A new framework for Kolyvagin systems

Alberto Angurel

University of Nottingham

01/12/2025

Motivation: Birch and Swinnerton-Dyer conjecture

- Let $E/\mathbb{Q}$ be an elliptic curve.
- $E(\mathbb{Q})$ is a finitely generated abelian group, so $E(\mathbb{Q}) \cong \mathbb{Z}^r \times T$.
- Computing T is easy, but the rank is hard.

BSD conjecture

There exists an L-function

$$L(E,s) = \prod_{\ell \text{ prime}} P_\ell(\ell^{-s})^{-1}$$

where P_ℓ are Euler factors, such that

$$r = \mathrm{ord}_{s=1} L(E,s)$$

Theorem (Kolyvagin)

If $\mathrm{ord}_{s=1} L(E,s) \leq 1$, then BSD holds true.

Idea: replace points with Galois cohomology

Fix a prime p and a natural number K.

Kummer map

There is an injection

$$E(\mathbb{Q})/p^k E(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E[p^k])$$

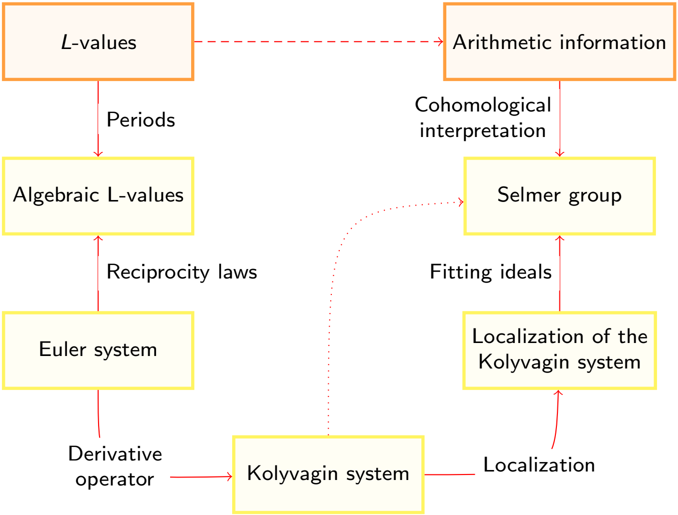
Proposition

The image of the Kummer map in the subgroup cut out by *local conditions*.

Selmer group

This is known as a *Selmer group*, and it is the object that will be studied by the Euler system machinery.

General picture



Tate module

Tate module

We will study the limit $T_pE = \varprojlim_k E[p^k]$, which is a free $\mathbb{Z}_p$-module of rank 2 endowed with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Remark

The Kummer map now reads as

$$E(\mathbb{Q}) \otimes \mathbb{Z}_p \hookrightarrow H^1(\mathbb{Q}, T_pE)$$

and the image is contained in $\mathrm{Sel}(\mathbb{Q}, T_pE)$.

Remark

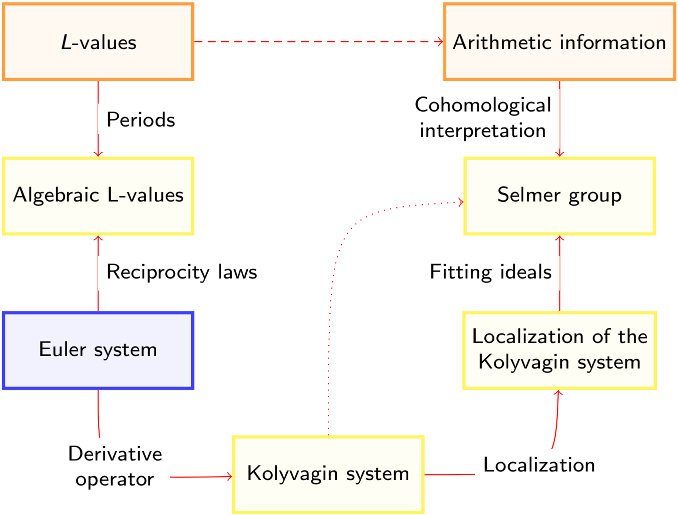
We can recover the torsion points from the Tate module since

$$E[p^k] = T_pE/p^k$$

Galois representations

We only need to assume that T is a free, finitely generated $\mathbb{Z}_p$-module, endowed with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

General picture



Assumptions

- T/pT is an absolutely irreducible Galois representation.
- The map $\rho: \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T)$ is surjective.
- The Selmer structure is cartesian (technical assumption).

Euler systems

An Euler system is a collection of classes

$$c_m \in H^1(\mathbb{Q}(\zeta_m), T)$$

satisfying norm-compatible relations as m changes.

Etymology

The norm-compatibility relations involve Euler factors.

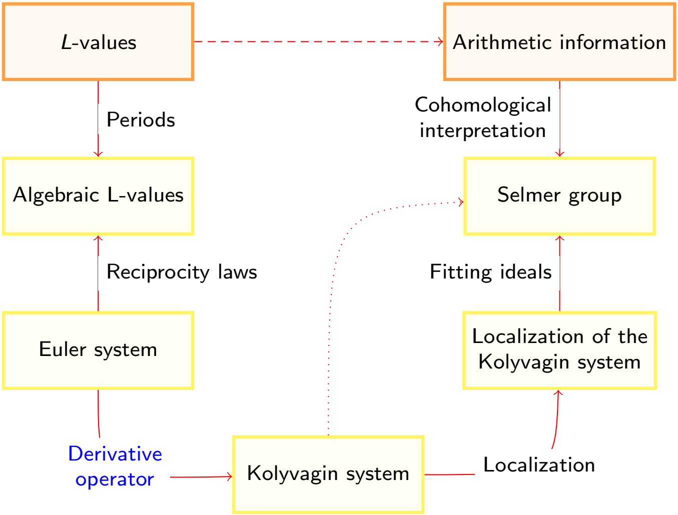
Reciprocity laws

The classes c_m are related to special (algebraic) L-values.

Construction

In general, it is hard to construct Euler systems and an active research area. For the particular case of an elliptic curve, an Euler system was constructed by Kato.

General picture



Kolyvagin derivative

Kolyvagin derivative

Fix $k \in \mathbb{N}$. Kolyvagin constructed a set of primes $\mathcal{P}$ in which

$$\ell \equiv 1 \mod p^k \ \forall \ell \in \mathcal{P}$$

We denote by $\mathcal{N}$ the set of square-free products of Kolyvagin primes $n = \ell_1 \cdots \ell_s$.
For $n \in \mathcal{N}$, we can define a Kolyvagin derivative operator

$$D_n : \ H^1(\mathbb{Q}(\zeta_n), T) \to H^1(\mathbb{Q}, T/p^k)$$

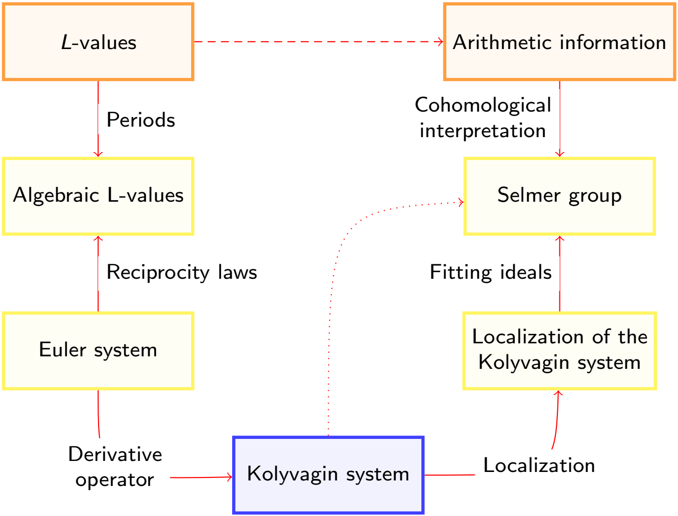
Then the Kolyvagin derivative class is

$$\kappa_n := D_n c_n \in H^1(\mathbb{Q}, T/p^k)$$

Kolyvagin system

The collection of derivative classes $\{\kappa_n : \ n \in \mathcal{N}\}$ is a Kolyvagin system.

General picture



Kolyvagin systems

Kolyvagin systems

A Kolyvagin system is a collection of classes $\{\kappa_n : n \in \mathcal{N}\}$ such that

- $\kappa_n \in H^1(\mathbb{Q}, T/p^k)$
- κ_n is unramified at primes not dividing n or p and *interestingly* ramified at primes dividing n.
- There is a relation between κ_n and $\kappa_{n\ell}$ for all $n \in \mathcal{N}$ and $\ell \in \mathcal{P}$.

Remark

There are Kolyvagin systems for all $k \in \mathbb{N}$. However, we cannot define Kolyvagin systems on $H^1(\mathbb{Q}, T)$, since there is no prime $\ell \equiv 1 \mod p^k$ for every k.

Dual Selmer group

- The dual Galois representation is $T^* = \mathrm{Hom}(T, \mu_{p^\infty})$.
- For every Selmer group, there exists the concept of a dual Selmer group $\mathrm{Sel}(\mathbb{Q}, T^*)$, defined in the cohomology of T^* via local Tate duality.
- Poitou-Tate duality relates the original Selmer group with the dual Selmer group.

Core rank

- There exists an integer χ such that

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

- χ is known as the core rank of the Selmer group.

Theorem (Mazur-Rubin, 2004)

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

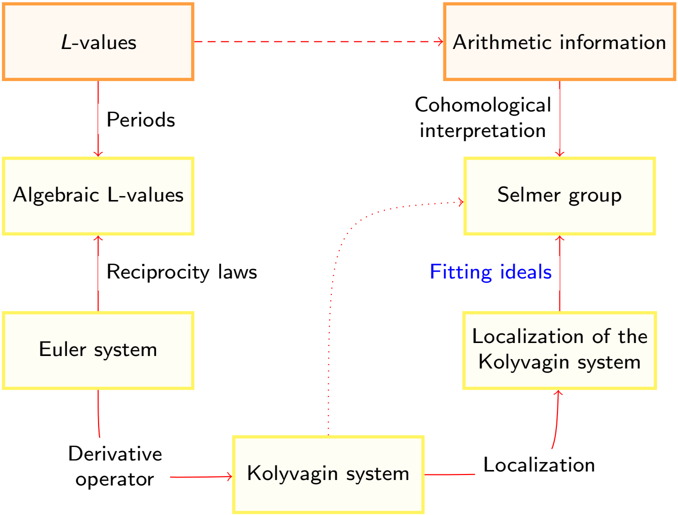
  There are no Kolyvagin system to control the Selmer group. We will see a possible solution later in the talk.

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

- If $\chi > 1$, then $\mathrm{KS}(T/p^k)$ 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.

General picture



Fitting ideals

Definition (Fitting ideal)

Let M be a finitely presented 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 ε is the natural map and μ 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 κ). 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 M up to isomorphism:

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

Fitting ideals over the Iwasawa algebra

Iwasawa algebra

The Iwasawa algebra can be represented as

$$\Lambda = \mathbb{Z}_p[[X]]$$

Structure theorem

Ever finitely generated Λ-module is pseudo-isomorphic to

$$M \approx \Lambda^r \times \prod \frac{\Lambda}{(p)^{\alpha_i}} \times \prod \frac{\Lambda}{(f_j)^{\beta^j}}$$

where f_j are irreducible distinguished polynomials.

Fitting ideals

Fitting ideals can recover the structure of a finitely generated Iwasawa module up to pseudo-isomorphism.

Indices and theta-ideals

Index of an element

Let M be an R-module and let $a \in M$. Denote by $M^+ = \mathrm{Hom}(M, R)$ the dual of M. There is a canonical map

$$\Phi : \; M \to M^{++} : \; x \mapsto (\varphi \mapsto \varphi(x))$$

Note that $\Phi(a) \in \mathrm{Hom}(M^+, R)$. Define the index of a as

$$\mathrm{ind}(a, M) = \mathrm{Im}(\Phi(a))$$

Remark

If R is a principal, artinian local ring, with π being a generator of the maximal ideal. Then

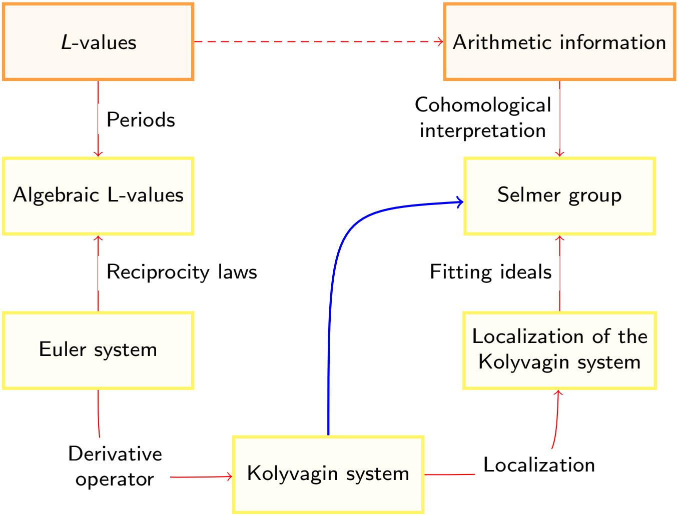
$$\mathrm{ind}(a, M) = \max\{j \in \mathbb{N} : \; j \in \pi^j M\}$$

Theta ideals

We denote by $\mathcal{N}_i$ the set of square-free products of exactly i Kolyvagin primes. We define the i^{th} theta ideal of a Kolyvagin system as

$$\Theta_i(\kappa) := \sum_{n \in \mathcal{N}_i} \mathrm{ind}(\kappa_n, H^1(\mathbb{Q}, T))$$

General picture



Core rank 1

Recall

When $\chi = 1$, the module of Kolyvagin system is

$$\mathrm{KS}(T/p^k) \cong \mathbb{Z}/p^k$$

Primitive Kolyvagin systems

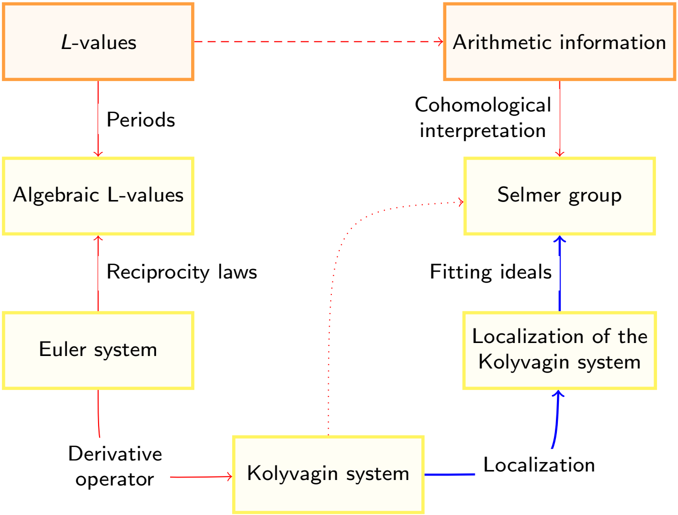
We call a Kolyvagin system primitive if it generates $\mathrm{KS}(T/p^k)$.

Theorem (Mazur-Rubin, 2004)

When $\chi = 1$ and κ is a primitive Kolyvagin system

$$\Theta_i(\kappa) = \mathrm{Fitt}_i\Big(\mathrm{Sel}\Big(\mathbb{Q}, (T/p^k)^*\Big)\Big) = \mathrm{Fitt}_{i+1}\Big(\mathrm{Sel}(\mathbb{Q}, T/p^k)\Big)$$

General picture



Core rank 0: non-self-dual Galois representations

- We need to relax the local condition at one prime ℓ in order to obtain a rank one Selmer group.
- Fix a primitive Kolyvagin system $\kappa = (\kappa_n)_{n \in \mathcal{N}}$.
- We now consider the cohomology classes

$$\delta_n := \mathrm{loc}_\ell(\kappa_n)$$

- We define the rank 0 theta-ideals of κ as

$$\boxed{\Theta_i^{(0)}(\kappa) := \sum_{n \in \mathcal{N}_i(\mathcal{P})} \mathrm{ind}(\delta_n)}$$

Theorem (A., 2025)

If T is **not** a residually self-dual Galois representation, then

$$\Theta_i^{(0)}(\kappa) = \mathrm{Fitt}_i(\mathrm{Sel}(\mathbb{Q}, T/p^k))$$

Theorem (A., 2025)

For all i, we have

$$\Theta_i^{(0)}(\kappa) \subset \mathrm{Fitt}_i\left(\mathrm{Sel}(\mathbb{Q}, T/p^k)\right)$$

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

- $\Theta_{i-1}^{(0)}(\kappa) \subsetneq \mathrm{Fitt}_{i-1}\left(\mathrm{Sel}(\mathbb{Q}, T/p^k)\right)$.
- $\Theta_{i-1}^{(0)}(\kappa)\left(\mathrm{Sel}(\mathbb{Q}, T/p^k)\right) = 0$.

Conjecture

If T is a self-dual Galois representation, either

- $\Theta_i^{(0)}(\kappa)$ for all even i.
- $\Theta_i^{(0)}(\kappa)$ for all odd i.

Example: elliptic Curve

Limit of Selmer groups

Note that $T_pE^* = E[p^\infty]$ and that

$$\mathrm{Sel}(\mathbb{Q}, E[p^\infty]) = \varinjlim_k \mathrm{Sel}(\mathbb{Q}, E[p^k])$$

Kurihara numbers

Kato's Euler system produces a Kolyvagin systems and $\mathrm{ind}(\delta_n) = \mathrm{ind}(\widetilde{\delta}_n)$, where $\widetilde{\delta}_n$ are known as the Kurihara numbers and are defined by the formula

$$\widetilde{\delta}_n := \sum_{a \in (\mathbb{Z}/n)^\times} \left(\left[\frac{a}{n}\right]^+ + \left[\frac{a}{n}\right]^- \right) \prod_{\ell \mid n} \log_{\eta_\ell}(a) \in \mathbb{Z}_p$$

By the functional eqqation of the L-function, the conjecture holds true in this case.

$\mathbb{Z}_p$-extensions

In Iwasawa theory, we are interested in the Selmer group over a $\mathbb{Z}_p$-extension. By Shapiro's lemma, it is equivalent to study Galois representations $\mathbf{T}$ with coefficients over the Iwasawa algebra Λ.

Selmer groups over the Iwasawa algebra

If $\mathbf{T}$ is a (finitely generated, free) Λ-module, it is more difficult to study the Selmer group as a limit of Selmer groups with finite coefficients, since the representation theory over the finite quotients of Λ is more complicated.

Idea

Use patched cohomology to overcome the lack of Kolyvagin primes and generalise the notion of Kolyvagin system to infinite coefficient rings.

Ultrafilters

Filters and ultrafilters

A filter of the natural numbers is a subset $\mathcal{U} \subset \mathbb{P}(\mathbb{N})$ such that

- $S \in \mathcal{U},\ S \subset T \Rightarrow T \in \mathcal{U}$
- $S_1, S_2 \in \mathcal{U} \Rightarrow S_1 \cap S_2 \in \mathcal{U}$

$\mathcal{U}$ is said to be an ultrafilter if

- For every $S \subset \mathcal{N}$, either $S \in \mathcal{U}$ or $(\mathbb{N} \setminus S) \in \mathcal{U}$.

Principal ultrafilters

Assume there is a finite set $S \in \mathcal{U}$. Then there is an element $a \in S$ such that

$$\mathcal{U} = \{T \subset \mathbb{N} :\ a \in T\}$$

In this case, $\mathcal{U}$ is said to be a principal ultrafilter.

Fix a non-principal ultrafilter $\mathcal{U}$.

Patching

Patching (Sweeting 2021)

Let $(M_n)_{n\in\mathbb{N}}$ be a sequence of sets/groups/rings, we define the patching via the ultrafilter $\mathcal{U}$ as

$$\mathcal{U}(M_n) = \prod_{n\in\mathcal{N}} M_n \Big/ \sim$$

where two sequences $(\alpha_n)_{n\in\mathbb{N}}$ and $(\beta_n)_{n\in\mathbb{N}}$ are said to be equivalent if $\alpha_n = \beta_n$ for $\mathcal{U}$-many n.

Proposition

$\mathcal{U}$ is an exact functor.

Constant patching of finite groups

If M is a finite group and $M_n = M$ for all $n \in \mathbb{N}$, then

$$\mathcal{U}(M_n) = M$$

Ultraprimes

Ultraprimes

An ultraprime is an element of $\mathcal{U}(\{\text{primes}\})$, so it can be represented by a sequence

$$\mathfrak{u} = (\ell_1, \dots, \ell_n, \dots)$$

Kolyvagin ultraprimes

An ultraprime $\mathfrak{u} = (\ell_i)_{i \in \mathbb{N}}$ is said to be a Kolyvagin ultraprime if, for every finite quotient of Λ, ℓ_i is a Kolyvagin prime for $\mathcal{U}$-many i.

Patched cohomology (Sweeting, 2021)

Finite coefficients

Assume T is a finite group endowed with an action a sequence of groups $G = (G_n)$. We define the patched cohomology as

$$\mathbf{H}^1(G, T) = \mathcal{U}(H^1(G, T))$$

Profinite coefficients

Assume T is profinite, the patched cohomology is defined as

$$\mathbf{H}^1(G, T) = \varprojlim_{T \twoheadrightarrow T'} \mathbf{H}^1(G, T')$$

where T' runs through the finite quotients of T.

Ind-finite coefficients

If T is ind-finite, then

$$\mathbf{H}^1(G, T) = \varinjlim_{T' \hookrightarrow T} \mathbf{H}^1(G, T')$$

where T' runs through the finite submodules of T.

Local and global patched cohomology

Local patched cohomology

Let T be a Galois representation, i.e., T is endowed with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $\mathfrak{u} = (\ell_n)$ be an ultraprime. Since $\mathrm{Gal}(\overline{\mathbb{Q}_{\ell_i}}/\mathbb{Q}_{\ell_i})$ is contained in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, it also acts on T.

Then the patched local cohomology $\mathbf{H}^1(\mathbb{Q}_{\mathfrak{u}}, T)$ is the patching of the sequence of local Galois groups with coefficients in T. In particular, when T is finite,

$$\mathbf{H}^1(\mathbb{Q}_{\mathfrak{u}}, T) = \mathcal{U}(H^1(\mathrm{Gal}(\overline{\mathbb{Q}_{\ell_i}}/\mathbb{Q}_{\ell_i}), T))$$

Global patched cohomology

There is also a notion of patched global cohomology unramified outside the square-free (formal) product of ultraprimes $n = \mathfrak{u}_1 \cdots \mathfrak{u}_s$, denoted by

$$\mathbf{H}^1(\mathbb{Q}_{\Sigma_n}/\mathbb{Q}, T)$$

Selmer groups

We can extend the notion of Selmer groups to this setting and define local conditions on the local cohomology of ultraprimes. We recover the classical Selmer groups when the local condition at every (non-constant) ultraprime is the unramified cohomology.

Notation

- $\mathcal{P}$: set of Kolyvagin ultraprimes.
- $\mathcal{N}(\mathcal{P})$: set of square-free products of Kolyvagin ultraprimesprimes
- $\mathcal{N}_i(\mathcal{P})$: set of square-free products of i Kolyvagin ultraprimes.

Ultra-Kolyvagin systems

A Kolyvagin system is a collection $\{\kappa_n : \ n \in \mathcal{N}\}$ such that

- $\kappa_n \in \mathrm{Sel}_{\mathcal{F}(n)}(\mathbb{Q}, \mathbf{T}) \subset \mathbf{H}^1(\mathbb{Q}_{\Sigma_n}/\mathbb{Q}, \mathbf{T})$
- κ_n and $\kappa_{n\ell}$ satisfy a Kolyvagin relation for all $n \in \mathcal{N}$ and

Theta ideals

$$\Theta_i(\kappa) := \sum_{n \in \mathcal{N}_i(\mathcal{P})} \mathrm{ind}(\kappa_n)$$

Selmer group over cyclotomic $\mathbb{Z}_p$-extensions

Assumptions

- T is residually irreducible.
- $\rho: \ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T)$ is surjective.
- The Selmer structure is cartesian.
- $\frac{\mathbf{H}^1(\mathbb{Q}_\mu, T \otimes \Lambda)}{\mathbf{H}^1_{\mathcal{F}}(\mathbb{Q}_\mu, T \otimes \Lambda)}$ is Λ-torsion free

Theorem (A., in progress)

Assume that the core rank is positive. Then the module of ultra-Kolyvagin systems $\mathrm{KS}(T \otimes \Lambda)$ is free of rank one over Λ. Moreover, if we choose a primitive ultra-Kolyvagin system κ, then

$$\Theta_i(\kappa) =_{f.i.} \mathrm{Fitt}^i_\Lambda(\mathrm{Sel}(\mathbb{Q}, \mathbf{T}^*)^\vee)$$

Corollary

The ideals $\Theta_i(\kappa)$ determine the the structure of the Selmer group up to pseudo-isomorphism.

Thank you for your attention!