Rational points on algebraic curves
Lecture IV, March 5, 1999

Ed Schaefer, Santa Clara University

Abstract:

In this fourth talk, we will start by showing the that map F, coming from functions on the curve, is indeed relating to a coboundary map, a map induced by a Weil pairing and a Kummer map. We will apply the algorithm developed thus far to cyclic covers of the projective line with a rational Weierstrass point. This class of curves includes elliptic curves.

REVIEW

We have two curves C/K and C'/K, where K is a number field, both with genus g. We have an isogeny $\phi : J' \to J$, defined over K, with $qJ'[\phi] = 0$ where q is prime. We want to find $J(K)/\phi J'(K)$ as a step in determining $J(K)$. We have

$$J(K)/\phi J'(K) \quad \hookrightarrow \quad H^1(K, J'[\phi]; S)$$

where S consists of the primes where C' has singular reduction, primes lying over q and if $q = 2$, real primes also.

Let $P_L = \{D_1, \ldots , D_n\}$ with $D_i \in \mathrm{Div}^0(C)$, a Galois-invariant set, where the set $\lambda P_L = \{\lambda[D_1], \ldots , \lambda[D_n]\}$ spans $\hat{J}[\hat{\phi}]$. The map λ is the canonical principal polarization of J, coming from its being the Jacobian of C. It is an isomorphism, over K, of J with its dual.

We let $\mathrm{div}(f_i) = qD_i$ with $K(f_i) = K(D_i)$. In addition, for each Galois-orbit of conjugate D_i's, the corresponding set of f_i's should be conjugate. We let $L = \prod K(f_i)$ and $F = \prod f_i$ where we take one representative from each Galois orbit for both products. A good divisor is K-rational, degree 0, and avoids the supports of the D_i's.

Assumption I: Each element of $J(K)/\phi J'(K)$ is represented by a good divisor.

We showed that $F : J(K)/qJ(K) \to L^*/L^{*q}$ is well-defined on the subgroup represented by good divisors. In the proofs, it is usually best to work with the n-tuples instead of products over orbits. Let $L' = L \otimes_K \overline{K} \cong \prod^n \overline{K}$. Define

$$w : J'[\phi] \to \mu_q(L') \ \text{ by } \ R \mapsto e_\phi(R, \lambda P_L) = (e_\phi(R, \lambda[D_1]), \ldots , e_\phi(R, \lambda[D_n])).$$

We also have $L \otimes \overline{K}(C) \cong \prod \overline{K}(C)$ and $F \mapsto (f_1, \ldots , f_n)$ so we write $\mathrm{div}(F) = qP_L$. This is a statement about n-tuples. We have

$$J(K)/\phi J'(K) \overset{\delta}{\hookrightarrow} H^1(K, J'[\phi]) \overset{\overline{w}}{\to} H^1(K, \mu_q(L')) \overset{k}{\cong} L^*/L^{*q}.$$

MAIN THEOREM

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

We will work with the multiplication by q map first. First, we have only shown that F is well defined on a subgroup of $J(K)/qJ(K)$. Second, we have a nice way of computing the Weil pairing for the multiplication by q map.

Proof. Let $\delta_q : J(K)/qJ(K) \to H^1(K, J[q])$ and $w_q : J[q] \to \mu_q(L')$ by $T \mapsto e_q(T, \lambda P_L)$. First we will show $F = k \circ \overline{w_q} \circ \delta_q$ on the subgroup of $J(K)/qJ(K)$ represented by good divisors.

Let R be a good divisor. We have $\delta_q([R]) = [\sigma \mapsto [\sigma Q - Q]]$ where Q is a degree 0 divisor, such that qQ is linearly equivalent to R. We can choose Q so that its support is disjoint from the $D_i's$. So $\overline{w_q} \circ \delta_q([R]) = [\sigma \mapsto e_q([\sigma Q - Q], \lambda P_L)] = [\sigma \mapsto e_q^{\lambda}([\sigma Q - Q], P_L)]$.

In order to use the Weil reciprocity definition of this Weil pairing, we need functions whose divisors are q times each of those divisors. Let $\mathrm{div}(g) = qQ - R$ with g defined over $K(Q)$. Then $\mathrm{div}(\sigma g) = q\sigma Q - R$ so $\mathrm{div}(\sigma g/g) = q\sigma Q - qQ$. Recall $\mathrm{div}(F) = qP_L$. We have the following equality of n-tuples

$$e_q^{\lambda}([\sigma Q - Q], P_L) = \frac{F(\sigma Q - Q)}{\sigma g/g(P_L)} = \frac{\sigma\beta}{\beta}$$

where $\beta = F(Q)/g(P_L)$. So $\overline{w_q} \circ \delta_q([R]) = [\sigma \mapsto \frac{\sigma\beta}{\beta}]$. Recall $k : H^1(K, \mu_q(L')) \cong L^*/L^{*q}$ by $[\sigma \mapsto \frac{\sigma \sqrt[q]{l}}{\sqrt[q]{l}}] \leftarrow l$. So

$$k \circ \overline{w_q} \circ \delta_q(R) = \beta^q = \frac{F(qQ)}{g(qP_L)} = \frac{F(qQ)}{F(qQ - R)} = F(R) \bmod L^{*q}.$$

Now we want to show that F and $k \circ \overline{w} \circ \delta$ are the same maps from $J(K)/\phi J'(K) \to L^*/L^{*q}$. Let $\tau : J \to J'$ with $\phi\tau = q$. We have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & J[q] & \to & J & \stackrel{q}{\to} & J & \to & 0 \\ & & \downarrow \tau & & \downarrow \tau & & \downarrow 1 & & \\ 0 & \to & J'[\phi] & \to & J' & \stackrel{\phi}{\to} & J & \to & 0. \end{array}$$

Take Galois-invariants we get

$$\begin{array}{ccc} J(K)/qJ(K) & \stackrel{\delta_q}{\hookrightarrow} & H^1(K, J[q]) \\ \downarrow & & \downarrow \tau \\ J(K)/\phi J'(K) & \stackrel{\delta}{\hookrightarrow} & H^1(K, J'[\phi]). \end{array}$$

From the compatibility of Weil pairings we have $e_q(T, \lambda P_L) = e_\phi(\tau(T), \lambda P_L)$. Thus the triangle in the following diagram commutes, so the whole diagram commutes.

$$\begin{array}{cccccccc} J(K)/qJ(K) & \stackrel{\delta_q}{\hookrightarrow} & H^1(K, J[q]) & \stackrel{\overline{w_q}}{\searrow} & & & \\ \downarrow & & \downarrow \tau & & H^1(K, \mu_q(L')) & \stackrel{k}{\to} & L^*/L^{*q}. \\ J(K)/\phi J'(K) & \stackrel{\delta}{\hookrightarrow} & H^1(K, J'[\phi]) & \stackrel{\nearrow}{\overline{w}} & & & \end{array}$$

Thus F factors through $\phi J'(K)$ and $F = k \circ \overline{w} \circ \delta$.
End proof.

Note that we can replace K by any completion of K in this theorem.

The maps k and δ are automatically injective. So F is injective if $\overline{w}$ is injective.

Assumption II. $\overline{w}$ is injective for K and $K_{\mathfrak{s}}$, $\mathfrak{s} \in S$.

APPLICATION TO SOME CYCLIC COVERS OF THE PROJECTIVE LINE

Let K be a number field and let $C = C' : y^q = f(x)$ where $\mu_q \subset K$, $f(x)$ is a monic, separable polynomial with K-integral coefficients, and $q \not| d = \deg(f)$. This includes elliptic curves and hyperelliptic curves with a rational Weierstrass point. Since f is separable, the projective curve defined by the affine equation $y^q = f(x)$ can only be singular at infinity. In the normalization, the smooth curve C has a single rational point ∞. Therefore assumption

I holds. From the Riemann-Hurwitz formula, the genus of C is $(q-1)(d-1)/2$. Let us find an isogeny. Isogenies of J to itself are called endomorphisms.

Let $\zeta = \zeta_q$ and $\tau : (x, y) \mapsto (x, \zeta y)$ be an automorphism of C. The automorphism τ induces an automorphism of divisors and sends principal divisors to principal divisors. Therefore τ induces an automorphism of J. The group J is generated by divisor classes of the form $[P - \infty]$ where $P \in C \setminus \infty$. We have

$$(\tau^{q-1} + \ldots + \tau + 1)[P - \infty] = [\tau^{q-1}P + \ldots + \tau P + P - q\infty] = [\mathrm{div}(x - x(P))] = 0.$$

Thus τ acts like a primitive qth root of unity in the endomorphism ring of J. By abuse of notation, we will sometimes denote τ by ζ. Let $\phi = 1 - \zeta \in \mathrm{End}(J)$. We need a Galois-invariant spanning set of $\lambda^{-1}\hat{J}[\hat{\phi}]$.

Proposition. $\lambda^{-1}\hat{J}[\hat{\phi}] = J[\phi]$.

Proof. We have

$$\begin{array}{ccc} J & \stackrel{1-\zeta}{\to} & J \\ \hat{J} & \stackrel{\widehat{1-\zeta}}{\leftarrow} & \hat{J} \end{array} \quad \text{and} \quad \begin{array}{ccc} J & & J \\ \lambda\downarrow & & \downarrow\lambda \\ \hat{J} & \stackrel{\widehat{1-\zeta}}{\leftarrow} & J. \end{array}$$

The endomorphism going from the right-hand J to the left-hand J making the right-hand diagram commute is, by definition, the image of $1-\zeta$ under the Rosati involution; it is denoted $(1-\zeta)^{\dagger}$.

$$\begin{array}{ccc} J & \stackrel{(1-\zeta)^{\dagger}}{\leftarrow} & J \\ \lambda\downarrow & & \downarrow\lambda \\ \hat{J} & \stackrel{\widehat{1-\zeta}}{\leftarrow} & J \end{array}$$

There is a theorem that states that if an automorphism of a Jacobian is induced by an automorphism of the curve, then the image of that automorphism under the Rosati involution is its inverse. Thus we have

$$\lambda^{-1}\hat{J}[\widehat{1-\zeta}] = J[(1-\zeta)^{\dagger}] = J[1-\zeta^{\dagger}] = J[1-\zeta^{-1}] = J[1-\zeta].$$

The last equality comes from the fact that $(1-\zeta^{-1})/(1-\zeta) = -1/\zeta$ is a unit. End proof.

In order to find a Galois-invariant spanning set of $J[\phi]$, we should know how big it is. We have $\phi^{q-1} = (1-\zeta)^{q-1} = \text{unit} \cdot q$. Since $\dim J[q] = 2g = (q-1)(d-1)$, we have $\dim J[\phi] = d-1$. Let α_i, for $1 \le i \le d$, denote a root of f.

Proposition. $[(\alpha_1, 0) - \infty], \ldots, [(\alpha_{d-1}, 0) - \infty]$ form a basis for $J[\phi]$.

Proof. (Michael Stoll) Let $\overline{K}(C)$ be the function field of C. We have the following two exact sequences

$$0 \to \overline{K}^* \to \overline{K}(C)^* \stackrel{\mathrm{div}}{\to} \mathrm{Princ} \to 0$$

$$0 \to \mathrm{Princ} \to \mathrm{Div}^0(C) \to J \to 0.$$

Let τ act on $\overline{K}(C)$ by fixing $\overline{K}(x)$, and $\tau(y) = \zeta^{-1}y$. Both are exact sequences of $\langle\tau\rangle$-modules. Taking $\langle\tau\rangle$-invariants we get

$$H^1(\langle\tau\rangle, \overline{K}(C)^*) \to H^1(\langle\tau\rangle, \mathrm{Princ}) \to H^2(\langle\tau\rangle, \overline{K}^*)$$

Since the action of $\langle\tau\rangle$ on $\overline{K}(C)^*$ is the same as the action of $\mathrm{Gal}(\overline{K}(C)/\overline{K}(x))$, the first cohomology group is trivial from Hilbert's theorem 90. Since $\langle\tau\rangle$ is a finite, cyclic group, $H^2(\langle\tau\rangle, \overline{K}^*) \cong \ker(\tau - 1)/\mathrm{im}(\mathrm{Norm}_\tau) = \overline{K}^*/\overline{K}^{*q} = 1$ and so $H^1(\langle\tau\rangle, \mathrm{Princ}) = 0$. Thus $\mathrm{Div}^0(C)^{\langle\tau\rangle}$ maps surjectively to $J^{\langle\tau\rangle} = J[\phi]$. So $J[\phi]$ is generated by τ-invariant divisors.

The group $\mathrm{Div}^0(C)^{\langle\tau\rangle}$ is generated by $P - \infty$ where $P \in C^{\langle\tau\rangle} \setminus \infty$ and $\mathrm{Norm}_\tau(P - \infty)$ for $P \in C \setminus C^{\langle\tau\rangle}$. Now $\mathrm{Norm}_\tau(P - \infty) = \mathrm{div}(x - x(P))$ so $J[\phi]$ is generated by $P - \infty$ where $P = (\alpha_i, 0)$. Since $\dim J[\phi] = d - 1$ and $\mathrm{div}(y) = (\alpha_1, 0) + \ldots + (\alpha_d, 0) - d\infty$, the result follows. End proof.

Thus $P_L = \{(\alpha_1, 0) - \infty, \ldots, (\alpha_d, 0) - \infty\}$ is a Galois-invariant spanning set of $J[\phi]$. Note $\mathrm{div}(x - \alpha_i) = q(\alpha_i, 0) - q\infty$. We will not worry about orbits for the moment; it is best to find L and F by thinking of n-tuples over an algebraic closure. The map $F \in L \otimes \overline{K}(C) \cong \prod \overline{K}(C)$ should be $(x - \alpha_1, \ldots, x - \alpha_d)$. So let $L = K[T]/(f(T))$ and $F = x - T$. The map $x - T$ is defined on good divisors, that is K-rational divisors of degree 0 whose supports avoid ∞ and points with y-coordinate 0. However, in practice, the K-rational, degree 0 divisors that you know about, typically have supports including ∞ or points with y-coordinate 0. The following proposition provides a time-saving alternative to finding linearly equivalent good divisors.

Proposition. Let $D = R_1 + \ldots + R_r - r\infty$ be defined over K, with $y(R_i) \neq 0$ and $R_i \neq \infty$. Then $x - T([D]) = \prod_{i=1}^{r} (x(R_i) - T) \ mod\ L^{*q}$.

Let $D = (\alpha_1, 0) + \ldots + (\alpha_r, 0) - r\infty$ be defined over K, with $r < d$. Then $x - T([D]) = \prod_{i=r+1}^{d} (\alpha_i - T)^{q-1} + \prod_{i=1}^{r} (\alpha_i - T) \ mod\ L^{*q}$.

This is proven by finding the images of linearly equivalent good divisors.

We have that the composition of maps

$$J(K)/\phi J(K) \overset{\delta}{\hookrightarrow} H^1(K, J[\phi]; S) \overset{k\circ\overline{w}}{\to} L^*/L^{*q}$$

is the same as the map $x - T$. We need make sure that $\overline{w}$ injective, i.e. that assumption II holds, and find the image of $H^1(K, J[\phi]; S)$ in L^*/L^{*q}. We have $S = \{\mathfrak{q}|q, \mathfrak{p}|\Delta(f), \text{real primes if } q = 2\}$. Let $L = K[T]/(f(T)) = \prod L_i$, number fields. Let $L_i(S, q)$ denote the subgroup of L_i^*/L_i^{*q} with the property that adjoining a qth root, gives an extension unramified outside S. Let $L(S, q) = \prod L_i(S, q)$.

Proposition. $H^1(K, J[\phi]; S) \cong \ker : L(S, q) \overset{norm}{\to} K^*/K^{*q}$.

Proof. First we will show that $0 \to J[\phi] \overset{w}{\to} \mu_q(L') \overset{norm}{\to} \mu_q(\overline{K}) \to 0$ is exact. The dimensions are $d - 1, d, 1$, respectively. The map w sends an element of $J[\phi]$ to its Weil pairing with $[(\alpha_i, 0) - \infty]$ in the ith coordinate of $\mu_q(L')$. In addition, $\mathrm{div}(y) = (\alpha_1, 0) + \ldots + (\alpha_d, 0) - d\infty$ so the $[(\alpha_i, 0) - \infty]$ sum to 0. The norm is the sum of coordinates and the Weil pairing is additive so the image of w is contained in the kernel of the norm. Since w and the norm respect Galois actions, it is an exact sequence of Galois-modules. Let Δ be the diagonal embedding of $\mu_q(\overline{K})$ in $\mu_q(L')$. Let $b \equiv d^{-1} (mod\ q)$. Then norm $\circ\, \Delta^b$ is the identity, so the exact sequence splits. Therefore the sequence of H^1's splits. We have that the following is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & H^1(K,J[\phi]) & \overset{\overline{w}}{\to} & H^1(K,\mu_q(L')) & \overset{norm}{\to} & H^1(K,\mu_q(\overline{K})) & \to & 0 \\ & & & & \cong & & \cong & & \\ & & & & L^*/L^{*q} & \overset{norm}{\to} & K^*/K^{*q} & & \end{array}$$

and restricting to parts unramified outside S we get that the following is also a commutative diagram.

$$\begin{array}{ccccccccc} 0 & \to & H^1(K,J[\phi];S) & \overset{\overline{w}}{\to} & H^1(K,\mu_q(L');S) & \overset{norm}{\to} & H^1(K,\mu_q(\overline{K})) & \to & 0 \\ & & & & \cong & & \cong & & \\ & & & & L(S,q) & \overset{norm}{\to} & K^*/K^{*q} & & \end{array}$$

End proof.

The same proof shows that $\overline{w}$ is injective, both globally and locally, so assumption II holds. There are examples of Jacobians and isogenies, for which the map $\overline{w}$ is not an injection. In addition, finding the image of $H^1(K,J[\phi];S)$ in L^*/L^{*q} is not always a trivial task. Michael Stoll and I have just figured out how to do it for elliptic curves and multiplication by q maps (where q is prime).

We can now use the following commutative diagram to define the Selmer group

$$\begin{array}{ccc} J(K)/\phi J(K) & \overset{x-T}{\hookrightarrow} & \ker : L(S,q) \overset{\text{norm}}{\to} K^*/K^{*q} \\ \downarrow & & \downarrow \\ \prod_{\mathfrak{p}\in S} J(K_{\mathfrak{p}})/\phi J(K_{\mathfrak{p}}) & \overset{x-T}{\hookrightarrow} & \prod_{\mathfrak{p}\in S} L_{\mathfrak{p}}^*/L_{\mathfrak{p}}^{*q} \end{array}$$

where $L_{\mathfrak{p}} = L \otimes_K K_{\mathfrak{p}}$.

Most pieces of the above diagram are under control. We can describe ker: $L(S,q) \overset{\text{norm}}{\to} K^*/K^{*q}$ and each $L_{\mathfrak{p}}^*/L_{\mathfrak{p}}^{*q}$ using algebraic number theory and a computer. How do we get from $J(K)/\phi J(K)$ to the Mordell-Weil rank and how do we get the sizes of the groups $J(K_{\mathfrak{p}})/\phi J(K_{\mathfrak{p}})$?

Proposition. Let $\zeta \in \mathcal{K}$ (a number field or the completion of a number field). Then $\dim J(\mathcal{K})/qJ(\mathcal{K}) - \dim J(\mathcal{K})[q] = (q-1)(\dim J(\mathcal{K})/\phi J(\mathcal{K}) - \dim J(\mathcal{K})[\phi])$.

The proof consists of an application of the snake lemma and rewriting sums.

Corollary. The Mordell-Weil rank of $J(K)$ is $(q-1)(\dim J(K)/\phi J(K) - \dim J(K)[\phi])$.

Proof. $J(K) \cong \mathbf{Z}^r \oplus J(K)_{\text{tors}}$. End proof.

Proposition. Let C/K, where K is a number field that does not necessarily contain ζ. The Mordell-Weil rank of $J(K)$ is the quotient of the Mordell-Weil rank of $J(K(\zeta))$ by $[K(\zeta):K]$.

I will not prove this. It is an exercise in linear algebra and cohomology and uses the fact that the Galois action on the subring $\mathbf{Z}[\tau]$ of the endomorphism ring is compatible with the action on the subring $\mathbf{Z}[\zeta]$ of the integer ring of K.

We will again assume that $\mu_q \subset K$.

Corollary (of two propositions ago). Let $\mathfrak{p} \not| q$, finite, then $\dim J(K_{\mathfrak{p}})/\phi J(K_{\mathfrak{p}}) = \dim J(K_{\mathfrak{p}})[\phi]$. Let $\mathfrak{q}|q$, then $\dim J(K_{\mathfrak{q}})/\phi J(K_{\mathfrak{q}}) = g[K_{\mathfrak{q}} : \mathbf{Q}_q(\zeta_q)] + \dim J(K_{\mathfrak{q}})[\phi]$.

Proof. The first statement comes from the last lecture. For the second statement, we use the following commutative diagram. The top row and bottom row consist of the kernels and cokernels of the multiplication by q map, respectively.

$$\begin{array}{ccccccccc}
0 & \to & 0 & \to & J(K_{\mathfrak{q}})[q] & \to & H_1 \to & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & (\mathcal{O}_{K_{\mathfrak{q}}})^g & \to & J(K_{\mathfrak{q}}) & \to & \text{finite quotient} & \to & 0 \\
 & & \downarrow q & & \downarrow q & & \downarrow q & & \\
0 & \to & (\mathcal{O}_{K_{\mathfrak{q}}})^g & \to & J(K_{\mathfrak{q}}) & \to & \text{finite quotient} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & \to & (\mathcal{O}_{K_{\mathfrak{q}}}/q\mathcal{O}_{K_{\mathfrak{q}}})^g & \to & J(K_{\mathfrak{q}})/qJ(K_{\mathfrak{q}}) & \to & H_2 & \to 0 &
\end{array}$$

From the snake lemma, the size of $J(K_{\mathfrak{p}})[q]$ times the size of $(\mathcal{O}_{K_{\mathfrak{q}}}/q\mathcal{O}_{K_{\mathfrak{q}}})^g$ times the size of H_2 is the same as the size of H_1 times the size of $J(K_{\mathfrak{q}})/qJ(K_{\mathfrak{q}})$. Since the finite quotient is finite, the sizes of the kernel (H_1) and cokernel (H_2) are the same; thus they cancel each other out. The size of $(\mathcal{O}_{K_{\mathfrak{q}}}/q\mathcal{O}_{K_{\mathfrak{q}}})^g$ is $(q^{[K_{\mathfrak{q}}:\mathbf{Q}_q]})^g$. Thus $\dim J(K_{\mathfrak{q}})/qJ(K_{\mathfrak{q}}) - \dim J(K_{\mathfrak{q}})[q] = g[K_{\mathfrak{q}} : \mathbf{Q}_q]$. Hence $(q-1)(\dim J(K_{\mathfrak{q}})/\phi J(K_{\mathfrak{q}}) - \dim J(K_{\mathfrak{q}})[\phi]) = g[K_{\mathfrak{q}} : \mathbf{Q}_q(\zeta_q)](q-1)$. End proof.

Proposition. If $C : y^2 = f(x)$ has genus g, where f is of odd degree, separable and has coefficients in $\mathbf{R}$, then $\dim J(\mathbf{R})/2J(\mathbf{R}) = \dim J(R)[2] - g$.