Math 7359 (Elliptic Curves and Modular Forms)

Lecture #9 of 24 $\sim$ October 5, 2023

Divisors on Curves

- Divisors
- Properties of Divisors
- Riemann-Roch Spaces

Preamble

Now that we have dispensed with all of the preliminary facts about algebraic curves, we can start our work on studying elliptic curves using the tools of algebraic geometry.

- Our next task is to study divisors on curves.
- In all of our discussion, C will be a smooth projective curve defined over the algebraically closed field k.
- To emphasize, references to "points of C" are always viewing C as being defined over an algebraically closed field, and the points have coordinates in this algebraically closed field.
- Also, for convenience I will usually give examples in affine form, because the notation is easier to follow.

Divisors, I

Definition

Let C be a smooth curve. The <u>divisor group</u> of C, written $\mathrm{Div}(C)$, is the additive free abelian group generated by the k-points of C. The <u>degree</u> of a divisor $D = \sum_{P \in C} n_P P$ is $\deg(D) = \sum_{P \in C} n_P$.

Divisors, I

Definition

Let C be a smooth curve. The divisor group of C, written $\mathrm{Div}(C)$, is the additive free abelian group generated by the k-points of C. The degree of a divisor $D = \sum_{P \in C} n_P P$ is $\deg(D) = \sum_{P \in C} n_P$.

- The elements of $\mathrm{Div}(C)$ are of the form $D = \sum_{P \in C} n_P P$ for $n_P \in \mathbb{Z}$, where all but finitely many of the n_P are zero. We will write $\mathrm{ord}_P(D) = n_P$.
- Some divisors on $\mathbb{A}^1(\mathbb{C})$ are P_0, $P_0 - 3P_\infty$, and $P_1 - P_i - 11P_{1-i} + 4P_{\pi - e}$.
- The degree map is well defined because only finitely many n_P are nonzero, and it is a homomorphism from D_C to $\mathbb{Z}$. Its kernel is the set of degree-0 divisors $\mathrm{Div}^0(C)$.

Divisors, II

You might be wondering why we call these formal linear combinations of points "divisors". Let me outline the reason:

- If $C_1 = V(f)$ and $C_2 = V(g)$ are two distinct projective plane curves sharing no common component, then their intersection $C_1 \cap C_2 = V(f, g)$ is finite. (Indeed, Bézout's theorem states that the number of intersection points is at most $\deg(f) \cdot \deg(g)$.)
- We may associate a divisor to this intersection $C_1 \cap C_2$ as $\sum_{P \in C_1 \cap C_2} n_P P$, where n_P is the <u>intersection number</u> of $C_1 \cap C_2$ at P given by $n_P = \dim_k \mathcal{O}_P(\mathbb{P}^2)/(f, g)$.

Divisors, III

Why do we take that intersection divisor $C_1 \cap C_2$ as $\sum_{P \in C_1 \cap C_2} n_P P$, where n_P is the intersection number given by $n_P = \dim_k \mathcal{O}_P(\mathbb{P}^2)/(f, g)$?

- For polynomials in one variable, the ideal (f, g) is principal and generated by the gcd of f and g. (One may check that the intersection number at a point P, under the definition above, is the power of $x - P$ that divides their gcd.)
- The idea is that in the one-variable case, this "intersection number" summed over all points precisely captures the notion of "common divisor".
- I'll do an example.

Divisors, IV

Take $f = x^3(x-1)(x+5)$ and $g = x^2(x-1)(x+2)$ as functions on $\mathbb{P}^1(\mathbb{C})$, where as usual $x = X/Y$.

- We have $(f,g) = (\gcd(f,g)) = (x^2(x-1))$. This function has a pole at P_∞, a double zero at P_0, and a single zero at P_1.

Divisors, IV

Take $f = x^3(x-1)(x+5)$ and $g = x^2(x-1)(x+2)$ as functions on $\mathbb{P}^1(\mathbb{C})$, where as usual $x = X/Y$.

- We have $(f,g) = (\gcd(f,g)) = (x^2(x-1))$. This function has a pole at P_∞, a double zero at P_0, and a single zero at P_1.
- At P_0, since x generates the maximal ideal of the local ring there, we see $\mathrm{ord}_{P_0}(f,g) = 2$ (note that $x-1$ is a unit in $\mathcal{O}_{P_0}$.
- Likewise, since $x-1$ generates the maximal ideal of the local ring at P_1, we see $\mathrm{ord}_{P_1}(f,g) = 1$,
- So the intersection divisor is $2P_0 + P_1$.
- If we instead think of this divisor multiplicatively, and replace P_0 with x and P_1 with $x-1$ (the respective local uniformizers), the "multiplicative divisor" comes out to be $x^2(x-1)$: precisely the "common divisor" of f and g.

Divisors, V

For polynomials in two variables (f, g) will no longer be principal, but it still carries the natural sense of being a "common divisor".

- Thus, we can think of the divisor $\sum_{P \in C_1 \cap C_2} n_P P$ as describing the precise way in which the curves C_1 and C_2 intersect.

It is not particularly obvious that this value $\dim_k \mathcal{O}_P(\mathbb{P}^2)/(f, g)$ is really the right definition. But here are a few reasons:

Divisors, V

For polynomials in two variables (f, g) will no longer be principal, but it still carries the natural sense of being a "common divisor".

- Thus, we can think of the divisor $\sum_{P \in C_1 \cap C_2} n_P P$ as describing the precise way in which the curves C_1 and C_2 intersect.

It is not particularly obvious that this value $\dim_k \mathcal{O}_P(\mathbb{P}^2)/(f, g)$ is really the right definition. But here are a few reasons:

- The value is invariant under linear changes of coordinates.
- The value is 1 whenever P is a simple point of C_1 and C_2 where C_1 and C_2 meet transversally (i.e., their tangent lines at P are different).
- The value is additive when we take unions of curves.

We will not really use this particular formulation of divisors; it is merely some motivation for how divisors arise in a fairly natural way in the context of curves.

Divisors, VI

If E is a subfield of the algebraically closed field k over which C is defined, the Galois group $\mathrm{Gal}(k/E)$ acts on the k-rational points of C, and thus it also acts on divisors pointwise.

Definition

Suppose C is a smooth curve defined over the algebraically closed field k, and E is a subfield of k with $\overline{E} = k$.

If $\sigma \in \mathrm{Gal}(k/E)$ is an element of the Galois group and $D = \sum_{P \in C} n_P P$ is a divisor, we define the action of σ on D via $\sigma(D) = \sum_{P \in C} n_p \sigma(P)$.
We then say a divisor D is <u>defined over E</u> when $\sigma(D) = D$ for all $\sigma \in \mathrm{Gal}(k/E)$, and we denote the subgroup of divisors defined over E as $\mathrm{Div}_E(C)$.

Divisors, VII

If all of the points having nonzero coefficients in a divisor D are defined over E, then certainly D is defined over E, but this is not necessary.

- Compare $\sigma(D) = \sum_{P \in C} n_p \sigma(P)$ to the reindexed sum $D = \sum_{P \in C} n_{\sigma(P)} \sigma(P)$.
- For those to be equal we need $n_{\sigma(P)} = n_P$ for all $P \in C$ and all $\sigma \in \mathrm{Gal}(k/E)$.
- So all that is required is for Galois-conjugate points to have the same coefficients (and this is also sufficient).
- For example, for the curve $C = \mathbb{A}^1(\mathbb{C})$, with $P = i$ and $Q = -i$, the divisor $2P + Q$ is defined over $\mathbb{Q}(i)$ (any element of the Galois group $\mathbb{C}/\mathbb{Q}(i)$ fixes i and $-i$, hence sends P to P and Q to Q) while the divisor $P + Q$ is defined over $\mathbb{Q}$ (any element of the Galois group $\mathbb{C}/\mathbb{Q}$ either fixes i or maps it to $-i$, and these operations map $P + Q$ to $P + Q$ or $Q + P$ respectively).

Divisors, VIII

For example, consider $C = \mathbb{A}^1(\mathbb{C})$ with points $P = i$ and $Q = -i$.

- Then the divisor $2P + Q$ is defined over $\mathbb{Q}(i)$: any element of the Galois group $\mathbb{C}/\mathbb{Q}(i)$ fixes i and $-i$, hence sends P to P and Q to Q.

Divisors, VIII

For example, consider $C = \mathbb{A}^1(\mathbb{C})$ with points $P = i$ and $Q = -i$.

- Then the divisor $2P + Q$ is defined over $\mathbb{Q}(i)$: any element of the Galois group $\mathbb{C}/\mathbb{Q}(i)$ fixes i and $-i$, hence sends P to P and Q to Q.
- On the other hand, the divisor $P + Q$ is actually defined over the smaller field $\mathbb{Q}$: any element of the Galois group $\mathbb{C}/\mathbb{Q}$ either fixes i or maps it to $-i$, and these operations map $P + Q$ to $P + Q$ or $Q + P$ respectively. In both cases the divisor $P + Q$ is fixed, and so $P + Q$ is defined over $\mathbb{Q}$.

Divisors of Functions, I

We can attach a divisor to a rational function on C using its zeroes and poles:

Definition

Let C be a smooth curve and $\alpha \in k(C)$ be a nonzero rational function on C. We define the divisor of α, denoted $\mathrm{div}(\alpha)$, as $\mathrm{div}(\alpha) = \sum_{P \in C} v_P(\alpha) P$. The divisors of the form $\mathrm{div}(\alpha)$ for some $\alpha \in k(C)^\times$ are called principal divisors.

Some notational remarks:

- You'd think there would be a notation for the set of principal divisors, but there isn't.
- In many sources, the divisor of α is often written (α). In our context, this can lead to ambiguities, since the same notation is also used for the ideal generated by α. As such, I will always write $\mathrm{div}(\alpha)$ for the divisor of α, since that's unambiguous.

Divisors of Functions, II

As we/you have already shown[1], for any nonzero α, $v_P(\alpha)$ is nonzero only for finitely many $P \in C$, so $\mathrm{div}(\alpha)$ is well defined.

- Now because $\mathrm{ord}_P(\alpha/\beta) = \mathrm{ord}_P(\alpha) - \mathrm{ord}_P(\beta)$, summing over all primes shows that $\mathrm{div}(\alpha/\beta) = \mathrm{div}(\alpha) - \mathrm{div}(\beta)$, so the principal divisors are a subgroup of the divisor group $\mathrm{Div}(C)$.[2]

I'll do some examples on the next slides. Just remember that when computing the divisor of a function on a smooth curve C, all of our curves are projective, so we need to remember to include the point at ∞.

[1] This was an exercise from the Sep 21 lecture, and is on homework 2

[2] I suppose technically I should point out that the divisor of a constant is zero, as well, so that the set of principal divisors contains the identity.

Divisors of Functions, III

Example: Let $C = \mathbb{P}^1(\mathbb{C})$ with points denoted $[X : Y]$. Consider the rational function $\alpha = X/Y$.

Divisors of Functions, III

Example: Let $C = \mathbb{P}^1(\mathbb{C})$ with points denoted $[X : Y]$. Consider the rational function $\alpha = X/Y$.

- Note that α has a pole when $Y = 0$, which is the point $[1 : 0]$, and α is defined everywhere else.
- When $X = 0$, namely at the point $[0 : 1]$, α is zero, and everywhere else α is nonzero.
- So since $\alpha = X/Y$ is a local uniformizer at $[0 : 1]$ and $1/\alpha = Y/X$ is a local uniformizer at $[1 : 0]$, we see that $\operatorname{ord}_{[0:1]} \alpha = 1$ and $\operatorname{ord}_{[1:0]} \alpha = -1$, and $\operatorname{ord}_P \alpha = 0$ for other points P.
- Thus $\operatorname{div}(\alpha) = P_{[0:1]} - P_{[1:0]}$

Divisors of Functions, IV

Example: Let $C = \mathbb{P}^1(\mathbb{C})$ with points denoted $[X : Y]$. Consider the rational function $\beta = \dfrac{X^3 - XY^2}{Y^3}$.

Divisors of Functions, IV

Example: Let $C = \mathbb{P}^1(\mathbb{C})$ with points denoted $[X : Y]$. Consider the rational function $\beta = \dfrac{X^3 - XY^2}{Y^3}$.

- Using similar calculations as for α, we can see that β has three single zeroes at $[0 : 1]$, $[1 : 1]$, and $[-1 : 1]$ and a triple pole at $[1 : 0]$.
- Therefore, we have $\mathrm{div}(\beta) = P_{[0:1]} + P_{[1:1]} + P_{[-1:1]} - 3P_{[1:0]}$.

Divisors of Functions, IV

Example: Let $C = \mathbb{P}^1(\mathbb{C})$ with points denoted $[X : Y]$. Consider the rational function $\beta = \dfrac{X^3 - XY^2}{Y^3}$.

- Using similar calculations as for α, we can see that β has three single zeroes at $[0 : 1]$, $[1 : 1]$, and $[-1 : 1]$ and a triple pole at $[1 : 0]$.
- Therefore, we have $\mathrm{div}(\beta) = P_{[0:1]} + P_{[1:1]} + P_{[-1:1]} - 3P_{[1:0]}$.

If we dehomogenize these last two examples, we see $\alpha_* = x$ and $\beta_* = x^3 - x$.

- The associated divisors are $\mathrm{div}(\alpha_*) = P_0 - P_\infty$ and $\mathrm{div}(\beta_*) = P_0 + P_1 + P_{-1} - 3P_\infty$.
- Note they are the same as the divisors we calculated using the projective model, just with the points given affine labels.

Divisors of Functions, V

Exercise: On $C = \mathbb{A}^1(\mathbb{C})$, suppose $\alpha = u\dfrac{(x-p_1)^{a_1}\cdots(x-p_l)^{a_l}}{(x-q_1)^{b_1}\cdots(x-q_m)^{b_m}}$ for $u \in \mathbb{C}^\times$ and take distinct elements $p_1, \dots, p_l, q_1, \dots, q_m \in \mathbb{C}$ having associated points $P_1, \dots, P_k, Q_1, \dots, Q_l$ respectively.

Show that
$\mathrm{div}(a) = a_1 P_1 + \cdots + a_l P_l - b_1 Q_1 - \cdots - b_m Q_m + [\sum_j b_j - \sum_i a_i] P_\infty$.
[Hint: This is a generalization of the examples we just did.]

Exercise: Show that for any $C = \mathbb{A}^1(\mathbb{C})$ and any nonzero rational function $\alpha \in \mathbb{C}(C)$ we have $\deg(\mathrm{div}(\alpha)) = 0$.

Divisors of Functions, VI

Example: For $C = V(Y^2Z - X^3 - XZ^2)$ consider the rational function $\gamma = Y/Z$.

[3] This is exercise 6 from Sep 21, on homework 2

Divisors of Functions, VI

Example: For $C = V(Y^2Z - X^3 - XZ^2)$ consider the rational function $\gamma = Y/Z$.

- The zeroes for γ can only occur when $Y = 0$ yielding the points $[0 : 0 : 1]$, $[i : 0 : 1]$, $[-i : 0 : 1]$, while the poles for γ can only occur when $Z = 0$ yielding the point $[0 : 1 : 0]$.
- To compute the order of vanishing γ at each point we may compute a local uniformizer[3] (for the three zeroes, $\gamma = Y/Z$ is itself a local uniformizer, while for the pole, Z/X is a local uniformizer).

[3] This is exercise 6 from Sep 21, on homework 2

Divisors of Functions, VI

Example: For $C = V(Y^2Z - X^3 - XZ^2)$ consider the rational function $\gamma = Y/Z$.

- The zeroes for γ can only occur when $Y = 0$ yielding the points $[0:0:1]$, $[i:0:1]$, $[-i:0:1]$, while the poles for γ can only occur when $Z = 0$ yielding the point $[0:1:0]$.
- To compute the order of vanishing γ at each point we may compute a local uniformizer[3] (for the three zeroes, $\gamma = Y/Z$ is itself a local uniformizer, while for the pole, Z/X is a local uniformizer).
- One obtains $\mathrm{ord}_{[0:0:1]}\gamma = \mathrm{ord}_{[i:0:1]}\gamma = \mathrm{ord}_{[-i:0:1]}\gamma = 1$ and also $\mathrm{ord}_{[0:1:0]}\gamma = -3$.
- Therefore, $\mathrm{div}(\gamma) = P_{[0:0:1]} + P_{[i:0:1]} + P_{[-i:0:1]} - 3P_{[0:1:0]}$.

[3] This is exercise 6 from Sep 21, on homework 2

Divisors of Functions, VII

Example (continued): For $C = V(Y^2Z - X^3 - XZ^2)$ consider the rational function $\gamma = Y/Z$.

- We computed $\mathrm{div}(\gamma) = P_{[0:0:1]} + P_{[i:0:1]} + P_{[-i:0:1]} - 3P_{[0:1:0]}$.

Divisors of Functions, VII

Example (continued): For $C = V(Y^2Z - X^3 - XZ^2)$ consider the rational function $\gamma = Y/Z$.

- We computed $\operatorname{div}(\gamma) = P_{[0:0:1]} + P_{[i:0:1]} + P_{[-i:0:1]} - 3P_{[0:1:0]}$.
- If we dehomogenize the example above, so as to work instead with the affine model $y^2 = x^3 + x$, the corresponding rational function is $\gamma_* = y$.
- The associated divisor is $\operatorname{div}(\gamma_*) = P_{(0,0)} + P_{(i,0)} + P_{(-i,0)} - 3P_\infty$.

Divisors of Functions, VIII

We can also pick out the zeroes (respectively, poles) of an element by extracting only the portion of its divisor with positive (respectively, negative) coefficients:

Definition

If $\alpha \in k(C)^{\times}$ *has divisor* $\mathrm{div}(\alpha) = \sum_P n_P P$, *we define the "zero divisor"* $\mathrm{div}_+(\alpha) = \sum_P \max(0, n_P)P = \sum_{P:n_P>0} n_P P$ *and the "pole divisor"* $\mathrm{div}_-(a) = \sum_P \min(0, n_P)P = \sum_{P:n_P<0} n_P P$.

Divisors of Functions, VIII

We can also pick out the zeroes (respectively, poles) of an element by extracting only the portion of its divisor with positive (respectively, negative) coefficients:

Definition

If $\alpha \in k(C)^\times$ *has divisor* $\mathrm{div}(\alpha) = \sum_P n_P P$*, we define the "zero divisor"* $\mathrm{div}_+(\alpha) = \sum_P \max(0, n_P) P = \sum_{P : n_P > 0} n_P P$ *and the "pole divisor"* $\mathrm{div}_-(a) = \sum_P \min(0, n_P) P = \sum_{P : n_P < 0} n_P P$.

- Notice that $\mathrm{div}(\alpha) = \mathrm{div}_+(\alpha) - \mathrm{div}_-(\alpha)$ for any $\alpha \in k(C)^\times$.
- There are various other notations for these quantities that are often used, such as $(a)_0$ for div_+ and $(a)_\infty$ for div_-, which are intended to evoke the idea of picking out the zeroes and poles of a.

Divisors of Functions, IX

Examples:

- For $\alpha = X/Y$ on $\mathbb{P}^1(\mathbb{C})$ with $\mathrm{div}(\alpha) = P_{[0:1]} - P_{[1:0]}$, we have $\mathrm{div}_+(\alpha) = P_{[0:1]}$ and $\mathrm{div}_-(\alpha) = P_{[1:0]}$.

Divisors of Functions, IX

Examples:

- For $\alpha = X/Y$ on $\mathbb{P}^1(\mathbb{C})$ with $\operatorname{div}(\alpha) = P_{[0:1]} - P_{[1:0]}$, we have $\operatorname{div}_+(\alpha) = P_{[0:1]}$ and $\operatorname{div}_-(\alpha) = P_{[1:0]}$.
- For $\beta = (X^3 - XY^2)/(Y^3)$ on $\mathbb{P}^1(\mathbb{C})$ with $\operatorname{div}(\beta) = P_{[0:1]} + P_{[1:1]} + P_{[-1:1]} - 3P_{[1:0]}$, we have $\operatorname{div}_+(\beta) = P_{[0:1]} + P_{[1:1]} + P_{[-1:1]}$ and $\operatorname{div}_-(\beta) = 3P_{[1:0]}$.

Divisors of Functions, IX

Examples:

- For $\alpha = X/Y$ on $\mathbb{P}^1(\mathbb{C})$ with $\operatorname{div}(\alpha) = P_{[0:1]} - P_{[1:0]}$, we have $\operatorname{div}_+(\alpha) = P_{[0:1]}$ and $\operatorname{div}_-(\alpha) = P_{[1:0]}$.
- For $\beta = (X^3 - XY^2)/(Y^3)$ on $\mathbb{P}^1(\mathbb{C})$ with $\operatorname{div}(\beta) = P_{[0:1]} + P_{[1:1]} + P_{[-1:1]} - 3P_{[1:0]}$, we have $\operatorname{div}_+(\beta) = P_{[0:1]} + P_{[1:1]} + P_{[-1:1]}$ and $\operatorname{div}_-(\beta) = 3P_{[1:0]}$.
- For $\gamma = Y/Z$ on $V(Y^2Z - X^3 - XZ^2)$ with $\operatorname{div}(\gamma) = P_{[0:0:1]} + P_{[i:0:1]} + P_{[-i:0:1]} - 3P_{[0:1:0]}$ we have $\operatorname{div}_+(\gamma) = P_{[0:0:1]} + P_{[i:0:1]} + P_{[-i:0:1]}$ and $\operatorname{div}_-(\gamma) = 3P_{[0:1:0]}$.

You may notice that in all of these cases, the degrees of the zero part and the pole part are the same.

Divisors of Functions, X: Marks The Spot

In fact, the degrees of the zero part and pole part of $\mathrm{div}(\alpha)$ will always be equal, and this common degree represents the degree of a field extension:

Theorem (Divisor Degrees)

For any nonconstant $\alpha \in k(C)^{\times}$ *on a curve* C/k*, we have* $\deg(\mathrm{div}_{+}(\alpha)) = \deg(\mathrm{div}_{-}(\alpha)) = [k(C) : k(\alpha)]$*. As a consequence,* $\deg(\mathrm{div}(\alpha)) = 0$ *for all* $\alpha \in k(C)^{\times}$*.*

Divisors of Functions, X: Marks The Spot

In fact, the degrees of the zero part and pole part of $\mathrm{div}(\alpha)$ will always be equal, and this common degree represents the degree of a field extension:

Theorem (Divisor Degrees)

For any nonconstant $\alpha \in k(C)^{\times}$ on a curve C/k, we have $\deg(\mathrm{div}_{+}(\alpha)) = \deg(\mathrm{div}_{-}(\alpha)) = [k(C) : k(\alpha)]$. *As a consequence,* $\deg(\mathrm{div}(\alpha)) = 0$ *for all* $\alpha \in k(C)^{\times}$.

- I will defer the proof of this result temporarily, since it would otherwise require developing a lot of additional material out of order.
- But the idea connecting the divisor to the field extension is to view α as a morphism from C to $\mathbb{P}^1$. (Recall from last time that we can view morphisms of curves as giving rise to field extensions of the function fields.)

Divisors of Functions, XI: This One Goes To Eleven

Here's how the field extension degrees work for the three divisors we wrote down:

- For $C = \mathbb{P}^1$ with function field $k(C) = \mathbb{C}(x)$ where $x = X/Y$, we have $\alpha = x$ so $k(\alpha) = \mathbb{C}(x)$ and so the extension degree $[k(C) : k(\alpha)] = [\mathbb{C}(x) : \mathbb{C}(x))] = 1$.

Divisors of Functions, XI: This One Goes To Eleven

Here's how the field extension degrees work for the three divisors we wrote down:

- For $C = \mathbb{P}^1$ with function field $k(C) = \mathbb{C}(x)$ where $x = X/Y$, we have $\alpha = x$ so $k(\alpha) = \mathbb{C}(x)$ and so the extension degree $[k(C) : k(\alpha)] = [\mathbb{C}(x) : \mathbb{C}(x))] = 1$.
- For $C = \mathbb{P}^1$ with $\beta = x^3 - x$ we have $k(\beta) = \mathbb{C}(x^3 - x)$ and so $[k(C) : k(\beta)] = [\mathbb{C}(x) : \mathbb{C}(x^3 - x))] = 3$.
- Why is this extension degree 3?

Divisors of Functions, XI: This One Goes To Eleven

Here's how the field extension degrees work for the three divisors we wrote down:

- For $C = \mathbb{P}^1$ with function field $k(C) = \mathbb{C}(x)$ where $x = X/Y$, we have $\alpha = x$ so $k(\alpha) = \mathbb{C}(x)$ and so the extension degree $[k(C) : k(\alpha)] = [\mathbb{C}(x) : \mathbb{C}(x))] = 1$.
- For $C = \mathbb{P}^1$ with $\beta = x^3 - x$ we have $k(\beta) = \mathbb{C}(x^3 - x)$ and so $[k(C) : k(\beta)] = [\mathbb{C}(x) : \mathbb{C}(x^3 - x))] = 3$.
- Why is this extension degree 3? Because x is a root of the irreducible polynomial $p(t) = t^3 - t - (x^3 - x)$ with coefficients in $\mathbb{C}(x^3 - x)$.

Divisors of Functions, XII: Something About Clocks

For $C = V(Y^2Z - X^3 - XZ^2)$ the situation is a bit more exciting.

- The function field is $k(x, y) = \mathbb{C}(x, y)$ where $x = X/Z$ and $y = Y/Z$ satisfy the relation $y^2 = x^3 + x$.
- For $\gamma = Y/Z = y$, we have $k(\gamma) = \mathbb{C}(y)$ and so $[k(C) : k(\gamma)] = [\mathbb{C}(x, y) : \mathbb{C}(y))] =$

Divisors of Functions, XII: Something About Clocks

For $C = V(Y^2Z - X^3 - XZ^2)$ the situation is a bit more exciting.

- The function field is $k(x, y) = \mathbb{C}(x, y)$ where $x = X/Z$ and $y = Y/Z$ satisfy the relation $y^2 = x^3 + x$.
- For $\gamma = Y/Z = y$, we have $k(\gamma) = \mathbb{C}(y)$ and so $[k(C) : k(\gamma)] = [\mathbb{C}(x, y) : \mathbb{C}(y))] = 3$.
- Why does this extension have degree 3? Because it's generated by x, which is a root of the irreducible polynomial $p(t) = t^3 + t - y^2$ with coefficients in $\mathbb{C}(y)$.

Divisors of Functions, XIII: Lucky Thirteen

Let me do another example with $C = V(Y^2Z - X^3 - XZ^2)$, for the rational function $\delta = X/Z = x$.

- As before the function field is $k(x, y) = \mathbb{C}(x, y)$ where $x = X/Z$ and $y = Y/Z$ satisfy the relation $y^2 = x^3 + x$.
- For $\delta = X/Z = x$, we have $k(\gamma) = \mathbb{C}(x)$ and so $[k(C) : k(\gamma)] = [\mathbb{C}(x, y) : \mathbb{C}(x))] =$

Divisors of Functions, XIII: Lucky Thirteen

Let me do another example with $C = V(Y^2Z - X^3 - XZ^2)$, for the rational function $\delta = X/Z = x$.

- As before the function field is $k(x, y) = \mathbb{C}(x, y)$ where $x = X/Z$ and $y = Y/Z$ satisfy the relation $y^2 = x^3 + x$.
- For $\delta = X/Z = x$, we have $k(\gamma) = \mathbb{C}(x)$ and so $[k(C) : k(\gamma)] = [\mathbb{C}(x, y) : \mathbb{C}(x))] = 2$.
- Why does this extension have degree 2? Because it's generated by y, which is a root of the irreducible polynomial $p(t) = t^2 - x^3 - x$ with coefficients in $\mathbb{C}(x)$.

Divisors of Functions, XIV

Computing degrees for these types of extensions can be difficult. Here's one general case you can work out explicitly for yourself:

Exercise: For any field k, if $f(t), g(t) \in k[t]$ are relatively prime (t is an indeterminate), show $[k(t) : k(\frac{f(t)}{g(t)})] = \max(\deg f, \deg g)$.

[Hint: Use Gauss's lemma to show that $q(y) = f(y) - \frac{f(t)}{g(t)} g(y) \in k(\frac{f(t)}{g(t)})[y]$ is the minimal polynomial of t over $k(\frac{f(t)}{g(t)})$.]

This example generalizes the observation $[k(x) : k(x^3 - x)] = 3$.

Equivalence of Divisors, I: Finally, Something Else

So, the main takeaway right now is that the divisor of an element $a \in k(C)^\times$ always has degree 0, which is to say, the principal divisors are actually a subgroup of the group of degree-0 divisors.

Definition

On a curve C/k, we say two divisors D_1 and D_2 are linearly equivalent (and write $D_1 \sim D_2$) if $D_1 - D_2$ is principal. The equivalence classes of divisors modulo principal divisors form a group called the class group, or the Picard group, of C.

Exercise: Verify that this relation is an equivalence relation and that the equivalence classes are the elements in the quotient group of divisors modulo principal divisors.

Equivalence of Divisors, II

There are a bunch of different groups of divisors. Let me summarize the notation for all of them:

- $\mathrm{Div}(C) = D_C$ is the group of all divisors on C.
- $\mathrm{Div}^0(C)$ is the group of degree-0 divisors on C.
- The principal divisors have no special notation.
- $\mathrm{Cl}(C) = \mathrm{Pic}(C) = \mathrm{Div}(C)/$[principal divisors] is the Picard group, or class group, of C.

Equivalence of Divisors, II

There are a bunch of different groups of divisors. Let me summarize the notation for all of them:

- $\mathrm{Div}(C) = D_C$ is the group of all divisors on C.
- $\mathrm{Div}^0(C)$ is the group of degree-0 divisors on C.
- The principal divisors have no special notation.
- $\mathrm{Cl}(C) = \mathrm{Pic}(C) = \mathrm{Div}(C)/$[principal divisors] is the Picard group, or class group, of C.

In fact, because principal divisors all have degree 0, we can actually take the quotient of degree-0 divisors by principal divisors:

- $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/$[principal divisors] is the reduced Picard group, or reduced class group, of C.

Equivalence of Divisors, III

For $\mathbb{P}^1$, the reduced Picard group is trivial:

Proposition (Reduced Picard Group of $\mathbb{P}^1$)

If $C = \mathbb{P}^1$, then $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/$[principal divisors] is the trivial group, and $\mathrm{Pic}(C) \cong \mathbb{Z}$.

- Once we show that $\mathrm{Pic}^0(C) = 0$, the statement that $\mathrm{Pic}(C) \cong \mathbb{Z}$ follows immediately from $\mathrm{Div}(C)/\mathrm{Div}^0(C) \cong \mathbb{Z}$.

Remark: It can be shown that the case $C = \mathbb{P}^1$ is essentially the only situation where the reduced Picard group is trivial. So do not be misled by the convenience of this particular result!

Equivalence of Divisors, IV

Proof:

- The result is equivalent to showing that every divisor of degree 0 is principal, so suppose $D = \sum_P b_P P$ has degree 0.
- For $P = [a : b] \in \mathbb{P}^1$ let $f_P = (bX - aY)/Y$, whose divisor is $\mathrm{div}(f_P) = P - P_\infty$.
- Now consider the rational function $\alpha = \prod_P f_P^{b_P}$: by the calculation above we have $\mathrm{ord}_P(\alpha) = b_P$ for each point $P \neq \infty$.
- But since $\sum_P b_P \deg(P) = 0$ by the assumption on D, and $\deg(\mathrm{div}(\alpha)) = 0$ as well, we must have $\mathrm{ord}_\infty(a) = b_\infty$ also.
- Then $\mathrm{ord}_P(\alpha) = b_p$ for all $P \in \mathbb{P}^1$, so $\mathrm{div}(\alpha) = D$ and so D is principal as claimed.

Equivalence of Divisors, V

We have a fundamental analogy between divisors on curves and ideals of algebraic number fields.

- If $K/\mathbb{Q}$ is an algebraic number field, we have an exact sequence $1 \to [\text{units of } \mathcal{O}_K] \to K^* \to [\text{fractional ideals of } \mathcal{O}_K] \to [\text{ideal class group of } K] \to 1$.
- If C is an algebraic curve defined over k, the analogous exact sequence is $1 \to k^* \to k(C)^* \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 1$.
- The constant field k plays the role of the units of an algebraic number field, the group of degree-0 divisors plays the role of the fractional ideals in the ring of integers, and the reduced Picard group plays the role of the ideal class group.

Orderings of Divisors, I

We now put a partial ordering on divisors that is motivated by the analogous idea of divisibility for integers and rational functions.

- The underlying idea is that if we want to understand divisibility for integers, we only need to compare the powers of each prime dividing the two integers: equivalently, we compare their p-adic valuations at each prime P.
- The analogous idea for functions would be to compare their order of vanishing at each point.
- As a particular special case, we can identify the elements of $\mathbb{Z}$ as those whose valuations are nonnegative at every finite prime p.
- The same principle holds for considering valuations of a rational function at points on an algebraic curve C: we can identify polynomial functions as those having no poles except at the points at ∞.

Orderings of Divisors, II

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.

Exercise (easy): Check that the relation $D_1 \leq D_2$ is a partial ordering on divisors.

Orderings of Divisors, II

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.

Exercise (easy): Check that the relation $D_1 \leq D_2$ is a partial ordering on divisors.

The partial ordering on divisors allows us to specify the order of zeroes and poles.

- To illustrate, for $\mathbb{A}^1$, saying that f has a pole of order at most 2 at $x = 0$ and a zero of order at least 3 at $x = 1$ is equivalent to saying $\mathrm{div}(f) \geq 2P_0 - 3P_1$.

Orderings of Divisors, III

Definition

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

- Equivalently, an element $\alpha \in k(C)^\times$ is in $L(D)$ if and only if $v_P(a) \geq -v_P(D)$ at all points $P \in C$.
- When D is an effective divisor, $L(D)$ represents all rational functions whose poles are "no worse" than D.

Orderings of Divisors, III

Definition

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

- Equivalently, an element $\alpha \in k(C)^\times$ is in $L(D)$ if and only if $v_P(a) \geq -v_P(D)$ at all points $P \in C$.
- When D is an effective divisor, $L(D)$ represents all rational functions whose poles are "no worse" than D.
- More generally, if $D = \sum_P n_P P - \sum_Q m_Q Q$ with $n_i, m_i > 0$, then $L(D)$ consists of all $\alpha \in k(C)^\times$ such that α has a zero of order at least m_Q at each point Q, and may have poles only at the points P, of order at most n_P at P.

Orderings of Divisors, IV

It is not hard to see that $L(D)$ is a k-vector space:

- Explicitly, suppose $\alpha, \beta \in L(D)$.
- Then $\alpha + \beta \in L(D)$ because $v_P(\alpha + \beta) \geq \min(v_P(\alpha), v_P(\beta)) \geq -v_P(D)$ for each point P.
- Likewise, for any $c \in k$, we see that $c\alpha \in L(D)$ because $v_P(c\alpha) = v_P(c) + v_P(\alpha) = v_P(\alpha) \geq -v_P(D)$ since $v_P(c) = 0$ at all points P.

Orderings of Divisors, V

Example: For $C = \mathbb{A}^1$, find $L(P_0)$.

Orderings of Divisors, V

Example: For $C = \mathbb{A}^1$, find $L(P_0)$.

- The only possible poles of an element $f/g \in L(P_0)$ function can occur at $x = 0$ (of order 1), so the denominator divides x. So we can just assume $g = x$, if we don't require the ratio in lowest terms.
- Also, because $\mathrm{ord}_{P_\infty}(f/g) = \deg g - \deg f$, we must have $1 = \deg g \geq \deg f$ since there is no pole at ∞.
- So the only possible f/g are of the form $\dfrac{ax+b}{x}$. Since all such functions are in $L(P_0)$, we see that $L(P_0) = \mathrm{span}(1, x^{-1})$.

Orderings of Divisors, VI

Example: For $C = \mathbb{A}^1$, find $L(3P_\infty)$.

Orderings of Divisors, VI

Example: For $C = \mathbb{A}^1$, find $L(3P_\infty)$.

- The only poles of an element $f/g \in L(3P_\infty)$ are allowed to be at ∞ of order at most 3, and so since there are no finite poles, g cannot have any roots, so we can just take $g = 1$: thus f/g is a polynomial.
- Again because $\mathrm{ord}_{P_\infty}(f/g) = \deg g - \deg f$, we must have $\deg f \leq 3$, so the only possible functions are polynomials of degree at most 3.
- Since all such functions are in $L(3P_\infty)$, we see that $L(3P_\infty) = \mathrm{span}(1, x, x^2, x^3)$.

Orderings of Divisors, VII

Example: For $C = \mathbb{A}^1$, find $L(-P_0)$.

Orderings of Divisors, VII

Example: For $C = \mathbb{A}^1$, find $L(-P_0)$.

- Any nonzero element $f/g \in L(-P_0)$ would need to be zero at $x = 0$ and defined at all other points.
- In particular that means g would have to be constant (otherwise as before any zeroes would yield poles of f/g) and f would be divisible by x.
- But then $\deg f > \deg g$ and this would force f/g to have a pole at P_∞, which is not allowed.
- So in fact, here $L(-P_0) = \{0\}$.

Orderings of Divisors, VIII

Example: For arbitrary C/k, find $L(0)$.

Orderings of Divisors, VIII

Example: For arbitrary C/k, find $L(0)$.

- Since $\mathrm{div}(c) = 0$ for all $c \in k^\times$, we see all the constants are in $L(0)$.
- However, any nonconstant rational function $x \in k(C)^\times \backslash k$ necessarily has at least one pole (its degree as a rational function must be positive, and then any zero of the denominator yields a pole – remember that we are working projectively!).
- Therefore the only elements of $L(0)$ are the constants, meaning $L(0) = k$.

Orderings of Divisors, VIII

Example: For arbitrary C/k, find $L(0)$.

- Since $\mathrm{div}(c) = 0$ for all $c \in k^\times$, we see all the constants are in $L(0)$.
- However, any nonconstant rational function $x \in k(C)^\times \backslash k$ necessarily has at least one pole (its degree as a rational function must be positive, and then any zero of the denominator yields a pole – remember that we are working projectively!).
- Therefore the only elements of $L(0)$ are the constants, meaning $L(0) = k$.

Exercise: Determine $L(D)$ when $C = \mathbb{A}^1(\mathbb{C})$ for $D = P_0 - P_\infty$, $P_0 + P_\infty$, and $P_0 + P_1$.

Orderings of Divisors, IX

We can also consider Riemann-Roch spaces over non-algebraically-closed fields.

- The only alteration to considering $L_E(D)$ for some subfield E of its algebraic closure k is that $L_E(D) = \{\alpha \in E(C)^\times : \mathrm{div}(\alpha) \geq -D\} \cup \{0\}$ consists only of the elements of the function field that are defined over E that satisfy the required divisor inequality.

Orderings of Divisors, X

Examples: Consider $C = \mathbb{A}^1$ and $D = P_\infty - P_i$.

- Over the field $\mathbb{R}$, we have $L_{\mathbb{R}}(D) = \{0\}$.
- Why? Any such rational function f/g would necessarily be a polynomial in $\mathbb{R}[x]$ of degree at most 1 (since it could only have a pole of order 1 at ∞).
- It would also have to be zero at $x = i$, but any such polynomial would also be zero at $x = -i$ meaning that its degree is at least 2: too big.

Orderings of Divisors, X

Examples: Consider $C = \mathbb{A}^1$ and $D = P_\infty - P_i$.

- Over the field $\mathbb{R}$, we have $L_{\mathbb{R}}(D) = \{0\}$.
- Why? Any such rational function f/g would necessarily be a polynomial in $\mathbb{R}[x]$ of degree at most 1 (since it could only have a pole of order 1 at ∞).
- It would also have to be zero at $x = i$, but any such polynomial would also be zero at $x = -i$ meaning that its degree is at least 2: too big.
- In contrast, over $\mathbb{C}$, we see that $L_{\mathbb{C}}(P_\infty - P_i) = \mathrm{span}(i - x)$.

Note that the field of definition affects the dimension of the space here: that is because the divisor $P_\infty - P_i$ is not defined over $\mathbb{R}$.

Orderings of Divisors, XI

Examples: Consider $C = \mathbb{A}^1$ and $D = 2P_\infty - P_i - P_{-i}$.

- Over the field $\mathbb{R}$, we have $L_\mathbb{R}(D) = \mathrm{span}(1 + x^2)$.
- Why? As in the last example, any element would be a real polynomial of degree at most 2 that is zero at both $x = i$ and $x = -i$, hence is a multiple of $1 + x^2$.

Orderings of Divisors, XI

Examples: Consider $C = \mathbb{A}^1$ and $D = 2P_\infty - P_i - P_{-i}$.

- Over the field $\mathbb{R}$, we have $L_\mathbb{R}(D) = \mathrm{span}(1 + x^2)$.
- Why? As in the last example, any element would be a real polynomial of degree at most 2 that is zero at both $x = i$ and $x = -i$, hence is a multiple of $1 + x^2$.
- Over $\mathbb{C}$ the same logic applies to show that we see that $L_\mathbb{C}(2P_\infty - P_i - P_{-i}) = \mathrm{span}(1 + x^2)$ as well.

Here, the field of definition does not affect the dimension of the space because the divisor $2P_\infty - P_i - P_{-i}$ is defined over $\mathbb{R}$.

Exercise: Suppose E is a subfield of k and D is a divisor of k that is defined over E. Show that $\dim_k[L_k(D)] = \dim_E[L_E(D)]$. [Hint: Show that a basis for L_E remains a basis over L_k.]

Summary

We introduced divisors on curves and established some of their basic properties.

We discussed principal divisors and effective divisors, and used them to write down Riemann-Roch spaces $L(D)$.

Next lecture: the Riemann-Roch theorem, elliptic curves via Riemann-Roch.