.