Ben Forrás (joint with Katharina Müller)

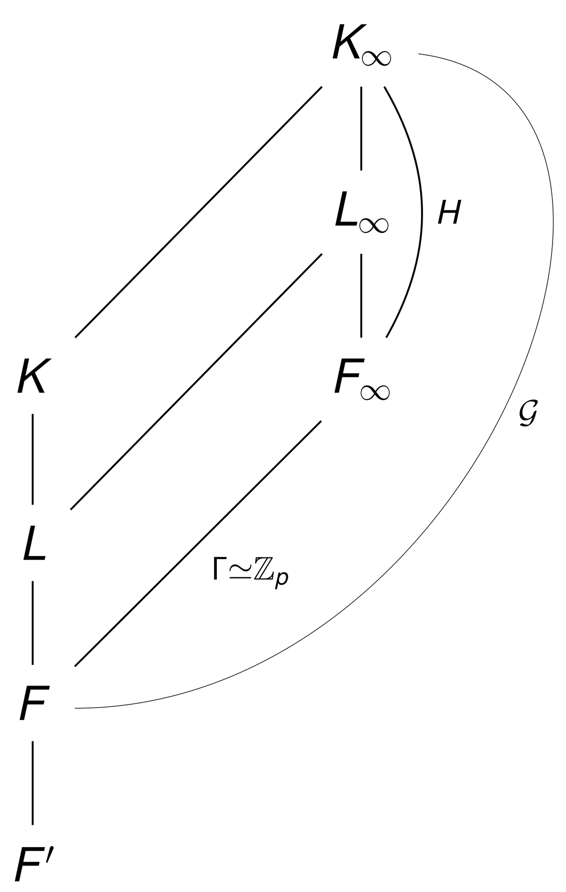
Signed Selmer groups of supersingular elliptic curves in weakly ramified base fields

Universität der Bundeswehr München

arXiv:2407.08430, accepted for publication in *Research in Number Theory*

Setup

- $p \geq 5$ rational prime
- $F'/\mathbb{Q}$ finite extension
- E/F' elliptic curve, good reduction at all p-adic places
- F/F' finite extension, F_∞/F cyclotomic $\mathbb{Z}_p$-extension



- K/F finite Galois
- Σ finite set of places of F containing p-adic, infinite, and bad places, and those ramifying in K/F or F/F'
- $\mathcal{G} = \mathrm{Gal}(K_\infty/F) \simeq H \rtimes \Gamma$ not necessarily abelian
- $\Lambda(\mathcal{G}) := \mathbb{Z}_p[\![\mathcal{G}]\!]$ completed group ring
- Fix a lift of Γ to $\mathcal{G}$, so that $\Lambda := \mathbb{Z}_p[\![\Gamma]\!] \subset \Lambda(\mathcal{G})$

Assumptions

1. There is a p-adic place where E has supersingular reduction.
2. p is completely split in $F'/\mathbb{Q}$
3. For all p-adic places v of F where E has supersingular reduction:
   (a) the ramification index $e_v(K/F')$ is not divisible by $p^2 - 1$,
   (b) there is a finite weakly ramified extension $\mathcal{K}_v$ of $\mathbb{Q}_p$ such that $\mathcal{K}_v \cap \mathbb{Q}_{p,\infty} = \mathbb{Q}_p$ and $K_v \subseteq \mathcal{K}_v\mathbb{Q}_{p,\infty}$.

Weakly ramified extension of local fields: the second ramification group vanishes. So arbitrary tame and even some wild ramification is allowed!

This generalises previous work of M.F. Lim, where p-adic supersingular places v were *unramified* in K/F'.

Definition of signed Selmer groups

Coherent choice of signs along the cyclotomic tower: For each $v \mid p$ supersingular place, choose $s_v \in \{+,-\}$. Let F_n/F be the unique degree p^n extension inside F_∞. For $u \mid v$ place in F_n, let $s_u := s_v$.

Let $\widehat{E}^\pm$ be the plus/minus norm subgroups of Kobayashi.

$$\mathrm{Sel}^{\vec{s}}(E/F_n) := \ker\left(H^1(F_n, E[p^\infty]) \xrightarrow{\oplus \mathrm{res}_v} \bigoplus_{\substack{v\in\Sigma \\ v\nmid p}} H^1(F_v, E[p^\infty]) \oplus \bigoplus_{\substack{v\in\Sigma \\ v\mid p \\ \text{ordinary}}} \frac{H^1(F_v, E[p^\infty])}{E(F_v)\otimes \mathbb{Q}_p/\mathbb{Z}_p} \oplus \bigoplus_{\substack{v\in\Sigma \\ v\mid p \\ \text{sup.s.}}} \frac{H^1(F_{n,v}, E[p^\infty])}{\widehat{E}^{s_v}(F_{n,v})\otimes \mathbb{Q}_p/\mathbb{Z}_p} \right)$$

$$\mathrm{Sel}^{\vec{s}}(E/F_\infty) := \varinjlim_n \mathrm{Sel}^{\vec{s}}(E/F_n), \qquad X^{\vec{s}}(E/F_\infty) := \mathrm{Hom}\left(\mathrm{Sel}^{\vec{s}}(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p\right)$$

$X^{\vec{s}}(E/F_\infty)$ is expected to be a torsion Λ-module.

Main technical result: cohomology of local conditions

$\mathcal{K}/\mathbb{Q}_p$ finite extension such that $p^2 - 1 \nmid e(\mathcal{K}/\mathbb{Q}_p)$ and $\mathcal{K}/\mathbb{Q}_p$ weakly ramified and $\mathbb{Q}_{p,\infty} \cap \mathcal{K} = \mathbb{Q}_p$

Proposition. For all $G \leq \mathrm{Gal}(\mathcal{K}/\mathbb{Q}_p)$:

$$H^i\left(G, \frac{H^1(\mathcal{K}_\infty, E[p^\infty])}{\widehat{E}^\pm(\mathcal{K}_\infty)\otimes\mathbb{Q}_p/\mathbb{Z}_p}\right) = \begin{cases} \dfrac{H^1(\mathcal{K}_\infty^G, E[p^\infty])}{\widehat{E}^\pm(\mathcal{K}_\infty^G)\otimes\mathbb{Q}_p/\mathbb{Z}_p} & i = 0 \\ 0 & i > 0 \end{cases}$$

The proof uses cohomological triviality of $\widehat{E}(\mathcal{K}_n)$ for all $n \geq 0$, relying on a result of Ellerbrock–Nickel (2018) on formal groups. This is where weak ramification is used.

The Proposition was proved in the unramified abelian case by M.F. Lim (2021).
His proof uses the existence a sequence of norm coherent points along the cyclotomic tower established by Kobayashi ($\mathcal{K} = \mathbb{Q}$, 2003) and B.D. Kim ($\mathcal{K}/\mathbb{Q}$ unramified abelian).
Such a sequence is not available in our ramified setting.

Kida formula

- $P_1 := \{v \in \Sigma : v \nmid p, p \mid e_v(K/L),\ E \text{ has split multiplicative reduction at } v\}$
- $P_2 := \{v \in \Sigma : v \nmid p, p \mid e_v(K/L),\ E \text{ has good reduction at } v \text{ and } E(K)[p] \neq 0\}$

Fix a (non-canonical) isomorphism $\Lambda = \mathbb{Z}_p[\![\Gamma]\!] \simeq \mathbb{Z}_p[\![T]\!]$.
For X a torsion Λ-module, there is a homomorphism of Λ-modules

$$X \to \bigoplus_{i\in I} \Lambda/p^{m_i}\Lambda \oplus \bigoplus_{j\in J} \Lambda/F_j(T)\Lambda$$

with finite kernel and cokernel, I, J are finite sets, $F_j(T)$ are certain polynomials.

$$\lambda(X) := \sum_{j\in J} \deg(F_j), \qquad \mu(X) := \sum_{i\in I} m_i, \qquad \theta(X) := \max\{m_i : i \in I\}$$

Theorem. Suppose that:

- K/L is a subextension of K/F satisfying Assumption 3 above
- $\mathrm{Gal}(K/L)$ is a p-group
- $X^{\vec{s}}(E/K_\infty)$ is Λ-torsion,
- $\theta(X^{\vec{s}}(E/K_\infty)) \leq 1$.

For $v \in \Sigma$, let e_v denote the ramification index of a place above v in K_∞/L_∞. Then:

$$\lambda\left(X^{\vec{s}}(E/K_\infty)\right) = [K_\infty : L_\infty] \cdot \lambda\left(X^{\vec{s}}(E/L_\infty)\right) + \sum_{v\in P_1}(e_v - 1) + 2\sum_{v\in P_2}(e_v - 1),$$

$$\mu\left(X^{\vec{s}}(E/K_\infty)\right) = [K_\infty : L_\infty] \cdot \mu\left(X^{\vec{s}}(E/L_\infty)\right).$$

Previously known in the ordinary case: Hachimori–Matsuno (1998) and Hachimori–Sharifi (2005), and in the supersingular unramified case: M.F. Lim (2021)

Integrality of characteristic elements

- Let $n_0 \gg 0$ such that $\Gamma_0 := \Gamma^{p^{n_0}}$ is central in $\mathcal{G}$, and let $\Lambda(\Gamma_0) := \mathbb{Z}_p[\![\Gamma_0]\!] \subset \Lambda(\mathcal{G})$.
- A $\Lambda(\Gamma_0)$-order $\mathfrak{M}$ in $\mathcal{Q}(\mathcal{G})$ is called *graduated* if there exist orthogonal indecomposable idempotents $e_1, \dots, e_t \in \mathfrak{M}$ such that $\sum_{i=1}^t e_i = 1$ and $e_i\mathfrak{M}e_i \subset e_i\mathcal{Q}(\mathcal{G})e_i$ is a maximal order for each $i = 1, \dots t$. Maximal orders are graduated.
- $\mathcal{Q}(\mathcal{G}) := \mathrm{Quot}(\Lambda(\mathcal{G}))$ total ring of quotients of the Iwasawa algebra $\Lambda(\mathcal{G})$.
- $\partial : K_1(\mathcal{Q}(\mathcal{G})) \to K_0(\Lambda(\mathcal{G}), \mathcal{Q}(\mathcal{G}))$ connecting homomorphism in the localisation exact sequence of relative K-theory.
- For X a finitely generated $\Lambda(\mathcal{G})$-module that is torsion over Λ and has projective dimension $\mathrm{pd}_{\Lambda(\mathcal{G})} X \leq 1$, a *characteristic element* is some $\xi_X \in K_1(\mathcal{Q}(\mathcal{G}))$ whose image $\partial(\xi_X) \in K_0(\Lambda(\mathcal{G}), \mathcal{Q}(\mathcal{G}))$ agrees with the class of X in the relative K_0-group.

Theorem. Suppose that:

- $X^{\vec{s}}(E/K_\infty)$ is Λ-torsion
- every ordinary p-adic place $v \in \Sigma$ is either tamely ramified in K/F or non-anomalous (i.e. if $w \mid v$ for w a place of K, then $p \nmid \#\widetilde{E}(\widetilde{K_w})$),
- $P_1 = P_2 = \emptyset$ (where P_1, P_2 are as in the Kida formula)

Let ξ_E be a characteristic element of $X^{\vec{s}}(E/K_\infty)$. Then for every graduated $\Lambda(\Gamma_0)$-order $\mathfrak{M}$ in $\mathcal{Q}(\mathcal{G})$ containing $\Lambda(\mathcal{G})$, we have

$$\xi_E \in \mathrm{im}\left(\mathfrak{M} \cap \mathcal{Q}(\mathcal{G})^\times \to K_1(\mathcal{Q}(\mathcal{G}))\right).$$

Previously known for maximal orders in the ordinary and split multiplicative case for elliptic curves admitting certain isogenies by Nichifor–Palvannan (2019), supersingular unramified case by M.F. Lim (2021).