Elliptic curves over function fields 2

Douglas Ulmer

Georgia Institute of Technology

and

The University of Arizona

Arizona's First University.

July 7, 2009

Overview

The goal today is to discuss surfaces; Tate's conjectures relating divisors, cohomology, and zetas; and Tate's theorem on products of curves.

There will be more algebraic geometry than in the previous lecture, but I hope to make the main ideas understandable to those without extensive background.

Motivation

If we think of the equation

$$y^2 + xy = x^3 + t$$

as having coefficients in $K = k(t)$, then we are looking at a curve, an elliptic curve. If we think of it as an equation with coefficients in k, then we are considering a surface. Obviously there will be close connections between the curve and the surface. Today we'll look at general surfaces over k; next time we'll deduce consequences for elliptic curves over $k(t)$ and more general function fields.

Divisors on surfaces

Throughout, k will be a field, often finite. Let S be a surface, namely a non-singular, projective, absolutely irreducible variety of dimension 2 defined over k.

A prime divisor $C \subset S$ is an irreducible, reduced, closed subset of dimension 1. A divisor is a $\mathbb{Z}$-linear combination of prime divisors. Since S is non-singular, C is defined locally by one equation (i.e., Cartier and Weil divisors are the same here.)

We write

$$D = \sum_{C} n_C C.$$

Linear equivalence

If C is a prime divisor on S and f is a non-zero rational function on S, then we have a well defined $\mathrm{ord}_C(f)$, the order of zero or pole of f along C.

The divisor of a non-zero rational function is

$$\mathrm{div}(f) = \sum_C \mathrm{ord}_C(f) C.$$

We say that a divisors D and D' are linearly equivalent if their difference is the divisor of a rational function: $D - D' = \mathrm{div}(f)$.

Exercise: This is the same as saying that there is a family of divisors D_x parameterized by $x \in \mathbb{P}^1$ such that $D_0 = D$ and $D_\infty = D'$.

Pic(S) is by definition the group of divisors modulo linear equivalence.

Algebraic equivalence

Assume that k is algebraically closed. We declare that two divisors are algebraically equivalent if they lie in a family of divisors parameterized by a curve.

The Néron-Severi group of $NS(S)$ is by definition the group of divisors modulo algebraic equivalence. It is obviously a quotient of $\mathrm{Pic}(S)$.

For general k, we define $NS(S)$ as the image of $\mathrm{Pic}(S)$ in $NS(\overline{S})$.

We define $\mathrm{Pic}^0(S)$ to make the sequence

$$0 \to \mathrm{Pic}^0(S) \to \mathrm{Pic}(S) \to NS(S) \to 0$$

exact.

Examples

If $S = \mathbb{P}^2$, then $\mathrm{Pic}(S) = NS(S) = \mathbb{Z}$. The class of a plane curve is its degree.

If E_1 and E_2 are elliptic curves and $S = E_1 \times E_2$, then $\mathrm{Pic}^0(S) \cong E_1 \times E_2$ and $NS(S) \cong \mathbb{Z}^2 \times \mathrm{Hom}(E_1, E_2)$. The projection onto $\mathrm{Hom}(\cdots)$ sends a divisor to the action of the induced correspondence. Note the arithmetic nature of $NS(S)$.

If C_1 and C_2 are curves each with a k-rational point, then $NS(C_1 \times C_2) \cong \mathbb{Z}^2 \times \mathrm{Hom}(J_{C_1}, J_{C_2})$.

In general, $\mathrm{Pic}^0(S)$ is closely related to an abelian variety and $NS(S)$ is a finitely generated abelian group. NS is analogous to a Mordell-Weil group (this is in fact more than an analogy) and is considered to be hard to compute.

Cohomology

For $\ell \neq \text{char}(k)$, general machinery gives us ℓ-adic cohomology groups $H^i(\overline{S}, \mathbb{Q}_\ell)$ which are finite dimensional $\mathbb{Q}_\ell$-vector spaces with a continuous action of $G = \text{Aut}(\overline{k}/k)$. They vanish unless $0 \leq i \leq 4 = 2 \dim S$.

Tate twists:

$$\mathbb{Z}_\ell(1) = \left(\operatorname*{proj\,lim}_{n} \mu_{\ell^n}\right) \quad \text{and} \quad \mathbb{Z}_\ell(m) = \mathbb{Z}_\ell(1)^{\otimes m}$$

These are legitimate coefficients and we have

$$H^i(\overline{S}, \mathbb{Z}_\ell(m)) \cong H^i(\overline{S}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(m) =: H^i(\overline{S}, \mathbb{Z}_\ell)(m).$$

Similarly for $\mathbb{Q}_\ell(m)$.

Cycle classes

Divisors on S have classes in $H^2(\overline{S}, \mathbb{Z}_\ell(1))$.

Take cohomology of

$$0 \to \mu_{\ell^n} \to \mathbb{G}_m \to \mathbb{G}_m \to 0$$

and an inverse limit to get

$$H^1(\overline{S}, \mathbb{G}_m) \hat{\otimes} \mathbb{Z}_\ell \to H^2(\overline{S}, \mathbb{Z}_\ell(1))$$

and note that

$$H^1(\overline{S}, \mathbb{G}_m) \hat{\otimes} \mathbb{Z}_\ell \cong \mathrm{Pic}(\overline{S}) \hat{\otimes} \mathbb{Z}_\ell \cong NS(\overline{S}) \otimes \mathbb{Z}_\ell.$$

Then use $NS(S) \hookrightarrow NS(\overline{S})$.

Tate's conjecture T_1

The image of the cycle class map obviously lands in the G-invariant part of cohomology. The conjecture says that when k is finitely generated, they are the same:

$$NS(S) \otimes \mathbb{Q}_\ell \cong H^2(\overline{S}, \mathbb{Q}_\ell(1))^G.$$

When k is finite, working a bit more we get an exact sequence

$$0 \to NS(S) \otimes \mathbb{Z}_\ell \to H^2(\overline{S}, \mathbb{Z}_\ell(1))^G \to T_\ell Br(S) \to 0$$

where $Br(S) = H^2(S, \mathbb{G}_m)$ is the (cohomological) Brauer group. It follows that Rank $NS(S) \leq \dim H^2(\overline{S}, \mathbb{Q}_\ell(1))^G$ with equality iff the ℓ part of $Br(S)$ is finite.

It turns out (see below) that if this happens for one ℓ, then it happens for all ℓ and $Br(S)$ is finite.

Zetas

From now on we take k finite. As usual,

$$Z(S,T) = \prod_{\text{closed } x} \left(1 - T^{\deg(x)}\right)^{-1} = \exp\left(\sum_{n\geq 1} N_n \frac{T^n}{n}\right)$$

where N_n is the number of $\mathbb{F}_{q^n}$-valued points of C.

$\zeta(S,s) = Z(S, q^{-s})$ has good analytic properties (analytic continuation, functional equation, RH).

More precisely

$$Z(S,T) = \frac{P_1(T)P_3(T)}{P_0(T)P_2(T)P_4(T)}$$

where $P_i(T) = \det(1 - T\,\mathrm{Fr}_q\,|H^i(\overline{S},\mathbb{Q}_\ell))$ and the analytic properties follow from this expression, PD, and RH.

Note that $-\operatorname{ord}_{s=1}\zeta(S,s)$ is the multiplicity of q as an eigenvalue of Fr on $H^2(\overline{S},\mathbb{Q}_\ell)$.

This is the same as the multiplicity of 1 as an eigenvalue of Fr on $H^2(\overline{S},\mathbb{Q}_\ell(1))$, and is $\geq$ the dimension of $H^2(\overline{S},\mathbb{Q}_\ell(1))^G$.

Tate's conjecture T_2

It says $-\operatorname{ord}_{s=1} \zeta(S, s) = \operatorname{Rank} NS(S)$.

Since we have a priori inequalities

$$\operatorname{Rank} NS(S) \leq \dim_{\mathbb{Q}_\ell} H^2(\overline{S}, \mathbb{Q}_\ell(1))^G \leq -\operatorname{ord}_{s=1} \zeta(S, s)$$

it's clear that T_2 implies T_1. It turns out that T_1 implies T_2 and since T_2 is independent of ℓ, so is T_1.

In the next lecture. we'll translate this string of inequalities into similar statements for Mordell-Weil, Selmer, and L-zeroes and this will yield several of the main theorems.

Properties of the Tate conjecture

T_1 is birationally invariant. More generally, if $X \to Y$ is a dominant rational map and T_1 holds for X, then it holds for Y.

For surfaces, both statements can be seen easily using the factorization of rational maps into blow ups along smooth centers. [sketch]

(See Tate's article in the Motives volume for a very elegant argument that works in the general case.)

This descent property will become our descent result for BSD.

Tate's theorem on products of curves

Let C_1 and C_2 be curves and assume for simplicity they have k-rational points. Then it follows from Tate's theorem on endomorphisms of abelian varieties that T_1 holds for $S = C_1 \times C_2$.

To see what's at issue, recall that

$$NS(C_1 \times C_2) \cong \mathbb{Z}^2 \times \mathrm{Hom}(J_{C_1}, J_{C_2})$$

and that

$$H^2(C_1 \times C_2) \cong \left(H^0(C_1) \otimes H^2(C_2)\right) \oplus \left(H^2(C_1) \otimes H^0(C_2)\right)$$
$$\oplus \left(H^1(C_1) \otimes H^1(C_2)\right)$$

Twisting and taking G-invariants, the first two terms match up trivially with the $\mathbb{Z}^2$.

Using auto-duality of Jacobians, the last term becomes

$$\left(H^1(C_1) \otimes H^1(C_2)\right)(1)^G \cong \mathrm{Hom}_G(H^1(C_1), H^1(C_2))$$
$$\cong \mathrm{Hom}_G(V_\ell J_{C_1}, V_\ell J_{C_2}).$$

Tate's general result on endomorphisms of abelian varieties over finite fields says

$$\mathrm{Hom}(J_{C_1}, J_{C_2}) \otimes \mathbb{Q}_\ell \tilde{\to} \mathrm{Hom}_G(V_\ell J_{C_1}, V_\ell J_{C_2})$$

and this is just what we need.

This argument can be used to show that T_1 for any product follows from T_1 for the factors.

[Remark on what is actually constructed in Tate's argument.]

[Zarhin and Faltings for general k]

DPC

Putting everything together we get a very useful result on the Tate conjecture: if S is dominated by a product of curves:

$$C_1 \times C_2 \dashrightarrow S$$

then T_1 holds:

$$\operatorname{Rank} NS(S) = \dim_{\mathbb{Q}_\ell} H^2(\overline{S}, \mathbb{Q}_\ell(1))^G$$

When k is finite, we also have T_2:

$$\operatorname{Rank} NS(S) = -\operatorname{ord}_{s=1} \zeta(S, s).$$