Math 7359 (Elliptic Curves and Modular Forms)

Lecture #12 of 24 $\sim$ October 19, 2023

Riemann-Roch and Ramification

- Differentials on Elliptic Curves (leftovers)
- Outline of Riemann-Roch
- Ramification

Recall, I

Recall differentials:

- The space of differentials $\Omega(C)$ consists of symbols dx for $x \in k(C)$, subject to the following three relations:
  1. The additivity relation $d(x+y) = dx + dy$ for all $x, y \in k(C)$.
  2. The Leibniz rule $d(xy) = x\,dy + y\,dx$ for all $x, y \in k(C)$.
  3. Derivatives of constants are zero: $da = 0$ for all $a \in k$.
- $\Omega(C)$ is a 1-dimensional $k(C)$-vector space.
- If t is a local uniformizer at some P, then any differential is of the form $\omega = f\,dt$ for some $f \in k(C)$.
- The <u>divisor</u> of ω is $\mathrm{div}(\omega) = \sum_P \mathrm{ord}_P(\omega)\,P$.
- The <u>canonical class</u> $\mathcal{C}$ is the divisor class of $\mathrm{div}(\omega)$ in $\mathrm{Pic}(C)$.
- A differential ω is <u>holomorphic</u> if $\mathrm{div}(\omega) \geq 0$. The space $\Omega(0)$ of holomorphic differentials is finite-dimensional, and its dimension is defined to be g, the <u>genus</u> of C.

Differentials on Elliptic Curves, II

Proposition (Differentials on Elliptic Curves)

Let C/k be a smooth projective curve with affine Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then

1. *The differential $\omega = \dfrac{dx}{2y + a_1x + a_3} = -\dfrac{dy}{3x^2 + 2a_2x + a_4}$ is holomorphic and nonvanishing on C.*
2. *The space of holomorphic differentials on C is a 1-dimensional k-vector space, whence C has genus 1.*
3. *Smooth projective genus-1 curves are equivalent to curves with nonsingular Weierstrass equations.*
4. *The differential ω from (1) is translation-invariant, meaning that for any point Q on E, if $(x, y) + Q = (\tilde{x}, \tilde{y})$, then $\omega = \dfrac{d\tilde{x}}{2\tilde{y} + a_1\tilde{x} + a_3}$ as well.*

Differentials on Elliptic Curves, III

2. The space of holomorphic differentials on C is a 1-dimensional k-vector space, whence C has genus 1.

Proof:

- Take ω as in (1): then $\mathrm{div}(\omega) = 0$.
- From our properties of differentials, any other differential ζ is of the form $f\omega$ for some $f \in k(C)$.

Differentials on Elliptic Curves, III

2. The space of holomorphic differentials on C is a 1-dimensional k-vector space, whence C has genus 1.

Proof:

- Take ω as in (1): then $\mathrm{div}(\omega) = 0$.
- From our properties of differentials, any other differential ζ is of the form $f\omega$ for some $f \in k(C)$.
- But then $\mathrm{div}(\zeta) = \mathrm{div}(f) + \mathrm{div}(\omega) = \mathrm{div}(f)$, so in order for ζ to be holomorphic we must have $\mathrm{div}(f) \geq 0$, meaning that f is a rational function with no poles.
- But the only such (projective) functions are constants, whence ζ is a k-scalar multiple of ω.
- Thus, the space of holomorphic differentials on C is a 1-dimensional k-vector space, so C has genus 1 as claimed.

Differentials on Elliptic Curves, IV

3. Every smooth projective genus-1 curve has a nonsingular Weierstrass equation, and conversely every nonsingular Weierstrass equation gives a smooth projective genus-1 curve.

Proof:

- We showed the first part earlier using Riemann-Roch.
- The second part is simply (2).

Differentials on Elliptic Curves, V

4. The differential ω from (1) is translation-invariant, meaning that for any point Q on E, if $(x, y) + Q = (\tilde{x}, \tilde{y})$, then $\omega = \dfrac{d\tilde{x}}{2\tilde{y} + a_1\tilde{x} + a_3}$ as well.

Differentials on Elliptic Curves, V

4. The differential ω from (1) is translation-invariant, meaning that for any point Q on E, if $(x, y) + Q = (\tilde{x}, \tilde{y})$, then $\omega = \dfrac{d\tilde{x}}{2\tilde{y} + a_1\tilde{x} + a_3}$ as well.

- We could in principle show this result just using the point addition formulas, since they give explicit expressions for $\tilde{x}$ and $\tilde{y}$ in terms of x, y, and the coordinates of Q.
- We will give a less tedious argument.

Because of this result, we call ω the invariant differential of E.

Differentials on Elliptic Curves, VI

4. The differential ω from (1) is translation-invariant, meaning that for any point Q on E, if $(x, y) + Q = (\tilde{x}, \tilde{y})$, then $\omega = \dfrac{d\tilde{x}}{2\tilde{y} + a_1\tilde{x} + a_3}$ as well.

Proof (part 1):

- Since $\tilde{\omega}$ is obtained by adding Q to all points on C, for any P on C we see that $\mathrm{ord}_P(\tilde{\omega}) = \mathrm{ord}_{P-Q}(\omega) = 0$, and so $\tilde{\omega}$ is also a nonvanishing holomorphic differential.

Differentials on Elliptic Curves, VI

4. The differential ω from (1) is translation-invariant, meaning that for any point Q on E, if $(x, y) + Q = (\tilde{x}, \tilde{y})$, then $\omega = \dfrac{d\tilde{x}}{2\tilde{y} + a_1\tilde{x} + a_3}$ as well.

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

- Since $\tilde{\omega}$ is obtained by adding Q to all points on C, for any P on C we see that $\mathrm{ord}_P(\tilde{\omega}) = \mathrm{ord}_{P-Q}(\omega) = 0$, and so $\tilde{\omega}$ is also a nonvanishing holomorphic differential.
- By (2) since the space of holomorphic differentials is 1-dimensional, that means $\tilde{\omega} = c_Q\omega$ for some scalar $c_Q \in k$ that (a priori) depends on Q.
- Now consider the map $\varphi : E \to \mathbb{P}^1$ sending $Q \mapsto [c_Q : 1]$ for each point Q.

Differentials on Elliptic Curves, VII

4. The differential ω from (1) is translation-invariant, meaning that for any point Q on E, if $(x, y) + Q = (\tilde{x}, \tilde{y})$, then $\omega = \dfrac{d\tilde{x}}{2\tilde{y} + a_1\tilde{x} + a_3}$ as well.

Proof (part 2):

- Now consider $\varphi : E \to \mathbb{P}^1$ sending $Q \mapsto [c_Q : 1]$.
- This map is necessarily rational (since after all the expressions for $\tilde{x}$ and $\tilde{y}$ are rational functions, so the ratio $\tilde{\omega}/\omega$ is some rational function), but it clearly omits $[1 : 0]$ since c_Q is defined for all Q.

Differentials on Elliptic Curves, VII

4. The differential ω from (1) is translation-invariant, meaning that for any point Q on E, if $(x, y) + Q = (\tilde{x}, \tilde{y})$, then $\omega = \dfrac{d\tilde{x}}{2\tilde{y} + a_1\tilde{x} + a_3}$ as well.

<u>Proof</u> (part 2):

- Now consider $\varphi : E \to \mathbb{P}^1$ sending $Q \mapsto [c_Q : 1]$.
- This map is necessarily rational (since after all the expressions for $\tilde{x}$ and $\tilde{y}$ are rational functions, so the ratio $\tilde{\omega}/\omega$ is some rational function), but it clearly omits $[1 : 0]$ since c_Q is defined for all Q.
- Thus φ is not surjective, meaning that it must be constant since nonconstant rational maps of curves are surjective.
- Finally, setting Q to be the identity O on E shows $\tilde{\omega}_O = \omega$, so the constant must be 1. We conclude that $\tilde{\omega} = \omega$ for all Q.

Riemann-Roch Redux — I

Now that we have defined the canonical class and the genus, we can outline the proof of Riemann-Roch:

Theorem (Riemann-Roch)

For any algebraic curve C/k, there exists an integer $g \geq 0$ called the genus of C, and a divisor class $\mathcal{C}$, called the canonical class of C, such that for any divisor $C \in \mathcal{C}$ and any divisor $A \in \mathrm{Div}(K)$, we have $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$.

Riemann-Roch Redux —— II

The main additional definition required is the residue of a rational function $f \in k(C)$ at a point P, which is the general analogue of the residue of a meromorphic function at a point in $\mathbb{C}$.

- There are various ways to give this definition, but the standard approach is as the coefficient a_{-1} in a local Laurent expansion $f = \sum_{n=-k}^{\infty} a_n t^n$ where t is a local uniformizer.

Riemann-Roch Redux —— II

The main additional definition required is the residue of a rational function $f \in k(C)$ at a point P, which is the general analogue of the residue of a meromorphic function at a point in $\mathbb{C}$.

- There are various ways to give this definition, but the standard approach is as the coefficient a_{-1} in a local Laurent expansion $f = \sum_{n=-k}^{\infty} a_n t^n$ where t is a local uniformizer.
- To show such an expansion exists, by definition $g = t^{-\mathrm{ord}_P f} f$ is defined at P: writing $a_{-k} = g(P)$, we see that $f - a_{-k} t^{-k}$ has a strictly smaller pole order.
- By repeating this procedure, we may write $f = [\sum_{n=-k}^{d} a_n t^n] + h$ where h is defined at P and has a zero of order at least $d + 1$. The Laurent expansion is just the formal limit as $d \to \infty$.

Riemann-Roch Redux ——— III

Here are some other facts about residues:

- The residue of a rational function is only nonzero when the function has a pole at P.
- By the analogue of Cauchy's residue theorem (or Stokes's theorem, depending on one's interpretation), the sum of the residues of any rational function over all its poles is zero.

Riemann-Roch Redux ——— IV

Now suppose we have an effective divisor $D = P_1 + P_2 + \cdots + P_d$ for distinct points P_i.

- Then we obtain a map $\varphi : L(D) \to k^d$ by taking $\varphi(D) = (\mathrm{Res}_{P_1} f, \mathrm{Res}_{P_2} f, \ldots, \mathrm{Res}_{P_d} f)$.

Riemann-Roch Redux ——— IV

Now suppose we have an effective divisor $D = P_1 + P_2 + \cdots + P_d$ for distinct points P_i.

- Then we obtain a map $\varphi : L(D) \to k^d$ by taking $\varphi(D) = (\mathrm{Res}_{P_1} f, \mathrm{Res}_{P_2} f, \dots, \mathrm{Res}_{P_d} f)$.
- The kernel of this map is the set of functions $g \in L(D)$ whose residue is zero at each P_i, which includes all constant functions.
- Thus, we obtain an exact sequence $0 \to k \to L(D) \xrightarrow{\varphi} k^d$.

Now we ask the question: how close is the map φ to being surjective? In other words, what conditions are there on the values of the residues of a function in $L(D)$ at the points P_i?

Riemann-Roch Redux ——— V

We can answer this question by looking at the residues of holomorphic and meromorphic differentials. Here is some motivation for why these things show up in Riemann-Roch:

Definition

Let D be a divisor on the curve C. We define $\Omega(D)$ to be the space of differentials ζ such that $\mathrm{div}(\zeta) \geq -D$. In particular, $\Omega(0)$ is the space of holomorphic differentials.

Riemann-Roch Redux ——— V

We can answer this question by looking at the residues of holomorphic and meromorphic differentials. Here is some motivation for why these things show up in Riemann-Roch:

Definition

Let D be a divisor on the curve C. We define $\Omega(D)$ to be the space of differentials ζ such that $\mathrm{div}(\zeta) \geq -D$. In particular, $\Omega(0)$ is the space of holomorphic differentials.

Exercise: Show $\Omega(D)$ is a k-vector space isomorphic to $L(\mathcal{C} - D)$, where $\mathcal{C}$ is any element of the canonical class of C. [Hint: Fix a differential ω and let $f \in L(\mathcal{C} - D)$ and consider $f \mapsto f\omega$. The proof that the space of holomorphic differentials is isomorphic to $L(\mathcal{C})$ is a special case.]

Riemann-Roch Redux — VI

Definition

If ω is holomorphic, we define the residue of ω at P as the residue of the ratio ω/dt at P where dt is a local uniformizer at P.

- In the same way as for functions, the sum of the residues of any meromorphic differential over all points must be zero.

Riemann-Roch Redux — VI

Definition

If ω is holomorphic, we define the residue of ω at P as the residue of the ratio ω/dt at P where dt is a local uniformizer at P.

- In the same way as for functions, the sum of the residues of any meromorphic differential over all points must be zero.
- So, again with $D = P_1 + P_2 + \cdots + P_d$ for distinct points P_i, for each holomorphic ω and each $f \in L(D)$, we see that the sum of the residues of $f\omega$ must be zero.
- This means each differential imposes a linear condition on the possible choices of residues for f.

Riemann-Roch Redux ——————— VII

More precisely, we obtain a map $\psi : \Omega(0) \to k^d$ by taking $\psi(D) = (\mathrm{Res}_{P_1}\omega, \mathrm{Res}_{P_2}\omega, \ldots, \mathrm{Res}_{P_k}\omega)$.

- The kernel of this map is the set of differentials $\omega \in \Omega(D)$ whose residue is zero at each P_i, which includes everything in $\omega \in \Omega(0)$.
- Thus, we get another exact sequence $0 \to \Omega(0) \to \Omega(D) \xrightarrow{\psi} k^d$, to go along with $0 \to k \to L(D) \xrightarrow{\varphi} k^d$.

Riemann-Roch Redux — VII

More precisely, we obtain a map $\psi : \Omega(0) \to k^d$ by taking $\psi(D) = (\mathrm{Res}_{P_1}\omega, \mathrm{Res}_{P_2}\omega, \ldots, \mathrm{Res}_{P_k}\omega)$.

- The kernel of this map is the set of differentials $\omega \in \Omega(D)$ whose residue is zero at each P_i, which includes everything in $\omega \in \Omega(0)$.
- Thus, we get another exact sequence $0 \to \Omega(0) \to \Omega(D) \xrightarrow{\psi} k^d$, to go along with $0 \to k \to L(D) \xrightarrow{\varphi} k^d$.

Exercise: If $D \geq 0$, show that Riemann-Roch is equivalent to the statement that $\dim_k[L(D)/L(0)] + \dim_k[\Omega(D)/\Omega(0)] = \deg(D)$. (Note that we require $D \geq 0$ in order for the quotient spaces to make sense.)

Riemann-Roch Redux ——— VIII

We have $0 \to \Omega(0) \to \Omega(D) \xrightarrow{\psi} k^d$ and $0 \to k \to L(D) \xrightarrow{\varphi} k^d$.
Now, observe that $\dim(\mathrm{im}\varphi)$ and $\dim(\mathrm{im}\psi)$ are orthogonal in k^d:

- For $f \in L(D)$ and $\omega \in \Omega(D)$, the dot product of $\varphi(f)$ and $\psi(\omega)$ is $\sum_{i=1}^d \mathrm{Res}_{P_i}(f)\mathrm{Res}_{P_i}(\omega) = \sum_{i=1}^d \mathrm{Res}_{P_i}(f\omega) = 0$ since this is the sum of the residues of a differential.

Riemann-Roch Redux —————— VIII

We have $0 \to \Omega(0) \to \Omega(D) \xrightarrow{\psi} k^d$ and $0 \to k \to L(D) \xrightarrow{\varphi} k^d$.
Now, observe that $\dim(\mathrm{im}\varphi)$ and $\dim(\mathrm{im}\psi)$ are orthogonal in k^d:

- For $f \in L(D)$ and $\omega \in \Omega(D)$, the dot product of $\varphi(f)$ and $\psi(\omega)$ is $\sum_{i=1}^{d} \mathrm{Res}_{P_i}(f)\mathrm{Res}_{P_i}(\omega) = \sum_{i=1}^{d} \mathrm{Res}_{P_i}(f\omega) = 0$ since this is the sum of the residues of a differential.
- So, since the images of φ and ψ are orthogonal, we see that $\dim(\mathrm{im}\varphi) + \dim(\mathrm{im}\psi) \leq d = \deg(D)$.
- By nullity-rank, since $\ker(\varphi) = k$ we get $\dim(\mathrm{im}\varphi) = \dim(L(D)) - 1 = \ell(D) - 1$.
- Likewise, since $\ker(\psi) = \Omega(D)$ we get $\dim(\mathrm{im}\psi) = \dim(\Omega(0)) - \dim(\Omega(D)) = g - \ell(C - D)$.
- Thus, we obtain Riemann's inequality $\ell(D) - 1 + g - \ell(C - D) \leq \deg(D)$.

Riemann-Roch is the statement that we actually have equality here.

Riemann-Roch Redux — IX

As it stands, we know $\ell(D) - 1 + g - \ell(C - D) \leq \deg(D)$ when D is effective.

- In the event that $C - D$ is also effective, however, we can extract the desired result.

Riemann-Roch Redux — IX

As it stands, we know $\ell(D) - 1 + g - \ell(C - D) \leq \deg(D)$ when D is effective.

- In the event that $C - D$ is also effective, however, we can extract the desired result.
- In such a case, we have both $\ell(D) - 1 + g - \ell(C - D) \leq \deg(D)$ and $\ell(C - D) - 1 + g - \ell(D) \leq \deg(C - D) = \deg(C) - \deg(D)$.
- Adding yields $2g - 2 \leq \deg(C)$. But since $\deg(C) = 2g - 2$ (a calculation we take for granted), we must have equality in both cases.
- This establishes Riemann-Roch for divisors D where both D and $C - D$ are effective divisors (or equivalent to effective divisors, since as we showed, $\ell(D_1) = \ell(D_2)$ when $D_1 \sim D_2$).

This is nearly enough: as we showed, if $L(D) \neq 0$ then D is equivalent to an effective divisor.

Riemann-Roch Redux — X

The only other item we need to justify is that when $\ell(C-D)=0$, one has $\deg(D) \geq \ell(D)-1+g$.

- Assuming that $\deg(D) \geq \ell(D)-1+g$, one obtains Riemann-Roch in general: if both D and $C-D$ are equivalent to effective divisors, the result is as above, and if D is but $C-D$ is not, the result follows from $\deg(D) \geq \ell(D)-1+g$, and if $C-D$ is but D is not, the result is equivalent by interchanging D and $C-D$.
- Finally, if neither D nor $C-D$ is equivalent to an effective divisor (i.e., if $\ell(D)=\ell(C-D)=0$), then by the inequality above we must have $\deg(D) \geq g-1$ and $\deg(C-D) \geq g-1$.
- But since $\deg(C)=2g-2$ this forces $\deg(D)=g-1$, in which case we do get $\deg(D)=\ell(D)-1+g-\ell(C-D)$, as required.

Preliminaries for Ramification, I

Our next object of study is how morphisms interact with divisors and differentials. We begin by discussing the notion of ramification.

- Recall, as we have previously discussed, that if $\varphi : C_1 \to C_2$ is a nonconstant morphism of curves then we obtain a corresponding injection $\varphi^* : k(C_2) \to k(C_1)$ on function fields given by $\varphi^* f = f \circ \varphi$ for $f \in k(C_2)$.

Preliminaries for Ramification, I

Our next object of study is how morphisms interact with divisors and differentials. We begin by discussing the notion of ramification.

- Recall, as we have previously discussed, that if $\varphi : C_1 \to C_2$ is a nonconstant morphism of curves then we obtain a corresponding injection $\varphi^* : k(C_2) \to k(C_1)$ on function fields given by $\varphi^* f = f \circ \varphi$ for $f \in k(C_2)$.
- More generally, this association yields an equivalence of categories, where E is an arbitrary field:

1. (Objects) Function fields K/E of transcendence degree 1 where $K \cap \overline{E} = E$
   (Morphisms) Field injections fixing 1 (up to isomorphism)
2. (Objects) Smooth projective curves defined over E
   (Morphisms) Non-constant morphisms defined over E (up to isomorphism)

Preliminaries for Ramification, II

Continue to assume $\varphi : C_1 \to C_2$ is a nonconstant morphism.

- Since both function fields have transcendence degree 1 over k and are finitely generated, the field extension $k(C_1)/\varphi^* k(C_2)$ has finite degree.
- We define the degree of this extension to be the degree $\deg(\varphi)$. For completeness also we define the degree of constant morphisms to be 0.
- Additionally, we say φ is separable (or inseparable) when the corresponding field extension is separable (or inseparable) and define the associated separable degree (and inseparable degree) of φ to be the corresponding separable degree (and inseparable degree) of the field extension.

Preliminaries for Ramification, III

Example: Consider the morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ given by $\varphi[X : Y] = [X^2 : Y^2]$, with $x = X/Y$ as usual.

Preliminaries for Ramification, III

Example: Consider the morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ given by $\varphi[X : Y] = [X^2 : Y^2]$, with $x = X/Y$ as usual.

- We have $k(C_1) = k(C_2) = k(x)$ and $\varphi(x) = x^2$, so $\varphi^* k(C_2) = k(x^2)$.
- Then the corresponding function-field extension is $k(x)/k(x^2)$, which has degree 2.

Preliminaries for Ramification, III

Example: Consider the morphism $\varphi : \mathbb{P}^1 \to \mathbb{P}^1$ given by $\varphi[X : Y] = [X^2 : Y^2]$, with $x = X/Y$ as usual.

- We have $k(C_1) = k(C_2) = k(x)$ and $\varphi(x) = x^2$, so $\varphi^* k(C_2) = k(x^2)$.
- Then the corresponding function-field extension is $k(x)/k(x^2)$, which has degree 2.
- Written affinely, the map is simply $\varphi(x) = x^2$, which we quite reasonably would expect to have degree 2 under any sensible definition.
- When the field characteristic is not equal to 2, this map is separable, and when the characteristic equals 2, it is (purely) inseparable.

Ramification, I

Now we can discuss ramification:

Definition

Let $\varphi : C_1 \to C_2$ be a nonconstant morphism. 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 $\varphi(P)$.

Intuitively, the ramification index $e_\varphi(P)$ measures by what factor the local order of vanishing changes when we apply φ to move from P to $\varphi(P)$.

Ramification, I

Now we can discuss ramification:

Definition

Let $\varphi : C_1 \to C_2$ be a nonconstant morphism. 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 $\varphi(P)$.

Intuitively, the ramification index $e_\varphi(P)$ measures by what factor the local order of vanishing changes when we apply φ to move from P to $\varphi(P)$.

- Note by definition that the evaluation $(\varphi^* t_{\varphi(P)})(P) = (t_{\varphi(P)} \circ \varphi)(P) = t_{\varphi(P)}(\varphi(P)) = 0$, so the function $\varphi^* t_{\varphi(P)}$ is defined at P and evaluates to zero there.
- Thus, we have $e_\varphi(P) \geq 1$ with equality if and only if $\varphi^* t_{\varphi(P)}$ is a local uniformizer at P.

Ramification, II

Now we can discuss ramification:

Definition

Let $\varphi : C_1 \to C_2$ be a nonconstant morphism, with ramification index $\mathrm{ord}_P(\varphi^* t_{\varphi(P)})$. When $e_\varphi(P) = 1$ we say that P is unramified and otherwise (when $e_\varphi(P) > 1$) we say that P is ramified.
We extend this to say a point $Q \in C_2$ is unramified when all its preimages $P \in \varphi^{-1}(Q)$ are unramified.

Equivalently, in terms of the characterization on the last slide, P is unramified precisely when applying the map φ^* maps a local uniformizer at $\varphi(P)$ to a local uniformizer at P.

Ramification, III

Example: Consider the squaring map $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(x) = x^2$ from earlier. Find the ramification index at 2, 0, and ∞.

- By definition, $\varphi^* f(x) = f(x^2)$.

Ramification, III

<u>Example</u>: Consider the squaring map $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(x) = x^2$ from earlier. Find the ramification index at 2, 0, and ∞.

- By definition, $\varphi^* f(x) = f(x^2)$.
- At $P = 2$ we have $\varphi(P) = 4$ and so $t_{\varphi(P)} = x - 4$ is a local uniformizer at $\varphi(P)$. Then $\varphi^* t_{\varphi(P)} = x^2 - 4$, so $\mathrm{ord}_P(\varphi^* t_{\varphi(P)}) = \mathrm{ord}_{x-2}(x^2 - 4) = 1$, so $P = 2$ is unramified.
- On the other hand, at $Q = 0$ we see that $t_{\varphi(Q)} = x$ so that $\varphi^* t_{\varphi(Q)} = x^2$ and $\mathrm{ord}_Q(\varphi^* t_{\varphi(Q)}) = \mathrm{ord}_x(x^2) = 2$, so $Q = 0$ is ramified.
- At $R = \infty$ we see that $t_{\varphi(R)} = 1/x$ so that $\varphi^* t_{\varphi(Q)} = 1/x^2$ and $\mathrm{ord}_Q(\varphi^* t_{\varphi(Q)}) = \mathrm{ord}_{1/x}(1/x^2) = 2$, so $R = \infty$ is ramified.

Indeed, one may check that 0 and ∞ are the only ramified points of this morphism.

Ramification, IV

Exercise: Compute the ramification index $e_\varphi(P)$ for all points $P \in \mathbb{P}^1$ for the map $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(x) = x^3$.

Exercise: Let $f \in k(x)$ be a nonconstant rational function. Show that a finite point $P \in k$ is ramified for the map $f : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$ if and only if $f'(P) = 0$. Deduce that f has only finitely many ramified points. Under what conditions on f will ∞ be ramified?

Ramification, V

The ramification index defined here is the natural function-field analogue for the ramification index of a prime in a number field.

- Explicitly, if L/K is an extension of number fields with corresponding rings of integers $\mathcal{O}_L$ and $\mathcal{O}_K$, then each prime ideal R of $\mathcal{O}_L$ lies over a unique prime ideal Q of $\mathcal{O}_K$ with $Q = \mathcal{O}_K \cap R$.
- If the prime ideal factorization of $Q\mathcal{O}_R$ has its power of R equal to $R^{e(R)}$, then the ramification index of R is $e(R)$. (This quantity is well defined since $\mathcal{O}_L$ is a Dedekind domain and therefore has unique factorization of ideals as a product of prime ideals.)
- In fact, the ramification index in our situation *literally is* the ramification index for the prime ideal m_P associated to the valuation ring $\mathcal{O}_P$ in the field extension $k(C_1)/\varphi^* k(C_2)$.

The Ramifications of Ramification, I

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 Ramifications of Ramification, II

1. For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.

Example:

- Consider the squaring map $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(x) = x^2$ of degree 2.

The Ramifications of Ramification, II

1. For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.

Example:

- Consider the squaring map $\varphi : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ with $\varphi(x) = x^2$ of degree 2.
- For $Q = 4$ we have $\varphi^{-1}(Q) = \{P_2, P_{-2}\}$ and as we half-computed already, $e_\varphi(P_2) = e_\varphi(P_{-2}) = 1$.
- For $Q' = 0$ we have $\varphi^{-1}(Q') = \{P_0\}$ and as we have already computed, $e_\varphi(P_0) = 2$.
- For $Q'' = \infty$ we have $\varphi^{-1}(Q'') = \{P_\infty\}$ and as we have already computed, $e_\varphi(P_\infty) = 2$.

The Ramifications of Ramification, III

1. For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.

Discussion:

- This result is the analogue of the so-called "*efg*" theorem of number fields: if L/K is an extension of number fields and $f_\varphi(R|Q)$ is the relative degree of the prime R of $\mathcal{O}_L$ lying over the prime Q of $\mathcal{O}_K$, then $\sum_{R|Q} e_i(R) f_i(R) = [L : K]$.

The Ramifications of Ramification, III

1. For all $Q \in C_2$, we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.

Discussion:

- This result is the analogue of the so-called "*efg*" theorem of number fields: if L/K is an extension of number fields and $f_\varphi(R|Q)$ is the relative degree of the prime R of $\mathcal{O}_L$ lying over the prime Q of $\mathcal{O}_K$, then $\sum_{R|Q} e_i(R) f_i(R) = [L : K]$.
- In our situation, the analogous definition of the relative degree would be the vector space dimension $\dim_{\mathcal{O}_P/m_P}(\mathcal{O}_{\mathcal{O}_{\varphi^* P}/m_{\varphi^* P}})$, but since k is algebraically closes both fields $\mathcal{O}_P/m_P$ and $\mathcal{O}_{\varphi^* P}/m_{\varphi^* P}$ are isomorphic to k, so the relative degree is always 1.
- The proof (in both the number field case and our case) follows from examining the prime ideal factorization in the appropriate extension of Dedekind domains.

The Ramifications of Ramification, IV

2. A point $Q \in C_2$ is unramified if and only if $\#\varphi^{-1}(Q) = \deg \varphi$.

Proof:

- By (1) we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.

The Ramifications of Ramification, IV

2. A point $Q \in C_2$ is unramified if and only if $\#\varphi^{-1}(Q) = \deg \varphi$.

Proof:

- By (1) we have $\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi$.
- Since there are $\deg \varphi$ terms in the sum and each term is at least 1, the sum is always at least $\#\varphi^{-1}(Q)$, and it equals $\#\varphi^{-1}(Q)$ if and only if $e_\varphi(P) = 1$ for all $P \in \varphi^{-1}(Q)$.
- So we see $e_\varphi(P) = 1$ for all $P \in \varphi^{-1}(Q)$ if and only if $\#\varphi^{-1}(Q) = \deg \varphi$, as claimed.

The Ramifications of Ramification, V

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.

Remarks:

- This result is the analogue of the statement that there are only finitely many ramified primes in any extension L/K of number fields, which for number fields is typically proven by examining discriminants.

The Ramifications of Ramification, V

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.

Remarks:

- This result is the analogue of the statement that there are only finitely many ramified primes in any extension L/K of number fields, which for number fields is typically proven by examining discriminants.
- The idea here is that typically a point $Q \in C_2$ has a total of $\deg_s \varphi$ preimages under φ, with the exceptions occuring when Q is ramified.
- Ramification corresponds to the situation where these preimages "collide" and yield fewer preimage points than expected (and the number of such collisions is measured by the ramification index).

The Ramifications of Ramification, VI

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.

Proof (second part):

- If φ is separable, the result follows immediately from the first part and (2), since $\deg_s \varphi = \deg \varphi$: so for all but finitely many Q we see that Q is unramified.

The Ramifications of Ramification, VI

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.

Proof (second part):

- If φ is separable, the result follows immediately from the first part and (2), since $\deg_s \varphi = \deg \varphi$: so for all but finitely many Q we see that Q is unramified.

Exercise: Suppose k is algebraically closed, $\operatorname{char} k = p$. Consider the Frobenius morphism $\mathrm{Frob} : \mathbb{P}^1(k) \to \mathbb{P}^1(k)$ with $\mathrm{Frob}(x) = x^p$.

a. Verify that $\#\mathrm{Frob}^{-1}(Q) = 1$ for all $Q \in \mathbb{P}^1$, and show that Frob is ramified at every point.

b. Deduce that the hypothesis that φ be separable in (3) above is necessary to ensure there are finitely many ramified points.

The Ramifications of Ramification, VII

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 $e_{\psi\circ\varphi}(P) = e_\varphi(P)e_\psi(\varphi(P))$.

Commentary:

- This result is the analogue of the fact that the ramification index is multiplicative in towers of number fields.

The Ramifications of Ramification, VII

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 $e_{\psi\circ\varphi}(P) = e_\varphi(P)e_\psi(\varphi(P))$.

Commentary:

- This result is the analogue of the fact that the ramification index is multiplicative in towers of number fields.

Proof (sketch):

- Applying φ changes the local order of vanishing by a factor of $e_\varphi(P)$, while applying ψ changes the local order of vanishing by a factor of $e_\psi(\varphi(P))$.
- Thus, the composition changes the local order of vanishing by the product of these two factors.

Summary

We used the invariant differential to show curves with a Weierstrass equation have genus 1.

We outlined the proof of Riemann-Roch.

We introduced ramification and established some properties of ramification.

Next lecture: Morphisms on divisors and differentials, Riemann-Hurwitz, isogenies.