Rational points on algebraic curves
Lecture III, February 19, 1999

Ed Schaefer, Santa Clara University

Abstract:

In this third lecture, we prove that the Selmer group is finite and show that it can be computed locally using a finite set of primes. We then use the Weil pairing and a Kummer map to remove the cohomology groups from the computation of a Selmer group.

REVIEW

We have C/K and C'/K, K a number field, and both curves have genus g. Let $J = \mathrm{Jac}(C)$, $J' = \mathrm{Jac}(C')$ and $\phi_K : J' \to J$ be an isogeny with $qJ'[\phi] = 0$, q a prime. We want $J(K)/\phi J'(K)$ as a step in finding $J(K)$.

We have the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \to & J(K)/\phi J'(K) & \stackrel{\delta}{\to} & H^1(K, J'[\phi]) & \to & H^1(K, J')[\phi] & \to & 0 \\ & & \downarrow & & \downarrow \prod \mathrm{res}_{\mathfrak{p}} & \searrow \prod \alpha_{\mathfrak{p}} & \downarrow \prod \mathrm{res}_{\mathfrak{p}} & & \\ 0 & \to & \prod J(K_{\mathfrak{p}})/\phi J'(K_{\mathfrak{p}}) & \stackrel{\prod \delta_{\mathfrak{p}}}{\to} & \prod H^1(K_{\mathfrak{p}}, J'[\phi]) & \to & \prod H^1(K_{\mathfrak{p}}, J')[\phi] & \to & 0 \end{array}$$

Recall $S^{\phi}(J', K) = \ker \prod_{\mathfrak{p}} \alpha_{\mathfrak{p}} = \{\gamma \in H^1(K, J'[\phi]) \mid \mathrm{res}_{\mathfrak{p}}(\gamma) \in \delta_{\mathfrak{p}} J(K_{\mathfrak{p}}),\ \text{for all } \mathfrak{p}\}$.

PROPERTIES OF $J(K_{\mathfrak{p}}), \mathfrak{p}$ FINITE

$J(K_{\mathfrak{p}})$ and $J'(K_{\mathfrak{p}})$ have subgroups of the same finite index isomorphic to $\mathcal{O}_{K_{\mathfrak{p}}}^g$, where $\mathcal{O}_{K_{\mathfrak{p}}}$ is the integer ring in $K_{\mathfrak{p}}$. This is a result of Mattuck's. In addition, ϕ maps one subgroup to the other.

Lemma. Let $\mathfrak{p}|p \neq q$ be a finite prime. Then $\dim J(K_{\mathfrak{p}})/\phi J'(K_{\mathfrak{p}}) = \dim J'(K_{\mathfrak{p}})[\phi]$.

Proof. The following is a commutative diagram.

$$\begin{array}{ccccccccc} 0 & \to & 0 & \to & J'(K_{\mathfrak{p}}) & \to & \ker(\phi) & \to & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & \text{sbgp} & \to & J'(K_{\mathfrak{p}}) & \to & \text{finite quotient} & \to & 0 \\ & & \downarrow \phi & & \downarrow \phi & & \downarrow \phi & & \\ 0 & \to & \text{sbgp} & \to & J(K_{\mathfrak{p}}) & \to & \text{finite quotient} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & \to & 0 & \to & J(K_{\mathfrak{p}})/\phi J'(K_{\mathfrak{p}}) & \to & \mathrm{coker}(\phi) & \to & 0 \end{array}$$

Since the two finite quotients have the same size, the result follows from the snake lemma. End proof.

We can describe C by integral equations and reduce it modulo $\mathfrak{p}$. If the reduction is non-singular, we say C has good reduction at $\mathfrak{p}$.

If $\mathfrak{p} \mid p$ is a prime of good reduction, and k is the residue class field of $K_{\mathfrak{p}}$, then

$$0 \to J_1(K_{\mathfrak{p}}) \to J(K_{\mathfrak{p}}) \to J(k) \to 0$$

is exact and $J_1(K_{\mathfrak{p}})$ is a pro-p group.

Consequence: the prime-to-p part of $J(K_{\mathfrak{p}})_{\mathrm{tors}}$ injects to $J(k)$.

EXAMPLE

For $E: y^2+y=x^3-x$ the only bad prime is 37. The prime-to-2 part of $E(\mathbf{Q})_{\mathrm{tors}}$ injects into $E(\mathbf{F}_2)\cong \mathbf{Z}/5\mathbf{Z}$. The prime-to-3 part injects into $E(\mathbf{F}_3)\cong \mathbf{Z}/7\mathbf{Z}$. Thus $E(\mathbf{Q})_{\mathrm{tors}}=0$. End example.

SELMER GROUP IS FINITE

Let $\mathcal{K}$ be a number field or the completion of a number field, and $\mathfrak{p}$ a prime of $\mathcal{K}$. Let M be a $\mathrm{Gal}(\overline{\mathcal{K}}/\mathcal{K})$-module. Let $\xi\in H^1(\mathcal{K},M)$ and $I_{\mathfrak{p}}$ denote the inertia group. We say ξ is unramified at $\mathfrak{p}$ if $\mathrm{res}(\xi)=0\in H^1(I_{\mathfrak{p}},M)$.

Let S denote the set of primes of K including primes at which C does not have good reduction, primes over q, and if $q=2$, real primes also.

Proposition. Let $\mathfrak{p}\notin S$ and let $R\in J(K_{\mathfrak{p}})$. Then $\delta_{\mathfrak{p}}(R)\in H^1(K_{\mathfrak{p}},J'[\phi])$ is unramified at $\mathfrak{p}$.

Proof. If q is odd and $\mathfrak{p}$ is infinite, then the exponents of $\mathrm{Gal}(\mathbf{C}/K_{\mathfrak{p}})$ and $J'[\phi]$ are relatively prime so $H^1(\mathrm{Gal}(\mathbf{C}/K_{\mathfrak{p}}),J'[\phi])$ is trivial. Assume $\mathfrak{p}\notin S$ is finite. Let $Q\in J'$ with $\phi Q=R$. Then $\delta_{\mathfrak{p}}(R)=[\sigma\mapsto\sigma Q-Q]$, where $\sigma Q-Q\in J'[\phi]$. Let $\sigma\in I_{\mathfrak{p}}$. In the reduction we have $\overline{\sigma Q-Q}=\sigma\overline{Q}-\overline{Q}=0$. If $\mathfrak{p}|p$ where p is a prime of $\mathbf{Q}$, then $\sigma Q-Q$ is a prime-to-p torsion point. The prime-to-p torsion points inject to the reduction, so $\sigma Q-Q=0$. End proof.

Corollary. If $P\in J[q]$, then $K(P)/K$ is unramified outside S.

Proposition. Let $\mathfrak{p}\notin S$. Then $\delta_{\mathfrak{p}}J(K_{\mathfrak{p}})/\phi J'(K_{\mathfrak{p}})$ is the unramified part of $H^1(K_{\mathfrak{p}},J'[\phi]))$.

Proof. From the last proposition, we know that the image is contained in the unramified part. It suffices to show they have the same size. A straightforward exercise shows that $H^1(\mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{unr}}/K_{\mathfrak{p}}),J'[\phi])$ is isomorphic to $J'[\phi]/(\mathrm{Frob}_{K_{\mathfrak{p}}}-1)J'[\phi]$ by the map sending $[\xi]\mapsto\xi(\mathrm{Frob}_{K_{\mathfrak{p}}})$. The groups $J'[\phi]/(\mathrm{Frob}_{K_{\mathfrak{p}}}-1)J'[\phi]$ and $J'(K_{\mathfrak{p}})[\phi]$ have the same size. From earlier, the groups $J'(K_{\mathfrak{p}})[\phi]$ and $J(K_{\mathfrak{p}})/\phi J'(K_{\mathfrak{p}})$ have the same size. End proof.

Let $H^1(K,J'[\phi];S)$ denote the subgroup of $H^1(K,J'[\phi])$ that is unramified outside S.

Corollary. $S^{\phi}(J',K)\cong\{\gamma\in H^1(K,J'[\phi];S)\mid \mathrm{res}_{\mathfrak{p}}(\gamma)\in\delta_{\mathfrak{p}}J(K_{\mathfrak{p}})\,\text{all}\,\mathfrak{p}\in S\}$.

This is true because for primes outside S, being in the image of $J(K_{\mathfrak{p}})$ is the same as being unramified. We now have

$$\begin{array}{ccc} J(K)/\phi J'(K) & \xrightarrow{\delta} & H^1(K,J'[\phi];S) \\ \downarrow & & \prod \mathrm{res}_{\mathfrak{p}} \\ \prod_{\mathfrak{p}\in S} J(K_{\mathfrak{p}})/\phi J'(K_{\mathfrak{p}}) & \xrightarrow{\prod\delta_{\mathfrak{p}}} & \prod_{\mathfrak{p}\in S} H^1(K_{\mathfrak{p}},J'[\phi]). \end{array}.$$

Proposition: $S^{\phi}(J',K)$ is finite.

Proof. We will show $H^1(K,J'[\phi];S)$ is finite. Let $M=K(J'[\phi],\mu_q)$ and $\dim_{\mathbf{F}_q}J'[\phi]=d$. The following is an inflation-restriction sequence

$$0\to H^1(\mathrm{Gal}(M/K),J'[\phi])\to H^1(K,J'[\phi];S)\to H^1(M,J'[\phi];S)$$

and $H^1(\mathrm{Gal}(M/K),J'[\phi])$ is finite. Now

$$H^1(M,J'[\phi];S)\cong\mathrm{Hom}(\mathrm{Gal}(\overline{M}/M),J'[\phi];S)\cong\mathrm{Hom}(\mathrm{Gal}(M'/M),J'[\phi])$$

where M' is the maximal abelian extension of M, unramified outside S with Galois group of exponent q. From algebraic number theory we know that M' is a finite extension of M. End proof.

Traditionally Selmer groups were computed using homogeneous spaces. This is all right for elliptic curves. However already for genus 2 curves, the description of the homogeneous spaces is unwieldy. We would like to find another way to compute Selmer groups.

REMOVING COHOMOLOGY

Goal: Define a finitely generated K-algebra L and a map F, derived from functions on C, so that we have a diagram of the following sort.

$$\begin{array}{ccccc} & & H^1(K, J'[\phi]) & \rightarrow & ``H^1(K,\mu_q)'' & & \\ & \delta \nearrow & & & & \searrow & \\ J(K)/\phi J'(K) & & & \overset{F}{\hookrightarrow} & & & L^*/L^{*q} \end{array}$$

The map from "$H^1(K,\mu_q)$" to L^*/L^{*q} will be some kind of Kummer map. We need a map, then from $J'[\phi]$ to μ_q.

WEIL PAIRING

There is a pairing $e_\phi : J'[\phi] \times \hat{J}[\hat{\phi}] \to \mu_q(\overline{K})$. I will not use the general definition for Weil pairings on an abelian variety. Instead I will show how to compute it for Jacobians. The Weil pairing has the following properties.

1. Bilinear.

2. Non-degenerate.

3. Galois-invariant: If $\sigma \in \mathrm{Gal}(\overline{K}/K)$ then $\sigma e_\phi(P,Q) = e_\phi(\sigma P, \sigma Q)$.

4. Compatible: If $J'' \xrightarrow{\tau} J' \xrightarrow{\phi} J$ and $P \in J''[\phi\circ\tau]$, $Q \in \hat{J}[\hat{\phi}]$, then $e_{\phi\circ\tau}(P,Q) = e_\phi(\tau P, Q)$.

5. Let $J' = J$, and $\phi = q$. Let $P, Q \in J[q]$. Note $\lambda^{-1}\hat{J}[\hat{q}] = J[q]$. Let $e_q^\lambda : J[q] \times J[q] \to \mu_q$ by $e_q^\lambda(P,Q) = e_q(P, \lambda Q)$.

Let D_P and D_Q be degree 0 divisors representing P and Q with disjoint support. Lang showed that in any divisor class you can find a divisor whose support avoids any given finite set of points. Then $qD_P = div(f_P)$ and $qD_Q = div(f_Q)$. We have $e_q^\lambda(P,Q) = f_Q(P)/f_P(Q)$. Note $(f_Q(P)/f_P(Q))^q = f_Q(qP)/f_P(qQ) = f_Q(div(f_P))/f_P(div(f_Q)) = 1$ from Weil reciprocity.
End properties.

Say we have $\phi : J' \to J$, and $qJ'[\phi] = 0$ and we want to compute the ϕ-Weil pairing. There is an isogeny $\tau : J \to J'$ such that $\tau\circ\phi = q$ on J' and $\phi\circ\tau = q$ on J. We can use properties 4 and 5 to evaluate the ϕ-Weil pairing.

CHOICE OF F AND L

We will Weil pair something from $J'[\phi]$ with something from $\hat{J}[\hat{\phi}]$. It is easier to work with J than its dual. There is a canonical principal polarization λ, defined over K, coming from the curve C. It is an isomorphism of J with $\hat{J}$.

$$\begin{array}{ccc} J' & \stackrel{\phi}{\to} & J \\ & & \downarrow \lambda_K \\ \hat{J}' & \stackrel{\hat{\phi}}{\leftarrow} & \hat{J} \end{array}$$

Step 1. Determine the image of $\lambda^{-1}(\hat{J}[\hat{\phi}]) \subset J[q]$. If $\phi = q$, then we have equality. We will see a non-trivial example later.

Step 2. Choose $\{D_1, \dots, D_n\}$, $D_i \in \mathrm{Div}^0(C)$ a $\mathrm{Gal}(\overline{K}/K)$-invariant set, for which $\{[D_1], \dots, [D_n]\}$ spans $\lambda^{-1}\hat{J}[\phi]$. The choice determines F and L. By abuse of notation, let P_L denote this set of divisors and divisor classes.

Let $qD_i = \mathrm{div}(f_i)$ where f_i has the same field of definition as D_i (existence guaranteed by Hilbert-90).

Step 3. Determine F and L. First assume $\{D_1, \dots, D_n\}$ is single Galois-orbit. Let $L = K(f_1)$ and Galois act trivially on L.

Let $L' = L \otimes_K \overline{K} \cong \prod_{i=1}^{n} \overline{K}$. In the tensor product, we let $\mathrm{Gal}(\overline{K}/K)$ act on the second coordinate. This induces an action on the product where $\mathrm{Gal}(\overline{K}/K)$ both acts on coordinates and permutes coordinates in the same manner that it permuts the n-tuple $(D_1, \dots, D_n)$. If there are several orbits, then for the ith orbit define L_i and F_i and let $L = \prod L_i$, $F = \prod F_i$.

Let us leave the steps for a moment and verify that everything is well-defined. We have an algebra L, and so far, F is only defined on (most) points C. We want F to be defined on $J(K)/\phi J'(K)$.

We call $D \in \mathrm{Div}^0(C)(K)$ a good divisor if the support of D does not intersect the supports of the D_i's.

Clearly F is a homomorphism from good divisors to L^*.

Assumption I. Every element of $J(\mathcal{K})/\phi J'(\mathcal{K})$ is represented by a good divisor for $\mathcal{K} = K$, $K_s, s \in S$.

¿From Joost's talk, we see that if q does not divide

$$\gcd\{[K' : K] \mid K \subseteq K' \subseteq \overline{K}, C(K') \text{ nonempty }\}$$

then assumption I holds. In particular, if C has a rational point over K, then assumption I holds.

Propostion. F induces a homomorphism from the subgroup of $J(K)/qJ(K)$ represented by good divisors to L^*/L^{*q}.

Proof: Let D and D' be linearly equivalent good divisors. Let h be a function on C, defined over K, with $\mathrm{div}(h) = D - D'$. Using Weil reciprocity, we have the following equalities of n-tuples

$$F(D - D') = F(\mathrm{div}(h)) = h(\mathrm{div}(F)) = h(qP_L) = h(P_L)^q \in L^{*q}.$$

End proof.

CONNECT F TO COHOMOLOGY MAPS

Define $w : J'[\phi] \to \mu_q(L') \cong \prod^n \mu_q(\overline{K_i})$ by $w(P) = (e_\phi(P, \lambda[D_1]), \ldots, e_\phi(P, \lambda[D_n]))$. We will denote this $w(P) = e_\phi(P, \lambda P_L)$.

The map w is injective from the non-degeneracy of the Weil pairing. It is also defined over K. This is a straightforward exercise comparing the action of Galois on L' with the Galois-invariance property of the Weil pairing. Let $H^1(K, J'[\phi]) \stackrel{\overline{w}}{\to} H^1(K, \mu_q(L'))$.

Since L' is a finitely generated $\overline{K}$-algebra with unit, it is also true that $H^1(K, L'^*) = 0$. Thus we have an isomorphism $k : H^1(K, \mu_q(L')) \cong L^*/L^{*q}$.

Theorem: F and $k \circ \overline{w} \circ \delta$ are same as maps from $J(K)/\phi A(K)$ to L^*/L^{*q}.

We will start the next lecture by proving this.