Math 7359 (Elliptic Curves and Modular Forms)

Lecture #10 of 24 ∼ October 12, 2023

Riemann-Roch and Applications

- $L(D)$ and $l(D)$
- Riemann-Roch and Consequences
- Elliptic Curves via Riemann-Roch

Recall

Definition

If a divisor $D = \sum_P n_P P$ *on a curve* C/k *has* $n_P \geq 0$ *at all points* P*, we say* D *is* *effective* *and we write* $D \geq 0$*. We extend this notion to a partial ordering on divisors by writing* $D_1 \leq D_2$ *if and only if* $D_2 - D_1$ *is effective.*

Definition

If D *is a divisor on a curve* C/k*, the* *Riemann-Roch space* *associated to* D *is the set*
$L(D) = \{\alpha \in k(C)^\times : \mathrm{div}(\alpha) \geq -D\} \cup \{0\}.$

Riemann-Roch Dimensions, I

As the last examples suggest, the dimension of the Riemann-Roch space $L(D)$ carries important information:

Definition

If D is a divisor on a curve C/k, we define $\ell(D) = \dim_k L(D)$.

Examples: From our earlier calculations,

- For $C = \mathbb{A}^1(\mathbb{C})$ we have $l(P_0) = 2$, $l(3P_\infty) = 4$, and $l(-P_0) = 0$.
- For $C = \mathbb{A}^1(\mathbb{C})$ we have $l_{\mathbb{C}}(P_\infty - P_i) = 1$ and $l_{\mathbb{C}}(2P_\infty - P_i - P_{-i}) = 1$.
- For an arbitrary C, we have $\ell(0) = 1$, since $L(0) = k$.

Riemann-Roch Dimensions, II

Let's establish some properties of $l(D)$:

Proposition (Properties of $l(D)$)

Let C/k be a curve and D be a divisor of C. Then

1. *If $D_1 \leq D_2$, then $\ell(D_1) \leq \ell(D_2)$.*
2. *If $D_1 \sim D_2$, then $L(D_1) \cong L(D_2)$ and so $\ell(D_1) = \ell(D_2)$.*
3. *If $\deg(D) \leq 0$, then $L(D) = \{0\}$ and $l(D) = 0$ except when $D = \mathrm{div}(\alpha)$ is principal, in which case $L(D) = \mathrm{span}(\alpha)$ and $l(D) = 1$.*
4. *If D_1 and D_2 are divisors with $D_1 \leq D_2$, then $\dim_k(L(D_2)/L(D_1)) \leq \deg(D_2) - \deg(D_1)$.*
5. *For any effective divisor D, we have $\ell(D) \leq \deg(D) + 1$. In fact, this inequality holds for any divisor D of degree ≥ 0.*
6. *For any divisor D, the quantity $\ell(D)$ is finite.*

Riemann-Roch Dimensions, III

1. If $D_1 \leq D_2$, then $\ell(D_1) \leq \ell(D_2)$.

Proof:

- This follows immediately from the definition, since $D_1 \leq D_2$ clearly implies that $L(D_1)$ is a subspace of $L(D_2)$.

Riemann-Roch Dimensions, III

1. If $D_1 \le D_2$, then $\ell(D_1) \le \ell(D_2)$.

Proof:

- This follows immediately from the definition, since $D_1 \le D_2$ clearly implies that $L(D_1)$ is a subspace of $L(D_2)$.

---

2. If $D_1 \sim D_2$, then $L(D_1) \cong L(D_2)$ and so $\ell(D_1) = \ell(D_2)$.

Proof:

- Suppose $D_1 = D_2 + \mathrm{div}(g)$.
- Then the map from $L(D_1)$ to $L(D_2)$ sending $f \mapsto fg$ is an isomorphism of vector spaces since it has an inverse map $h \mapsto h/g$.

Riemann-Roch Dimensions, IV

3. If $\deg(D) \leq 0$, then $L(D) = \{0\}$ and $l(D) = 0$ except when $D = \mathrm{div}(\alpha)$ is principal, in which case $L(D) = \mathrm{span}(\alpha)$ and $l(D) = 1$.

Proof:

- Suppose $f \in L(D)$ and $f \neq 0$. Then $0 = \deg(\mathrm{div}(f)) \geq \deg(-D) = -\deg(D)$.
- Furthermore, equality can hold only if $D = -\mathrm{div}(f)$ for some $f \in k(C)^{\times}$, in which case D is principal.
- If D is principal, then $\ell(D) = \ell(0) = 1$ by (2), and $L(D) = \mathrm{span}(\alpha)$ by the same calculation.

Riemann-Roch Dimensions, V

4. If D_1 and D_2 are divisors with $D_1 \leq D_2$, then $\dim_k(L(D_2)/L(D_1)) \leq \deg(D_2) - \deg(D_1)$.

Proof (part 1):

- Induct on the sum of the coefficients of the points in the effective divisor $B - A$. The base case $B - A = 0$ is trivial.
- For the inductive step, suppose that $D_2 = D_1 + P$ for some point P, and choose $x \in k(C)$ such that $v_P(x) = v_P(D_2) = v_P(D_1) + 1$.
- Then for any $y \in L(D_2)$, we have $v_P(xy) = v_P(x) + v_P(y) \geq v_P(D_2) - v_P(D_2) \geq 0$, so $xy \in \mathcal{O}_P$, the local ring at P.
- By composing with the evaluation map at P, we obtain a k-linear transformation $\varphi : L(D_2) \to \mathcal{O}_P/m_P \cong k$ with $\varphi(y) = (xy)(P)$.

Riemann-Roch Dimensions, VI

4. If D_1 and D_2 are divisors with $D_1 \le D_2$, then $\dim_k(L(D_2)/L(D_1)) \le \deg(D_2) - \deg(D_1)$.

Proof (part 2):

- By composing with the evaluation map at P, we obtain a k-linear transformation $\varphi : L(D_2) \to \mathcal{O}_P/m_P \cong k$ with $\varphi(y) = (xy)(P)$.
- Then $y \in \ker(\varphi)$ if and only if $(xy)(P) = 0$ if and only if $v_P(xy) \ge 1$ if and only if $v_P(y) \ge 1 - v_P(D_2) = -v_P(D_1)$, and this last statement is equivalent to $y \in L(D_1)$.
- Thus, by the first isomorphism theorem, we have an injection from $L(D_2)/L(D_1)$ to $\mathcal{O}_P/m_P$.
- Take dimensions: $\dim_k(L(D_2)/L(D_1)) \le \dim_k(\mathcal{O}_P/m_P) = 1$. This establishes the inductive step. Done.

Riemann-Roch Dimensions, VII

5. For any effective divisor D, we have $\ell(D) \leq \deg(D) + 1$. In fact, this inequality holds for any divisor D of degree ≥ 0.

Proof:

- For effective divisors, this follows immediately by induction on the degree of D using (4), starting with the base case $l(0) = 1$.
- For general divisors, the result is trivial if $\ell(D) = 0$, so suppose otherwise that $\ell(D) \geq 1$ and let $\alpha \in L(D)$ be nonzero.
- Then $\mathrm{div}(\alpha) \geq -D$ which is equivalent to $D - \mathrm{div}(\alpha^{-1}) \geq 0$.
- Then for $D' = D - \mathrm{div}(\alpha^{-1})$, we see that D is equivalent to the effective divisor D', and so by (2) we have $\ell(D) = \ell(D') \leq \deg(D') + 1 = \deg(D) + 1$, as required.

Riemann-Roch Dimensions, VIII

6. For any divisor D, the quantity $\ell(D)$ is finite.

Proof:

- If $\deg(D) < 0$ then (3) gives $\ell(D) = 0$, while if $\deg(D) \geq 0$ then (5) gives $\ell(D) \leq \deg(D) + 1$.

Riemann-Roch, I

What we would like to be able to do now is to calculate the actual dimension $\ell(D)$ for arbitrary divisors D. Rather than delaying the point, let me just state the main result:

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

Remark: The divisor class $\mathcal{C}$, as I will explain later in our discussion of differentials, is the divisor class associated with the meromorphic differentials of C.

Riemann-Roch, II

I don't intend to give the full proof of the Riemann-Roch theorem, since it would take us a little far afield of the actual intended path.

- But I may have time later to give a sketch of the argument in concert with our discussion of differentials, or possibly much later when we talk about elliptic curves over $\mathbb{C}$.
- The main obstacle is that we would need to discuss how to define the residue of a function at a pole in the algebraic case, which turns out to be a bit convoluted.
- But in the situation of $k = \mathbb{C}$, the residue of a meromorphic function at a pole is something easily understood in terms of power series.

Riemann-Roch: $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$, III

So let's prove some consequences of Riemann-Roch:

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 $\mathcal{C}$.*

Riemann-Roch: $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$, IV

1. For any divisor A with $\deg(A) \geq 0$, we have $\deg(A) - g + 1 \leq \ell(A) \leq \deg(A) + 1$.

Proof:

- We showed the upper bound earlier using an inductive argument.
- The lower bound follows immediately from Riemann-Roch since $\ell(C - A) \geq 0$.

Riemann-Roch: $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$, V

2. For $C \in \mathcal{C}$ we have $\ell(C) = g$ and $\deg(C) = 2g - 2$.

Proof:

- First set $A = 0$ in Riemann-Roch: this yields $\ell(0) = \deg(0) - g + 1 + \ell(C)$, so since $\ell(0) = 1$ and $\deg(0) = 0$, we get $\ell(C) = g$.
- Now set $A = C$ in Riemann-Roch: this yields $\ell(C) = \deg(C) - g + 1 + \ell(0)$, and so $\deg(C) = \ell(C) + g - 1 - \ell(0) = 2g - 2$.

Riemann-Roch: $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$, VI

3. If $\deg(A) \geq 2g - 2$, then $\ell(A) = \deg(A) - g + 1$ except when $A \in \mathcal{C}$ (in which case $\ell(A) = g$).

Proof:

- If $\deg(A) \geq 2g - 2$, then $\deg(C - A) \leq 0$.
- Hence by our earlier results, this says $\ell(C - A) = 0$ except when $C - A$ is principal (i.e., when $A \in \mathcal{C}$).
- When $\ell(C - A) = 0$ Riemann-Roch immediately gives $\ell(A) = \deg(A) - g + 1$, and when $A \in \mathcal{C}$ we have $\ell(A) = g$ by (2).

Riemann-Roch: $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$, VII

4. The genus g is unique, as is the equivalence class $\mathcal{C}$.

Proof:

- Pick A of sufficiently large degree: then $\deg(A) - \ell(A) + 1 = g$ by (3), so g is uniquely determined.
- For uniqueness of $\mathcal{C}$, if $\ell(A) = \deg(A) - g + 1 + \ell(C - A) = \deg(A) - g + 1 + \ell(D - A)$ for some other divisor D, then $\ell(C - A) = \ell(D - A)$ for all A.
- Setting $A = C$ yields $\ell(D - C) = 1$ and setting $A = D$ yields $\ell(C - D) = 1$, and these are contradictory unless $D - C$ is principal, which is to say, $D \sim C$.

Riemann-Roch: $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$, IX

Our main highlight is that we can use Riemann-Roch to study smooth projective curves of small genus over an arbitrary field F with algebraic closure k.

- We start with the simplest genus $g = 0$ to illustrate the ideas.
- Then we will move on to genus $g = 1$, which (as you will see) corresponds precisely to the situation of elliptic curves.

Riemann-Roch: $\ell(A) = \deg(A) - g + 1 + \ell(C - A)$, X

So suppose that C is a curve of genus 0 over the field F, and let $K = F(C)$ be its function field.

- By Riemann-Roch, we have $\ell(A) = \deg(A) + 1 + \ell(C - A)$ for any divisor A, and also $\deg(C) = -2$.
- Also, by (3), if $\deg(A) \geq -1$ then $\ell(A) = \deg(A) + 1$. In particular, since $\deg(-C) = 2$, we have $\ell(-C) = 3$.
- Now, for any point P, we have $\ell(P) \leq \deg(P) + 1$. So, if P is any point with $P \leq C$ (there must be at least one since $\deg(-C)$ is positive), we see $\ell(P) \leq \ell(-C) = 3$.
- Thus, $\deg(P)$ must be either 1 or 2. (Remember here that F is not algebraically closed, so points can have a degree larger than 1, if their coordinates don't lie in F itself.)

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XI

First suppose that there is a point P of degree 1.

- Then $\ell(P) = 2$.
- Since F is a subspace of $L(P)$, there is a basis of $L(P)$ of the form $\{1, x\}$ for some $x \notin F$.
- Then since $\deg(\mathrm{div}(x) + P) = 1$ and $\mathrm{div}(x) + P \geq 0$, we must have $\mathrm{div}(x) + P = Q$ for some point Q (necessarily of degree 1).
- Then $\mathrm{div}(x) = P - Q$, and so $[K : F(x)] = \deg(\mathrm{div}_+(x)) = \deg(P) = 1$, which means $K = F(x)$.
- Thus, we obtain an isomorphism $x : C \to \mathbb{P}^1$.

Reformulation: A smooth projective curve of genus 0 having a rational point is isomorphic to $\mathbb{P}^1$.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XII

Now suppose that there are no points of degree 1: per earlier, we must have a point $P \leq C$ of degree 2.

- Then $\ell(P) = 3$, so again since $L(P)$ contains k, we may take a basis for $L(P)$ of the form $\{1, x, y\}$ for some F-linearly independent $x, y \notin F$.
- In the same way as before, we see that $\mathrm{div}(x) = P - Q$ and $\mathrm{div}(y) = P - R$ for some (necessarily distinct) points Q and R of degree 2.
- Then $[K : F(x)] = \deg(\mathrm{div}_+(x)) = 2$ and $[K : F(y)] = \deg(\mathrm{div}_+(y)) = 2$ also.
- Since $F(x) \neq F(y)$ (by linear independence and the fact that K is a degree-2 extension of both), we see $K = F(x, y)$.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XIII

So, we know that $K = F(x, y)$ for some rational functions x, y. Since C is a curve, these functions x and y must satisfy some algebraic relation.

- We can use Riemann-Roch to identify this relation.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XIII

So, we know that $K = F(x, y)$ for some rational functions x, y. Since C is a curve, these functions x and y must satisfy some algebraic relation.

- We can use Riemann-Roch to identify this relation.
- Explicitly, observe that $\ell(2P) = 1 + \deg(2P) = 5$, but we can find six different elements in $L(2P)$, namely $\{1, x, y, x^2, xy, y^2\}$.
- They must therefore be F-linearly dependent, so we see that x and y satisfy some quadratic relation $ax^2 + bxy + cy^2 + dx + ey = f$, where at least one of the quadratic terms is nonzero.

Reformulation: A smooth projective curve of genus 0 having no F-rational point is isomorphic to a conic.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XIV

Now suppose C is a curve of genus 1 over F, again with function field K.

- In this case, for $g = 1$ Riemann-Roch and its corollaries say that $\ell(A) = \deg(A) + \ell(C - A)$, that $\deg(C) = 0$ and $\ell(C) = 1$, and that if $\deg(A) \geq 1$ then $\ell(A) = \deg(A)$.
- Unlike the case $g = 0$, we are not necessarily guaranteed to have a point of any given degree any more, since we cannot use C to construct a point of small degree.
- Indeed, since $\deg(C) = 0$ and $\ell(C) = 1$, in fact C is principal (and $C \sim 0$).
- So let us instead merely suppose that we do have a point P of degree 1.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XV

So: C has genus 1, and P is a point of degree 1. Let's look at the spaces $L(nP)$ like in the genus-0 case.

- From Riemann-Roch, we have $\ell(nP) = n$.
- $\ell(2P) = 2$. Choose a basis $\{1, x\}$ for $L(2P)$, where we necessarily must have $v_P(x) = 2$ since $x \notin L(P)$.
- $\ell(3P) = 3$. Since $1, x \in L(3P)$ we can extend these to a basis $\{1, x, y\}$ for $L(3P)$, where necessarily $v_P(y) = 3$ since $y \notin L(2P)$.
- Now we observe that $[K : F(x)] = \deg(\mathrm{div}_+(x)) = 2$ and $[K : F(y)] = \deg(\mathrm{div}_+(y)) = 3$, so since 2 and 3 are relatively prime, we see $K = F(x, y)$.
- Our task again is to find an algebraic relation between x and y.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XV

So: C has genus 1, P is a point of degree 1, and we have $x, y \in F(C)$ with $v_P(x) = 2$ and $v_P(y) = 3$ such that $F(C) = F(x, y)$.

- Since the various monomials $x^i y^j$ will all only have poles at P, we can (hope to) find a relation by considering more spaces $L(nP)$.
- We have $\ell(4P) = 4$, but we can only identify 4 elements that must lie in this space: $\{1, x, y, x^2\}$. In fact, they are all linearly independent since they all have different valuations at P.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XV

So: C has genus 1, P is a point of degree 1, and we have $x, y \in F(C)$ with $v_P(x) = 2$ and $v_P(y) = 3$ such that $F(C) = F(x, y)$.

- Since the various monomials $x^i y^j$ will all only have poles at P, we can (hope to) find a relation by considering more spaces $L(nP)$.
- We have $\ell(4P) = 4$, but we can only identify 4 elements that must lie in this space: $\{1, x, y, x^2\}$. In fact, they are all linearly independent since they all have different valuations at P.
- Likewise, $\ell(5P) = 5$, but we only have 5 elements in this space: $\{1, x, y, x^2, xy\}$. Again, these elements are all linearly independent since they have different valuations at P.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XVI

So: C has genus 1, P is a point of degree 1, and we have $x, y \in F(C)$ with $v_P(x) = 2$ and $v_P(y) = 3$ such that $F(C) = F(x, y)$.

- But with $\ell(6P) = 6$ we hit paydirt, because here are 7 elements in this space: $\{1, x, y, x^2, xy, x^3, y^2\}$.

Riemann-Roch: $\ell(A) = \deg(A) + 1 + \ell(C - A)$, XVI

So: C has genus 1, P is a point of degree 1, and we have $x, y \in F(C)$ with $v_P(x) = 2$ and $v_P(y) = 3$ such that $F(C) = F(x, y)$.

- But with $\ell(6P) = 6$ we hit paydirt, because here are 7 elements in this space: $\{1, x, y, x^2, xy, x^3, y^2\}$.
- Thus, we must have a linear dependence among these elements, and in fact since x^3 and y^2 are the only elements with valuation 6 at P, they both have nonzero coefficients.
- Then by rescaling x, y appropriately, we obtain an algebraic relation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for some $a_1, a_2, a_3, a_4, a_6 \in E$.
- In other words, C has an equation in Weierstrass form!
- Also, here I can mention why the a_i are so labeled: they are giving the "missing" pole valuation at P for the corresponding monomial term.

Elliptic Curves But Properly, I

This proves the following theorem:

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 $a_1, a_2, a_3, a_4, a_6 \in F$.

Elliptic Curves But Properly, I

This proves the following theorem:

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 $a_1, a_2, a_3, a_4, a_6 \in F$.

Elliptic Curves But Properly, II

We can now adopt the more highbrow definition of elliptic curves:

Definition (Elliptic Curves, Properly)

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

Note that the specific choice of F-rational point O is part of the definition of an elliptic curve.

- If we take the same projective curve but choose different selections for O, we view the resulting elliptic curves as distinct.
- As we will see, however, they will be isomorphic, so the distinction is not of great importance.

Elliptic Curves But Properly, III

Let's use the highbrow approach to show that elliptic curves have a group law:

- In the discussion that follows, we will need to keep separate the notion of P as a divisor and P as a point on the curve.
- If you're wondering why, it's because we have a group operation on divisors (namely, addition of divisors) and also a group operation on points (namely, addition on the elliptic curve).
- As you can probably imagine, we will be using the group operation on divisors to construct the group operation on points.

So, in this discussion, the divisor of a point P will always be denoted $[P]$.

Elliptic Curves But Properly, IV

Theorem (The Group Law, Again)

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

1. *If P and Q are F-rational points such that $[P] \sim [Q]$ as divisors, then $P = Q$.*
2. *For every degree-zero divisor D, there exists a unique point $P \in E$ such that $D \sim [P] - [O]$.*
3. *If $\sigma : \mathrm{Div}^0(E) \to E$ denotes the map in (2), then σ induces a bijection $\tilde{\sigma} : \mathrm{Pic}^0(E) \to E$.*
4. *With $\tilde{\sigma}$ as in (3), the group operation on E induced from $\mathrm{Pic}^0(E)$ via $\tilde{\sigma}$ is the same as the geometric group law on E. (In other words, if we think of E as a group with the geometric law, then E is isomorphic to $\mathrm{Pic}^0(E)$ via $\tilde{\sigma}$.)*

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, VI

1. If P and Q are F-rational points such that $[P] \sim [Q]$ as divisors, then $P = Q$.

Proof:

- Suppose that $[P] \sim [Q]$, so that $[P] - [Q] = \mathrm{div}(f)$ for some f.
- Then in particular, $f \in L([Q])$.
- But Riemann-Roch on E says that $l([Q]) = 1$, so since the constants all lie in $L([Q])$, f must be constant.
- Then $\mathrm{div}(f) = 0$ and hence $P = Q$, as claimed.

Elliptic Curves But Properly, VII

2. For every degree-zero divisor D, there exists a unique point $P \in E$ such that $D \sim [P] - [O]$.

Proof:

- For existence, since $\deg(D + [O]) = 1$, our consequences of Riemann-Roch imply that $l(D + [O]) = 1$.
- Let f span $L(D + [O])$: then $\mathrm{div}(f) \geq -D - [O]$ and $\deg(\mathrm{div}(f)) = 0$.
- So since $-D - [O]$ has degree -1, we must have $\mathrm{div}(f) = -D - [O] + [P]$ for some degree-1 point P, whence $D \sim [P] - [O]$.
- Finally, the uniqueness of Q then follows immediately from (1), since if $[P] - [O] \sim D \sim [Q] - [O]$ then $P = Q$.

Elliptic Curves But Properly, VIII

3. If $\sigma : \mathrm{Div}^0(E) \to E$ denotes the map with $D \sim [\sigma(D)] - [O]$, then σ induces a bijection $\tilde{\sigma} : \mathrm{Pic}^0(E) \to E$.

Proof:

- First observe that $\sigma([P] - [O]) = P$ so σ is certainly surjective from $\mathrm{Div}^0(E)$ to E.
- Also, by the definition of σ for any divisors D_1 and D_2 we have $\sigma(D_1) - \sigma(D_2) \sim D_1 - D_2$, so $D_1 \sim D_2$ if and only if $\sigma(D_1) = \sigma(D_2)$.
- This shows that σ descends to a bijection $\tilde{\sigma}$ from $\mathrm{Pic}^0(E)$ to E.

Elliptic Curves But Properly, IX

4. With $\tilde{\sigma} : \mathrm{Pic}^0(E) \to E$ with $\tilde{\sigma}(D) =\sim [\sigma(D)] - [O]$, the group operation on E induced from $\mathrm{Pic}^0(E)$ via $\tilde{\sigma}$ is the same as the geometric group law on E.

Proof (preamble):

- The inverse map of $\tilde{\sigma}$ is $\tau : P \to [P] - [O]$.
- We want to see that $\tau(P + Q) = \tau(P) + \tau(Q)$, where the addition on the left is the geometric group law, and the addition on the right is the addition of divisor classes in the Picard group.
- Equivalently, we want to see that $[P + Q] - [P] - [Q] + [O] \sim 0$, where again $P + Q$ represents addition via the geometric group law.

Elliptic Curves But Properly, IX

4. With $\tilde{\sigma} : \mathrm{Pic}^0(E) \to E$ with $\tilde{\sigma}(D) \sim [\sigma(D)] - [O]$, the group operation on E induced from $\mathrm{Pic}^0(E)$ via $\tilde{\sigma}$ is the same as the geometric group law on E.

Proof:

- To show: $[P+Q] - [P] - [Q] + [O] \sim 0$.
- Let f be the line through P and Q, let R be the third intersection point of E with this line, and let g be the line through R and O. Then since the line $Z = 0$ intersects E at O with multiplicity 3, we have
  $\mathrm{div}(f/Z) = [P] + [Q] + [R] - 3[O]$ and
  $\mathrm{div}(g/Z) = [R] + [P+Q] - 2[O]$.
- Therefore, $[P+Q] - [P] - [Q] + [O] = \mathrm{div}(f/g) \sim 0$, as required. This means τ is a group homomorphism and thus a group isomorphism, as desired.

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

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

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.

Summary

We discussed Riemann-Roch spaces $L(D)$ and properties of their dimensions $l(D)$.

We stated the Riemann-Roch theorem and discussed a number of its consequences.

We constructed Weierstrass equations and the group law on genus-1 curves using Riemann-Roch.

Next lecture: Differentials.