Cassels-Tate pairing on hyperelliptic curves

Himanshu Shukla

Mathematisches Institut, Universität Bayreuth

Oberseminar Arithmetic Geometry

17th June, 2021

Outline

Some notations

- Fix a number field k.
- $f := \prod_{i=1}^{l}(X - e_i) \in k[X]$, with $e_i \in \bar{k}$ are pairwise distinct, and l odd.
- Define
$$C := Y^2 = f(X), \tag{1}$$
and let $\Delta := \{T_i := (e_i, 0) : 1 \leq i \leq l\}$, and T_0 be the point at infinity. (Δ is a $G_k := \mathrm{Gal}(\bar{k}/k)$ set.)
- For a place v of k, k_v denotes its completion with respect to v and $\mathfrak{k}_v$ the residue field.
- Let J be the jacobian variety associated to C.
- Let J_v denote the variety J defined over k_v.

preliminaries contd...

- J can be identified with $\mathrm{Pic}^0(C)$.
- $P \in J$, then $P := [(P_1) + (P_2) + \ldots + (P_m) - m(T_0)]$, $m \leq g = (l-1)/2$, with $(P_1) + (P_2) + \ldots + (P_m) \in \div(C)$ in general position.
- $C \hookrightarrow J$ via the map $P \mapsto [(P) - (T_0)]$.
- The etalé algebra associated to Δ

$$L := k[X]/\langle f(X)\rangle \cong \bigoplus_{\Delta_i} k[X]/\langle f_i(X)\rangle \cong \bigoplus_{\Delta_i} L_i,$$

  Δ_is are orbits of Δ.
- $\alpha \in \mathrm{Sel}^{(2)}(J) \subset L^\times/(L^\times)^2$ and $\alpha \notin J/2J$, then $\alpha := (d_1, \ldots, d_l)$ with $d_i = \alpha(e_i)$.

Some theoretical aspects

Theorem (Mordell-Weil)

$$J(k) \cong J(k)_{tors} \oplus Z^{r_J},$$

where $\#J(k)_{tors} < \infty$, $r_J :=$ *algebraic rank.*

- In order to compute $J(k)_{tors}$ we use the injection $J(k)_{tors} \hookrightarrow J(\mathfrak{k}_v)$, for a place of good reduction.
- No unconditional algorithm to compute r_J is known.
- Assuming BSD, r_J may be computed using $r_{\mathrm{an}}(J) := \mathrm{ord}(L(J, s = 1))$.

Upper and lower bounds

- **Lower bound:** Find points and check for independence.
- **Upper bound:** Use descent.
- See if they match!

The Kummer sequence:

$$0 \longrightarrow J[n] \hookrightarrow J \longrightarrow J \longrightarrow 0 \tag{2}$$

Applying galois cohomology:

$$\begin{tikzcd}
0 \arrow[r] & \frac{J(k)}{nJ(k)} \arrow[r, hook] \arrow[d] & H^1(G_k, J[n]) \arrow[r] \arrow[d] \arrow[dr, "\alpha"] & H^1(G_k, J)[n] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \prod_v \frac{J(k_v)}{nJ(k_v)} \arrow[r, hook] & \prod_v H^1(G_{k_v}, J[n]) \arrow[r] & \prod_v H^1(G_{k_v}, J_v)[n] \arrow[r] & 0,
\end{tikzcd}$$

Descent sequence

We have the $n-$descent sequence.

$$0 \longrightarrow \frac{J(k)}{nJ(k)} \hookrightarrow \mathrm{Sel}^{(n)}(J) \longrightarrow Ш[n] \longrightarrow 0, \tag{3}$$

where n^{th} Selmer group

$$\mathrm{Sel}^{(n)}(J) = \ker(\alpha),$$

and the Tate-Shafarevich group

$$Ш := \ker\left(H^1(G_k, J) \longrightarrow \prod_v H^1(G_{k_v}, J_v) \right).$$

- $\mathrm{Sel}^{(n)}(J)$ is finite and effectively computable in principle.
- $\mathrm{rank}_{\mathbb{F}_p}(\mathrm{Sel}^{(p)}(J))$ bounds the $\mathrm{rank}_{\mathbb{F}_p}(\frac{J(k)}{pJ(k)})$.
- If $Ш[n]$ is trivial then $\mathrm{Sel}^{(n)}(J) \cong \frac{J(k)}{nJ(k)}$.

Higher descent

- If $(m, n) = 1$, $\mathrm{Sel}^{(mn)}(J) \cong \mathrm{Sel}^{(n)}(J) \times \mathrm{Sel}^{(m)}(J)$.
- If $t \geq 2$, then $\mathrm{Sel}^{p^t}(J)$ is known as higher $p-$descent.
- We have the following commutative diagram:

$$\begin{tikzcd} \frac{J(k)}{p^t J(k)} \arrow[r, hook] \arrow[d] & \mathrm{Sel}^{(p^t)}(J) \arrow[d, "p"] \\ \frac{J(k)}{p^{t-1} J(k)} \arrow[r, hook] & \mathrm{Sel}^{(p^{t-1})}(J) \end{tikzcd} \tag{4}$$

We have

$$\frac{J(k)}{pJ(k)} \subseteq p\mathrm{Sel}^{(p^2)}(J) \subseteq \mathrm{Sel}^{(p)}(J). \tag{5}$$

Cassels-Tate pairing (CTP)

- CTP (denoted by $\langle ., . \rangle_{CT}$) was defined by **J.W.S. Cassels** for elliptic curves.
- **John Tate** generalized it to abelian varieties.
- CTP has following properties:
  - $\langle ., . \rangle_{CT} : Ш \times Ш \longrightarrow \mathbb{Q}/\mathbb{Z}$.
  - CTP is an anti-symmetric pairing.
  - $\forall \alpha \in Ш[n]$, $\langle \beta, \alpha \rangle_{CT} = 0 \iff \beta \in nШ$.

Pulling back $\langle ., . \rangle_{CT}$ on $\mathrm{Sel}^{(n)}(J)$, we have:

Theorem (Cassels)

$\langle \alpha, \beta \rangle_{CT} = 0$ *for all* $\beta \in \mathrm{Sel}^{(n)}(J)$, $\iff \alpha \in n\mathrm{Sel}^{(n^2)}(J)$.

Known results

- Poonen and Stoll give three definitions of CTP on polarized abelian varieties and show that CTP at best is anti-symmetric.
- Swinnerton-Dyer computed CTP between $\mathrm{Sel}^(2)(E)$ and $\mathrm{Sel}^{(2^n)}(E)$.
- Fischer and Newton computed CTP on $\mathrm{Sel}^{(3)}(E)$.
- van Beek and Fischer compute CTP on Selmer groups of odd prime degree isogeny on elliptic curves.
- The above computations were based on Weil-pairing based definition.

Known results (contd.)

- Fischer and Donelly used homogenous space based definition to compute CTP on $\mathrm{Sel}^{(2)}(J)$.
- CTP can be defined in general for $Ш(A) \times Ш(A^\vee)$, for an abelian variety A and its dual $A^\vee$.

Known results (contd.)

- Fischer and Donelly used homogenous space based definition to compute CTP on $\mathrm{Sel}^{(2)}(J)$.
- CTP can be defined in general for $Ш(A) \times Ш(A^\vee)$, for an abelian variety A and its dual $A^\vee$.

- We aim to compute CTP on jacobians of genus 2 curves.
- Jiali Yan has computed the CTP for genus 2 curves where f splits completely over $k[X]$ for the following:
  - 2-selmer group using homogenous space definition.
  - Richelot's isogeny using Weil-pairing definition.
- If one of the twisted Kummer surface has a $k-$rational point.
- Use Albanese-Albanese definition of CTP to compute it.

Albanese-Albanese defintion

We have two partially defined, evaluation based, galois equivariant pairings:

- $\langle \mathrm{div}(f), D\rangle_1 : (\mathrm{Princ}(C) \times \mathrm{Div}^0(C))^{\perp} \longrightarrow \bar{k}^{\times}$,
  $$\langle \mathrm{div}(f), D\rangle_1 = \prod_{P \in \mathrm{Supp(D)}} f(P)^{v_P(D)}.$$
- $\langle D, \mathrm{div}(f)\rangle_2 : (\mathrm{Div}^0(C) \times \mathrm{Princ}(C))^{\perp} \longrightarrow \bar{k}^{\times}$,
  $$\langle D, \mathrm{div}(f)\rangle_2 = \prod_{P \in \mathrm{Supp(D)}} f(P)^{v_P(D)}.$$
- $\langle ., .\rangle_1$ and $\langle ., .\rangle_2$ match on $(\mathrm{Princ}(C) \times \mathrm{Princ}(C))^{\perp}$ (Weil Reciprocity), and are defined when $\mathrm{Supp}(\mathrm{div}(f)) \cap \mathrm{Supp}(D) = \emptyset$.
- Let $\cup_1$, $\cup_2$ be the induced cup-products on galois cohomology.

Albanese-Albanese definition contd.

Let $\alpha, \alpha' \in \mathrm{Sel}^{(n)}(J)$.

- **Global part:**
  - Lift α, α' to $\mathfrak{a}, \mathfrak{a}' \in C^1(G_k, \mathrm{Div}^0(C))$.
  - $\partial\mathfrak{a}, \partial\mathfrak{a}'$ take values in $\mathrm{Princ}(C)$.
  - Let $\eta := \partial\mathfrak{a} \cup_1 \mathfrak{a}' - \mathfrak{a} \cup_2 \partial\mathfrak{a}' \in Z^3(k, \bar{k}^\times) \implies \eta = \partial\varepsilon$, for $\varepsilon \in C^2(k, \bar{k}^\times)$.
  - The above statements follow using the galois cohomology on Kummer sequence and on

    $$0 \longrightarrow \mathrm{Princ}(C) \hookrightarrow \mathrm{Div}^0(C) \longrightarrow \mathrm{Pic}^0(C) \longrightarrow 0,$$

    and using $H^3(k, \bar{k}^\times)$ is trivial.
- **Local part:**
  - There exists $P_v \in J_v$, with $\partial P_v = \alpha_v$.
  - Lift P_v to a degree zero divisor $\mathfrak{p}_v$, and $\mathfrak{a}_v - \partial\mathfrak{p}_v$ takes values in $\mathrm{Princ}(C)$.
  - Consider $\gamma_v := (\mathfrak{a}_v - \partial\mathfrak{p}_v) \cup_1 \mathfrak{a}'_v - \mathfrak{p}_v \cup_2 \partial\mathfrak{a}'_v - \varepsilon_v$.

Albanese-Albanese definition contd.

γ_v represents some class $c_v \in H^2(k_v, \bar{k_v}^\times) \cong \mathrm{Br}(k_v)$.

Definition

For $(\alpha, \alpha') \in \mathrm{Sel}^{(n)}(J) \times \mathrm{Sel}^{(n)}(J)$ we have:

$$\langle \alpha, \alpha' \rangle_{CT} = \sum_v \mathrm{inv}_v(c_v)$$

Two bottelnecks:

1. **Global bottleneck:** Computation of ε s.t $\partial\varepsilon = \eta$
   - Determining the field extension M in which ε takes values, and the field M' through which it factors.
   - M, M' are depend on the solutions to the system of "skewed" linear equations:

$$\sigma\varepsilon(\tau,\rho) + \varepsilon(\sigma,\tau\rho) - \varepsilon(\sigma\tau,\rho) + \varepsilon(\sigma,\tau) = \eta(\sigma,\tau,\rho).$$

2. **Local bottleneck/s:** Computation of c_v represented by 2-cocycle γ_v
   - γ_v mostly will have a complicated description.
   - Determine a 1-cochain ξ_v s.t. $\gamma_v - \partial\xi_v$ has a description simple enough to compute c_v.

We prove the following theorem:

Theorem

Let C be an elliptic curve ($l = 3$), and $\alpha, \alpha' \in \mathrm{Sel}^{(2)}(J)$, represented by (d_1, d_2, d_3), (d_1', d_2', d_3'), with $d_1 d_2 d_3 \in k^2$, and $d_1' d_2' d_3' \in k^2$ and $d_i, d_i' \in k(e_i)$, then

$$(-1)^{2\langle \alpha, \alpha' \rangle_{CT}} = \prod_v [\alpha, \alpha']_v,$$

where

$$[\alpha, \alpha']_v = \begin{cases} \prod_{i=1}^{3} (\delta_{v,i}, d_i')_{k_v}, & f \text{ splits over } k, \\ (\delta_{v,1}, d_1')_{k_v} (\delta_{v,2}, d_2')_{k_v(e_2)} & e_1 \in k \text{ and } [k(e_2) : k] = 2, \\ (\delta_{v,1}, d_1')_{k_v(e_1)} & [k(e_1) : k] \geq 3, \end{cases}$$

where $\delta_{v,i} \in k_v(e_i)$, and $(.,.)$ denotes the Hilbert's symbol.

Some simplifications!

- Let $M^{\Delta} := \{(m_P)_{P\in\Delta} : m_P \in M\}$, for a G_k module M.
- M^{Δ} is a galois module under the natural action:

$$\theta_P^{\sigma} = \sigma(\theta_{\sigma^{-1}P}).$$

True 2-descent: Following generalized explicit descent technique of Bruin, Poonen, and Stoll we have:

- $\Delta \hookrightarrow J[2]$.
- $0 \longrightarrow \langle (1)_{P\in\Delta}\rangle \longrightarrow (\mathbb{Z}/2\mathbb{Z})^{\Delta} \longrightarrow J[2] \longrightarrow 0.$

Dualizing we get:

$$0 \longrightarrow J[2] \longrightarrow \mu_2^{\Delta} \longrightarrow \langle (1)_{P\in\Delta}\rangle^{\vee} \longrightarrow 0.$$

Galois cohomology gives:

$$
\begin{tikzcd}
\mu_2^{\Delta}(k) \arrow[d, two heads] & & \\
R(k) \arrow[r] & H^1(k, J[2]) \arrow[r, hook] & H^1(k, \mu_2^{\Delta}) \\
\bigoplus_{\Delta_i} H^1(L_i, \mu_2^{\{P_i\}}) \arrow[r, hook] \arrow[d, leftrightarrow, "\simeq"] & \bigoplus_{\Delta_i} H^1(L_i, \mu_2^{\Delta_i}) \arrow[r, "cor"] & \bigoplus_{\Delta_i} H^1(k, \mu_2^{\Delta_i}) \arrow[u, leftrightarrow, "\simeq"'] \\
\bigoplus_{\Delta_i} H^1(L_i, \langle [P_i - T_0] \rangle). & &
\end{tikzcd}
$$

Lemma

If $\alpha \in H^1(k, J[2])$, *then we have:*

$$\alpha := \sum_{\Delta_i} \mathrm{cor}(\alpha_i),$$

where $\alpha_i \in H^1(L_i, \langle [P_i - T_0] \rangle)$.

Corollary

$\langle \alpha, \alpha' \rangle_{CT} = \sum_{\Delta_i} \langle \alpha, cor(\alpha'_i) \rangle_{CT}$.

Theorem

We have: $\langle \alpha, cor(\alpha'_i) \rangle_{CT} = \langle res(\alpha), \alpha'_i \rangle_{CT}$.

The above theorem follows by using: $a \cup cor(b) = cor(res(a) \cup b)$, for cochains a and b.

Assume $e_1 \in k$, $\eta_1'(\sigma,\tau,\rho)$ is only depended on $\chi(\sigma), \chi(\tau), \chi'(\tau), \chi'(\rho)$ where χ, χ_1' are elements of $H^1(k, \mu_2^{\Delta})$ and $H^1(k, \mu_2^{\{P_1\}})$ (resp.) representing α, α_1'.
Let M be a galois extension of $k(\sqrt{d_1}, \ldots, \sqrt{d_l})$, s.t. $M \cap k(\sqrt{d_1'}) = k$, and M is also galois over k.

Lemma

If there is an ε_1 satisfying $\partial\varepsilon_1 = \eta_1$ with such that $\varepsilon_1(\sigma,\tau)$ takes values in M and only depends on $\sigma\big|_M, \chi_1'(\sigma)$, and $\chi_1'(\tau)$, then:

- $\sigma\varepsilon_1(id,1,1) = \varepsilon_1(\sigma\big|_M, \chi_1'(\sigma), 1)$.
- $\frac{\varepsilon_1(id,1,1)=\varepsilon_1(id,1,-1)}{\varepsilon_1(id,-1,-1)} = \frac{\varepsilon_1(\sigma\big|_M,1,-1)}{\varepsilon_1(\sigma\big|_M,-1,-1)}$.
- $\frac{\sigma(\varepsilon_1(id,1,1)*\varepsilon_1(id,-1,-1))}{\varepsilon_1(id,-1,-1)\varepsilon_1(\sigma\big|_M,1,-1)^2} = \eta_1(\chi(\sigma), \chi(\tau) = (1,\ldots,1), -1, -1)$.

Hence we require only $\varepsilon_1(id,1,1), \varepsilon_1(id,-1,-1)$ to compute ε_1 entirely.

Definition

An $\alpha = (d_1, \ldots, d_l) \in \mathrm{Sel}^{(2)}(J)$ is said to be good if each of the conics $C_{1j}(u, v) := d_1 u^2 - d_j v^2 + e_1 - e_j$, has a solution over $k(e_1, e_j)$. A curve C is good if the subgroup generated by good elementsis of index 2.

If α is good, then we have an ε_1 of the above form with $M = K(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_l})$.

- Hope: Most of the curves are good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 0$: 1207 on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 2$, $r_{an}(J) = 1$: 538 on LMFDB, all good.
- $\mathrm{rk}_{\mathbb{F}_2}\mathrm{Sel}^{(2)}(J) \geq 4$, $r_{an}(J) \geq 2$: 4 on LMFDB, all good.
- $x^5 + A$, $0 < A < 1000$, and A is prime: 168 curves, all good.

An example with complex multiplication

Let

$$C := Y^2 = X^l + A,$$

- The jacobian of C has an isogeny $\lambda := 1 - \zeta_l$ of degree l defined over $K = \mathbb{Q}(\zeta_l)$.
- $L := K(\sqrt{A})$, then $\mathrm{Sel}^{(\lambda)} \subset \mathrm{Ker}\left(N_{L/K} : L^\times/(L^\times)^l \longrightarrow K^\times/(K^\times)^l\right)$.
- If $A := 2^{l-2}b^l$, then one can compute ε.
- Otherwise we obtain $\eta' := \eta - \partial\varepsilon \in Z^3(L, \mu_l)$.
- Since $H^3(L, \mu_L) = 0$, the aim is to find 2-cochain $\varepsilon' \in C^2(L, \mu_l)$ s.t. $\partial\varepsilon = \eta'$.

Thank You!