Rational points on algebraic curves
Lecture II, February 5, 1999

Ed Schaefer, Santa Clara University

**Abstract:**

In this second talk, we will first define Jacobians. In attempting to determine the structure of the Mordell-Weil group of a Jacobian, we are drawn into Galois cohomology. We will have a short course on Galois cohomolgy, covering just enough to get by. Putting local cohomological information together, we get a Selmer group. Selmer groups contain a quotient of the Mordell-Weil group and so are used to get an upper boundon the free **Z**-rank of the Mordell-Weil group. We will also define the obstruction between the Selmer group and the quotient of the Mordell-Weil group, which is a piece of the Tate-Shafarevich group.

**Divisors**

Let $C$ be a curve. A divisor is a formal finite sum of points. $\sum n_P P$. They are added in the obvious way and form a group, $\mathrm{Div}(C)$. The degree of $\sum n_P P$ is $\sum n_P$. Divisors of degree 0 form a subgroup of $\mathrm{Div}(C)$ denoted $\mathrm{Div}^0(C)$.

**Principal divisors**

A function on a curve is a map to $\mathbf{P}^1$ given locally by a rational function. Let $f$ be a function on $C$. To it we can associate a divisor. The usual definition is $\mathrm{div}(f) = \sum ord_P(f)P$. If you do not know this, then it is easier to be informal about it. People do not use the above in when computing Mordell-Weil ranks anyway. If $f$ is a constant function, then $\mathrm{div}(f) = 0$. Assume $C$ is in $\mathbf{P}^2$ (all curves can be embedded in $\mathbf{P}^2$, though you may get a singular model; we will show soon how to get around that in an example). If $f$ is not a constant function, then take the function $f$ and homogenize it, $f^{\mathrm{hom}} = F/G$. $F$ and $G$ are two homogenous polynomials of the same degree. Each describes a set of curves. For $C$ and $D$ different curves, let $C.D$ denote the intersection divisor of $C$ and $D$, that is the formal sum of points where they intersect, counting multiplicities.

Theorem (Bezout): Let $C$ and $D$ be different curves in $\mathbf{P}^2$ defined by homogeneous polynomials of degrees $n$ and $m$, then $\deg(C.D) = nm$.

We take $\mathrm{div}(f) = (F = 0).C - (G = 0).C$. ¿From Bezout's theorem, it has degree 0. If either $F = 0$ or $G = 0$ is reducible, just sum the intersection divisor from each component.

Examples

On $E : y^2 + y = x^3 - x$, what is the divisor of $y$? Go to $\mathbf{P}^2$. We have $y = Y/Z$ and the curve is $Y^2Z + YZ^2 = X^3 - XZ^2$. $\mathrm{div}(y)$ "$= \mathrm{div}(Y/Z)$" $= E.(Y = 0) - E.(Z = 0)$. Now if $Y = 0$, we have $0 = X^3 - XZ^2$. $Z \neq 0$ so let $Z = 1$. We have $X^3 - X = 0$. We get $E.(Y = 0) = [-1 : 0 : 1] + [0 : 0 : 1] + [1 : 0 : 1] = (-1, 0) + (0, 0) + (1, 0)$. $Z = 0$ meets the curve at $(X - 0)^3 = 0$, so that is the point $[0 : 1 : 0] = \mathbf{O}$ with multiplicity three. So $(Z = 0).E = 3\mathbf{O}$. Thus $\mathrm{div}(y) = (-1, 0) + (0, 0) + (1, 0) - 3\mathbf{O}$. End of example.

The principal divisors form a group, $\mathrm{Princ}(C)$, since $\mathrm{div}(fg) = \mathrm{div}(f)+\mathrm{div}(g)$. This is a subgroup of $\mathrm{Div}^0(C)$. The group structure of the Jacobian of $C$ is isomorphic to $\mathrm{Div}^0(C)/\mathrm{Princ}(C)$. It is denoted $J = \mathrm{Jac}(C)$.

### Weil reciprocity

Let $D = \sum n_P P$. Let $f$ be a function whose divisor has support disjoint from that of $D$. Define $f(D) = \prod f(P)^{n_P}$. Let $f, g$ be functions on $C$ whose divisors have disjoint support. Then $f(\mathrm{div}(g)) = g(\mathrm{div}(f))$.

### Jacobians of elliptic curves

For an elliptic curve $E$, we have an isomorphism $E \cong \mathrm{Jac}(E)$ by $P \mapsto [P - \mathbf{O}]$.

Example

Recall on $E : y^2 + y = x^3 - x$ we have $(-1,-1) + (0,0) = (2,-3)$. Thus we should have $[(-1,-1)-\mathbf{O}]+[(0,0)-\mathbf{O}] = [(2,-3)-\mathbf{O}]$. This is true if $(-1,-1)-\mathbf{O}+(0,0)-\mathbf{O}-(2,-3)+\mathbf{O}$ is principal. Recall that we used the lines $y = x$ and $x = 2$ to do this addition. Find $\mathrm{div}((y-x)/(x-2))$. $E.(y = x) = (-1,-1)+(0,0)+(2,2)$ and $E.(x = 2) = (2,2)+(2,-3)+\mathbf{O}$. Thus $\mathrm{div}((y-x)/(x-2)) = (-1,-1) + (0,0) - (2,-3) - \mathbf{O}$. End of example.

### Example of addition on the Jacobian of a genus 2 curve

Let $C : y^2 = x^5 + 1$. This curve has genus 2. There is a problem in that the completion of this curve in $\mathbf{P}^2$ has a singular point at infinity. There are ways of smoothing the curve; the resulting curve is in a high-dimensional projective space and has an ugly representation. After smoothing, the curve is isomorphic, over $\mathbf{Q}$, to the following curve. Consider the two affine covers: $y^2 = x^5 + 1$ and $v^2 = u^6 + u$. They glue together by $ux = 1$ and $v = u^3 y$ where $ux \neq 0$. Where did this come from? Let $x = 1/u$, then $y^2 = 1/u^5 + 1$, $u^6 y^2 = u + u^6$. Such a description can also be useful for determining the divisor of a function at infinity.

The only point on $C$ not on the cover $y^2 = x^5 + 1$ is where $(u, v) = (0, 0)$ and the cover $v^2 = u^6 + u$ is non-singular at this point. Denote $(u, v) = (0, 0)$ by $\infty$.

It follows from the Riemann-Roch theorem that every divisor class in $\mathrm{Jac}(C)$ contains a unique divisor of the form $P + Q - 2\infty$ except for the trivial divisor class which contains divisors of the form $(a, b) + (a, -b) - 2\infty$ (where $(a, b) \in C$). Note $(a, b) + (a, -b) - 2\infty = \mathrm{div}(x - a)$. This also tells us that $-[(a, b) + (c, d) - 2\infty] = [(a, -b) + (c, -d) - 2\infty]$.

Let us add $[P+Q-2\infty]+[R+S-2\infty]$. When possible, find the cubic $y = ax^3+bx^2+cx+d$ through $P, Q, R, S$. If $P$ appears with multiplicity $n$ then make sure that the derivatives of $y^2 = x^5 + 1$ and $y = ax^3 + bx^2 + cx + d$ agree at $P$ up to the $n - 1$st derivative. When it is impossible to find such a cubic, the sum is obvious.

Let us add $[(0, 1) + (-1, 0) - 2\infty] + [2(0, 1) - 2\infty]$. We want $y = ax^3 + bx^2 + cx + d$ to pass through $(0, 1)$ and $(-1, 0)$. In addition, for $y^2 = x^5 + 1$ we have $dy/dx(0, 1) = d^2y/dx^2(0, 1) = 0$. So we want the same to hold true for $y = ax^3 + bx^2 + cx + d$. We find $y = x^3 + 1$. We solve $y = x^3 + 1$ and $y^2 = x^5 + 1$ simultaneously and get $(x^3 + 1)^2 = x^5 + 1$ or $x^6 - x^5 + 2x^3 = 0 = (x - 0)^3(x + 1)(x^2 - 2x + 2)$. Thus $\mathrm{div}(y - x^3 - 1) = 3(0, 1) + (-1, 0) + (1 + i, -1 + 2i) + (1 - i, -1 - 2i) - 6\infty$. Therefore

$$[(0, 1) + (-1, 0) - 2\infty] + [2(0, 1) - 2\infty] + [(1 + i, -1 + 2i) + (1 - i, -1 - 2i) - 2\infty] = 0$$

and

$$[(0, 1) + (-1, 0) - 2\infty] + [2(0, 1) - 2\infty]$$

$$= -[(1 + i, -1 + 2i) + (1 - i, -1 - 2i) - 2\infty]$$

$$= [(1+i, 1-2i) + (1-i, 1+2i) - 2\infty].$$

**Mordell-Weil theorem for Jacobians**

Let $C/K$, where $K$ is a number field. Then $\mathrm{Gal}(\overline{K}/K)$ acts on points by acting on their coordinates. By extension it acts on divisors. It sends principal divisors to principal divisors, so it has an action on $J = \mathrm{Jac}(C)$. Let $J(K)$ denote the $\mathrm{Gal}(\overline{K}/K)$-invariant subgroup of $J = J(\overline{K})$.

Theorem (Mordell-Weil): $J(K)$ is a finitely generated abelian group.

Thus $J(K) \cong \mathbf{Z}^r \oplus J(K)_{\mathrm{tors}}$. There is not yet an effective algorithm for computing $J(K)_{\mathrm{tors}}$. In practice, it is not difficult and Michael Stoll has just come up with one for curves of genus 2. There is no known effective algorithm for computing $r$.

**Short course in cohomology**

Assume that you have $J(K)_{\mathrm{tors}}$. If you can find $J(K)/qJ(K)$, for $q$ a prime, then you know $r$. Let $J[q]$ denote the $q$-torsion in $J$ (that is the kernel of the multiplication-by-$q$ map). We see $\dim_{\mathbf{F}_q} J(K)/qJ(K) = r + \dim_{\mathbf{F}_q} J(K)[q]$. Aside: $\dim_{\mathbf{F}_q} J[q] = 2$genus. In fact, this is true over any field of characteristic other than $q$.

We have

$$0 \to J[q] \to J(\overline{K}) \xrightarrow{q} J(\overline{K}) \to 0.$$

Taking $\mathrm{Gal}(\overline{K}/K)$-invariants is left-exact.

$$0 \to J(K)[q] \to J(K) \xrightarrow{q} J(K) \to ?$$

What is "?"? $J(K)/qJ(K)$ injects into it.

Let $M$ be abelian group, $G$ a finite or infinite Galois group acting on $M$. If $G$ is infinite Galois, then it should act continuously on $M$ where $M$ is is given the discrete topology otherwise.

$H^1(G, M)$ is the quotient of

$\{f : G \to M \mid \text{for all } s, t \in G,\ f(st) = sf(t) + f(s) \text{ and continuous if } G \text{ infinite Galois}\}$

by

$\{f : G \to M \mid \text{there's } m \in M \text{ such that } f(s) = sm - m\}$. The first set consists of cocycles. The second set consists of coboundaries. Often, though not always, you can keep your hands clean and not deal with cocycles and coboundaries. Mostly we want to remember that it is a quotient of groups of functions.

We see from the definition, however, that if $G$ acts trivially on $M$, then $H^1(G, M) = \mathrm{Hom}(G, M)$.

If $0 \to M \to N \to R \to 0$ is an exact sequence of $G$-modules then

$$0 \to M^G \to N^G \to R^G \xrightarrow{\delta} H^1(G, M) \to H^1(G, N) \to H^1(G, R) \to \dots$$

is exact.

The maps between the $H^1$'s are just compositions of the maps between the modules and the cocycles.

Let us define $\delta$. Let $r \in R^G$ and let $n \in N$ be a pre-image. Then $\delta(r) = [g \mapsto gn - n]$.

Facts: 1. If $H \subset G$ we have a restiction map $H^1(G,M) \stackrel{\text{res}}{\to} H^1(H,M)$. If $H$ is normal in $G$ and $N$ is the quotient then

$$0 \to H^1(N, M^H) \stackrel{\text{inf}}{\to} H^1(G,M) \stackrel{\text{res}}{\to} H^1(H,M)$$

is exact. Let us describe the inflation map. Let $[\xi]$ be a cocycle class in $H^1(N, M^H)$. Its image in $H^1(G,M)$ is the class containing the cocycle that takes $g \in G$, factors it through $N$, and maps it via $\xi$ to $M^H \subset M$.

2. $H^1(\mathrm{Gal}(\overline{K}/K), \overline{K}^*) = 0$ (Hilbert's theorem 90) so from $1 \to \mu_m \to \overline{K}^* \stackrel{m}{\to} \overline{K}^* \to 1$ we get

$$\dots K^* \stackrel{m}{\to} K^* \stackrel{\delta}{\to} H^1(\mathrm{Gal}(\overline{K}/K), \mu_m) \to 0.$$

Thus $K^*/K^{*m} \cong H^1(\mathrm{Gal}(\overline{K}/K), \mu_m)$ by $k \mapsto [\sigma \mapsto \sigma \sqrt[m]{k} / \sqrt[m]{k}]$.

The point is that we have turned an ugly cohomology group into one we understand from algebraic number theory. We often try to do that with cohomology groups (or show that they are trivial).

3. The exponents of $G$ and $M$ kill $H^1(G,M)$.

### Isogenies

Let $K$ be a number field and let $C/K$ and $C'/K$, have the same genus. Let $J = \mathrm{Jac}(C)$ and $J' = \mathrm{Jac}(C')$ be their Jacobians. Let $\phi : J' \to J$ be an isogeny. That is a homomorphism, given by rational functions with a finite kernel. Isogenies are always surjective. Note if $m \in \mathbf{Z}$, then the multiplication-by-$m$ map, $m : J \to J$, is an isogeny. Let $\hat{J}$, $\hat{J}'$ be the duals (as abelian varieties, which I will not define). Then there is a dual isogeny $\hat{\phi} : \hat{J} \to \hat{J}'$. I will get away with not defining duals since there is an isomorphism of $J$ with $\hat{J}$, defined over $K$, called the canonical principal polarization coming from the curve. We will continue to use this notation.

### Selmer group

Let us return to the computation of $J(K)/qJ(K)$. For greater generality we will replace the multiplication-by-$q$ map with a general isogeny. Sometimes isogenies are more useful for computing Mordell-Weil ranks than multiplication-by-$q$ maps, as we will see later. We will first have to go into a lot of cohomology. Our goal, however, is to remove all the cohomology groups from the algorithm for bounding a Mordell-Weil rank.

From the exact sequence

$$0 \to J'(\overline{K})[\phi] \to J'(\overline{K}) \stackrel{\phi}{\to} J(\overline{K}) \to 0$$

we take $\mathrm{Gal}(\overline{K}/K)$-invariants and get the exact sequence

$$0 \to J'(K)[\phi] \to J'(K) \stackrel{\phi}{\to} J(K) \stackrel{\delta}{\to} H^1(\mathrm{Gal}(\overline{K}/K), J'[\phi]) \to H^1(\mathrm{Gal}(\overline{K}/K), J'(\overline{K}))$$

$$\stackrel{\phi}{\to} H^1(\mathrm{Gal}(\overline{K}/K), J(\overline{K})) \to \dots$$

For a $\mathrm{Gal}(\overline{K}/K)$-module $M$ denote $H^1(\mathrm{Gal}(\overline{K}/K), M)$ by $H^1(K,M)$. Recall $J = J(\overline{K})$. We have the exact sequence

$$0 \to J(K)/\phi J'(K) \stackrel{\delta}{\to} H^1(K, J'[\phi]) \to H^1(K, J')[\phi] \to 0.$$

Let $\mathfrak{p}$ be a prime of $K$. We can replace $K$ by $K_{\mathfrak{p}}$ in the above. Since $\mathrm{Gal}(\overline{K_{\mathfrak{p}}}/K_{\mathfrak{p}})$ is isomorphic to a decomposition subgroup of $\mathrm{Gal}(\overline{K}/K)$, we have $H^1(K,M) \stackrel{\mathrm{res}}{\to} H^1(K_{\mathfrak{p}},M)$. We get the following commutative diagram

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

Our goal is to simplify this and remove all the cohomology groups.

Define $S^{\phi}(J',K) = \ker(\prod \alpha_{\mathfrak{p}})$. This is the $\phi$-Selmer group for $J'$ over $K$. Clearly it contains the image of $J(K)/\phi J'(K)$. We will see later that it is finite. It is also effectively computeable. We use Selmer groups to find an upper bound on a Mordell-Weil rank. With luck, you can find enough rational divisor classes whose images generate the whole Selmer group. If you can do this for isogenies whose composition is a multiplication-by-$q$ map, then you have the Mordell-Weil rank.

**Tate-Shafarevich group**

What is the obstruction? Define $\text{Ш}(J',K) = \ker: H^1(K,J') \stackrel{\prod \mathrm{res}}{\to} \prod H^1(K_{\mathfrak{p}},J')$. This is a mysterious group called the Tate-Shafarevich group. It is sometimes known to be finite and is conjectured to always be finite. The following is an exact sequence

$$0 \to J(K)/\phi J'(K) \to S^{\phi}(J,K) \to \text{Ш}(J',K)[\phi] \to 0.$$