Kolyvagin systems and Selmer structures of rank 0

Alberto Angurel Andrés

University of Nottingham

05/09/24

Selmer structures

Setup

- $p \geq 5$ is a prime number.
- T is a p-adic Galois representation over $\mathbb{Q}$, i.e.,
  - T is a finitely generated free $\mathbb{Z}_p$-module.
  - There is a continuous action of $G_{\mathbb{Q}}$ on T.

Selmer structure $\mathcal{F}$

- A finite set Σ of primes containing p, ∞ and those where T is ramified.
- For every $\ell \in \Sigma$, a subgroup $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \subset H^1(\mathbb{Q}_\ell, T)$ called local condition.

Selmer group

$$\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T) := \ker\left(H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, T) \to \bigoplus_{\ell \in \Sigma} \frac{H^1(\mathbb{Q}_\ell, T)}{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)}\right) \subset H^1(\mathbb{Q}, T)$$

Dual Selmer structure

Dual representation

$$T^* := \mathrm{Hom}(T, \mu_{p^\infty})$$

Dual Selmer structure

- Same set of primes Σ.
- Local duality: there exists a non-degenerate pairing

$$H^1(\mathbb{Q}_\ell, T) \times H^1(\mathbb{Q}_\ell, T^*) \to \mathbb{Q}_p/\mathbb{Z}_p$$

- $H^1_{\mathcal{F}^*}(\mathbb{Q}_\ell, T^*)$ is defined as the orthogonal complement of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$.
- There is a dual Selmer group $\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)$ defined similarly.

Examples of Selmer groups

Example

- Let $T = \varprojlim_n \mu_{p^n}$ and let K be a number field.
- Let Σ be the primes above p and ∞.
- Hilbert 90 $\Rightarrow$ $K_v^* \otimes \mathbb{Z}_p \cong H^1(K_v, T)$.
- $H^1_{\mathcal{F}}(K_v, T) := U_v \otimes \mathbb{Z}_p \hookrightarrow H^1(K_v, T)$.
- There are canonical isomorphisms

$$\mathrm{Sel}_{\mathcal{F}}(K, T) \cong O_K \otimes \mathbb{Z}_p, \qquad \mathrm{Sel}_{\mathcal{F}^*}(K, T^*) = \mathrm{Hom}(\mathrm{Cl}(K), \mathbb{Q}_p/\mathbb{Z}_p)$$

Example

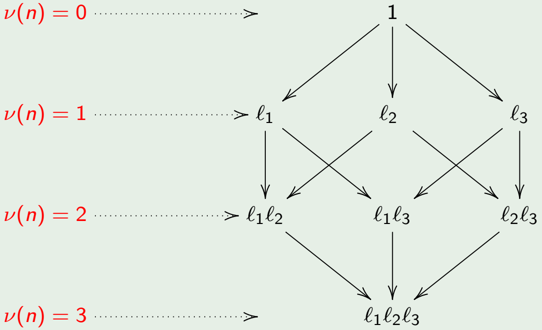
- Let T be the Tate module of an elliptic curve $E/\mathbb{Q}$.
- Let Σ be the primes p, ∞ and all bad reduction primes.
- $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) = \mathrm{Im}\left(E(\mathbb{Q}_\ell) \otimes \mathbb{Z}_p \to H^1(\mathbb{Q}_\ell, T)\right)$
- If $\text{Ш}(E/\mathbb{Q})$ is finite, then $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T) = E(\mathbb{Q}) \otimes \mathbb{Z}_p$

Kolyvagin graph

- Let $\mathcal{P}$ be a set of primes and let $\mathcal{N}$ be the square-free products of primes in $\mathcal{P}$.
- The vertices of the graph are the elements in $\mathcal{N}$.
- For every $n \in \mathcal{N}$ and $q \in \mathcal{P}$ such that $(n, q) = 1$, there is an edge between n and nq.

Example

Assume $\mathcal{P} = \{\ell_1, \ell_2, \ell_3\}$.



Kolyvagin primes

Kolyvagin primes $\mathcal{P}_k$

- $\ell \equiv 1 \mod p^k$.
- $T/(p^k, \mathrm{Frob}_\ell - 1) \cong \mathbb{Z}/p^k$.

Remark

- $\mathcal{P}_1 \supset \mathcal{P}_2 \supset \cdots \supset \mathcal{P}_k \supset \cdots$
- Chebotarev density theorem $\Rightarrow$ All $\mathcal{P}_k$ are infinite.

Graphs

- We will consider a big Kolyvagin graph with vertices $\mathcal{N}_1$ and a a 'filtration' of subgraphs formed by the vertices in $\mathcal{N}_k$.
- The vertices in $\mathcal{N}_k$ carry more information for bigger values of k.
- Given some $n \in \mathcal{N}_1$, we denote by e_n the maximal k such that $n \in \mathcal{P}_k$.
- The idea is that n sees the Selmer group mod p^{e_n}.

Kolyvagin systems

Kolyvagin system

- For every vertex $n \in \mathcal{N}_1$, we choose an element $\kappa_n \in \mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T) \subset H^1(\mathbb{Q}, T)$.
- For every edge $n \to n\ell$, we impose a relation between κ_n and κ_{nl}.

Core rank

- $\chi(\mathcal{F}) = \dim_{\mathbb{F}_p} \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T/pT) - \dim_{\mathbb{F}_p} \mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*[p])$

Rigidity of Kolyvagin systems

- $\chi(\mathcal{F}) = 0 \Rightarrow \mathrm{KS}(T) = 0$
- $\chi(\mathcal{F}) = 1 \Rightarrow \mathrm{KS}(T) = \mathbb{Z}_p$
- $\chi(\mathcal{F}) > 1 \Rightarrow \mathrm{KS}(T)$ is too big.

Structure of the Selmer group when $\chi(\mathcal{F}) = 1$

Theorem (Mazur-Rubin): relation with the Selmer group

Let κ be a primitive Kolyvagin system

- $\mathrm{ord}(\kappa_1) := \sup\{j : \kappa_1 \in p^j \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T)_{/\mathrm{tors}}\}$
- $\mathrm{ord}(\kappa_1) = \mathrm{length}(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee)$
- In particular, $\kappa_1 \neq 0 \Leftrightarrow \mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)$ is finite.

Orders of other vertices

- $H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}, T/p^{e_n}), \ \kappa_n \mapsto \overline{\kappa_n}$.
- $\mathrm{ord}(\kappa_n) := \sup\{j : \overline{\kappa_n} \in p^j \mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T/p^{e_n})\}$

Derivatives

- $\partial^{(0)}(\kappa) = \mathrm{ord}(\kappa_1)$
- $\partial^{(i)}(\kappa) = \inf\{\mathrm{ord}(\kappa_n) : \nu(n) = i\}$

Theorem (Mazur-Rubin)

$$p^{\partial^{(i)}(\kappa)} = \mathrm{Fitt}_i(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee)$$

Structure of the Selmer group when $\chi(\mathcal{F}) = 0$

- Problem There are no non-zero Kolyvagin systems.
- Solution We choose a suitable prime ℓ and consider the relaxed Selmer structure $\mathcal{F}^\ell$.

$$\Sigma \to \Sigma \cup \{l\}, \qquad H^1_{\mathcal{F}^\ell}(\mathbb{Q}_\ell, T) = H^1(\mathbb{Q}_\ell, T)$$

- $\chi(\mathcal{F}^\ell) = 1 \to$ choose a primitive Kolyvagin system κ_n.
- Consider the map

$$\mathrm{loc}_\ell : \ H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}_\ell, T) \to \frac{H^1(\mathbb{Q}_\ell, T)}{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)}$$

- $\delta_n := \mathrm{loc}_\ell(\kappa_n)$
- $\mathrm{ord}(\delta_n) = \sup \left\{ j : \ \delta_n \in p^j \left(\frac{H^1(\mathbb{Q}_\ell, T/p^{e_n})}{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/p^{e_n})} \right) \right\}$
- $\partial^{(i)}(\delta) = \inf\{\mathrm{ord}(\delta_n) : \ \nu(n) = i\}$
- $\partial^{(i)}(\delta)$ are related to the exponents of the Fitting ideals of the Selmer group $\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee$.

Structure of the Selmer group when $\chi(\mathcal{F}) = 0$

Theorem 1 (A.)

Assume that the residual representations T/pT and $T^*[p]$ have no isomorphic subquotients. Then

$$p^{\partial^{(i)}(\delta)} = \mathrm{Fitt}_i\left(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right) \; \forall i \in \mathbb{Z}^{\geq 0}$$

Theorem 2 (A.)

If we drop the non-self-duality assumption, we get

$$p^{\partial^{(i)}(\delta)} \subset \mathrm{Fitt}_i\left(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right) \; \forall i \in \mathbb{Z}^{\geq 0}$$

Moreover, for some fixed index i, the equality holds if either

- The equality does not hold for $i-1$.
- $\partial^{(i-1)}(\delta) = \infty$.

Remark

$\{\partial^{(i)}(\delta)\}_{i\in\mathbb{Z}^{\geq 0}}$ determines all the Fitting ideal of the Selmer group and, consequently, its group structure.

Elliptic curves: Selmer group over $\mathbb{Q}$

- Assume $E/\mathbb{Q}$ and consider the classical Selmer structure.
- Kato constructed an Euler system for T_pE. From it, we can obtain a Kolyvagin system $\kappa \in \mathrm{KS}(T_pE, \mathcal{F}^p)$.
- Under certain assumptions, Kato's Kolyvagin system is primitive.

$$\delta_n = \mathrm{loc}_p(\kappa_n) = \sum_{a \in (\mathbb{Z}/n)^*} \left(\left[\frac{a}{n}\right]^+ + \left[\frac{a}{n}\right]^- \right) \prod_{\ell \mid n} \log_{\eta_\ell(a)} \in \mathbb{Z}/p^{e_n}$$

- Functional equation $\Rightarrow \delta_n = 0$ when $(-1)^n \neq \varepsilon$.

$$(-1)^i = \varepsilon \Rightarrow p^{\partial^{(i)}(\delta)} = \mathrm{Fitt}_i \left(\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T^*)^\vee \right)$$

Theorem (Kim)

The structure of the Selmer group can be written explicitly. Let $r = \min \left\{ i \in \mathbb{Z}^{\geq 0} : \exists n \in \mathcal{N} : \nu(n) = i \wedge \delta_n \neq 0 \right\}$. Then

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \approx \left(\frac{\mathbb{Q}_p}{\mathbb{Z}_p} \right)^r \times \left(\frac{\mathbb{Z}}{p^{\frac{\partial^{(r)}(\delta) - \partial^{(r+2)}(\delta)}{2}}} \right)^2 \times \cdots \times \left(\frac{\mathbb{Z}}{p^{\frac{\partial^{(s-2)}(\delta) - \partial^{(s)}(\delta)}{2}}} \right)^2$$

Elliptic curves: Selmer group over number fields

- Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ be an abelian extension of degree prime-to-p.
- Assume the conductors of E and K are coprime.
- We want to study $\mathrm{Sel}(K, E[p^\infty])$. Using Shapiro's lemma

$$\mathrm{Sel}(K, E[p^\infty]) \cong \mathrm{Sel}(\mathbb{Q}, E[p^\infty]) \otimes \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})] \sim \bigoplus_{\chi} \mathrm{Sel}(\mathbb{Q}, E[p^\infty]_\chi)$$

- Kato's Euler system can be twisted to obtain a Kolyvagin system $\kappa_\chi \in KS(T_p E_{\overline{\chi}}, \mathcal{F}^p)$

$$\delta_{n,\chi} = \sum_{a \in (\mathbb{Z}/nc)^*} \chi(a) \left(\left[\frac{a}{n}\right]^+ + \left[\frac{a}{n}\right]^- \right) \prod_{\ell | n} \log_{\eta_\ell(a)} \in \mathbb{Z}_p(\chi)/p^{e_n}$$

Theorem 3 (A.)

The Galois structure of $\mathrm{Sel}(\mathbb{Q}, E[p^\infty]_\chi)$ can be described explicitly in terms of modular symbols.
Let $r = \min\left\{i \in \mathbb{Z}^{\geq 0} : \exists n \in \mathcal{N} : \nu(n) = i \wedge \delta_{n,\chi} \neq 0\right\}$.

- If χ is quadratic, by theorem 2

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]_\chi) \approx \left(\frac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)^r \times \left(\frac{\mathbb{Z}}{p^{\frac{\partial^{(r)}(\delta) - \partial^{(r+2)}(\delta)}{2}}}\right)^2 \times \cdots \left(\frac{\mathbb{Z}}{p^{\frac{\partial^{(s-2)}(\delta) - \partial^{(s)}(\delta)}{2}}}\right)^2$$

- If χ is not quadratic, by theorem 1

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]_\chi) \approx \left(\frac{\mathbb{Q}_p(\chi)}{\mathbb{Z}_p(\chi)}\right)^r \times \left(\frac{\mathbb{Z}_p(\chi)}{p^{\partial^{(r)}(\delta) - \partial^{(r+1)}(\delta)}}\right) \times \cdots \left(\frac{\mathbb{Z}_p(\chi)}{p^{\partial^{(s-1)}(\delta) - \partial^{(s)}(\delta)}}\right)$$

Remark

We can describe the structure of $\mathrm{Sel}(K, E[p^\infty])$ using modular symbols.