Math 7359 (Elliptic Curves and Modular Forms)

Lecture #13 of 24 $\sim$ October 23, 2023

Riemann-Hurwitz and Isogenies

- The Riemann-Hurwitz Genus Theorem
- Isogenies of Elliptic Curves

Recall, I

Suppose that $\varphi : C_1 \to C_2$ is a nonconstant morphism of curves.

Definition

The map $\varphi^* : k(C_2) \to k(C_1)$ is defined by $\varphi^* f = f \circ \varphi$ for $f \in k(C_2)$. The degree $\deg(\varphi)$ is defined to be the degree of the extension $k(C_1)/\varphi^* k(C_2)$.

Definition

For each $P \in C_1$ we define the ramification index $e_\varphi(P)$ to be $\mathrm{ord}_P(\varphi^* t_{\varphi(P)})$, where $t_{\varphi(P)}$ is a local uniformizer at $\varphi(P)$. We say $P \in C_1$ is unramified when $e_\varphi(P) = 1$ and otherwise P is ramified.

Recall, II

We have various other results:

Proposition (Properties of Ramification)

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

1. *For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.*
2. *A point $Q \in C_2$ is unramified if and only if $\#\varphi^{-1}(Q) = \deg \varphi$.*
3. *For all but finitely many $Q \in C_2$, $\#\varphi^{-1}(Q) = \deg_s \varphi$. As a consequence, when φ is separable, there are only finitely many ramified points Q.*
4. *The ramification index is multiplicative under composition: explicitly, if $\psi : C_2 \to C_3$ is another nonconstant morphism and $P \in C_1$, we have $e_{\psi\circ\varphi}(P) = e_\varphi(P) e_\psi(\varphi(P))$.*

The Direct Image Map

When we think of $k(C_1)$ as a finite extension of $\varphi^* k(C_2)$, we may use the norm in this extension to construct a map $\varphi_* : k(C_1) \to k(C_2)$.

- Explicitly, we define $\varphi_* : k(C_1) \to k(C_2)$ via $\varphi_* = (\varphi^*)^{-1} \circ N_{k(C_1)/\varphi^* k(C_2)}$.
- We will not bother being more explicit here, because our main interest is in the actions of the maps φ^* and φ_* on divisors and differentials, where we can give much nicer formulas.

Actions of φ^* and φ_*, I

As usual we start with divisors:

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.

Actions of φ^* and φ_*, 2

Example: Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be the squaring map $\varphi(x) = x^2$. Find $\varphi^*(D)$ and $\varphi_*(D)$ for $D = P_4 + 2P_0 - P_\infty$.

Actions of φ^* and φ_*, 2

Example: Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be the squaring map $\varphi(x) = x^2$. Find $\varphi^*(D)$ and $\varphi_*(D)$ for $D = P_4 + 2P_0 - P_\infty$.

- The value of $\varphi_*(D)$ is easier, since we just apply φ to all of the points.
- So we see that $\varphi_*(D) = P_{16} + 2P_0 - P_\infty$.
- For $\varphi^*(D)$ we need to compute the preimages of the various points that appear in D.
- We easily find $\varphi^{-1}(P_4) = \{P_2, P_{-2}\}$, $\varphi^{-1}(P_0) = P_0$, and $\varphi^{-1}(P_\infty) = P_\infty$.
- As we worked out last time, the ramification index of φ at all points of $\mathbb{P}^1$ other than 0 and ∞ is 1, and at 0 and ∞ it is 2.
- So, for $D = P_4 + 2P_0 - P_\infty$ we have $\varphi^*(D) = P_2 + P_{-2} + 4P_0 - 2P_\infty$.

Actions of φ^* and φ_*, Three

The actions also extend naturally to differentials. We will only need the action of φ^*, but for completeness we also give φ_*.

Definition

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

We define $\varphi^* : \Omega(C_2) \to \Omega(C_1)$ *by setting* $\varphi^*(f\,dx) = (\varphi^* f)\,d(\varphi^* x)$ *for all* $f, x \in k(C_2)$.

We define $\varphi_* : \Omega(C_1) \to \Omega(C_2)$ *by setting* $\varphi_*(g\,dy) = (\varphi_* g)\,d(\varphi_* y)$ *for all* $g, y \in k(C_1)$.

Actions of φ^* and φ_*, Three

The actions also extend naturally to differentials. We will only need the action of φ^*, but for completeness we also give φ_*.

Definition

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

We define $\varphi^* : \Omega(C_2) \to \Omega(C_1)$ by setting $\varphi^*(f\,dx) = (\varphi^* f)\,d(\varphi^* x)$ for all $f, x \in k(C_2)$.

We define $\varphi_* : \Omega(C_1) \to \Omega(C_2)$ by setting $\varphi_*(g\,dy) = (\varphi_* g)\,d(\varphi_* y)$ for all $g, y \in k(C_1)$.

Example: Let $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ be the squaring map $\varphi(x) = x^2$.

- Then for $\omega_2 = (x+2)\,dx$ we have $\varphi^*(\omega_2) = (x^2+2)\,d(x^2) = (x^2+2)\,2xdx$.

Actions of φ^* and φ_*, Quatre

And now for the properties:

Proposition (Properties of φ_* and φ^*)

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

1. *For any $D \in \mathrm{Div}(C_2)$, we have $\deg(\varphi^* D) = (\deg \varphi)(\deg D)$.*
2. *For any $D \in \mathrm{Div}(C_1)$, we have $\deg(\varphi_* D) = \deg D$.*
3. *For all $D \in \mathrm{Div}(C_2)$ we have $\varphi_*(\varphi^* D) = (\deg \varphi) D$.*
4. *If $\psi : C_2 \to C_3$ is another map, then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$ and $(\psi \circ \varphi)_* = \psi_* \circ \varphi_*$ as maps on divisor groups.*
5. *For all nonzero $f \in k(C_2)$ we have $\varphi^*(\mathrm{div}\, f) = \mathrm{div}(\varphi^* f)$.*
6. *For all nonzero $g \in k(C_1)$ we have $\varphi_*(\mathrm{div}\, g) = \mathrm{div}(\varphi_* g)$.*
7. *The map φ is separable if and only if $\varphi^* : \Omega(C_2) \to \Omega(C_1)$ is injective (or equivalently, nonzero).*

Actions of φ^* and φ_*, Cinque

1. For any $D \in \mathrm{Div}(C_2)$, we have $\deg(\varphi^* D) = (\deg \varphi)(\deg D)$.

Proof:

- Recall property (1) of the ramification index: For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.

Actions of φ^* and φ_*, Cinque

1. For any $D \in \mathrm{Div}(C_2)$, we have $\deg(\varphi^* D) = (\deg \varphi)(\deg D)$.

Proof:

- Recall property (1) of the ramification index: For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.
- For a single point Q we have $\varphi^* Q = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) P$.
- So $\deg(\varphi^* Q) = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$ by property (1).
- Now sum over all points in D and apply linearity.

---

2. For any $D \in \mathrm{Div}(C_1)$, we have $\deg(\varphi_* D) = \deg D$.

Proof:

Actions of φ^* and φ_*, Cinque

1. For any $D \in \mathrm{Div}(C_2)$, we have $\deg(\varphi^* D) = (\deg \varphi)(\deg D)$.

Proof:

- Recall property (1) of the ramification index: For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.
- For a single point Q we have $\varphi^* Q = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) P$.
- So $\deg(\varphi^* Q) = \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$ by property (1).
- Now sum over all points in D and apply linearity.

---

2. For any $D \in \mathrm{Div}(C_1)$, we have $\deg(\varphi_* D) = \deg D$.

Proof:

- Obvious, since if $D = \sum_{P \in C_1} n_P P$ then $\varphi_* D = \sum_{P \in C_1} n_P \varphi(P)$, whose degree is still $\sum_{P \in C_1} n_P$.

Actions of φ^* and φ_*, Seis

3. For all $D \in \mathrm{Div}(C_2)$ we have $\varphi_*(\varphi^* D) = (\deg \varphi) D$.

Proof:

Actions of φ^* and φ_*, Seis

3. For all $D \in \mathrm{Div}(C_2)$ we have $\varphi_*(\varphi^* D) = (\deg \varphi) D$.

Proof:

- For a single point Q we have
  $\varphi_*(\varphi^* Q)$
  $= \varphi_* \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) P$
  $= \sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) \varphi(P)$
  $= [\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)] Q$
  $= (\deg \varphi) Q$ using property (1) again.
- Now sum over all points in D and apply linearity.

Actions of φ^* and φ_*, Sieben

4. If $\psi : C_2 \to C_3$ is another map, then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$ and $(\psi \circ \varphi)_* = \psi_* \circ \varphi_*$ as maps on divisor groups.

Proof:

Actions of φ^* and φ_*, Sieben

4. If $\psi : C_2 \to C_3$ is another map, then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$ and $(\psi \circ \varphi)_* = \psi_* \circ \varphi_*$ as maps on divisor groups.

<u>Proof</u>:

- For a single point divisor $R \in C_3$ we have $(\psi \circ \varphi)^* R$
  $= \sum_{P \in (\psi \circ \varphi)^{-1} R} e_{\psi \circ \varphi}(P) P$
  $= \sum_{P \in \varphi^{-1}(Q)} [\sum_{Q \in \psi^{-1}(R)} e_\varphi(Q)] e_\psi(P) P$
  $= \varphi^* \psi^* R$ using the ramification-in-towers property; now apply linearity.
- Likewise, for a single point divisor $P \in C_1$ we have $(\psi \circ \varphi)_* P = \psi(\varphi(P)) = (\psi_* \circ \varphi_*)(P)$ rather trivially.

Actions of φ^* and φ_*, Kahdeksan

5. For all nonzero $f \in k(C_2)$ we have $\varphi^*(\operatorname{div} f) = \operatorname{div}(\varphi^* f)$.

Actions of φ^* and φ_*, Kahdeksan

5. For all nonzero $f \in k(C_2)$ we have $\varphi^*(\operatorname{div} f) = \operatorname{div}(\varphi^* f)$.

Exercise: For any nonzero $f \in k(C_2)$ and any $P \in C_1$, show that $\operatorname{ord}_P(\varphi^* f) = e_\varphi(P)\operatorname{ord}_{\varphi(P)}(f)$.

Proof:

Actions of φ^* and φ_*, Kahdeksan

5. For all nonzero $f \in k(C_2)$ we have $\varphi^*(\operatorname{div} f) = \operatorname{div}(\varphi^* f)$.

Exercise: For any nonzero $f \in k(C_2)$ and any $P \in C_1$, show that $\operatorname{ord}_P(\varphi^* f) = e_\varphi(P)\operatorname{ord}_{\varphi(P)}(f)$.

Proof:

- By the exercise we see that $\operatorname{div}(\varphi^* f)$
$= \sum_{P \in C_1} \operatorname{ord}_P(\varphi^* f) P$
$= \sum_{P \in C_1} \operatorname{ord}_{\varphi(P)}(f) \cdot [e_\varphi(P) P]$
$= \sum_{Q \in C_2} \operatorname{ord}_Q(f) \cdot [\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P)] P$
$= \sum_{Q \in C_2} \operatorname{ord}_Q(f)\, \varphi^* Q$
$= \varphi^* \sum_{Q \in C_2} \operatorname{ord}_Q(f) Q$
$= \varphi^*(\operatorname{div} f)$
as claimed.

Actions of φ^* and φ_*, Delapan

6. For all nonzero $g \in k(C_1)$ we have $\varphi_*(\operatorname{div} g) = \operatorname{div}(\varphi_* g)$.

Discussion:

Actions of φ^* and φ_*, Delapan

6. For all nonzero $g \in k(C_1)$ we have $\varphi_*(\mathrm{div}\, g) = \mathrm{div}(\varphi_* g)$.

Discussion:

- This property follows by general facts about the behavior of norms in finite extensions of Dedekind domains.
- It requires the definition of φ_* in terms of norms, and is hard to motivate otherwise.
- As an outline, if $(\mathrm{div}\, g) = \sum_{P \in C_1} \mathrm{ord}_P(g) P$ then $\varphi_*(\mathrm{div}\, g)$
$= \sum_{P \in C_1} \mathrm{ord}_P(g) \varphi(P)$
$= \sum_{Q \in C_2} [\sum_{\varphi(P)=Q} \mathrm{ord}_P(g)] Q$
$= \sum_{Q \in C_2} \mathrm{ord}_Q(\varphi_* g)] Q$
where the last equality follows from the definition of $\varphi_* g$.

Actions of φ^* and φ_*, Decem

7. The map φ is separable if and only if $\varphi^* : \Omega(C_2) \to \Omega(C_1)$ is injective (or equivalently, nonzero).

Proof:

Actions of φ^* and φ_*, Decem

7. The map φ is separable if and only if $\varphi^* : \Omega(C_2) \to \Omega(C_1)$ is injective (or equivalently, nonzero).

<u>Proof</u>:

- Recall $y \in k(C_2)$ has $\{dy\}$ a basis for $\Omega(C_2)$ if and only if $k(C_2)/k(y)$ is a finite-degree separable extension.
- Choose such an element y.
- Applying φ^* shows that $\varphi^* k(C_2)/\varphi^* k(y)$ is also a finite-degree separable extension, and by definition of the action of $\varphi^* y = y \circ \varphi$ we see that $\varphi^* k(y) = k(\varphi^* y)$.
- Then φ^* is injective $\iff$ $d(\varphi^* y) \neq 0$ $\iff$ $\{d(\varphi^* y)\}$ is a basis for $k(\Omega_1)$ $\iff$ $k(C_1)/k(\varphi^* y)$ is separable $\iff$ $k(C_1)/\varphi^* k(C_2)$ is separable.
- The last statement is the definition of separability for φ.

Riemann-Hurwitz, I

We can now establish the fundamental relationship between the genera of curves related by a morphism.

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. Let $\omega \in \Omega(C_2)$ be any nonzero differential and define the <u>*ramification divisor*</u> *$R = \mathrm{div}(\varphi^*\omega) - \varphi^*(\mathrm{div}\omega) \in \mathrm{Div}(C_1)$.*

1. *The ramification divisor R is independent of the choice of ω.*
2. *We have $\deg R \geq \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if the characteristic of k does not divide $e_\varphi(P)$ for any $P \in C_1$. (In particular, equality holds when the characteristic is zero.)*
3. *We have $2g_1 - 2 = (\deg \varphi)(2g_2 - 2) + \deg R$.*
4. *We have $2g_1 - 2 \geq (\deg \varphi)(2g_2 - 2) + \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if $\mathrm{char}(k) \nmid e_\varphi(P)$ for any $P \in C_1$.*

Riemann-Hurwitz, II

1. The ramification divisor $R = \mathrm{div}(\varphi^*\omega) - \varphi^*(\mathrm{div}\omega) \in \mathrm{Div}(C_1)$ is independent of the choice of $\omega \in \Omega(C_2)$.

Proof:

Riemann-Hurwitz, II

1. The ramification divisor $R = \mathrm{div}(\varphi^*\omega) - \varphi^*(\mathrm{div}\omega) \in \mathrm{Div}(C_1)$ is independent of the choice of $\omega \in \Omega(C_2)$.

Proof:

- Let $\{dx\}$ be any basis for $\Omega(C_2)$ and write $\omega = f\,dx$.
- Then $\varphi^*\omega = (\varphi^* f)\,d(\varphi^* x)$ so
  $\mathrm{div}(\varphi^*\omega) = \mathrm{div}(\varphi^* f) + \mathrm{div}[d(\varphi^* x)]$, whereas
  $\varphi^*(\mathrm{div}\omega) = \varphi^*(\mathrm{div} f) + \varphi^*(\mathrm{div}\, dx)$.
- Hence $R = \mathrm{div}(\varphi^*\omega) - \varphi^*(\mathrm{div}\omega)$
  $= [\mathrm{div}(\varphi^* f) - \varphi^*(\mathrm{div} f)] + \mathrm{div}[d(\varphi^* x)] - \varphi^*(\mathrm{div}\, dx)$
  $= \mathrm{div}[d(\varphi^* x)] - \varphi^*(\mathrm{div}\, dx)$ by property (5) above.
- This last quantity is independent of ω, as desired.

Riemann-Hurwitz, III

2. We have $\deg R \geq \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if the characteristic of k does not divide $e_\varphi(P)$ for any $P \in C_1$.

<u>Proof</u> (part 1):

Riemann-Hurwitz, III

2. We have $\deg R \geq \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if the characteristic of k does not divide $e_\varphi(P)$ for any $P \in C_1$.

<u>Proof</u> (part 1):

- As shown in (1) we have $R = \mathrm{div}[d(\varphi^* x)] - \varphi^*(\mathrm{div}\, dx)$ for any basis $\{dx\}$ of $\Omega(C_2)$.
- To compute the order of R at P, we may take $x = t$ where t is a uniformizer at $Q = \varphi(P)$, since as we showed previously, $\{dt\}$ is a basis for $\Omega(C_2)$.
- By definition, we have $\varphi^* t = us^e$ where s is a uniformizer at P, $e = e_\varphi(P)$ is the ramification index, and $u \in \mathcal{O}_P$ is defined at P with $u(P) \neq 0$.

Riemann-Hurwitz, IV

2. We have $\deg R \geq \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if the characteristic of k does not divide $e_\varphi(P)$ for any $P \in C_1$.

Proof (part 2):

Riemann-Hurwitz, IV

2. We have $\deg R \geq \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if the characteristic of k does not divide $e_\varphi(P)$ for any $P \in C_1$.

Proof (part 2):

- We take t a uniformizer at $Q = \varphi(P)$. Then $\varphi^* t = us^e$ where s is a uniformizer at P, $e = e_\varphi(P)$ is the ramification index, and $u \in \mathcal{O}_P$ is defined at P with $u(P) \neq 0$.
- Then $d(\varphi^* t) = [(du/ds)s^e + eus^{e-1}]ds$ so $\mathrm{ord}_P[d(\varphi^* t)] = \mathrm{ord}_P[(du/ds)s^e + eus^{e-1}] = (e-1) + \mathrm{ord}_P[s(du/ds) + eu]$, and we also have $\mathrm{ord}_P[\varphi^*(\mathrm{div}\, dt)] = 0$.
- Since u is defined at P we see that du/ds is also defined at P, and quite similarly to our calculations with differentials previously, we see that $\mathrm{ord}_P[d(\varphi^* t)] \geq e - 1$ with equality if and only if the characteristic of k does not divide $e = e_\varphi(P)$.
- Summing over all points $P \in C_1$ yields the result immediately.

Riemann-Hurwitz, V

3. We have $2g_1 - 2 = (\deg \varphi)(2g_2 - 2) + \deg R$.

Proof:

Riemann-Hurwitz, V

3. We have $2g_1 - 2 = (\deg \varphi)(2g_2 - 2) + \deg R$.

Proof:

- Taking degrees in the definition of R and rearranging yields $\deg[\varphi^*(\mathrm{div}\omega)] = \deg[\mathrm{div}(\varphi^*\omega)] + \deg R$.
- By property (1) of φ^*, we have $\deg(\varphi^*\omega) = (\deg \varphi)(\deg \omega) = (\deg \varphi)(2g_2 - 2)$ since ω is a differential on C_2 hence the degree of its divisor is $2g_2 - 2$ as we showed using Riemann-Roch.
- Since $\varphi^*(\mathrm{div}\omega)$ is a differential on C_1, its degree is $2g_1 - 2$.
- So we are done.

Riemann-Hurwitz, VI

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

Proof:

Riemann-Hurwitz, VI

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

Proof:

- From (2), $\deg R \geq \sum_{P \in C_1} [e_\varphi(P) - 1]$ with equality if and only if the characteristic of k does not divide $e_\varphi(P)$ for any $P \in C_1$.
- From (3), $2g_1 - 2 = (\deg \varphi)(2g_2 - 2) + \deg R$.
- Then $(2) + (3) = (4)$.

Riemann-Hurwitz, VII

The Riemann-Hurwitz theorem is really a topological result, and we can give some geometric motivation for where it comes from in the situation of Riemann surfaces, where $k = \mathbb{C}$.

- We view the curves C_1 and C_2 as surfaces over $\mathbb{R}$.
- Then the morphism φ represents a d-sheeted covering of C_2 by C_1, where each unramified point of C_2 has exactly d preimages in C_1.

Riemann-Hurwitz, VII

The Riemann-Hurwitz theorem is really a topological result, and we can give some geometric motivation for where it comes from in the situation of Riemann surfaces, where $k = \mathbb{C}$.

- We view the curves C_1 and C_2 as surfaces over $\mathbb{R}$.
- Then the morphism φ represents a d-sheeted covering of C_2 by C_1, where each unramified point of C_2 has exactly d preimages in C_1.
- If φ were unramified everywhere, then (e.g., by considering a triangulation of C_1) we see that the Euler characteristic $\chi_1 = 2 - 2g_1$ of C_1 would be d times the Euler characteristic $\chi_2 = 2 - 2g_2$ of C_2.
- That would say $\chi_1 = (\deg \varphi)\chi_2$, which is precisely the statement of Riemann-Hurwitz without the ramification term.

Riemann-Hurwitz, VIII

So now what happens if there are ramified points?

- As we have seen, at ramified points of φ, there are fewer preimage points than expected, meaning that sheets of the covering collide, which introduces an error term into the characteristic calculation.

Riemann-Hurwitz, VIII

So now what happens if there are ramified points?

- As we have seen, at ramified points of φ, there are fewer preimage points than expected, meaning that sheets of the covering collide, which introduces an error term into the characteristic calculation.
- Precisely, at a ramified point the ramification index $e_\varphi(P)$ counts the number of sheets that collide at P, and so relative to unramified points (with ramification index 1) the overall characteristic χ_1 is lowered by a total of $e_\varphi(P)$ from what would be expected if the point were unramified.
- Summing this correction over all of the ramified points yields the general statement of Riemann-Hurwitz: $\chi_1 = (\deg \varphi)\chi_2 - \sum_{P \in C_1} [e_\varphi(P) - 1]$.

Isogenies, I

We are now – finally! – done with all of the preliminary results, and will narrow our focus to elliptic curves permanently. Our first task is to study maps from one elliptic curve to another.

- Since we defined an elliptic curve as a smooth projective curve of genus 1 together with a marked rational point O, we require the maps also to preserve the marked point:

Isogenies, I

We are now – finally! – done with all of the preliminary results, and will narrow our focus to elliptic curves permanently. Our first task is to study maps from one elliptic curve to another.

- Since we defined an elliptic curve as a smooth projective curve of genus 1 together with a marked rational point O, we require the maps also to preserve the marked point:

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.

Since nonconstant morphisms of curves are surjective, and the only constant isogeny is the zero map, nonzero isogenies are surjective.

Isogenies, II

As we will show later, being isogenous is an equivalence relation on elliptic curves.

- It is self-evidently reflexive and transitive, since the identity morphism is an isogeny and the composition of two isogenies is an isogeny.

Isogenies, II

As we will show later, being isogenous is an equivalence relation on elliptic curves.

- It is self-evidently reflexive and transitive, since the identity morphism is an isogeny and the composition of two isogenies is an isogeny.

When φ is nonzero, recall that we define the degree of φ to be degree of the function-field extension $k(C_2)/\varphi^* k(C_1)$. We also set $\deg(0) = 0$ for convenience.

Exercise: Show that the degree map is multiplicative on isogenies: $\deg(\varphi \circ \psi) = (\deg \varphi)(\deg \psi)$.

Isogenies, III

Since E_1 and E_2 are groups, the collection of all isogenies from E_1 to E_2 forms an abelian group, and since compositions of isogenies are isogenies, the set of isogenies from E to E forms a ring.

Isogenies, III

Since E_1 and E_2 are groups, the collection of all isogenies from E_1 to E_2 forms an abelian group, and since compositions of isogenies are isogenies, the set of isogenies from E to E forms a ring.

Exercise: Let E_1 and E_2 be elliptic curves and define $\mathrm{Hom}(E_1, E_2)$ to be the collection of all isogenies from E_1 to E_2. Show that $\mathrm{Hom}(E_1, E_2)$ is an abelian group under the addition operation $(\varphi + \psi)P = \varphi(P) + \psi(P)$ for all $P \in E_1$ (the addition on the right is the sum under the group law on E_2) for $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$.

Isogenies, III

Since E_1 and E_2 are groups, the collection of all isogenies from E_1 to E_2 forms an abelian group, and since compositions of isogenies are isogenies, the set of isogenies from E to E forms a ring.

Exercise: Let E_1 and E_2 be elliptic curves and define $\mathrm{Hom}(E_1, E_2)$ to be the collection of all isogenies from E_1 to E_2. Show that $\mathrm{Hom}(E_1, E_2)$ is an abelian group under the addition operation $(\varphi + \psi)P = \varphi(P) + \psi(P)$ for all $P \in E_1$ (the addition on the right is the sum under the group law on E_2) for $\varphi, \psi \in \mathrm{Hom}(E_1, E_2)$.

Exercise: Let E be an elliptic curve and define $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ to be the collection of all isogenies from E to itself. Show that E is a ring with 1 having no zero divisors, with addition given as in the exercise above and multiplication given by composition. [Hint: For the lack of zero divisors, consider degrees.]

Isogenies, IV

Our most basic example of an isogeny is the multiplication-by-m map:

- For an integer m, the multiplication-by-m map $[m] : E \to E$ is an isogeny, since as we have previously discussed it is a morphism, and it clearly preserves the group identity O.

Isogenies, IV

Our most basic example of an isogeny is the multiplication-by-m map:

- For an integer m, the multiplication-by-m map $[m] : E \to E$ is an isogeny, since as we have previously discussed it is a morphism, and it clearly preserves the group identity O.
- We showed much earlier during our discussion of Mordell's theorem that the multiplication-by-m map has degree m^2, since as a rational map it is defined by a quotient of polynomials of degree m^2.
- We will later give a far nicer and minimally computational proof that $[m]$ has degree m^2.

Isogenies, V

In particular, since its degree is m^2, $[m] \neq 0$ for $m \neq 0$. There are some nice consequences to this fact:

- First, we see that the endomorphism ring $\mathrm{End}(E)$ always contains the subring $\mathbb{Z}$ generated by the identity map [1].

Isogenies, V

In particular, since its degree is m^2, $[m] \neq 0$ for $m \neq 0$. There are some nice consequences to this fact:

- First, we see that the endomorphism ring $\mathrm{End}(E)$ always contains the subring $\mathbb{Z}$ generated by the identity map $[1]$.
- Additionally, if $\varphi : E_1 \to E_2$ is any isogeny, we see that $\deg(m\varphi) = \deg([m] \circ \varphi) = \deg([m]) \deg(\varphi) = m^2 \deg(\varphi)$.
- Thus, if φ is a torsion element of $\mathrm{Hom}(E_1, E_2)$ so that $m\varphi = 0$, the above implies $\deg(\varphi) = 0$ whence $\varphi = 0$.
- Thus, $\mathrm{Hom}(E_1, E_2)$ is a torsion-free abelian group.

As we will see in a few lectures, for many elliptic curves the multiplication-by-m maps are the only endomorphisms! So it requires some nontrivial effort to give other examples.

Isogenies, VI

Example: Consider the map $i : E \to E$ with $i(x, y) = (-x, iy)$ on the elliptic curve $E : y^2 = x^3 - x$, where $i^2 = -1$ inside the underlying field k (where we assume $\mathrm{char}(k) \neq 2$ to avoid trivialities).

Isogenies, VI

Example: Consider the map $i : E \to E$ with $i(x, y) = (-x, iy)$ on the elliptic curve $E : y^2 = x^3 - x$, where $i^2 = -1$ inside the underlying field k (where we assume $\mathrm{char}(k) \neq 2$ to avoid trivialities).

- This map is a morphism from E to E since $(-x, iy)$ is also a point of E and it is described by rational functions that are defined everywhere, and since it maps $O = \infty$ to itself, it is an isogeny of E.
- Since $[i] \circ [i]$ maps $(x, y) \mapsto (x, -y)$ we see $[i] \circ [i] = [-1]$.
- Taking $b[i]$ to be the b-fold sum of $[i]$ with itself, we see that the endomorphism ring $\mathrm{End}(E)$ contains the elements $[a] + b[i]$ for all $a, b \in \mathbb{Z}$.

Isogenies, VII

Example: Consider the map $i : E \to E$ with $i(x, y) = (-x, iy)$ on the elliptic curve $E : y^2 = x^3 - x$, where $i^2 = -1$ inside the underlying field k (where we assume $\mathrm{char}(k) \neq 2$ to avoid trivialities).

- As we just saw, the maps of the form $[a] + b[i]$ for $a, b \in \mathbb{Z}$ are endomorphisms of E.

Isogenies, VII

Example: Consider the map $i : E \to E$ with $i(x, y) = (-x, iy)$ on the elliptic curve $E : y^2 = x^3 - x$, where $i^2 = -1$ inside the underlying field k (where we assume $\mathrm{char}(k) \neq 2$ to avoid trivialities).

- As we just saw, the maps of the form $[a] + b[i]$ for $a, b \in \mathbb{Z}$ are endomorphisms of E.
- Since $[i] \circ [i] = [-1]$, when k is a subfield of $\mathbb{C}$ we see that the ring of such elements embeds in the Gaussian integer ring $\mathbb{Z}[i]$ via the obvious map $[a] + b[i] \mapsto a + bi$.
- In fact, these are all of the endomorphisms of E.
- This curve is an example of an elliptic curve with complex multiplication, as it possesses an endomorphism that behaves like multiplication by a complex number (in this case, $i = \sqrt{-1}$).

Isogenies, VIII

Example: Let $E = V(f)$ be an elliptic curve and let $E^{(p)} = V(f^{(p)})$, where $f^{(p)}$ is obtained by raising all of the coefficients of f to the pth power[1].

- Then the Frobenius map $\mathrm{Frob} : E \to E^{(p)}$ with $\mathrm{Frob}(x, y) = (x^p, y^p)$ is an isogeny from E to $E^{(p)}$ since it is clearly a morphism and it preserves the point at ∞.

[1] Since the discriminant is a polynomial function of the coefficients of the Weierstrass equation, since the Frobenius map is a field automorphism, the discriminant of $f^{(p)}$ is the pth power of the discriminant of E, so $E^{(p)}$ is also nonsingular when E is nonsingular.

Isogenies, VIII

<u>Example</u>: Let $E = V(f)$ be an elliptic curve and let $E^{(p)} = V(f^{(p)})$, where $f^{(p)}$ is obtained by raising all of the coefficients of f to the pth power[1].

- Then the Frobenius map $\mathrm{Frob} : E \to E^{(p)}$ with $\mathrm{Frob}(x, y) = (x^p, y^p)$ is an isogeny from E to $E^{(p)}$ since it is clearly a morphism and it preserves the point at ∞.
- If E is defined over the field $\mathbb{F}_p$, Frob fixes all of the coefficients (indeed, $\mathbb{F}_p$ is precisely the fixed field of Frob): then $E^{(p)} = E$ and so Frob is an endomorphism of E.
- More generally, if E is defined over $\mathbb{F}_q$ for some prime power q, then the qth-power Frobenius map $\mathrm{Frob}(x, y) = (x^q, y^q)$ is an endomorphism of E.

[1] Since the discriminant is a polynomial function of the coefficients of the Weierstrass equation, since the Frobenius map is a field automorphism, the discriminant of $f^{(p)}$ is the pth power of the discriminant of E, so $E^{(p)}$ is also nonsingular when E is nonsingular.

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)

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, III

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

Discussion:

Properties of Isogenies, III

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:

- In fact this result is 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.

Properties of Isogenies, II: Wait, Two?

Next time we will prove 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 $\ker \varphi = \Phi$.*

Summary

We discussed the direct and inverse image maps φ_* and φ^*

We proved the Riemann-Hurwitz genus theorem.

We introduced isogenies and established some of their basic properties.

Next lecture: More with isogenies, dual isogenies.