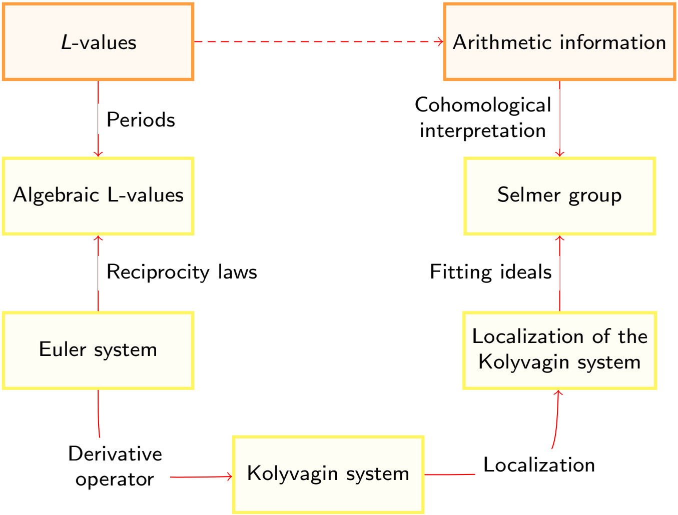
# Kolyvagin systems and Fitting ideals of Selmer group of rank 0

Alberto Angurel Andrés

University of Nottingham

30/09/2025

# General picture



# For today

- We are going to focus on

| Kolyvagin system $\kappa_n \in H^1(\mathbb{Q}, T)$ | $\longrightarrow$ | Localization $\mathrm{loc}_p(\kappa_n) \in H^1(\mathbb{Q}_p, T)$ | $\longrightarrow$ | Group structure of the Selmer group |
|---|---|---|---|---|

- We cannot apply the theory of Kolyvagin systems directly, because
  - The classical Selmer group is self-dual, so its core rank is zero.
  - There are no non-zero Kolyvagin systems for this Selmer group.

- The general theory of Kolyvagin systems only describes the structure of the Selmer group *restricted at p*.

- We extend this theory to Selmer groups of rank zero by considering Kolyvagin systems over an auxiliary Selmer structure.

# Setting and assumptions

- (H0) Let $p \geq 5$ and let $\mathbf{T}$ be free $\mathbb{Z}_p$-module of finite rank endowed with a continuous action of $G_{\mathbb{Q}}$, ramifying only at a finite amount of primes.
- (H1) $\rho: \; G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbf{T})$ is surjective.
- (H2) (will appear later)

# Selmer pre-structures



- Selmer groups are formed by the elements of the global cohomology groups $H^1(\mathbb{Q}, \mathbf{T})$ that satisfy *local conditions*.
- What is a local condition? A local condition for a prime $\ell$ is a choice of a subgroup

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, \mathbf{T}) \subset H^1(\mathbb{Q}_\ell, \mathbf{T})$$

**Definition (Selmer pre-structure)**

A Selmer pre-structure $\mathcal{F}$ is a choice of a local condition for every prime (including the archimedean one).

**Definition (Selmer group)**

The Selmer group for $\mathcal{F}$ is defined as

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

# Selmer structures

## Definition (finite cohomology)

$$H^1_f(\mathbb{Q}_\ell, \mathbf{T}) := \ker\left(H^1(\mathbb{Q}, \mathbf{T}) \to H^1(I_\ell, \mathbf{T} \otimes \mathbb{Q}_p)\right)$$

## Definition (Selmer structure)

A Selmer structure is a Selmer pre-structure such that there is a finite set of primes $\Sigma$ such that

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, \mathbf{T}) = H^1_f(\mathbb{Q}_\ell, \mathbf{T}) \ \forall \ell \notin \Sigma$$

## Proposition (Selmer groups)

If $\mathbb{Q}_\Sigma$ denotes the maximal extension of $\mathbb{Q}$ unramified outside $\Sigma$, we have that

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

## Corollary

$\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, \mathbf{T}) \subset H^1(\mathbb{Q}_\Sigma/\mathbb{Q}, \mathbf{T})$ is a finitely generated $\mathbb{Z}_p$-module.

# Fitting ideals

## Definition (Fitting ideal)

Let $M$ be a finitely generated $R$-module. Choose a resolution

$$R^n \xrightarrow{A} R^m \longrightarrow M \longrightarrow 0$$

$\mathrm{Fitt}_i^R(M)$ is the ideal generated by the minors of size $(m-i)$ of $A$.

**Fact**: Fitting ideals are well defined.

## Example

Consider $R = \mathbb{Z}_p$ and $M = \mathbb{Z}_p \times \mathbb{Z}_p/p^3 \times \mathbb{Z}_p/p^2$.A resolution is given by

$$(\mathbb{Z}_p)^3 \xrightarrow{\mu} (\mathbb{Z}_p)^3 \xrightarrow{\varepsilon} M \longrightarrow 0$$

Here $\varepsilon$ is the natural map and $\mu$ is given by the matrix $A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & p^3 & 0 \\ 0 & 0 & p^2 \end{pmatrix}$

| | |
|---|---|
| $Fitt_0(M) = (0)$, | $\mathrm{Fitt}_1(M) = (p^5)$, |
| $\mathrm{Fitt}_2(M) = (p^2) + (p^3) = (p^2)$ | $\mathrm{Fitt}_i(M) = (1)\ \forall i \geq 3$ |

# Fitting ideals over Discrete Valuation Rings

Let $R$ be a DVR (with maximal ideal $\mathfrak{m}$ and residue field $\kappa$). Then

$$M \cong R^r \times R/\mathfrak{m}^{\alpha_1} \times \cdots \times R/\mathfrak{m}^{\alpha_s}$$

for some non-negative integers $r, s, \alpha_1 \geq \ldots \geq \alpha_s$.

## Proposition

- $i \in \{0, \ldots, r-1\} \Rightarrow \mathrm{Fitt}_i(M) = (0)$
- $j \in \{0, \ldots, s-1\} \Rightarrow \mathrm{Fitt}_{r+j} = \prod_{k=j+1}^{s} \mathfrak{m}^{i_k} = \mathfrak{m}^{\sum_{k=j+1}^{s} i_k}$
- $i \geq r+s \Rightarrow \mathrm{Fitt}_i(M) = (1)$.

## Corollary

The Fitting ideals determine $i$ up to isomorphism:

- $r$ is the minimum $i$ such that $\mathrm{Fitt}_i(M) \neq 0$.
- For $i \geq 0$, $\alpha_i = \mathrm{Fitt}_{r+i+1}(M)\mathrm{Fitt}_{r+i}(M)^{-1}$.

SLIDES



# Local duality

## Definition (dual Galois modules)

- Pontryagin dual: $\mathbf{T}^\vee = \mathrm{Hom}(\mathbf{T}, \mathbb{Q}_p/\mathbb{Z}_p)$.
- Cartier dual: $\mathbf{T}^* = \mathrm{Hom}(\mathbf{T}, \mu_{p^\infty})$.

## Proposition (local duality)

The cup-product induces a non-degenerate pairing

$$H^1(\mathbb{Q}_\ell, \mathbf{T}) \times H^1(\mathbb{Q}_\ell, \mathbf{T}^*) \to H^2(\mathbb{Q}_\ell, \mu_{\mathfrak{p}^\infty}) \cong \mathbb{Q}_p/\mathbb{Z}_p$$

Moreover, $H^1_f(\mathbb{Q}_\ell, \mathbf{T})$ and $H^1_f(\mathbb{Q}_\ell, \mathbf{T}^*)$ are exact annihilators of each other.

## Corollary

$$H^1(\mathbb{Q}_\ell, \mathbf{T})^\vee \cong H^1(\mathbb{Q}_\ell, \mathbf{T}^*)$$

$$H^1_f(\mathbb{Q}_\ell, \mathbf{T})^\vee \cong \frac{H^1(\mathbb{Q}_\ell, \mathbf{T}^*)}{H^1_f(\mathbb{Q}_\ell, \mathbf{T}^*)}$$

# Dual Selmer structure

## Definition (dual Selmer structure)

The dual Selmer structure $\mathcal{F}^*$ is defined by the local conditions

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, \mathbf{T}^*) := Ann\big(H^1_{\mathcal{F}}(\mathbb{Q}_\ell, \mathbf{T})\big) \subset H^1(\mathbb{Q}_\ell, \mathbf{T}^*)$$

These are the elements of $H^1(\mathbb{Q}_\ell, \mathbf{T}^*)$ which annihilate $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ under the local duality pairing.

## Remark (well defined)

The dual Selmer structure is well defined since

$$H^1_f(\mathbb{Q}_\ell, \mathbf{T}^*) := \mathrm{Ann}\big(H^1_f(\mathbb{Q}_\ell, \mathbf{T})\big)$$

# Global duality

Let $\mathcal{F}$ and $\mathcal{G}$ be Selmer structures such that

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \subset H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \ \forall \ell$$

Then the dual local conditions satisfy the opposite relations

$$H^1_{\mathcal{G}^*}(\mathbb{Q}_\ell, T^*) \subset H^1_{\mathcal{F}^*}(\mathbb{Q}_\ell, T^*) \ \forall \ell$$

Clearly,

$$\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, \mathbf{T}) \subset \mathrm{Sel}_{\mathcal{G}}(\mathbb{Q}, \mathbf{T}), \quad \mathrm{Sel}_{\mathcal{G}^*}(\mathbb{Q}, \mathbf{T}^*) \subset \mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, \mathbf{T}^*)$$

## Global duality

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T) \arrow[r] & \mathrm{Sel}_{\mathcal{G}}(\mathbb{Q}, T) \arrow[r] & \prod_\ell \dfrac{H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)}{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)} \arrow[dlll, out=0, in=180] \\
\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee \arrow[r] & \mathrm{Sel}_{\mathcal{G}^*}(\mathbb{Q}, T^*)^\vee \arrow[r] & 0 &
\end{tikzcd}$$

# Assumptions

- (H0) Let $\mathfrak{p} \geq 5$ and let $\mathbf{T}$ be free $\mathbb{Z}_p$-module of finite rank endowed with a continuous action of $G_{\mathbb{Q}}$, ramifying only at a finite amount of primes.
- (H1) $\rho: \ G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbf{T})$ is surjective.
- (H2) $H^1(\mathbb{Q}_\ell, \mathbf{T})/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, \mathbf{T})$ is a torsion-free $\mathbb{Z}_p$-module.

# Propagation to positive characteristic



Fix $k \in \mathbb{N}$ and let $T = \mathbf{T}/p^k$. Denote $\pi : \mathbf{T} \to T$ to the canonical projection.

## Definition (propagated local condition)

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) = \pi\left(H^1_{\mathcal{F}}(\mathbb{Q}_\ell, \mathbf{T})\right)$$

## Proposition

Under assumptions (H0), (H1) and (H2), the following equalities hold true.

$$\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T) = \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, \mathbf{T})/p^k$$

$$\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T^*) = \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, \mathbf{T}^*)[p^k]$$

## Remark

A study of $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, \mathbf{T}/p^k)$ for all $k$ will determine $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, \mathbf{T})$.

# Kolyvagin primes

## Definition

A prime $\ell$ is a Kolyvagin prime if

- $\ell \equiv 1 \mod p^k$.
- $P_\ell(1) = \det(1 - \mathrm{Frob}_\ell | T) = 0$.

## Notation

$\mathcal{P}$ denotes the set of Kolyvagin primes.

$\mathcal{N}(\mathcal{P})$ denotes the set of square free products of Kolyvagin primes.

$\mathcal{N}_i(\mathcal{P})$ denotes the set of square free products of exactly $i$ Kolyvagin primes.

# Transverse local condition and finite-singular map



## Definition (transverse local condition)

$$H^1_{tr}(\mathbb{Q}_\ell, T) := \mathrm{Im}\big(H^1(\mathbb{Q}_\ell(\mu_\ell)/\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell, T)\big)$$

## Proposition (split of the local cohomology group)

If $\ell$ is Kolyvagin prime, then

$$H^1(\mathbb{Q}_\ell, T) = H^1_f(\mathbb{Q}_\ell, T) \oplus H^1_{tr}(\mathbb{Q}_\ell, T) \cong \mathbb{Z}/p^k \oplus \mathbb{Z}/p^k$$

## Definition (finite-singular map)

There is a canonical isomorphism

$$\phi_{fs} : \; H^1_f(\mathbb{Q}_\ell, T) \cong H^1_{tr}(\mathbb{Q}_\ell, T)$$

# Modified Selmer structures

Let $a, b, c \in \mathbb{N}$ be such that $abc$ is square free.

Assume all primes dividing $a$, $b$ and $c$ are Kolyvagin primes.

We can define a new Selmer structure $\mathcal{F}_a^b(c)$ by

- $H^1_{\mathcal{F}_a^b(c)}(\mathbb{Q}_\ell, T) := H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ if $\ell \nmid abc$.
- $H^1_{\mathcal{F}_a^b(c)}(\mathbb{Q}_\ell, T) = 0$ if $\ell \mid a$.
- $H^1_{\mathcal{F}_a^b(c)}(\mathbb{Q}_\ell, T) = H^1(\mathbb{Q}_\ell, T)$ if $\ell \mid b$.
- $H^1_{\mathcal{F}_a^b(c)}(\mathbb{Q}_\ell, T) = H^1_{tr}(\mathbb{Q}_\ell, T)$ if $\ell \mid c$.

# Kolyvagin systems

## Definition (Kolyvagin system)

A Kolyvagin system is a collection of elements

$$\kappa_n \in \mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T) \subset H^1(\mathbb{Q}, T)$$

for every $n \in \mathcal{N}(\mathcal{P})$, satisfying the following Kolyvagin conditions.

For every $n \in \mathcal{N}(\mathcal{P})$ and $\ell \in \mathcal{P}$ such that $\ell \nmid n$, consider the localization maps at $\ell$.

$$\mathrm{loc}_\ell(\kappa_n) \in H^1_{\mathcal{F}(n)}(\mathbb{Q}_\ell, T) = H^1_f(\mathbb{Q}_\ell, T)$$

$$\mathrm{loc}_\ell(\kappa_{n\ell}) \in H^1_{\mathcal{F}(n\ell)}(\mathbb{Q}, T) = H^1_{tr}(\mathbb{Q}_\ell, T)$$

The Kolyvagin condition for $n \in \mathcal{N}(\mathcal{P})$ and $\ell \in \mathcal{P}$ is

$$\phi_{fs}(\kappa_n) = \kappa_{n\ell}$$

## Notation

The module of Kolyvagin systems will be denoted by $\mathrm{KS}(T, \mathcal{F})$.

SLIDES



# Core rank

## Definition/proposition (core rank)

There exists a non-negative integer $\chi(\mathcal{F})$ and a non-canonical homomorphism

$$\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T) \cong \left(\mathbb{Z}/p^k\right)^{\chi(T)} \oplus \mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)$$

(possibly after swapping the roles of $T$ and $T^*$.)

The integer $\chi(T)$ is called the core rank of $T$.

## Proposition (Sakamoto, 2021)

$$\chi(\mathcal{F}_a^b(c)) = \chi(\mathcal{F}) + \nu(b) - \nu(a)$$

where $\nu(b)$ and $\nu(a)$ are the number of primes dividing $b$ and $a$, respectively.

# Core rank and Kolyvagin systems

**Theorem (Mazur-Rubin, 2004)**

- If $\chi(\mathcal{F}) = 0$, then $\mathrm{KS}(T, \mathcal{F}) = 0$.

  There are no Kolyvagin system to control the Selmer group. We will see a posible solution later in the talk.

- If $\chi(\mathcal{F}) = 1$, then $\mathrm{KS}(T, \mathcal{F}) \cong \mathbb{Z}/p^k$.

  A generator of $\mathrm{KS}(T, \mathcal{F})$ is called a primitive Kolyvagin system. We will see next that they carry information to compute all the Fitting ideals of the Selmer group $\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)$.

- If $\chi(\mathcal{F}) > 1$, then $\mathrm{KS}(T, \mathcal{F})$ is too large.

  In order to compute the Selmer group, [Mazur-Rubin, 2016] and [Burns-Sakamoto-Sano, 2025] modified the definition of Kolyvagin system in (biduals of) exterior powers of the Selmer groups.

# Selmer groups of core rank 1



## Definition (order of a Kolyvagin element)

$$\mathrm{ord}(\kappa_n) := \max\left\{j \in \{0, \ldots, k\} : \kappa_n \in p^j H^1_{\mathcal{F}(n)}(\mathbb{Q}, T)\right\}$$

## Proposition

If $\kappa$ is a primitive Kolyvagin system

$$\mathrm{ord}(\kappa_n) = \min\left\{k, \mathrm{length}\left(H^1_{(\mathcal{F}^*)(n)}(\mathbb{Q}, T^*)\right)\right\}$$

## Definition

$$\Theta_i := (p)^{\min\{\mathrm{ord}(\kappa_n):\ n \in \mathcal{N}_i\}}$$

## Theorem (Mazur-Rubin, 2004)

When $\chi(\mathcal{F}) = 1$ and $\kappa$ is a primitive Kolyvagin system

$$\Theta_i = \mathrm{Fitt}_i\left(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T)^*\right)$$

# Core rank 0

- We have seen that there are no non-zero Kolyvagin systems.
- Choose a prime $\ell$ such that $H^1_f(\mathbb{Q}_\ell, T) \cong \mathbb{Z}/p^k$.
- Note that all Kolyvagin primes satisfy the above condition, but we do not restrict to them.
- Then $\mathcal{F}^\ell$ is cartesian and $\chi(\mathcal{F}^\ell) = 1$.

**Definition**

Let $\kappa \in \mathrm{KS}(T, \mathcal{F}^\ell)$. Define

$$\delta_n = \delta_n(\kappa) := \mathrm{loc}_\ell(\kappa_n) \in H^1(\mathbb{Q}_\ell, T) \cong \mathbb{Z}/p^k$$

**Definition (order)**

$$\mathrm{ord}(\delta_n) = \max\left\{ j \in \{0, \ldots, k\} : \delta^n \in \left(p^j\right) \right\}$$

**Proposition (Kim, 2025)**

$$\mathrm{ord}(\delta_n) = \min\left\{ k, \mathrm{length}\left( H^1_{(\mathcal{F}^*)(n)}(\mathbb{Q}, T^*) \right) \right\}$$

# Fitting ideals of Selmer groups of rank 0

## Definition

$$\Theta_i := (p)^{\min\{\mathrm{ord}(\delta_n) : n \in \mathcal{N}_i(\mathcal{P})\}} = \langle \{\delta_n : \ n \in \mathcal{N}_i(\mathcal{P})\} \rangle \subset \mathbb{Z}/p^k$$

## Theorem (A., 2025)

For all $i$, we have

$$\Theta_i \subset \mathrm{Fitt}_i \left( H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*) \right)$$

The equality for some index $i$ holds if any of the following is true:

- $\Theta_{i-1} \subsetneq \mathrm{Fitt}_{i-1} \left( H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*) \right)$.
- $\Theta_{i-1} = \mathrm{Fitt}_{i-1} \left( H^1_{\mathcal{F}^*}(\mathbb{Q}, T^*) \right) = 0$.

## Remark

When $T = \mathbf{T}/p^k$ for some $\mathbb{Z}_p$-module $\mathbf{T}$ and $k$ is large enough, the ideals $\Theta_i$ determine $H^1_{\mathcal{F}}(\mathbb{Q}, \mathbf{T}^*)$ up to isomorphism

# Galois representations which are not residually self-dual

**Theorem (A., 2025)**

Under the following assumption on non self-duality,

- (N1) $T/p \ncong T^*[p]$.

Then for all $i \in \mathbb{Z}_{\geq 0}$, we have the equality

$$\Theta_i \subset \mathrm{Fitt}_i \left(H^1_{\mathcal{F}}(\mathbb{Q}, T^*)\right)$$

# Connection to Euler systems

- Assume that we have an Euler system $\mathbf{z}$.
- The Kolyvagin derivative operator produces a Kolyvagin system for $\mathbf{T}/p^k$ for all $k$ and the *canonical Selmer structure*, defined as

$$\begin{cases} H^1_{\mathcal{F}^{\mathrm{can}}}(\mathbb{Q}_\ell, \mathbf{T}/p^k) = H^1_f(\mathbb{Q}_\ell, \mathbf{T}/p^k) \text{ if } \ell \neq p, \infty \\ H^1_{\mathcal{F}^{\mathrm{can}}}(\mathbb{Q}_p, \mathbf{T}/p^k) = H^1(\mathbb{Q}_p, \mathbf{T}/p^k) \\ H^1_{\mathcal{F}^{\mathrm{can}}}(\mathbb{R}, \mathbf{T}/p^k) = H^1(\mathbb{R}, \mathbf{T}/p^k) \end{cases}$$

  This is also known as *relaxed at $p$*. Its dual Selmer structure will be called *restricted at $p$*.
- We call $\mathrm{ord}(z_{\mathbb{Q}}) = \sup\left\{j \in \mathbb{N} : z_{\mathbb{Q}} \in p^j H^1(\mathbb{Q}, \mathbf{T})_{/\mathrm{tors}}\right\}$.

**Theorem (Kolyvagin, 1995)**

$$\mathrm{ord}(z_{\mathbb{Q}}) \geq \mathrm{ord}(\kappa_1) \geq \mathrm{length}\left(H^1_{(\mathcal{F}^{\mathrm{can}})^*}(\mathbb{Q}, \mathbf{T}^*)\right)$$

# Elliptic curves: construction of the Euler system

We apply the results to $\mathbf{T} = T_pE \otimes \chi$. We assume the following:

- (E0) $E$ is defined over $\mathbb{Q}$.
- ($\chi$1) The conductor of $\chi$ is not divisible by $p$ or any bad prime of $E$.
- ($\chi$2) The order of $\chi$ is prime to $p$.

**Modularity** There exists a modular form $\mathrm{f}_\chi = \sum \chi(n) a_n q^n$ such that

$$T_{f_\chi} = T_pE \otimes \chi$$

Kato constructed an Euler system for this representation.

# Elliptic curves: Bloch-Kato Selmer structure

## Bloch-Kato Selmer structure

The classical local conditions are defined by Bloch-Kato condition

$$\begin{cases} H^1_{\mathcal{F}_{BK}}(\mathbb{Q}_\ell, \mathbf{T}) = H^1_f(\mathbb{Q}_\ell, \mathbf{T}) \quad \forall \ell \neq p \\ H^1_{\mathcal{F}_{BK}}(\mathbb{Q}_p, \mathbf{T}) = \ker\left(H^1(\mathbb{Q}_p, \mathbf{T}) \to H^1(\mathbb{Q}_p, \mathbf{T} \otimes_{Z_p} B_{\mathrm{crys}})\right) \end{cases}$$

Assume the following:

- (E1) $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathbf{T})$ is surjective.

## Proposition

Assuming (E1), $\mathcal{F}_{BK}$ satisfies all the assumptions (H0), (H1) and (H2) and $\chi(\mathcal{F}_{BK}) = 0$.

# Ellliptic curves: construction of the Kolyvagin system

## Kolyvagin derivative

The Kolyvagin derivative operator applied to Kato's Euler system, produces a Kolyvagin system for $\mathcal{F}^{\mathrm{can}} = (\mathcal{F}_{BK})^p$.

Denote $K_\chi$ to the fixed field of $\chi$. Assume:

- $(\chi 3)$ $E((K_\chi)_\mathfrak{p})[p] = \{O\}$ for every prime $\mathfrak{p}$ above $p$.

## Proposition

Assuming $(\chi 3)$, the Selmer structure $(\mathcal{F}_{BK})^p$ satisfies all the assumptions (H0), (H1) and (H2) and $\chi\big((\mathcal{F}_{BK})^p\big) = 1$.

Assume further:

- $(\chi 4)$ The Tamagawa numbers of $E$ over $K_\chi$ are prime to $p$.
- $(\chi 5)$ Iwasawa main conjecture (in the sense of Kato) holds for $f_\chi$.

## Proposition

The Kolyvagin derivative produced from Kato's Euler system is a primitive Kolyvagin system.

# Elliptic curves: Kurihara numbers



The final goal is to compute $\delta_{n,\chi} = \mathrm{loc}_p(\kappa_n)$. Assume

- (E2) The Manin constant is prime to $p$.

## Proposition (Kurihara numbers)

Let $n$ be a square-free product of Kolyvagin systems for $\mathbf{T}/p^k$.

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

where

- $c$ is the conductor of $\chi$.
- $\left[\frac{a}{cn}\right]^\pm$ are the real and imaginary part of the modular symbols of $E$.
- $\eta_\ell$ is a primitive root of $(\mathbb{Z}/\ell)^\times$ and $\log_{\eta_\ell}(a)$ is the image of the logarithm under the projection $(\mathbb{Z}/\ell)^\times \cong \mathbb{Z}/(\ell - 1) \twoheadrightarrow Z/p^k$.

## Remark

If $K/\mathbb{Q}$ is an abelian extension such that all the characters of $\mathrm{Gal}(K/\mathbb{Q})$ satisfy ($\chi$1)-($\chi$5), then the twisted Kurihara numbers determine $\mathrm{Sel}(K, E[p^\infty])$ up to isomorphism of $\mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})]$-modules.

# Proofs: first inequality

## Proposition

Consider the exact sequence of $(\mathbb{Z}/p^k)$-modules

$$0 \longrightarrow C \longrightarrow M \xrightarrow{\phi} (\mathbb{Z}/p^k)^i$$

Then

$$(p)^{\mathrm{length}(C)} \subset \mathrm{Fitt}_i(M)$$

If we choose $\phi$ and $C$ maximizing the image of $\phi$, the equality holds.

## Theorem (first inequality)

$$\Theta_i \subset \mathrm{Fitt}_i(\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T^*)^\vee)$$

**Proof** Apply the proposition to

$$0 \longrightarrow \mathrm{Sel}_{(\mathcal{F}^*)_n}(\mathbb{Q}, T) \longrightarrow \mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*) \longrightarrow \prod_{\ell | n} H^1_f(\mathbb{Q}_\ell, T^*) \cong (\mathbb{Z}/p^k)^{\nu(n)}$$

Then

$$(p)^{\mathrm{length}(\mathrm{Sel}_{(\mathcal{F}^*)(n)}(\mathbb{Q}, T^*))} \subset (p)^{\mathrm{length}(\mathrm{Sel}_{(\mathcal{F}^*)_n}(\mathbb{Q}, T^*))} \subset \mathrm{Fitt}_i(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T))$$

The proof is completed by taking the minimum over all $n \in \mathcal{N}_i(\mathcal{P})$.

# Proofs: what is needed for the equality?

- The localization map

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

has the largest possile image.

This can be achieved using Chebotarev density theorem.

- We want to choose $n \in \mathcal{N}(\mathcal{P})$ such that

$$\mathrm{Sel}_{(\mathcal{F}^*)_n}(\mathbb{Q}, T^*) = \mathrm{Sel}_{(\mathcal{F}^*)(n)}(\mathbb{Q}, T^*)$$

**Proposition**

Assume the following localization map is surjective

$$\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T) \to H^1_f(\mathbb{Q}_\ell, T)$$

Then

$$\mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, T^*) = \mathrm{Sel}_{(\mathcal{F}^*)_\ell(n)}(\mathbb{Q}, T^*)$$

# Proofs: what is needed for the equality?

**Proposition**

Assume the following localization map is surjective

$$\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T) \to H^1_f(\mathbb{Q}_\ell, T)$$

Then

$$\mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, T^*) = \mathrm{Sel}_{(\mathcal{F}^*)_\ell(n)}(\mathbb{Q}, T^*)$$

## Proof

- $$\begin{tikzcd} 0 \arrow[r] & \mathrm{Sel}_{\mathcal{F}_\ell(n)}(\mathbb{Q}, T) \arrow[r] & \mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T) \arrow[r] & H^1_f(\mathbb{Q}_\ell, T) \arrow[dll] \\ & \mathrm{Sel}_{(\mathcal{F}^*)^\ell(n)}(\mathbb{Q}, T^*)^\vee \arrow[r] & \mathrm{Sel}_{(\mathcal{F}^*)(n)}(\mathbb{Q}, T^*)^\vee \arrow[r] & 0 \end{tikzcd}$$
- $\mathrm{Sel}_{(\mathcal{F}^*)(n)}(\mathbb{Q}, T^*) = \mathrm{Sel}_{(\mathcal{F}^*)^\ell(n)}(\mathbb{Q}, T^*)$
- $\mathrm{Sel}_{(\mathcal{F}^*)_\ell(n)} = \mathrm{Sel}_{(\mathcal{F}^*)(n)} \cap \mathrm{Sel}_{(\mathcal{F}^*)(n\ell)} = \mathrm{Sel}_{(\mathcal{F}^*)^\ell(n)} \cap \mathrm{Sel}_{(\mathcal{F}^*)(n\ell)} = \mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}$

# Proofs: equality in rank one

## Proposition

$$\mathrm{Fitt}_i(\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T^*)^\vee) = \Theta_i := (p)^{\min\{\mathrm{ord}(\kappa_n):n\in\mathcal{N}_i(\mathcal{P})\}}$$

**Proof** Inductively, assume we have constructed some $n_i$ such that

$$\mathrm{Fitt}_i(\mathrm{Sel}_{\mathcal{F}(n_i)}(\mathbb{Q}, T^*)^\vee) = p^{\mathrm{ord}(\kappa_{n_i})}$$

Since the core rank is one,

$$\mathrm{Sel}_{\mathcal{F}(n_i)}(\mathbb{Q}, T) \cong (\mathbb{Z}/p^k) \oplus \mathrm{Sel}_{\mathcal{F}^*(n_i)}(\mathbb{Q}, T^*)$$

Then there exists a surjective map $\mathrm{Sel}_{\mathcal{F}(n_i)}(\mathbb{Q}, T) \to \mathbb{Z}/p^k$.

By Chebotarev density theorem, we can find a prime $\ell_{i+1}$ such that

- $\mathrm{loc}_{\ell_{i+1}} : \mathrm{Sel}_{\mathcal{F}(n_i)}(\mathbb{Q}, T) \to H^1_f(\mathbb{Q}_\ell, T)$ is surjective.
- $\mathrm{loc}_{\ell_{i+1}} : \mathrm{Sel}_{\mathcal{F}^*(n_i)}(\mathbb{Q}, T^*) \to H^1_f(\mathbb{Q}_\ell, T^*)$ has maximal image.

For $n_{i+1} := n_i\ell_{i+1}$, we get that

$$\mathrm{Sel}_{(\mathcal{F}^*)(n_{i+1})}(\mathbb{Q}, T^*) = \mathrm{Sel}_{(\mathcal{F}^*)_{\ell_{i+1}}(n_i)}(\mathbb{Q}, T^*)$$

Moreover,

$$(p)^{\mathrm{ord}(\kappa_{n_{i+1}})} = (p)^{\mathrm{length}(\mathrm{Sel}_{(\mathcal{F}^*)(n_{i+1})})} = \mathrm{Fitt}_{i+1}(\mathrm{Sel}_{(\mathcal{F}^*)}(\mathbb{Q}, T))$$

# Proofs: equality in rank zero: characteristic reduction



When $\chi(\mathcal{F}) = 0$,

$$\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T) \cong \mathrm{Sel}_{(\mathcal{F}^*)(n)}(\mathbb{Q}, T)\ \forall n \in \mathcal{N}(\mathcal{P})$$

It might not exist a surjective map $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T) \to \mathbb{Z}/p^k$.

By the structure theorem,

$$\mathrm{Sel}_{\mathcal{F}(n)} = \mathbb{Z}/p^{e_1} \times \cdots \times \mathbb{Z}/p^{e_s}$$

for some $e_1 \geq \cdots \geq e_s$.

**Trick** Swap $T$ by $T_{e_1} := T/p^{e_1}$.

Similarly, we can find a prime $\ell$ such that the maps

- $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, T_{e_1}) \to H^1_f(\mathbb{Q}_\ell, T_{e_1})$.
- $\mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, (T_{e_1})^*) \to H^1_f(\mathbb{Q}_\ell, (T_{e_1})^*)$.

are surjective. We obtain the following for the Selmer group over $T_{e_1}$.

$$\mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, (T_{e_1})^*) = \mathrm{Sel}_{(\mathcal{F}^*)_\ell(n)}(\mathbb{Q}, (T_{e_1})^*) \cong \mathbb{Z}/p^{e_2} \times \cdots \times \mathbb{Z}/p^{e_s}$$

# Proofs: equality in rank zero: recover information

**What information can we deduce from this to the Selmer group over $T$?**

- $\mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, T^*)[p^{e_1}] \cong \mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, (T_{e_1})^*) \cong \mathbb{Z}/p^{e_2} \times \cdots \times \mathbb{Z}/p^{e_s}$.
- If either $e_1 = k$ or $e_1 > e_2$, we can conclude that

$$\mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, T^*) \cong \mathbb{Z}/p^{e_2} \times \cdots \times \mathbb{Z}/p^{e_s}$$

- When $e_1 = e_2$, we only know that

$$\mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, T^*) \subset \mathrm{Sel}_{(\mathcal{F}^*)^{\ell}(n)}(\mathbb{Q}, T^*) \cong$$
$$\mathbb{Z}/p^k \times \mathrm{Sel}_{\mathcal{F}_\ell(n)}(\mathbb{Q}, T) \cong \mathbb{Z}/p^k \times \mathbb{Z}/p^{e_2} \times \cdots \times \mathbb{Z}/p^{e_s}$$

- The structure theorem implies that

$$\mathrm{Sel}_{(\mathcal{F}^*)(n\ell)}(\mathbb{Q}, T^*) \cong \mathbb{Z}/p^{f_2} \times \mathbb{Z}/p^{e_3} \times \cdots \times \mathbb{Z}/p^{e_s}$$

for some $f_2 \geq e_2$.

# Proofs: equality in rank zero: inductive step

We start with $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T)$ and choose a prime $\ell_1$ such that the localization maps for $T_{e_1}$ and $T^*_{e_1}$ are surjective, and minimizing $f_2$.

We have two cases

- If $f_2 = e_2$, then $\Theta_1 = \mathrm{Fitt}_1\left(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right)$.
- If $f_2 > e_2$, then $\Theta_1 \subsetneq \mathrm{Fitt}_1\left(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right)$.

  In this case,
  $$\mathrm{Sel}_{\mathcal{F}(\ell_1)} \cong \mathbb{Z}/p^{f_2} \times Z/p^{e_3} \times \cdots \times \mathbb{Z}/p^{e_s}$$
  Since $f_2 > e_3$, we can choose a prime $\ell_2$ in a way such that $f_3 = e_3$, so
  $$\Theta_2 = \mathrm{Fitt}_2\left(\mathrm{Sel}_{\mathcal{F}^*}(\mathbb{Q}, T^*)^\vee\right)$$

# Non self-dual representations

- Chebotarev density theorem is stronger in this case:

  For every pair of subgroups $C \subset \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T)$ and $D \subset \mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T^*)$ such that the quotients $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T)/C$ and $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T^*)/D$ are cyclic, we can find a prime $\ell$ such that the kernels of the localization maps are $C$ and $D$.

- If $\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T) \cong \mathbb{Z}/p^{e_1} \times \cdots \times \mathbb{Z}/p^{e_s}$, a technical argument constructs a prime $\ell$ such that

$$\mathrm{Sel}_{\mathcal{F}(\ell)} \cong \mathbb{Z}/p^{e_2} \times \cdots \times \mathbb{Z}/p^{e_s}$$

- Therefore, the equality $\Theta_i = \mathrm{Fitt}_i(\mathrm{Sel}_{\mathcal{F}}(\mathbb{Q}, T^*)^{\vee})$ holds for all $i$.

# Thank you for your attention!



PREPRINT

SLIDES