Seminar: Elliptic curves and the Weil conjectures

The Dual Isogeny

Johannes Loher

July 20, 2016

Theorem 1. *Let $\phi\colon E_1 \to E_2$ be a nonconstant isogeny of degree m.*

(a) There is a unique isogeny

$$\hat{\phi}\colon E_2 \to E_1 \qquad \textit{satisfying} \qquad \hat{\phi} \circ \phi = [m].$$

(b) As a group homomorphism, $\hat{\phi}$ equals the composition

$$\begin{array}{ccccccc} E_2 & \longrightarrow & \mathrm{Div}^0(E_2) & \xrightarrow{\phi^*} & \mathrm{Div}^0(E_1) & \xrightarrow{\text{sum}} & E_1, \\ Q & \longmapsto & (Q) - (O) & & \sum n_P(P) & \longmapsto & \sum [n_p]P. \end{array}$$

Proof. (a) First we show uniqueness. Suppose that $\hat{\phi}$ and $\hat{\phi}'$ are two such isogenies, then

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

Because ϕ is nonconstant, the map $\hat{\phi} - \hat{\phi}$ must be constant and thus equal to $[0]$. So $\hat{\phi} = \hat{\phi}'$.

Now suppose that $\psi\colon E_2 \to E_3$ is another nonconstant isogeny of degree n and suppose that $\hat{\phi}$ and $\hat{\psi}$ exist. Then

$$(\hat{\phi} \circ \hat{\psi}) \circ (\psi \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm].$$

So $\hat{\phi} \circ \hat{\phi}$ has the defining property of $\widehat{\psi \circ \phi}$. If $\mathrm{char}(K) = 0$, then ϕ is separable and if $\mathrm{char}(K) = p > 0$, then by [II.2.12 Sil09] we can write ϕ as the composition of a separable morphism and a Frobenius morphism. Thus it suffices to show the existence of $\hat{\phi}$ when ϕ is either separable or a Frobenius morphism.

Case 1. ϕ is separable Because ϕ has degree m, by [III.4.10c Sil09] we have

$$\#\ker \phi = m,$$

so every element of $\ker \phi$ has order dividing m. Hence

$$\ker \phi \subset \ker[m]$$

and by [III.4.11 Sil09] it follows that there is an isogeny

$$\hat{\phi}\colon E_2 \to E_1 \qquad \text{satisfying} \qquad \hat{\phi} \circ \phi = [m].$$

Case 2. ϕ is a Frobenius morphism If ϕ is the q^{th}-power Frobenius morphism with $q = p^e$, then ϕ is the composition of the p^{th}-power Frobenius morphism with itself e times. Thus it suffices to consider the case that ϕ is the p^{th}-power Frobenius morphism. So by [II.2.11 Sil09] we have $\deg \phi = p$.

We now consider the map $[p]$ on E. Let ω be an invariant differential, then by [III.5.3 Sil09] and the fact that $\operatorname{char}(K) = p$, it follows that

$$[p]^*\omega = p\omega = 0.$$

Hence by [II.4.2c Sil09] the map $[p]$ is not separable, and thus when we decompose $[p]$ as a Frobenius morphism followed by a separable map, the Frobenius morphism does appear:

$$[p] = \psi \circ \phi^e$$

for some integer $e \geq 1$ and some separable isogeny ψ. Then the map

$$\hat{\phi} = \psi \circ \phi^{e-1}$$

has the desired property.

(b) Let $Q \in E_2$, and $P \in \phi^{-1}(Q)$, then the image of Q under the indicated composition is

$$\begin{aligned}
\operatorname{sum}(\phi^*((Q) - (O))) &= \sum_{P' \in \phi^{-1}(Q)} [e_\phi(P')]P' - \sum_{T \in \phi^{-1}(O)} [e_\phi(T)]T && \text{by definition of } \phi^*, \\
&= [\deg_i \phi] \left(\sum_{P' \in \phi^{-1}(Q)} P' - \sum_{T \in \phi^{-1}(O)} T \right) && \text{from [III.4.10a Sil09]}, \\
&= [\deg_i \phi] \circ [\#\phi^{-1}(Q)]P \\
&= [\deg \phi]P && \text{from [III.4.10a Sil09]}.
\end{aligned}$$

By construction,

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

so the two maps are the same.

$\square$

Definition 2 (Dual isogeny)**.** Let $\phi \colon E_1 \to E_2$ be an isogeny. If $\phi \neq [0]$, then the **dual isogeny** to ϕ is the isogeny given by Theorem 1 a). Otherwise it is defined to be $[0]$.

We will now present some basic properties of the dual isogeny, from which we will deduce several important corollaries, including a good description of the kernel of the map $[m]$.

Theorem 3. *Let $\phi \colon E_1 \to E_2$ be an isogeny.*

a) Let $m = \deg \phi$, then

$$\hat{\phi} \circ \phi = [m] \text{ on } E_1 \quad \text{and} \quad \phi \circ \hat{\phi} = [m] \text{ on } E_2.$$

b) Let $\lambda\colon E_2 \to E_3$ *be another isogeny. Then*

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

c) Let $\psi\colon E_1 \to E_2$ *be another isogeny. Then*

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

d) For all $m \in \mathbb{Z}$*,*

$$\widehat{[m]} = [m] \quad \textit{and} \quad \deg[m] = m^2.$$

e) $\deg\hat{\phi} = \deg\phi$*.*

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

Proof. If ϕ is constant, then the theorem is trivial, and if λ and ψ are constant, then b) and c) are trivial. So we can assume all isogenies to be nonconstant.

a) The first statement is the defining property of $\hat{\phi}$. For the second consider

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

Because ϕ is nonconstant, this implies $\phi \circ \hat{\phi} = [m]$.

b) We have already seen this in the proof of Theorem 1 a).

c) See [III.6.3c Sil09].

d) By definition, this is true for $m = 0$ and it is trivial for $m = 1$. By using c) with $\phi = [m]$ and $\psi = [1]$, we obtain

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

Then, by induction we see that $\widehat{[m]} = [m]$ for all $m \in \mathbb{Z}$.

Now let $d = \deg[m]$ and consider the map $[d]$:

$$[d] = \widehat{[m]} \circ [m] = [m] \circ [m] = [m^2]$$

By [III.4.2b Sil09], the endomorphism ring of an elliptic curve is a torsion free $\mathbb{Z}$-module, so it follows that $d = m^2$.

e) Let $m = \deg\phi$, then by d) and a), we obtain

$$m^2 = \deg[m] = \deg(\phi \circ \hat{\phi}) = (\deg\phi)(\deg\hat{\phi}) = m(\deg\hat{\phi}).$$

Thus $m = \deg\hat{\phi}$.

f) Again, let $m = \deg\phi$, then by a), b) and d), we obtain

$$\hat{\phi} \circ \phi = [m] = \widehat{[m]} = \widehat{\hat{\phi} \circ \phi} = \hat{\phi} \circ \hat{\hat{\phi}}.$$

Therefore $\phi = \hat{\hat{\phi}}$.

□

Definition 4 (quadratic form)**.** Let A be an abelian group. A function

$$d \colon A \to \mathbb{R}$$

is a **quadratic form**, if it satisfies the following conditions

i) $d(\alpha) = d(-\alpha)$ for all $\alpha \in A$.

ii) The pairing

$$A \times A \to \mathbb{R},\ (\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$$

is bilinear.

A quadratic form d is **positive definite** if it further satisfies the following conditions:

iii) $d(\alpha) \geq 0$ for all $\alpha \in A$

iv) $d(\alpha) = 0$ if and only if $\alpha = 0$

Corollary 5. *Let E_1 and E_2 be elliptic curves. The degree map*

$$\deg \colon \operatorname{Hom}(E_1, E_2) \to \mathbb{Z}$$

is a positive definite quadratic form.

Proof. Everything is clear except for the fact that the pairing

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

is bilinear. To proof this, we use the injection

$$[-] \colon \mathbb{Z} \to \operatorname{End}(E_1)$$

and compute

$$\begin{aligned}
[\langle \phi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg(\psi)] \\
&= \widehat{\phi + \psi} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\
&= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \qquad \text{from Theorem 3 c)}
\end{aligned}$$

Using Theorem 3 c again, we see that the last expression is linear in both ϕ and ψ. □

Lemma 6. *Let A be a finte abelian group of order N^r and suppose that for every $D \mid N$, we have $\#A[D] = D^r$, where $A[D]$ is the subgroup of A consisting of all elements of order D. Then*

$$A \cong \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^r.$$

Corollary 7. *Let E be an elliptic curve and let $m \in \mathbb{Z}$ with $m \neq 0$.*

a) if $m \neq 0$ in K, then

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

b) If $\mathrm{char}(K) = p > 0$, then one of the following is true:

- *i) $E[p^e] = \{O\}$ for all $e \in \mathbb{N} \setminus \{0\}$.*
- *ii) $E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}}$ for all $e \in \mathbb{N} \setminus \{0\}$*

Proof. a) By the assumption on m and the fact, that $\deg[m] = m^2$, we know that $[m]$ is a finite separable map. So from [III.4.10c Sil09],

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

Similarly, for every integer d dividing M we have

$$\#E[d] = d^2.$$

Then by Lemma 6,

$$E[m] = \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

b) Let ϕ be the p^{th}-power Frobenius morphism. Then

$$\begin{aligned}
\#E[p^e] &= \deg_s[p^e] && \text{from [III.4.10a Sil09]} \\
&= (\deg_s(\hat{\phi} \circ \phi))^e && \text{from Theorem 3 a)} \\
&= (\deg_s \hat{\phi})^e && \text{from [II.2.11b Sil09].}
\end{aligned}$$

By Theorem 3 e) and [II.2.11c Sil09], we have

$$\deg \hat{\phi} = \deg \phi = p,$$

so there are two possible cases. If $\hat{\phi}$ is inseparable, then $\deg_s \hat{\phi} = 1$, so

$$\#E[p^e] = 1 \qquad \text{for all } e \in \mathbb{N} \setminus \{0\}.$$

Otherwise $\hat{\phi}$ is separable, so $\deg_s \hat{\phi} = p$ and thus

$$\#E[p^e] = p^e \qquad \text{for all } e \in \mathbb{N} \setminus \{0\}.$$

Then we verify that this actually implies

$$E[p^e] = \frac{\mathbb{Z}}{p^e\mathbb{Z}} \qquad \text{for all } e \in \mathbb{N} \setminus \{0\}.$$

$\square$

Bibliography

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946. URL: https://books.google.de/books?id=Z90CA%5C_EUCCkC.