Math 7359 (Elliptic Curves and Modular Forms)

Lecture #14 of 24 $\sim$ October 26, 2023

More Isogenies

- Properties of Isogenies
- Dual Isogenies

Recall, I

Recall the actions of φ^* and φ_*:

Definition

Let $\varphi : C_1 \to C_2$ be a nonconstant map of (smooth projective) curves.

We define the inverse image map $\varphi^* : \mathrm{Div}(C_2) \to \mathrm{Div}(C_1)$ on divisor groups by setting $\varphi^*(Q) = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)P$ for all $Q \in C_2$ and extending linearly.

We also define the direct image map $\varphi_* : \mathrm{Div}(C_1) \to \mathrm{Div}(C_2)$ by setting $\varphi_*(P) = \varphi(P)$ for all $P \in C_1$ and extending linearly.

Rather vacuously, both φ_* and φ^* are homomorphisms.

Recall, II

And recall the short version of Riemann-Hurwitz:

Theorem (Riemann-Hurwitz)

Let $\varphi : C_1 \to C_2$ be a nonconstant separable morphism where C_1 and C_2 are smooth projective curves of respective genera g_1 and g_2.

Then $2g_1 - 2 \geq (\deg \varphi)(2g_2 - 2) + \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if $\mathrm{char}(k) \nmid e_\varphi(P)$ for any $P \in C_1$.

And also isogenies:

Definition

Let (E_1, O_1) and (E_2, O_2) be two elliptic curves. An isogeny $\varphi : E_1 \to E_2$ is a morphism from E_1 to E_2 such that $\varphi(O_1) = O_2$. If E_1 and E_2 are elliptic curves such that there exists a nonzero isogeny between them, we say they are isogenous.

Properties of Isogenies, I

Now let's prove some properties of isogenies using all of the results about morphisms and ramification we have developed:

Proposition (Properties of Isogenies, Part 1)

Let $\varphi : E_1 \to E_2$ be a nonzero isogeny. Then

1. *The map φ is a group homomorphism from E_1 to E_2.*
2. *For all $Q \in E_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$. In particular, $\ker \varphi = \varphi^{-1}(O)$ is a finite subgroup of E_1.*
3. *For all $P \in E_1$, the ramification index $e_\varphi(P) = \deg_i \varphi$, the inseparable degree of φ.*
4. *If φ is separable then φ is everywhere unramified and $\#\ker \varphi = \deg \varphi$.*

Properties of Isogenies, II

1. The map φ is a group homomorphism from E_1 to E_2.

Discussion:

Properties of Isogenies, II

1. The map φ is a group homomorphism from E_1 to E_2.

Discussion:

- Since isogenies are the natural maps in the category of elliptic curves, and elliptic curves carry a natural group structure (which as we have discussed can be described purely in terms of the divisor group), the fact that isogenies are group homomorphisms is quite reasonable.
- Indeed, the reason we impose the additional condition that isogenies map the identity of E_1 to the identity of E_2 is precisely to ensure that isogenies are group homomorphisms.

Properties of Isogenies, III

1. The map φ is a group homomorphism from E_1 to E_2.

Proof:

Properties of Isogenies, III

1. The map φ is a group homomorphism from E_1 to E_2.

Proof:

- Let P, Q be points of C_1 and O be the identity of C_1.
- Then by our earlier results, $[P+Q]-[P]-[Q]+[O]$ is a principal divisor on E_1 as it has degree 0 and the underlying sum of points resolves to the identity on E_1.
- For $\mathrm{div}(f) = [P+Q]-[P]-[Q]+[O]$, we then have $\mathrm{div}(\varphi^* f) = \varphi^* \mathrm{div}(f) = [\varphi(P+Q)]-[\varphi(P)]-[\varphi(Q)]+[\varphi(O)]$, so this latter divisor is principal on E_2.
- But that implies the resulting sum of points $\varphi(P+Q)-\varphi(P)-\varphi(Q)+\varphi(O)$ resolves to the identity on E_2, so since $\varphi(O)$ is the identity on E_2, we conclude immediately that $\varphi(P+Q) = \varphi(P)+\varphi(Q)$ as claimed.

Properties of Isogenies, III, Again

1. The map φ is a group homomorphism from E_1 to E_2.

More Discussion:

Properties of Isogenies, III, Again

1. The map φ is a group homomorphism from E_1 to E_2.

More Discussion:

- The proof on the last slide might make it seem like there is real content to the result, but in fact it's really just bookkeeping. Here's a way that makes it clearer.
- We have constructed group isomorphisms $\tau_1 : E_1 \to \mathrm{Pic}^0(E_1)$ and $\tau_2 : E_2 \to \mathrm{Pic}^0(E_2)$ with $\tau_i(P) = [P] - [O]$ as divisor classes.
- Then $\varphi_* \circ \tau_1 = \tau_2 \circ \varphi$ essentially by definition and the fact that $\varphi(O) = O$, so since φ_* is a homomorphism on the Picard groups (it's certainly a homomorphism on the divisor groups, and it preserves degree), $\varphi = \tau_2^{-1} \circ \varphi_* \circ \tau_1$ is a composition of homomorphisms and thus also a homomorphism.

Properties of Isogenies, III, Still?

2. For all $Q \in E_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$. In particular, $\ker \varphi = \varphi^{-1}(O)$ is a finite subgroup of E_1.

Properties of Isogenies, III, Still?

2. For all $Q \in E_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$. In particular, $\ker \varphi = \varphi^{-1}(O)$ is a finite subgroup of E_1.

Exercise: Suppose that $\varphi : G \to H$ is a surjective group homomorphism. Show that for any $h \in H$ there is a bijection between $\varphi^{-1}(h)$ and $\ker \varphi$.

Proof:

Properties of Isogenies, III, Still?

2. For all $Q \in E_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$. In particular, $\ker \varphi = \varphi^{-1}(O)$ is a finite subgroup of E_1.

Exercise: Suppose that $\varphi : G \to H$ is a surjective group homomorphism. Show that for any $h \in H$ there is a bijection between $\varphi^{-1}(h)$ and $\ker \varphi$.

Proof:

- By our results on ramification we know that $\#\varphi^{-1}(Q) = \deg_s \varphi$ for all but finitely many $Q \in E_2$.
- Since φ is a group homomorphism by (1) and surjective since it is a nonzero morphism, applying the exercise above yields both results immediately.

Properties of Isogenies, III? Really?

3. For all $P \in E_1$, the ramification index $e_\varphi(P) = \deg_i \varphi$, the inseparable degree of φ.

Proof:

Properties of Isogenies, III? Really?

3. For all $P \in E_1$, the ramification index $e_\varphi(P) = \deg_i \varphi$, the inseparable degree of φ.

Proof:

- First, let $Q = \varphi(P)$ and take P' to be another point in $\varphi^{-1}(Q)$, and also define $R = P' - P$.

Properties of Isogenies, III? Really?

3. For all $P \in E_1$, the ramification index $e_\varphi(P) = \deg_i \varphi$, the inseparable degree of φ.

Proof:

- First, let $Q = \varphi(P)$ and take P' to be another point in $\varphi^{-1}(Q)$, and also define $R = P' - P$.
- Since the translation morphism $\tau_R : E \to E$ defined by $\varphi(A) = A + R$ is an isomorphism and hence unramified, we have $\varphi(R) = O$ and so $\varphi \circ \tau_R = \varphi$.
- Then $e_\varphi(P) = e_{\varphi\circ\tau_R}(P) = e_\varphi(\tau_R(P))e_{\tau_R}(P) = e_\varphi(P')$ by the ramification composition formula. This means all points in $\varphi^{-1}(P)$ have the same ramification index.
- Then $\deg_s \varphi \deg_i \varphi = \deg \varphi = \sum_{P\in\varphi^{-1}(Q)} e_\varphi(P) = \#\varphi^{-1}(Q) \cdot e_\varphi(P) = \deg_s \varphi \cdot e_\varphi(P)$, so we must have $e_\varphi(P) = \deg_i \varphi$ as claimed.

Properties of Isogenies, III? Apparently?

4. If φ is separable then φ is everywhere unramified and $\#\ker\varphi = \deg\varphi$.

Proof:

Properties of Isogenies, III? Apparently?

4. If φ is separable then φ is everywhere unramified and $\#\ker\varphi = \deg\varphi$.

Proof:

- By (3) we see immediately that if φ is separable, then $e_\varphi(P) = \deg_i\varphi = 1$ for all P, so φ is unramified.
- The cardinality of the kernel is immediate from (2).

Properties of Isogenies, III? Apparently?

4. If φ is separable then φ is everywhere unramified and $\#\ker\varphi = \deg\varphi$.

Proof:

- By (3) we see immediately that if φ is separable, then $e_\varphi(P) = \deg_i\varphi = 1$ for all P, so φ is unramified.
- The cardinality of the kernel is immediate from (2).

Exercise: Use Riemann-Hurwitz to prove directly that if $\varphi : E_1 \to E_2$ is a nonconstant separable morphism of elliptic curves then φ is everywhere unramified.

Galois Theory and Isogenies, I

More properties, involving Galois theory:

Proposition (Properties of Isogenies, continued)

Let $\varphi : E_1 \to E_2$ be a nonzero isogeny. Then

5. *The kernel $\ker \varphi$ is isomorphic to the automorphism group of the extension $k(E_1)/\varphi^* k(E_2)$ via the map Ξ sending $R \mapsto \tau_R^*$ where τ_R is the translation-by-R morphism.*
6. *If φ is separable then the extension $k(E_1)/\varphi^* k(E_2)$ is a Galois extension of degree $\#\ker \varphi$.*
7. *Suppose that $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ are nonconstant isogenies and that φ is separable. If $\ker \varphi \subseteq \ker \psi$ then there exists a unique isogeny $\gamma : E_2 \to E_3$ such that $\psi = \gamma \circ \varphi$.*
8. *Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.*

Properties of Isogenies, III? Yes, Still III.

5. The kernel $\ker \varphi$ is isomorphic to the automorphism group of the extension $k(E_1)/\varphi^* k(E_2)$ via the map Ξ sending $R \mapsto \tau_R^*$ where τ_R is the translation-by-R morphism.

Proof:

Properties of Isogenies, III? Yes, Still III.

5. The kernel $\ker \varphi$ is isomorphic to the automorphism group of the extension $k(E_1)/\varphi^* k(E_2)$ via the map Ξ sending $R \mapsto \tau_R^*$ where τ_R is the translation-by-R morphism.

Proof:

- First, in the same way as noted in the proof of (3), for any $R \in \ker \varphi$ we have $\varphi \circ \tau_R = \varphi$, since $\varphi(x + R) = \varphi(x) + \varphi(R) = \varphi(x)$ since φ is a homomorphism.
- Then for any $f \in k(E_2)$ we have $\tau_R^*(\varphi^* f) = (\varphi \circ \tau_R)^* f = \varphi^* f$, and so τ_R^* fixes $k(E_2)$. Therefore τ_R^* is an automorphism of the extension $k(E_1)/\varphi^* k(E_2)$ so Ξ is well defined.
- Next, for any $R, S \in \ker \varphi$ since rather obviously $\tau_{R+S} = \tau_S \circ \tau_R$, we have $\tau_{R+S}^* = (\tau_S \circ \tau_R)^* = \tau_R^* \tau_S^*$ so Ξ is a homomorphism.

Properties of Isogenies, III: Yes, III, Not IV

5. The kernel $\ker \varphi$ is isomorphic to the automorphism group of the extension $k(E_1)/\varphi^* k(E_2)$ via the map Ξ sending $R \mapsto \tau_R^*$ where τ_R is the translation-by-R morphism.

Proof (continued):

Properties of Isogenies, III: Yes, III, Not IV

5. The kernel $\ker \varphi$ is isomorphic to the automorphism group of the extension $k(E_1)/\varphi^* k(E_2)$ via the map Ξ sending $R \mapsto \tau_R^*$ where τ_R is the translation-by-R morphism.

Proof (continued):

- Third, if τ_R^* fixes $k(E_1)$, then for any $f \in k(E_1)$ we have $f \circ \tau_R = f$. Taking f to be a function with poles only at O (which exist by Riemann-Roch since $l(2O) = 2$) we see that $f \circ \tau_R$ has poles only at $-R$, so $R = O$. Thus $\ker \Xi = \{O\}$ so Ξ is injective.
- Finally, by basic facts about field automorphisms, the cardinality of $\mathrm{Aut}[k(E_1)/\varphi^* k(E_2)]$ is at most the separable degree of the extension $\deg_s(\varphi)$, so by (2) and the fact that Ξ is an injective homomorphism, we must have equality and Ξ is an isomorphism.

Properties of Isogenies, III: Uh Huh, Still III

6. If φ is separable then the extension $k(E_1)/\varphi^* k(E_2)$ is a Galois extension of degree $\#\ker\varphi$.

Proof:

Properties of Isogenies, III: Uh Huh, Still III

6. If φ is separable then the extension $k(E_1)/\varphi^* k(E_2)$ is a Galois extension of degree $\#\ker\varphi$.

Proof:

- By basic Galois theory, the cardinality of $\mathrm{Aut}[k(E_1)/\varphi^* k(E_2)]$ equals the degree of the extension if and only if the extension is Galois.
- By (4) and (5) combined, this occurs, and the degree equals $\deg\varphi = \#\ker\varphi$.

Properties of Isogenies, III: How Is It Still III?

7. Suppose that $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ are nonconstant isogenies and that φ is separable. If $\ker \varphi \subseteq \ker \psi$ then there exists a unique isogeny $\gamma : E_2 \to E_3$ such that $\psi = \gamma \circ \varphi$.

Proof:

Properties of Isogenies, III: How Is It Still III?

7. Suppose that $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ are nonconstant isogenies and that φ is separable. If $\ker \varphi \subseteq \ker \psi$ then there exists a unique isogeny $\gamma : E_2 \to E_3$ such that $\psi = \gamma \circ \varphi$.

Proof:

- Since φ is separable, by (6) we know that $k(E_1)/\varphi^* k(E_2)$ is Galois of degree $\#\ker \varphi$. Let the Galois group be G.
- Since $\ker \varphi \subseteq \ker \psi$, every element of G fixes $\psi^* k(E_3)$, so $\varphi^* k(E_2)$ is a field extension of $\psi^* k(E_3)$.

Properties of Isogenies, III: How Is It Still III?

7. Suppose that $\varphi : E_1 \to E_2$ and $\psi : E_1 \to E_3$ are nonconstant isogenies and that φ is separable. If $\ker \varphi \subseteq \ker \psi$ then there exists a unique isogeny $\gamma : E_2 \to E_3$ such that $\psi = \gamma \circ \varphi$.

Proof:

- Since φ is separable, by (6) we know that $k(E_1)/\varphi^* k(E_2)$ is Galois of degree $\#\ker \varphi$. Let the Galois group be G.
- Since $\ker \varphi \subseteq \ker \psi$, every element of G fixes $\psi^* k(E_3)$, so $\varphi^* k(E_2)$ is a field extension of $\psi^* k(E_3)$.
- Since field extensions of function fields correspond to morphisms of curves, there exists a unique morphism $\gamma : E_2 \to E_3$ such that $\varphi^*(\gamma^* k(E_3)) = \psi^* k(E_3)$ which on the level of morphisms is equivalent to saying that $\gamma \circ \varphi = \psi$.
- Finally, we have $\gamma(O) = \gamma(\varphi(O)) = \psi(O) = O$ since φ and ψ are isogenies, and so γ is an isogeny as well.

Properties of Isogenies, III: Like, III The Tenth Maybe

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Discussion:

Properties of Isogenies, III: Like, III The Tenth Maybe

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Discussion:

- Since φ is a surjective group homomorphism, the first isomorphism theorem immediately implies that the group structure of E' is that of the quotient group E/Φ, so since E' is unique here we often simply write $E' = E/\Phi$.
- Of course, we can certainly construct the quotient group as a group by itself, but it is not immediately obvious why this quotient should also carry the structure of an algebraic variety (let alone why it should be another elliptic curve).
- But in fact, one can show that the quotient of any smooth projective curve by a finite group of automorphisms also carries the structure of a variety.

Properties of Isogenies, III: Come On, Now

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Organization of Proof:

Properties of Isogenies, III: Come On, Now

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Organization of Proof:

- First we will construct a unique curve C and separable morphism $\varphi : E \to C$ such that the function field of C is fixed by the action of Φ, which is equivalent to saying that $\varphi(\Phi)$ is a single point.
- Then we will show φ is everywhere unramified.
- Finally, we will apply Riemann-Hurwitz to show that C has genus 1, and then finish by observing that $\ker \varphi = \varphi^{-1}(O) = \Phi$.

Properties of Isogenies, III: Seriously, III?

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof:

Properties of Isogenies, III: Seriously, III?

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof:

- As noted in (5), for each $R \in \Phi$ the translation-by-R map $\tau_R(x) = x + R$ yields an automorphism τ_R^* of $k(E)$; note it is an automorphism since it has an inverse map τ_{-R}^*.
- By the fundamental theorem of Galois theory, if K is the fixed field of the automorphism group $\Phi^* = \{\tau_R^* : R \in \Phi\}$, then $k(E)/K$ is a Galois extension of degree $\#\Phi^* = \#\Phi$.
- In particular, K has transcendence degree 1 over k, so by our equivalence of categories, there exists a unique (up to isomorphism) smooth projective curve C/k and a unique finite-degree morphism $\varphi : E \to C$ such that $\varphi^* k(C) = K$.

Properties of Isogenies, III: Forever Three

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof (continued):

- We have a curve C and morphism $\varphi : E \to C$ with $\varphi^* k(C) = K$, the fixed field of $\Phi^* = \{\tau_R^* : R \in \Phi\}$.

Properties of Isogenies, III: Forever Three

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof (continued):

- We have a curve C and morphism $\varphi : E \to C$ with $\varphi^* k(C) = K$, the fixed field of $\Phi^* = \{\tau_R^* : R \in \Phi\}$.
- Now, since $k(E)/K$ is Galois hence separable, φ is separable.
- For any $P \in E$ and $R \in \Phi$ and $f \in k(C)$, we have $f(\varphi(P+R)) = f(\varphi(\tau_R(P)) = (\varphi \circ \tau_R)^* f(P) = \tau_R^* \varphi^* f(P) = \varphi^* f(P) = f(\varphi(P))$ because τ_R^* fixes $\varphi^* f$.
- Since this equality holds for all functions f, by choosing f to be a function with poles only at one point (as in the argument in (5) above) we see that $\varphi(P+R) = \varphi(P)$.

Properties of Isogenies, III: Three Three Three

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof (continued more):

- We have a curve C and morphism $\varphi : E \to C$ with $\varphi^* k(C) = K$, the fixed field of $\Phi^* = \{\tau_R^* : R \in \Phi\}$.
- We also know that $\varphi(P + R) = \varphi(P)$ for all $R \in \Phi$.

Properties of Isogenies, III: Three Three Three

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof (continued more):

- We have a curve C and morphism $\varphi : E \to C$ with $\varphi^* k(C) = K$, the fixed field of $\Phi^* = \{\tau_R^* : R \in \Phi\}$.
- We also know that $\varphi(P + R) = \varphi(P)$ for all $R \in \Phi$.
- Therefore, for any $Q = \varphi(P)$ on C, the set $\varphi^{-1}(Q)$ contains the $\#\Phi$ translates $\{Q + R : R \in \Phi\}$.
- But by our properties of ramification, $\#\varphi^{-1}(Q) \leq \deg \varphi = \#\Phi$ with equality iff Q is unramified.
- Since this holds for all $Q \in C$, φ is everywhere unramified.

Properties of Isogenies, III: III: III: III: III: III: III: III:

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof (continued even more):

- We have a curve C and morphism $\varphi : E \to C$ with $\varphi^* k(C) = K$, the fixed field of $\Phi^* = \{\tau_R^* : R \in \Phi\}$.
- We also just showed φ is unramified.

Properties of Isogenies, III: III: III: III: III: III: III: III:

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof (continued even more):

- We have a curve C and morphism $\varphi : E \to C$ with $\varphi^* k(C) = K$, the fixed field of $\Phi^* = \{\tau_R^* : R \in \Phi\}$.
- We also just showed φ is unramified.
- Now, since φ is separable and unramified everywhere, by Riemann-Hurwitz we have $2g_E - 2 = (\deg \varphi)(2g_C - 2) + 0$ and so since $\deg \varphi$ is positive and $g_E = 1$, we must have $g_C = 1$ also.

Properties of Isogenies, III: III: III: III: III: III: III: III:

8. Suppose that Φ is a finite subgroup of the elliptic curve E. Then there exists a unique elliptic curve E' and a separable isogeny $\varphi : E \to E'$ such that $\ker \varphi = \Phi$.

Proof (continued even more):

- We have a curve C and morphism $\varphi : E \to C$ with $\varphi^* k(C) = K$, the fixed field of $\Phi^* = \{\tau_R^* : R \in \Phi\}$.
- We also just showed φ is unramified.
- Now, since φ is separable and unramified everywhere, by Riemann-Hurwitz we have $2g_E - 2 = (\deg \varphi)(2g_C - 2) + 0$ and so since $\deg \varphi$ is positive and $g_E = 1$, we must have $g_C = 1$ also.
- Finally, if we define $O_C = \varphi(O_E)$, then φ is an isogeny, and then as calculated above $\ker \varphi$ equals $\{O_E + R : R \in \Phi\} = \Phi$ since φ is unramified.

Properties of Isogenies, *III* $\cdot \infty$

And now a few more things:

Proposition (Properties of Isogenies, Part 3)

Let $\varphi : E_1 \to E_2$ be a nonzero isogeny and ω be the invariant differential on E_1. Then

9. *If $\mathrm{char}(k) = p$ and φ is not separable, then for $q = \deg_i \varphi$ and $\mathrm{Frob}_q : E_1 \to E_1^{(q)}$ the qth-power Frobenius map, we have $\varphi = \alpha \circ \mathrm{Frob}_q$ where $\alpha : E_1^{(q)} \to E_2$ is a separable isogeny.*
10. *For any $Q \in E_1$, if $\tau_Q : E_1 \to E_1$ is the translation-by-Q map then $\tau_Q^* \omega = \omega$.*
11. *We have $[-1]^* \omega = -\omega$.*
12. *If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega$.*
13. *For any integer m we have $[m]^* \omega = m\omega$. In particular, $[m]$ is separable if and only if $\mathrm{char}(k) \nmid m$.*

Properties of Isogenies, *III* $\cdot \infty$

9. If $\mathrm{char}(k) = p$ and φ is not separable, then for $q = \deg_i \varphi$ and $\mathrm{Frob}_q : E_1 \to E_1^{(q)}$ the qth-power Frobenius map, we have $\varphi = \alpha \circ \mathrm{Frob}_q$ where $\alpha : E_1^{(q)} \to E_2$ is a separable isogeny.

Discussion:

- The point of this result is that if we want to understand an inseparable isogeny, it's enough just to understand the separable piece α along with the Frobenius map Frob_q.
- Embedded in this result is the fact that the degree of the qth-power Frobenius map Frob is q. This can also be calculated directly by computing the relevant field extension.
- Explicitly, $\deg \mathrm{Frob}_q = [k(E) : k(E^{(q)})] = [k(x, y) : k(x^q, y^q)]$, and since $[k(x, y) : k(x)] = 2 = [k(x^q, y^q) : k(x^q)]$, the result follows from the fact that $k(x)/k(x^q) = q$.

Properties of Isogenies, *III* $\cdot \infty + 1$

9. If $\mathrm{char}(k) = p$ and φ is not separable, then for $q = \deg_i \varphi$ and $\mathrm{Frob}_q : E_1 \to E_1^{(q)}$ the qth-power Frobenius map, we have $\varphi = \alpha \circ \mathrm{Frob}_q$ where $\alpha : E_1^{(q)} \to E_2$ is a separable isogeny.

Proof:

- Let K be the separable closure of $\varphi^* k(E_2)$ in $k(E_1)$.
- By standard results about separable extensions over perfect fields, $k(E_1)/K$ is purely inseparable of degree $q = \deg_i \varphi = p^d$ for some d with $K = k(E_1)^q$, while $K/\varphi^* k(E_2)$ is separable of degree $\deg_s \varphi$.
- Then by definition, we see $K = \varphi^* k(E_1^{(q)})$.
- Now convert the existence of the tower $k(E_1)/K/\varphi^* k(E_2)$ to statements about morphisms: it says $\varphi = \alpha \circ \mathrm{Frob}_q$ where $\alpha : E_1^{(q)} \to E_2$ corresponds to $K/\varphi^* k(E_2)$ and $\mathrm{Frob}_q : E_1 \to E_1^{(q)}$ corresponds to $k(E_1)/\varphi^* k(E_1^{(q)})$.

Properties of Isogenies, *III* $\cdot \infty + \infty$

10. For any $Q \in E_1$, if $\tau_Q : E_1 \to E_1$ is the translation-by-Q map then $\tau_Q^* \omega = \omega$.

Proof:

Properties of Isogenies, *III* $\cdot \infty + \infty$

10. For any $Q \in E_1$, if $\tau_Q : E_1 \to E_1$ is the translation-by-Q map then $\tau_Q^* \omega = \omega$.

Proof:

- We showed this earlier in our discussion of differentials (it is why ω is called the invariant differential).

---

11. We have $[-1]^* \omega = -\omega$.

Proof:

Properties of Isogenies, *III* $\cdot \infty + \infty$

10. For any $Q \in E_1$, if $\tau_Q : E_1 \to E_1$ is the translation-by-Q map then $\tau_Q^* \omega = \omega$.

Proof:

- We showed this earlier in our discussion of differentials (it is why ω is called the invariant differential).

---

11. We have $[-1]^* \omega = -\omega$.

Proof:

- Suppose E_1 has general Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
- Then $[-1](x, y) = (x, -y - a_1x - a_3)$, so $d[-1]^*x = dx$.
- Thus $$[-1]^* \omega = [-1]^* \frac{dx}{2y + a_1x + a_3}$$
$$= \frac{dx}{2(-y - a_1x - a_3) + a_1x + a_3} = -\omega.$$

Properties of Isogenies, *III* $\cdot \infty + \infty \cdot \infty$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega$.

Proof (part 1):

Properties of Isogenies, *III* $\cdot \infty + \infty \cdot \infty$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega$.

Proof (part 1):

- If φ or ψ is the zero isogeny the result is trivial.
- If $\varphi + \psi = 0$ then $\psi = [-1] \circ \varphi$ and thus $\psi^* = \varphi^* \circ [-1]^*$.
- Then $\varphi^* \omega + \psi^* \omega = \varphi^* \omega + \varphi^*(-\omega) = 0$ by linearity and (11).
- Now assume that none of $\varphi, \psi, \varphi + \psi$ is zero.
- Take independent coordinates (x_1, y_1) and (x_2, y_2) and let $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ via the group law, so that x_3 and y_3 are rational functions of x_1, y_1, x_2, y_2.
- What we will do is work out how to express the differential $\omega_3(x_3, y_3)$ in terms of $\omega_1(x_1, y_1)$ and $\omega_2(x_2, y_2)$.

Properties of Isogenies, $III \cdot \infty + \infty^{\infty}$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.

Proof (part 2):

[1] $f = \left(\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}\right)^2 + a_1\left(\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}\right) - a_2 - x_1 - x_2$

Properties of Isogenies, $III \cdot \infty + \infty^{\infty}$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.

Proof (part 2):

- We have coordinates with $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ under the group law. Let $\omega_i(x_i, y_i)$ be the associated invariant differential $dx_i/(2y_i + a_1x_i + a_3)$ for each $i = 1, 2, 3$.
- Writing $x_3 = f(x_1, y_1, x_2, y_2)$,[1] the chain rule for differentials yields $dx_3 = f_{x_1}dx_1 + f_{y_1}dy_1 + f_{x_2}dx_2 + f_{y_2}dy_2$.
- But since dx_1 and dy_1 are $k(x_1, y_1)$-multiples of $\omega(x_1, y_1)$ and dx_2, dy_2 are $k(x_2, y_2)$-multiples of $\omega(x_2, y_2)$, we see that $\omega(x_3, y_3)$ is a $k(x_1, y_1, x_2, y_2)$-linear combination of the differentials $\omega(x_1, y_1)$ and $\omega(x_2, y_2)$.

[1] $f = \left(\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}\right)^2 + a_1\left(\frac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}\right) - a_2 - x_1 - x_2$

Properties of Isogenies, $Ш^{\infty}$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.

Proof (part 3):

- We have coordinates with $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ under the group law. Let $\omega_i(x_i, y_i)$ be the associated invariant differential $dx_i/(2y_i + a_1x_i + a_3)$ for each $i = 1, 2, 3$.

Properties of Isogenies, $Ш^\infty$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.

Proof (part 3):

- We have coordinates with $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ under the group law. Let $\omega_i(x_i, y_i)$ be the associated invariant differential $dx_i/(2y_i + a_1x_i + a_3)$ for each $i = 1, 2, 3$.
- We just showed that we can express $\omega_3(x_3, y_3) = g(x_1, y_1, x_2, y_2)\,\omega_1(x_1, y_1) + h(x_1, y_1, x_2, y_2)\,\omega_2(x_2, y_2)$ for some $g, h \in k(x_1, y_1, x_2, y_2)$.
- By working through the rather horrendous calculations explicitly, one may show that in fact the coefficients g and h are both just 1.
- Instead of doing that, let's give a more clever argument.

Properties of Isogenies, $Ш^{\infty} + 1$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega$.

Proof (part 4):

- We have coordinates with $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, and $\omega_3 = g(x_1, y_1, x_2, y_2)\,\omega_1 + h(x_1, y_1, x_2, y_2)\,\omega_2$.

Properties of Isogenies, $Ш^{\infty} + 1$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega$.

Proof (part 4):

- We have coordinates with $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, and $\omega_3 = g(x_1, y_1, x_2, y_2)\,\omega_1 + h(x_1, y_1, x_2, y_2)\,\omega_2$.
- Choose any $P \in E_1$ and evaluate $x_1 = x_1(P)$ and $y_1 = y_1(P)$: then $dx_1 = 0$ so $\omega_1 = 0$, and $(x_3, y_3) = P + (x_2, y_2) = \tau_P(x_2, y_2)$.
- Thus $\omega_3 = \tau_P^* \omega_2 = \omega_2$ by translation-invariance from (10), so the linear combination expression reads as $\omega_3 = h(x_1(P), y_1(P), x_2, y_2)\omega_3$ whence $h(x_1(P), y_1(P), x_2, y_2)$ is identically 1 as a rational function in x_2 and y_2.
- Since this is true for every point $P \in C$, in fact h is the constant 1. Similarly, $g = 1$ as well.
- So now we know that $\omega_3(x_3, y_3) = \omega_1(x_1, y_1) + \omega_2(x_2, y_2)$.

Properties of Isogenies, $Ш^{\infty} + 2$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^* \omega = \varphi^* \omega + \psi^* \omega$.

Proof (part 5):

- We have coordinates with $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$.
- We now know that $\omega_3(x_3, y_3) = \omega_1(x_1, y_1) + \omega_2(x_2, y_2)$.

Properties of Isogenies, $Ш^{\infty} + 2$

12. If ω is the invariant differential on E_1 and φ, ψ are two isogenies from $E_1 \to E_2$, then $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$.

Proof (part 5):

- We have coordinates with $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$.
- We now know that $\omega_3(x_3, y_3) = \omega_1(x_1, y_1) + \omega_2(x_2, y_2)$.
- Now apply this result to the case where $(x_1, y_1) = \varphi(x, y)$ and $(x_2, y_2) = \psi(x, y)$, so that $(x_3, y_3) = (\varphi + \psi)(x, y)$.
- Compose with the differential ω to conclude that $(\omega \circ (\varphi + \psi))(x, y) = (\omega \circ \varphi)(x, y) + (\omega \circ \psi)(x, y)$, whence $(\varphi + \psi)^*\omega = \varphi^*\omega + \psi^*\omega$, as desired.

Properties of Isogenies, $Ш^{\infty} + \infty^{\infty}$

13. For any integer m we have $[m]^*\omega = m\omega$. In particular, $[m]$ is separable if and only if $\mathrm{char}(k) \nmid m$.

Proof:

Properties of Isogenies, $Ш^{\infty} + \infty^{\infty}$

13. For any integer m we have $[m]^*\omega = m\omega$. In particular, $[m]$ is separable if and only if $\mathrm{char}(k) \nmid m$.

Proof:

- For $m \geq 0$, induct on m. The base case $m = 0$ is trivial.
- For the inductive step observe that $[m+1]^*\omega = [m]^*\omega + [1]^*\omega = (m+1)\omega$ using (12) for additivity and the obvious $[1]^*\omega = \omega$.
- For negative m note that $[m] = [-1] \circ [-m]$ and apply the result for positive m and (11).
- The last statement follows immediately from the fact discussed earlier that a morphism is separable iff it is nonzero on differentials.

Dual Isogenies, I

Our goal now is to show that "being isogenous" is an equivalence relation on elliptic curves.

- Since being isogenous is reflexive and transitive as we have already noted, it remains to show that every nonzero isogeny $\varphi : E_1 \to E_2$ induces some other nonzero isogeny $\hat{\varphi} : E_2 \to E_1$.

Dual Isogenies, I

Our goal now is to show that "being isogenous" is an equivalence relation on elliptic curves.

- Since being isogenous is reflexive and transitive as we have already noted, it remains to show that every nonzero isogeny $\varphi : E_1 \to E_2$ induces some other nonzero isogeny $\hat{\varphi} : E_2 \to E_1$.
- To see that this "dual isogeny" exists, we exploit the contravariant nature of the map $\varphi^* : \mathrm{Div}(E_2) \to \mathrm{Div}(E_1)$.
- Specifically, because φ^* scales degrees by $\deg \varphi$, as we showed earlier, it maps $\mathrm{Div}^0(E_2)$ into $\mathrm{Div}^0(E_1)$, and therefore it descends onto a well-defined map $\varphi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$.
- But as we also showed, the group operation in $\mathrm{Pic}^0(E)$ is isomorphic to the group law on E (namely, via the map sending a point $P \in E$ to the divisor class $[P] - [O]$), and so by composing these isomorphisms appropriately, we obtain a group homomorphism $\hat{\varphi} : E_2 \to E_1$.

Dual Isogenies, II

To see that this "dual isogeny" exists, we exploit the contravariant nature of the map $\varphi^* : \mathrm{Div}(E_2) \to \mathrm{Div}(E_1)$.

- Specifically, because φ^* scales degrees by $\deg \varphi$, as we showed earlier, it maps $\mathrm{Div}^0(E_2)$ into $\mathrm{Div}^0(E_1)$, and therefore it descends onto a well-defined map $\varphi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$.
- But as we also showed, the group operation in $\mathrm{Pic}^0(E)$ is isomorphic to the group law on E (namely, via the map sending a point $P \in E$ to the divisor class $[P] - [O]$), and so by composing these isomorphisms appropriately, we obtain a group homomorphism $\hat{\varphi} : E_2 \to E_1$.

Of course, it is not at all obvious that this group homomorphism $\hat{\varphi}$ is actually an isogeny, since there are very many possible homomorphisms between the point groups, most of which will not be defined by rational functions.

Dual Isogenies, III

Let's work out exactly what this map does to a point $Q \in E_2$:

- First, we map Q to the divisor class $[Q] - [O]$.
- Then we apply φ^* and (3) to obtain $\deg_i \varphi \left(\sum_{P \in \varphi^{-1}(Q)} [P] - \sum_{R \in \varphi^{-1}(O)} [R] \right)$.
- Finally we must resolve this sum to write it in the form $[S] - [O]$: the result is then S.
- By our results from equivalence of divisors, we can just sum everything using the group law: this yields $S = \deg_i \varphi \left(\sum_{P \in \varphi^{-1}(Q)} P - \sum_{R \in \varphi^{-1}(O)} R \right)$.
- Since $\varphi^{-1}(Q) = \{P + R : R \in \varphi^{-1}(O)\}$ for any fixed $P \in \varphi^{-1}(Q)$, the difference is simply $[\deg_i \varphi \cdot \#\varphi^{-1}(Q)]P$.

Dual Isogenies, IV

So, to summarize, this map $\hat{\varphi} : E_2 \to E_1$ maps a point $Q \in E_2$ to $[\deg \varphi]P$ where P is any point in $\varphi^{-1}(Q)$.

- Note that this description of $\hat{\varphi}$ is well posed: regardless of which representative $P \in \varphi^{-1}(Q)$ is chosen, since the difference between any of these representatives lies in $\varphi^{-1}(O) = \ker \varphi$.

Dual Isogenies, IV

So, to summarize, this map $\hat{\varphi} : E_2 \to E_1$ maps a point $Q \in E_2$ to $[\deg \varphi]P$ where P is any point in $\varphi^{-1}(Q)$.

- Note that this description of $\hat{\varphi}$ is well posed: regardless of which representative $P \in \varphi^{-1}(Q)$ is chosen, since the difference between any of these representatives lies in $\varphi^{-1}(O) = \ker \varphi$.
- Equivalently, this says $\hat{\varphi}(\varphi(P)) = [\deg \varphi]P$ for all $P \in E_1$, meaning that the composition $\hat{\varphi} \circ \varphi$ is simply the multiplication-by-$[\deg \varphi]$ map on E_1.

The whole point of this calculation (aside from giving an explicit description of what this map would look like) is that this last description actually provides us with a way to prove that $\hat{\varphi}$ actually is an isogeny: we can use the universal property (9) of isogenies.

Dual Isogenies, V

So, let's go through the details:

Theorem (Existence of Dual Isogenies)

Let $\varphi : E_1 \to E_2$ be a nonconstant isogeny.

1. *If φ is separable, then there exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi$ is multiplication by $\deg \varphi$ on E_1.*
2. *If $\mathrm{char}(k) = p > 0$ and Frob_p is the pth-power Frobenius morphism $\mathrm{Frob}_p : E \to E^{(p)}$, then there exists a unique isogeny $\widehat{\mathrm{Frob}_p} : E^{(p)} \to E$ such that $\widehat{\mathrm{Frob}_p} \circ \mathrm{Frob}_p$ is multiplication by $p = \deg(\mathrm{Frob}_p)$ on E.*
3. *There exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = [\deg \varphi]$ on E_1. This isogeny is called the dual isogeny of φ.*

Dual Isogenies, VI

1. If φ is separable, then there exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi$ is multiplication by $\deg \varphi$ on E_1.

Proof:

Dual Isogenies, VI

1. If φ is separable, then there exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi$ is multiplication by $\deg \varphi$ on E_1.

Proof:

- Let $\psi = [\deg \varphi]$ be the multiplication-by-$\deg \varphi$ map on E_1 and $E_3 = E_1$. Then since $\# \ker \varphi = \deg \varphi$, by Lagrange's theorem we see that $\ker \varphi \subseteq \ker \psi$.
- Now by the universal property (7) of separable isogenies, there exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = \psi = [\deg \varphi]$, as claimed.

Dual Isogenies, VII

2. If $\mathrm{char}(k) = p > 0$ and Frob_p is the pth-power Frobenius morphism $\mathrm{Frob}_p : E \to E^{(p)}$, then there exists a unique isogeny $\widehat{\mathrm{Frob}_p} : E^{(p)} \to E$ such that $\widehat{\mathrm{Frob}_p} \circ \mathrm{Frob}_p$ is multiplication by $p = \deg(\mathrm{Frob}_p)$ on E.

Proof:

Dual Isogenies, VII

2. If $\mathrm{char}(k) = p > 0$ and Frob_p is the pth-power Frobenius morphism $\mathrm{Frob}_p : E \to E^{(p)}$, then there exists a unique isogeny $\widehat{\mathrm{Frob}_p} : E^{(p)} \to E$ such that $\widehat{\mathrm{Frob}_p} \circ \mathrm{Frob}_p$ is multiplication by $p = \deg(\mathrm{Frob}_p)$ on E.

Proof:

- Let ω be the invariant differential on E.
- By property (13) of isogenies we see that $[p]^*\omega = p\omega = 0$, so $[p]$ is not separable since it is not injective on differentials.
- Hence by property (9) of isogenies, we may factor $[p]$ as $[p] = \alpha \circ \mathrm{Frob}_q$ where $q = \deg_i[p] = p^d$ for some integer $d \geq 1$ (note $d \geq 1$ because $[p]$ is not separable).
- Then since $\mathrm{Frob}_q = (\mathrm{Frob}_p)^d$ we see that $[p] = \alpha \circ (\mathrm{Frob}_p)^{d-1} \circ \mathrm{Frob}_p$.
- We can then take $\hat{\varphi} = \alpha \circ (\mathrm{Frob}_p)^{d-1}$.

Dual Isogenies, VIII

3. There exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = [\deg \varphi]$ on E_1.

Proof (existence):

Dual Isogenies, VIII

3. There exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = [\deg \varphi]$ on E_1.

Proof (existence):

- By property (9) of isogenies, we may decompose $\varphi = \alpha \circ \mathrm{Frob}_q = \alpha \circ (\mathrm{Frob}_p)^d$ where α is separable.
- By (1) there exists an isogeny $\hat{\alpha}$ with $\hat{\alpha} \circ \alpha = [\deg \alpha]$ and by (2) there exists an isogeny $\widehat{\mathrm{Frob}_p}$ with $\widehat{\mathrm{Frob}_p} \circ \mathrm{Frob}_p = [\deg \mathrm{Frob}_p]$.
- Then for $\hat{\varphi} = (\widehat{\mathrm{Frob}_p})^d \circ \hat{\alpha}$ we have $\hat{\varphi} \circ \varphi = (\widehat{\mathrm{Frob}_p})^d \circ \hat{\alpha} \circ \alpha \circ (\mathrm{Frob}_p)^d = (\widehat{\mathrm{Frob}_p})^d \circ [\deg \alpha] \circ (\mathrm{Frob}_p)^d = [\deg \alpha] \circ (\widehat{\mathrm{Frob}_p})^d \circ (\mathrm{Frob}_p)^d = [\deg \alpha][\deg \mathrm{Frob}_p]^d = [\deg \varphi]$.

Dual Isogenies, IX

3. There exists a unique isogeny $\hat{\varphi} : E_2 \to E_1$ such that $\hat{\varphi} \circ \varphi = [\deg \varphi]$ on E_1.

Proof (uniqueness):

- For uniqueness, suppose $\tilde{\varphi} \circ \varphi = [\deg \varphi] = \hat{\varphi} \circ \varphi$.
- Then $(\tilde{\varphi} - \hat{\varphi}) \circ \varphi = 0$.
- Taking degrees yields $\deg(\tilde{\varphi} - \hat{\varphi}) \deg \varphi = 0$, so since $\deg \varphi \neq 0$ that means $\deg(\tilde{\varphi} - \hat{\varphi}) = 0$ whence $\tilde{\varphi} = \hat{\varphi}$.

Dual Isogenies, X

We will now establish some additional properties of dual isogenies, which will allow us in particular to understand the kernel of the multiplication-by-m map on an elliptic curve E more explicitly.

- Since the kernel of $[m]$ is just the group of m-torsion points, this will represent substantial progress in our understanding of the group structure of E, since the torsion subgroup of E is simply the union of the m-torsion subgroups for $m \geq 1$.

Summary

We established an almost uncountably infinite number of properties of isogenies.

We introduced dual isogenies.

Next lecture: Applications of dual isogenies, the Tate module.