Math 7359 (Elliptic Curves and Modular Forms)

Lecture #11 of 24 $\sim$ October 16, 2023

Differentials

- Elliptic Curves via Riemann-Roch (leftovers)
- Differentials on Curves

Recall, I

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 $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$.

Proposition (Corollaries of Riemann-Roch)

Let C/k be an algebraic curve.

1. *For any divisor A with $\deg(A) \geq 0$, we have $\deg(A) - g + 1 \leq \ell(A) \leq \deg(A) + 1$.*
2. *For $C \in \mathcal{C}$ we have $\ell(C) = g$ and $\deg(C) = 2g - 2$.*
3. *If $\deg(A) \geq 2g - 2$, then $\ell(A) = \deg(A) - g + 1$ except when $A \in \mathcal{C}$ (in which case $\ell(A) = g$).*
4. *The genus g is unique, as is the equivalence class $\mathcal{C}$.*

Recall, II

Theorem (Genus-1 Curves)

Suppose C is a smooth curve of genus 1 defined over the field F that has a rational point $P \in F$. Then there exist $x, y \in F(C)$ with $v_P(x) = 2$ and $v_P(y) = 3$ such that $F(C) = F(x, y)$ and $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for some $a_1, a_2, a_3, a_4, a_6 \in F$.

Definition (Elliptic Curves, Properly)

Let F be a field. An <u>elliptic curve</u> E over F is a smooth projective curve defined over F with genus 1 that has an F-rational point O.

Elliptic Curves But Properly, V

Theorem (The Group Law, Again, Continued)

Let F be a field and E be an elliptic curve defined over F with an F-rational point O.

5. *The group law defines morphisms $+ : E \times E \to E$ mapping $(P, Q) \mapsto P + Q$ and $- : E \to E$ mapping $P \mapsto -P$.*
6. *For any divisor $D \in \mathrm{Div}(E)$, D is principal if and only if $\deg(D) = 0$ and the formal sum representing D evaluates to O when viewed as a sum of points using the group law.*

Elliptic Curves But Properly, X

5. The group law defines morphisms $+ : E \times E \to E$ mapping $(P, Q) \mapsto P + Q$ and $- : E \to E$ mapping $P \mapsto -P$.

Proof (outline):

- The actual details involve various special cases, but it suffices to show that the maps are rational, since rational maps from a smooth curve to a variety are automatically morphisms.
- But the addition map and the additive-inverse map are both rational on almost all points, as we have already seen via the explicit formulas.
- The only possible exceptions involve adding a point to itself or a point to O.
- One may check explicitly in these cases that the maps still yield morphisms by rearranging the formulas using projective equivalences like the ones we did a few weeks ago.

Elliptic Curves But Properly, XI

6. For any divisor $D \in \mathrm{Div}(E)$, D is principal if and only if $\deg(D) = 0$ and the formal sum representing D evaluates to O when viewed as a sum of points using the group law.

Proof:

- As we have previously noted, the degree of any principal divisor is 0, so certainly we must have $\deg(D) = 0$.
- Now if $D \in \mathrm{Div}^0(E)$ is $D = \sum_P n_P[P]$ we have $D \sim 0$ if and only if $\sigma(D) = O$.
- But $\sigma(D) = \sigma(\sum_P n_P[P]) = \sum_P n_P \sigma([P]) = \sum_P n_P(P - O) = \sum_P n_P P$ by definition of σ and the equivalence of the group operations in (4).
- So we see $\sigma(D) = O$ if and only if $\sum_P n_P P = O$ when viewed as a sum of points using the group law.

Elliptic Curves But Properly, XII

Some of these results can be packaged together via an exact sequence:

Exercise: Show that we have an exact sequence

$$1 \to k^* \to k(E)^* \xrightarrow{\mathrm{div}} \mathrm{Div}^0(E) \xrightarrow{(6)} E \to 0$$

where div represents the divisor map $f \mapsto \mathrm{div}(f)$ and (6) represents the map discussed in (6) that takes a divisor $\sum_P n_P[P]$ and evaluates it as a sum of points on E.

Differentials, I

We would now like to establish the converse of our theorem above: namely, that every smooth projective curve with a Weierstrass equation $Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$ is actually an elliptic curve.

- Since $[0 : 1 : 0]$ (the affine point at ∞) is always a rational point on this curve, we need only show it has genus 1.
- In order to do this, we need to discuss differentials, since they allow us to understand the genus.

Differentials, II

So, let's get right to it:

Definition

Let C/k be a (smooth projective) curve. The space $\Omega(C)$ of meromorphic differential 1-forms on C is the k-vector space consisting of symbols of the form 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 $a \in k$.*

There is a more general notion of differential form defined using the notion of a derivation from a commutative ring R to an R-module M. We won't bother with this.

Differentials, III

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 $a \in k$.

- Although $\Omega(C)$ contains differentials of the form df for all $f \in k(C)$, and may therefore appear to be very large, in fact the relations impose all of the familiar rules of calculus.

Differentials, III

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 $a \in k$.

- Although $\Omega(C)$ contains differentials of the form df for all $f \in k(C)$, and may therefore appear to be very large, in fact the relations impose all of the familiar rules of calculus.
- Exercise: Show that (1)-(3) also imply the power rule $d(x^n) = nx^{n-1}dx$ and the quotient rule $d(\frac{x}{y}) = \frac{x\,dy - y\,dx}{y^2}$.
- Exercise: Suppose C/k is a curve and $x_1, x_2, \ldots, x_n \in k(C)$. For any rational function $f \in k(x_1, \ldots, x_n)$, show the "chain rule": that $df = f_{x_1}\,dx_1 + \cdots + f_{x_n}\,dx_n$, where f_{x_i} denotes the usual partial derivative. [Hint: First show the result for polynomials f, then use the quotient rule.]

Differentials, IV

As a corollary of the above exercises, we see immediately that if the function field $k(C)$ is generated (as a field extension) by $x_1, \dots, x_n$ then $\Omega(C)$ is spanned by dx_1, dx_2, ... , dx_n as a $k(C)$-vector space.

Differentials, IV

As a corollary of the above exercises, we see immediately that if the function field $k(C)$ is generated (as a field extension) by $x_1, \dots, x_n$ then $\Omega(C)$ is spanned by dx_1, dx_2, ... , dx_n as a $k(C)$-vector space.

Example:

- For $C = \mathbb{P}^1$, we have $k(C) = k(x)$ for $x = X/Y$.
- Since x generates the function field by itself we see that $\Omega(C)$ is spanned by dx.
- In fact, $\{dx\}$ is a basis, since there are no additional relations arising in the definition of $\Omega(C)$.

Differentials, V

Example:

- Let p be a prime. For $C = \mathbb{P}^1$ over a field of characteristic not equal to p, we know that $\{dx\}$ is a basis of $\Omega(C)$.
- Then for $f = x^p$, since $df = px^{p-1}dx$ is a nonzero scalar multiple of dx, we see that $\{df\}$ is also a basis of $\Omega(C)$.
- On the other hand, over a field of characteristic p, we have $df = px^{p-1}\,dx = 0$, and so $\{df\}$ is not a basis of $\Omega(C)$.

Differentials, V

Example:

- Let p be a prime. For $C = \mathbb{P}^1$ over a field of characteristic not equal to p, we know that $\{dx\}$ is a basis of $\Omega(C)$.
- Then for $f = x^p$, since $df = px^{p-1}dx$ is a nonzero scalar multiple of dx, we see that $\{df\}$ is also a basis of $\Omega(C)$.
- On the other hand, over a field of characteristic p, we have $df = px^{p-1}\,dx = 0$, and so $\{df\}$ is not a basis of $\Omega(C)$.

Example:

- For $C = V(Y^2Z - X^3 - XZ^2)$ with $x = X/Z$ and $y = Y/Z$, we have $k(C) = k(x, y)$, so $\Omega(C)$ is spanned by dx and dy.
- But since $y^2 = x^3 + x$, taking differentials yields a linear dependence $2y\,dy = (3x^2 + 1)\,dx$. Thus in fact either dx or dy suffices to span $\Omega(C)$.

Differentials, VI

More generally, one may show similarly that $\Omega(C)$ is always a 1-dimensional $k(C)$-vector space for any curve C.

- In general, dx generates $\Omega(C)$ if and only if $k(C)/k(x)$ is a separable extension of finite degree.

Differentials, VI

More generally, one may show similarly that $\Omega(C)$ is always a 1-dimensional $k(C)$-vector space for any curve C.

- In general, dx generates $\Omega(C)$ if and only if $k(C)/k(x)$ is a separable extension of finite degree.
- The second example shows that separability is necessary, since if k has characteristic p then $k(x)/k(x^p)$ is not separable, and as we saw, in that situation dx^p does not span $\Omega(C)$.

Our goal now is to show that we may do calculations with differentials that mirror those for rational functions. First, we will give a well-defined notion of the order of a differential ω at a point P, and then we use it to attach a divisor to a differential.

Properties of Differentials, I

Proposition (Properties of Differentials)

Let C/k be a curve, let ω be a differential in $\Omega(C)$, and let P be a point of C with a local uniformizer t. Then the following hold:

1. *There exists a unique rational function $f \in k(C)$ such that $\omega = f\,dt$. (Since f is unique, we may think of it as the "quotient" ω/dt.)*
2. *If $f \in k(C)$ is defined at P, then df/dt is also defined at P.*
3. *If t' is another local uniformizer at P, then $\mathrm{ord}_P(\omega/dt) = \mathrm{ord}_P(\omega/dt')$. We may therefore define $\mathrm{ord}_P(\omega)$ to be the value $\mathrm{ord}_P(\omega/dt)$ for any local uniformizer t.*
4. *Let $x \in k(C)^\times$ with $x(P) = 0$. Then $\mathrm{ord}_P(dx) = \mathrm{ord}_P(x) - 1$ except when the characteristic of k divides $\mathrm{ord}_P(x)$, in which case we have $\mathrm{ord}_P(f\,dx) \geq \mathrm{ord}_P(x)$.*

Properties of Differentials, II

Proposition (Properties of Differentials, continued)

Let C/k be a curve, let ω be a differential in $\Omega(C)$, and let P be a point of C with a local uniformizer t. Then the following hold:

5. *For all but finitely many P, we have $\mathrm{ord}_P(\omega) = 0$.*
6. *For any differential ω, its divisor $\mathrm{div}(\omega) = \sum_P \mathrm{ord}_P(\omega)\, P$ is well defined, and for any other differential ω_1 we have $\mathrm{div}(\omega) \sim \mathrm{div}(\omega_1)$. We define the canonical class $\mathcal{C}$ to be the resulting divisor class of $\mathrm{div}(\omega)$ in $\mathrm{Pic}(C)$.*

A differential ω is holomorphic if $\mathrm{div}(\omega) \geq 0$: equivalently, when $\mathrm{ord}_P(\omega) \geq 0$ for all P, which is to say, when ω has no poles.

7. *The holomorphic differentials form a finite-dimensional vector space, whose dimension is defined to be g, the genus of C.*

Properties of Differentials, III

1. There exists a unique rational function $f \in k(C)$ such that $\omega = f\,dt$. (Since f is unique, we may think of it as the "quotient" ω/dt.)

Proof:

- First, since t is a local uniformizer, the extension $k(C)/k(t)$ has finite degree and is separable.
- Hence by the discussion above, we see that $\{dt\}$ spans $\Omega(C)$ as a $k(C)$-vector space.
- This means so there exists a unique rational function $f \in k(C)$ such that $\omega = f\,dt$.

Properties of Differentials, IV

2. If $f \in k(C)$ is defined at P, then df/dt is also defined at P.

- The most direct proof of this fact follows by working with local Laurent expansions near P. We will not need to (or really, we will not want to) do this explicitly, so here is an outline of the idea.

Properties of Differentials, IV

2. If $f \in k(C)$ is defined at P, then df/dt is also defined at P.

- The most direct proof of this fact follows by working with local Laurent expansions near P. We will not need to (or really, we will not want to) do this explicitly, so here is an outline of the idea.
- One may expand functions in $\mathcal{O}_P$ as infinite formal power series in the formal Laurent series ring of $k((t))$, and the resulting map $D : k(C) \to k((t))$ is a derivation.
- Elements in the local ring $\mathcal{O}_P$ (i.e., functions f defined at P) have images lying in the formal power series ring $k[[t]]$, and for such elements, one may show that the term-by-term power series derivative f' yields the rational function with $df = f'\,dt$. Since the term-by-term derivative f' lies in $k[[t]]$, it is defined at P.

Properties of Differentials, V

3. If t' is another local uniformizer at P, then $\mathrm{ord}_P(\omega/dt) = \mathrm{ord}_P(\omega/dt')$.

Proof:

- Taking $f = t'$ in (2) shows that $dt'/dt = g$ is defined at P, and interchanging t and t' shows that $dt'/dt = 1/g$ is also defined at P.

Properties of Differentials, V

3. If t' is another local uniformizer at P, then $\operatorname{ord}_P(\omega/dt) = \operatorname{ord}_P(\omega/dt')$.

Proof:

- Taking $f = t'$ in (2) shows that $dt'/dt = g$ is defined at P, and interchanging t and t' shows that $dt'/dt = 1/g$ is also defined at P.
- Therefore, we have $\operatorname{ord}_P(g) \geq 0$ and $\operatorname{ord}_P(1/g) \geq 0$ whence $\operatorname{ord}_P(g) = 0$.
- Then we immediately have $\operatorname{ord}_P(\omega/dt) = \operatorname{ord}_P(\omega/dt' \cdot dt'/dt) = \operatorname{ord}_P(\omega/dt') + \operatorname{ord}_P(g) = \operatorname{ord}_P(\omega/dt')$.

We now define $\operatorname{ord}_P(\omega)$ to be the value $\operatorname{ord}_P(\omega/dt)$ for *any* local uniformizer t.

Properties of Differentials, VI

4. Let $x \in k(C)^{\times}$ with $x(P) = 0$. Then $\mathrm{ord}_P(dx) = \mathrm{ord}_P(x) - 1$ except when the characteristic of k divides $\mathrm{ord}_P(x)$, in which case we have $\mathrm{ord}_P(f\, dx) \geq \mathrm{ord}_P(x)$.

Proof (part 1):

- Intuitively, the idea of this result is the extremely reasonable notion that taking the derivative of a function lowers its order of vanishing by 1, except in situations where the function is something times a pth power in characteristic p.

Properties of Differentials, VI

4. Let $x \in k(C)^\times$ with $x(P) = 0$. Then $\mathrm{ord}_P(dx) = \mathrm{ord}_P(x) - 1$ except when the characteristic of k divides $\mathrm{ord}_P(x)$, in which case we have $\mathrm{ord}_P(f\,dx) \geq \mathrm{ord}_P(x)$.

Proof (part 1):

- Intuitively, the idea of this result is the extremely reasonable notion that taking the derivative of a function lowers its order of vanishing by 1, except in situations where the function is something times a pth power in characteristic p.
- Since x is not zero we may write $x = ut^n$ for some u of order 0, and $n = \mathrm{ord}_P(x)$. Then $dx = unt^{n-1}\,dt + (du/dt)t^n\,dt$ by the chain rule.
- From (2) we know that du/dt is defined at P so $\mathrm{ord}_P(du/dt) \geq 0$.
- Now we look at the orders of the terms unt^{n-1} and $(du/dt)t^n$.

Properties of Differentials, VII

4. Let $x \in k(C)^\times$ with $x(P) = 0$. Then $\mathrm{ord}_P(dx) = \mathrm{ord}_P(x) - 1$ except when the characteristic of k divides $\mathrm{ord}_P(x)$, in which case we have $\mathrm{ord}_P(f\,dx) \geq \mathrm{ord}_P(x)$.

Proof (part 2):

- We have $x = ut^n$ for some u of order 0, and $n = \mathrm{ord}_P(x)$.
- Then $dx = unt^{n-1}\,dt + (du/dt)t^n\,dt$ and $\mathrm{ord}_P(du/dt) \geq 0$.
- If the characteristic of k divides n, then $n = 0$ (in k), so $dx = (du/dt)t^n\,dt$. Then $\mathrm{ord}_P(dx) = \mathrm{ord}_P(dx/dt) = \mathrm{ord}_P(du/dt) + n \geq \mathrm{ord}_P(x)$ as desired.

Properties of Differentials, VII

4. Let $x \in k(C)^\times$ with $x(P) = 0$. Then $\mathrm{ord}_P(dx) = \mathrm{ord}_P(x) - 1$ except when the characteristic of k divides $\mathrm{ord}_P(x)$, in which case we have $\mathrm{ord}_P(f\,dx) \geq \mathrm{ord}_P(x)$.

Proof (part 2):

- We have $x = ut^n$ for some u of order 0, and $n = \mathrm{ord}_P(x)$.
- Then $dx = unt^{n-1}\,dt + (du/dt)t^n\,dt$ and $\mathrm{ord}_P(du/dt) \geq 0$.
- If the characteristic of k divides n, then $n = 0$ (in k), so $dx = (du/dt)t^n\,dt$. Then $\mathrm{ord}_P(dx) = \mathrm{ord}_P(dx/dt) = \mathrm{ord}_P(du/dt) + n \geq \mathrm{ord}_P(x)$ as desired.
- Otherwise, if the characteristic does not divide n, then $n \neq 0$ in k so $\mathrm{ord}_P(unt^{n-1}) = n - 1$ while the order of the second term $(du/dt)t^n$ is at least n (as just calculated above).
- So since ord_P is a discrete valuation, the order of the sum $unt^{n-1} + (du/dt)t^n$ is $n - 1 = \mathrm{ord}_P(x) - 1$, as desired.

Properties of Differentials, VIII

5. For all but finitely many P, we have $\mathrm{ord}_P(\omega) = 0$.

Proof (part 1):

- Pick x to be a local uniformizer at an arbitrary point of C: then by (1) we may write $\omega = f\,dx$.

Properties of Differentials, VIII

5. For all but finitely many P, we have $\operatorname{ord}_P(\omega) = 0$.

Proof (part 1):

- Pick x to be a local uniformizer at an arbitrary point of C: then by (1) we may write $\omega = f\, dx$.
- Now, f has finitely many zeroes and poles, as noted in our discussion of divisors of functions.
- Additionally, as we will discuss in more detail later, there are only finitely many points at which $x - x(P)$ fails to be a local uniformizer at P. (These are the points at which x is ramified, when thought of as a map $x : C \to \mathbb{P}^1$.)
- So there are only finitely many points P where f has a zero or pole, or where $x - x(P)$ fails to be a local uniformizer.

Properties of Differentials, IX

5. For all but finitely many P, we have $\mathrm{ord}_P(\omega) = 0$.

Proof (part 2):

- So there are only finitely many points P where f has a zero or pole, or where $x - x(P)$ fails to be a local uniformizer.
- Let Q be any other point.

Properties of Differentials, IX

5. For all but finitely many P, we have $\operatorname{ord}_P(\omega) = 0$.

Proof (part 2):

- So there are only finitely many points P where f has a zero or pole, or where $x - x(P)$ fails to be a local uniformizer.
- Let Q be any other point.
- Then $x - x(Q)$ is a local uniformizer, so we have $\operatorname{ord}_Q(dx) = \operatorname{ord}_Q(d(x - x(Q)) = 1 - 1 = 0$ by (4).
- Hence $\operatorname{ord}_Q(\omega) = \operatorname{ord}_Q(f\,dx) = \operatorname{ord}_Q(f) + \operatorname{ord}_Q(dx) = 0 + 0 = 0$ because f is defined and does not vanish at Q.
- This applies for all but finitely many points Q, so we are done.

Properties of Differentials, X

Now, (5) tells us that for any differential ω, its divisor $\mathrm{div}(\omega) = \sum_P \mathrm{ord}_P(\omega)\, P$ is well defined.

6. Define $\mathrm{div}(\omega) = \sum_P \mathrm{ord}_P(\omega)\, P$. Then for any other differential ω_1 we have $\mathrm{div}(\omega) \sim \mathrm{div}(\omega_1)$.

Proof:

Properties of Differentials, X

Now, (5) tells us that for any differential ω, its divisor $\mathrm{div}(\omega) = \sum_P \mathrm{ord}_P(\omega)\, P$ is well defined.

6. Define $\mathrm{div}(\omega) = \sum_P \mathrm{ord}_P(\omega)\, P$. Then for any other differential ω_1 we have $\mathrm{div}(\omega) \sim \mathrm{div}(\omega_1)$.

Proof:

- Suppose ω_1 is any other differential.
- By (1) there exists $f \in k(C)$ such that $\omega/\omega_1 = f$: thus $\mathrm{div}(\omega) - \mathrm{div}(\omega_1) = \mathrm{div}(f)$ which means by definition that $\mathrm{div}(\omega) \sim \mathrm{div}(\omega_1)$.
- The well-definedness of the canonical class is then immediate from the equivalence.

Properties of Differentials, XI

The result (6) says that the divisors of any two differentials differ by the divisor of a rational function, meaning that their divisor classes are the same.

Definition

We define the *canonical class* $\mathcal{C}$ *to be the resulting divisor class of* $\mathrm{div}(\omega)$ *in* $\mathrm{Pic}(C)$*.*

The differential analogue of effective divisors are holomorphic differentials:

Definition

A differential ω *is* *holomorphic* *if* $\mathrm{div}(\omega) \geq 0$*: equivalently, when* $\mathrm{ord}_P(\omega) \geq 0$ *for all* P*, which is to say, when* ω *has no poles.*

Properties of Differentials, XII

7. The holomorphic differentials form a finite-dimensional vector space, whose dimension is defined to be g, the genus of C.

Proof:

- Writing $\omega = f\,dt$ we see that ω is holomorphic if and only if $\mathrm{div}(f) \geq -\mathrm{div}(\omega)$.

Properties of Differentials, XII

7. The holomorphic differentials form a finite-dimensional vector space, whose dimension is defined to be g, the genus of C.

Proof:

- Writing $\omega = f\,dt$ we see that ω is holomorphic if and only if $\mathrm{div}(f) \geq -\mathrm{div}(\omega)$.
- Therefore, the map $\omega \mapsto \omega/dt$ is an isomorphism of the space of holomorphic differentials with the Riemann-Roch space $L(\mathrm{div}(\omega))$, whose dimension $l(\mathrm{div}(\omega)) = l(\mathcal{C})$ is finite, as follows from our properties of Riemann-Roch spaces.

The Genius of Genus, I

Of course, the real point of (6) and (7) is to give a proper definition of the canonical class and the genus of a curve that appear in the statement of the Riemann-Roch theorem.

- We can also give some explanation of why the genus g, defined here as the dimension of the space of holomorphic differentials C, corresponds to the topological genus.
- The idea is that when we are working over $k = \mathbb{C}$, then viewing C as a (compact, connected) Riemann surface, we may integrate a holomorphic differential along a path inside C.
- Let $\Omega(0)$ denote the space of holomorphic differentials.

The Genius of Genus, II

- By standard results from complex analysis, if two paths are homotopic then integrating any differential along the two paths yields the same value.
- Since the set of paths up to homotopy is the first homology group $H_1(C)$, which is a free abelian group of rank g (the topological genus of C), we obtain a pairing between $H_1(C)$ and $\Omega(0)$ given by $\langle C, \omega \rangle = \int_C \omega$.
- One then shows that this is a perfect pairing, and so these vector spaces are isomorphic.
- Essentially, the idea is that we can obtain independent holomorphic differentials by integrating around independent non-contractible paths on C.
- We remark that all of this is just a rephrasing of Poincaré duality applied to the de Rham cohomology groups of C, considered as a 2-dimensional manifold.

Examples of Differentials, I

<u>Example</u>: On $C = \mathbb{P}^1$ with $x = X/Y$ as usual, find $\mathrm{div}(dx)$.

Examples of Differentials, I

<u>Example</u>: On $C = \mathbb{P}^1$ with $x = X/Y$ as usual, find $\operatorname{div}(dx)$.

- First, since $k(C) = k(x)$, so rather trivially $k(C)/k(x)$ is separable and of finite degree, we see $\Omega(C)$ is spanned by dx.
- Thus, every differential on C is of the form $\omega = f\,dx$ for some rational function $f \in k(x)$, so $\operatorname{div}(\omega) = \operatorname{div}(f) + \operatorname{div}(dx)$.

Examples of Differentials, I

Example: On $C = \mathbb{P}^1$ with $x = X/Y$ as usual, find $\mathrm{div}(dx)$.

- First, since $k(C) = k(x)$, so rather trivially $k(C)/k(x)$ is separable and of finite degree, we see $\Omega(C)$ is spanned by dx.
- Thus, every differential on C is of the form $\omega = f\,dx$ for some rational function $f \in k(x)$, so $\mathrm{div}(\omega) = \mathrm{div}(f) + \mathrm{div}(dx)$.
- To find $\mathrm{div}(dx)$, first observe that for all $c \in k$ the function $x - c$ is a uniformizer at $[c:1]$, so $\mathrm{ord}_{[c:1]}(dx) = \mathrm{ord}_{[c:1]}(x-c) - 1 = 0$ by our results in (4).
- Also, at the point at infinity $[1:0]$, the function $1/x$ is a uniformizer, so $\mathrm{ord}_{[1:0]}(x) = -1$ and thus $\mathrm{ord}_{[1:0]}(dx) = \mathrm{ord}_{[1:0]}(x) - 1 = -2$, again by (4).
- Therefore, $\mathrm{div}(dx) = -2P_{[1:0]}$.

Examples of Differentials, II

Example: Show that there are no nonzero holomorphic differentials on $C = \mathbb{P}^1$: in other words, that $\mathbb{P}^1$ has genus 0.

Examples of Differentials, II

Example: Show that there are no nonzero holomorphic differentials on $C = \mathbb{P}^1$: in other words, that $\mathbb{P}^1$ has genus 0.

- Now, since $\operatorname{div}(dx) = -2P_{[1:0]}$, the canonical class is the image of $-2P_{[1:0]}$ in $\operatorname{Pic}(C)$.
- In particular, the degree of any differential must be -2. But since the degree of a holomorphic differential is nonnegative, we see immediately that there are no nonzero holomorphic differentials.
- Hence we see that the genus of $\mathbb{P}^1$ is 0 – as it should be, of course, given the results of our earlier calculations for genus-0 curves using Riemann-Roch.

Examples of Differentials, III

Example: On $C = V(Y^2Z - X^3 - XZ^2)$ with $x = X/Z$ and $y = Y/Z$ as usual, show that dx/y is a nonvanishing holomorphic differential, when the characteristic of k is not 2.

Examples of Differentials, III

<u>Example</u>: On $C = V(Y^2Z - X^3 - XZ^2)$ with $x = X/Z$ and $y = Y/Z$ as usual, show that dx/y is a nonvanishing holomorphic differential, when the characteristic of k is not 2.

- We have previously shown $\mathrm{div}(y) = P_{[0:0:1]} + P_{[i:0:1]} + P_{[-i:0:1]} - 3P_{[0:1:0]}$.
- To find $\mathrm{div}(dx)$ we need to compute its zeroes and poles.
- Recall that when $g(P) = 0$ property (4) says $\mathrm{ord}_P(dg) = \mathrm{ord}_P(g) - 1$ when $\mathrm{char}(k) \nmid \mathrm{ord}_P(g)$.
- Since $dx = d(x - c)$ for any $c \in k$ we can compute the zero orders by looking for points P where $x - x(P) = 0$.
- Since $x - x(P)$ is only zero at $x = 0, i, -i$, we can start with computing $\mathrm{div}(x)$.

Examples of Differentials, IV

Example: On $C = V(Y^2Z - X^3 - XZ^2)$ with $x = X/Z$ and $y = Y/Z$ as usual, show that dx/y is a nonvanishing holomorphic differential, when the characteristic of k is not 2.

- Since x is only zero at $[0:0:1]$ and since y is a local uniformizer there, to check the zero order we observe that $x/y^2 = XZ/Y^2 = Z^2/(X^2+Z^2) = 1$ is defined and nonzero, so $\mathrm{ord}_{[0:0:1]} x = 2$. Then since the only pole of x is at $[0:1:0]$ the pole also has order 2, and so $\mathrm{div}(x) = 2P_{[0:0:1]} - 2P_{[0:1:0]}$.

Examples of Differentials, IV

Example: On $C = V(Y^2Z - X^3 - XZ^2)$ with $x = X/Z$ and $y = Y/Z$ as usual, show that dx/y is a nonvanishing holomorphic differential, when the characteristic of k is not 2.

- Since x is only zero at $[0:0:1]$ and since y is a local uniformizer there, to check the zero order we observe that $x/y^2 = XZ/Y^2 = Z^2/(X^2+Z^2) = 1$ is defined and nonzero, so $\mathrm{ord}_{[0:0:1]}x = 2$. Then since the only pole of x is at $[0:1:0]$ the pole also has order 2, and so $\mathrm{div}(x) = 2P_{[0:0:1]} - 2P_{[0:1:0]}$.
- In the same way we can show that $\mathrm{div}(x-i) = 2P_{[i:0:1]} - 2P_{[0:1:0]}$ and $\mathrm{div}(x+i) = 2P_{[-i:0:1]} - 2P_{[0:1:0]}$.
- Then since $x - x(P)$ is only zero at $x = 0, i, -i$, by property (4) we deduce that the zeroes of dx occur only at $[0:0:1]$, $[-i:0:1]$, and $[i:0:1]$ and the zero order there is $2-1=1$ in each case.

Examples of Differentials, V

Example: On $C = V(Y^2Z - X^3 - XZ^2)$ with $x = X/Z$ and $y = Y/Z$ as usual, show that dx/y is a nonvanishing holomorphic differential, when the characteristic of k is not 2.

- The zeroes of dx occur only at $[0 : 0 : 1]$, $[-i : 0 : 1]$, and $[i : 0 : 1]$, and the zero order there is $2 - 1 = 1$ in each case.

Examples of Differentials, V

Example: On $C = V(Y^2Z - X^3 - XZ^2)$ with $x = X/Z$ and $y = Y/Z$ as usual, show that dx/y is a nonvanishing holomorphic differential, when the characteristic of k is not 2.

- The zeroes of dx occur only at $[0:0:1]$, $[-i:0:1]$, and $[i:0:1]$, and the zero order there is $2-1=1$ in each case.
- Likewise, since the only pole of dx is at $[0:1:0]$, by (4) again we see the pole order is $-2-1=-3$. (Here is where we need the fact that the characteristic is not 2.)
- Putting all of this together shows that $\mathrm{div}(dx) = P_{[0:0:1]} + P_{[i:0:1]} + P_{[-i:0:1]} - 3P_{[0:1:0]}$. But this is precisely $\mathrm{div}(y)$, and so that means $\mathrm{div}(dx/y) = 0$ whence dx/y is holomorphic and also nonvanishing.

Differentials on Elliptic Curves, I

Let us now generalize the last example to complete the proof that smooth projective curves of genus 1 having a rational point (per our highbrow definition of elliptic curves) are the same as nonsingular cubic curves in Weierstrass form (per our original definition).

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

1. The differential $\omega = \dfrac{dx}{2y + a_1 x + a_3} = -\dfrac{dy}{3x^2 + 2a_2 x + a_4}$ is holomorphic and nonvanishing on C.

Proof (part 1):

- Let $f = y^2 + a_1 xy + a_3 y - (x^3 + a_2 x^2 + a_4 x + a_6)$: then by the chain rule we see that $\dfrac{dx}{f_y(x,y)} = -\dfrac{dy}{f_x(x,y)}$, showing that the two expressions are equal.

Differentials on Elliptic Curves, III

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.

Proof (part 1):

- Let $f = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$: then by the chain rule we see that $\dfrac{dx}{f_y(x,y)} = -\dfrac{dy}{f_x(x,y)}$, showing that the two expressions are equal.
- For any finite point $P = (x_0, y_0)$ we also have $\omega = \dfrac{d(x - x_0)}{f_y(x,y)} = -\dfrac{d(y - y_0)}{f_x(x,y)}$ since translating by a constant does not affect differentials.
- In particular we see that P cannot be a pole of ω since this would require $f_x(P) = f_y(P) = 0$, but that cannot occur because C is smooth at P. So ω could only possibly have a pole at ∞.

Differentials on Elliptic Curves, IV

1. The differential $\omega = \dfrac{dx}{2y + a_1 x + a_3} = -\dfrac{dy}{3x^2 + 2a_2 x + a_4}$ is holomorphic and nonvanishing on C.

Proof (part 2):

- For zeroes of ω we observe that the map $\varphi : C \to \mathbb{P}^1$ with $[X : Y : Z] \mapsto [X : Z]$ has degree 2.
- Therefore we have $\mathrm{ord}_P(x - x_0) \leq 2$ with equality if and only if $f(x_0, y)$ has a double root in y at $y = y_0$, which occurs if and only if $f_y(x_0, y_0) = 0$.

Differentials on Elliptic Curves, IV

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.

Proof (part 2):

- For zeroes of ω we observe that the map $\varphi : C \to \mathbb{P}^1$ with $[X : Y : Z] \mapsto [X : Z]$ has degree 2.
- Therefore we have $\mathrm{ord}_P(x - x_0) \leq 2$ with equality if and only if $f(x_0, y)$ has a double root in y at $y = y_0$, which occurs if and only if $f_y(x_0, y_0) = 0$.
- Therefore by property (4) we see that $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(dx) - \mathrm{ord}_P(f_y) = \mathrm{ord}_P(x - x_0) - \mathrm{ord}_P(f_y) - 1 = 0$ in both the situation when $\mathrm{ord}_P(x - x_0) = 1$ and in the situation when $\mathrm{ord}_P(x - x_0) = 2$.
- So ω has order 0 at all finite points. Now for ∞.

Differentials on Elliptic Curves, V

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.

Proof (part 3):

- Let t be a uniformizer at ∞: then because $\mathrm{ord}_\infty(x) = -2$ and $\mathrm{ord}_\infty(y) = -3$ we have $x = t^{-2}u$ and $y = t^{-3}w$ for some $u, w \in k(C)$ that are defined and nonzero at ∞.

Differentials on Elliptic Curves, V

1. The differential $\omega = \dfrac{dx}{2y + a_1 x + a_3} = -\dfrac{dy}{3x^2 + 2a_2 x + a_4}$ is holomorphic and nonvanishing on C.

Proof (part 3):

- Let t be a uniformizer at ∞: then because $\mathrm{ord}_\infty(x) = -2$ and $\mathrm{ord}_\infty(y) = -3$ we have $x = t^{-2}u$ and $y = t^{-3}w$ for some $u, w \in k(C)$ that are defined and nonzero at ∞.
- Then
$$\frac{\omega}{dt} = \frac{dx/dt}{f_y(x,y)} = \frac{-2t^{-3}u + t^{-2}(du/dt)}{2t^{-3}w + a_1 t^{-2}u + a_3}\, dt$$
$$= \frac{-2u + t(du/dt)}{2w + a_1 tu + a_3 t^3}\, dt.$$
- When the characteristic of k is not equal to 2, we can then evaluate this last function at ∞ (note that $t = 0$ at ∞) to obtain $-u(\infty)/w(\infty)$ which is defined and nonzero.

Differentials on Elliptic Curves, VI

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.

Exercise: When the characteristic of k does equal 2, show that the equivalent formula $\omega = -\dfrac{dy}{f_x(x, y)}$ evaluates to a quantity that is defined and nonzero at ∞.

Proof (part 4):

Differentials on Elliptic Curves, VI

1. The differential $\omega = \dfrac{dx}{2y + a_1 x + a_3} = -\dfrac{dy}{3x^2 + 2a_2 x + a_4}$ is holomorphic and nonvanishing on C.

Exercise: When the characteristic of k does equal 2, show that the equivalent formula $\omega = -\dfrac{dy}{f_x(x, y)}$ evaluates to a quantity that is defined and nonzero at ∞.

Proof (part 4):

- By the calculation on the last slide (when $\mathrm{char}(k) \neq 2$) and the exercise above (when $\mathrm{char}(k) \neq 3$) we deduce that in all cases, $\mathrm{ord}_\infty(\omega) = 0$.
- Putting everything together, we obtain $\mathrm{div}(\omega) = 0$, whence ω is holomorphic and nonvanishing as claimed.

Differentials on Elliptic Curves, VII

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, VII

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, VIII

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, IX

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, IX

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, X

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, X

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.
- 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, XI

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, XI

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.
- 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.

Wrap-Up

Now that we have defined differentials, the canonical class, and the genus of C, we can return to our discussion of Riemann-Roch.

- Since it won't take too long, I will start next lecture with an outline of the proof of Riemann-Roch.
- Then we will talk about how morphisms interact with divisors and differentials. This will lead us naturally into our next main topic: isogenies, which are morphisms from one elliptic curve to another.

Summary

We defined the space of differentials on an algebraic curve C and established some of their basic properties and gave some examples.

We constructed the invariant differential on an elliptic curve and used it to show curves with a Weierstrass equation have genus 1.

Next lecture: Riemann-Roch proof outline, interactions of morphisms with divisors and differentials