Class Groups and (Fine) Selmer Groups in Iwasawa Theory

Debanjana Kundu

CTNT 2020

June 14, 2020

Iwasawa Theory

Iwasawa theory involves the study of Galois modules over infinite towers of number fields.

Iwasawa Theory

Iwasawa theory involves the study of Galois modules over infinite towers of number fields.

IDEA: Studying class groups or Selmer groups in isolation is hard. But, these properties stabilize in *certain* towers; in such cases studying them becomes easier.

Classical Iwasawa Theory

Consider the tower

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \bigcup_n \mathbb{Q}_n =: \mathbb{Q}_{cyc}$$

where $\mathbb{Q}_n$ is the unique subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Classical Iwasawa Theory

Consider the tower

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \bigcup_n \mathbb{Q}_n =: \mathbb{Q}_{cyc}$$

where $\mathbb{Q}_n$ is the unique subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

So $\Gamma := \mathrm{Gal}(\mathbb{Q}_{cyc}/\mathbb{Q}) \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p$.

Classical Iwasawa Theory

Consider the tower

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \bigcup_n \mathbb{Q}_n =: \mathbb{Q}_{cyc}$$

where $\mathbb{Q}_n$ is the unique subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

So $\Gamma := \text{Gal}(\mathbb{Q}_{cyc}/\mathbb{Q}) \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p$.

$\mathbb{Q}_{cyc}$, called the *cyclotomic extension* is the *unique* $\mathbb{Z}_p$ extension of $\mathbb{Q}$ contained inside $\mathbb{Q}(\mu_{p^\infty})$.

Classical Iwasawa Theory

Consider the tower

$$\mathbb{Q} = \mathbb{Q}_0 \subset \mathbb{Q}_1 \subset \cdots \subset \mathbb{Q}_n \subset \cdots \subset \bigcup_n \mathbb{Q}_n =: \mathbb{Q}_{cyc}$$

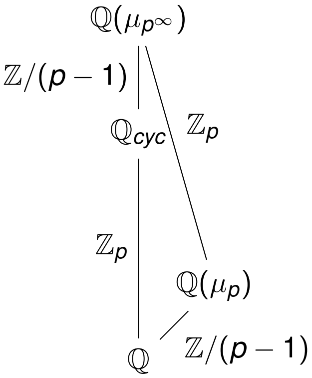
where $\mathbb{Q}_n$ is the unique subfield of $\mathbb{Q}(\mu_{p^{n+1}})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

So $\Gamma := \mathrm{Gal}(\mathbb{Q}_{cyc}/\mathbb{Q}) \simeq \varprojlim \mathbb{Z}/p^n\mathbb{Z} \simeq \mathbb{Z}_p$.

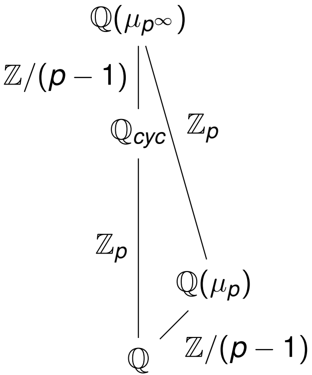
$\mathbb{Q}_{cyc}$, called the *cyclotomic extension* is the *unique* $\mathbb{Z}_p$ extension of $\mathbb{Q}$ contained inside $\mathbb{Q}(\mu_{p^\infty})$.

For a number field $F/\mathbb{Q}$, the cyclotomic $\mathbb{Z}_p$ extension always exists but it may not be the only $\mathbb{Z}_p$-extension.

Field Diagram



Field Diagram



We have

$$\mathrm{Gal}\left(\mathbb{Q}\left(\mu_{p^\infty}\right)/\mathbb{Q}\right) \simeq \mathbb{Z}_p^\times \simeq \mathbb{Z}_p \times \mathbb{Z}/(p-1) \simeq (1+p\mathbb{Z}_p) \times \mathbb{Z}/(p-1).$$

Iwasawa algebra

Let G be a profinite group.

Iwasawa algebra

Let G be a profinite group.

Definition

The ***Iwasawa algebra****,* $\Lambda(G) := \varprojlim \mathbb{Z}_p[G/H]$
where the inverse limit runs over all open normal subgroups H of G and is taken with respect to the natural surjection maps.

Iwasawa algebra

Let G be a profinite group.

Definition

*The **Iwasawa algebra**, $\Lambda(G) := \varprojlim \mathbb{Z}_p[G/H]$ where the inverse limit runs over all open normal subgroups H of G and is taken with respect to the natural surjection maps.*

Let $G = \Gamma = \mathrm{Gal}\,(F_{cyc}/F) \simeq \mathbb{Z}_p$. Then

Iwasawa algebra

Let G be a profinite group.

Definition

The ***Iwasawa algebra****,* $\Lambda(G) := \varprojlim \mathbb{Z}_p[G/H]$
where the inverse limit runs over all open normal subgroups H of G and is taken with respect to the natural surjection maps.

Let $G = \Gamma = \mathrm{Gal}\,(F_{cyc}/F) \simeq \mathbb{Z}_p$. Then

$$\Lambda(\Gamma) = \mathbb{Z}_p[\![\Gamma]\!] \xrightarrow{\sim} \mathbb{Z}_p[\![T]\!]$$
$$\gamma \mapsto 1 + T$$

Structure Theorem: Iwasawa and Serre

Theorem

Let M be a finitely generated $\Lambda(\Gamma)$-module. Then

$$M \sim \Lambda(\Gamma)^r \oplus \left(\bigoplus_{i=1}^{t} \Lambda(\Gamma)/p^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda(\Gamma)/f_j^{m_j} \right)$$

where f_j are irreducible distinguished polynomials in $\mathbb{Z}_p[T]$.

Invariants for M

$$M \sim \Lambda(\Gamma)^r \oplus \left(\bigoplus_{i=1}^{t} \Lambda(\Gamma)/p^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda(\Gamma)/f_j^{m_j} \right)$$

The integer r is called the **rank.**

Invariants for M

$$M \sim \Lambda(\Gamma)^r \oplus \left(\bigoplus_{i=1}^{t} \Lambda(\Gamma)/p^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda(\Gamma)/f_j^{m_j} \right)$$

The integer r is called the **rank.**

If $r = 0$, we define two more invariants:

Invariants for M

$$M \sim \Lambda(\Gamma)^r \oplus \left(\bigoplus_{i=1}^{t} \Lambda(\Gamma)/p^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda(\Gamma)/f_j^{m_j} \right)$$

The integer r is called the **rank.**
If $r = 0$, we define two more invariants:
The μ-invariant is defined

$$\mu(M) := \sum_{i=1}^{t} n_i.$$

Invariants for M

$$M \sim \Lambda(\Gamma)^r \oplus \left(\bigoplus_{i=1}^{t} \Lambda(\Gamma)/p^{n_i} \right) \oplus \left(\bigoplus_{j=1}^{s} \Lambda(\Gamma)/f_j^{m_j} \right)$$

The integer r is called the **rank.**
If $r = 0$, we define two more invariants:
The μ-invariant is defined

$$\mu(M) := \sum_{i=1}^{t} n_i.$$

The λ-invariant is defined

$$\lambda(M) := \sum_{j=1}^{s} m_j \deg(f_j).$$

Classical Theorem

Theorem (Iwasawa)

Let F_∞/F be a $\mathbb{Z}_p$-extension and let e_n be the integer so that $p^{e_n}||h_n$ where h_n is the order of the class group of F_n. There exist integers $\lambda,\ \mu \geq 0$ and ν such that

$$e_n = \lambda n + \mu p^n + \nu$$

for all n sufficiently large where $\lambda,\ \mu,\ \nu$ are all independent of n.

Classical $\mu = 0$ Conjecture

Conjecture (Iwasawa)

In a cyclotomic $\mathbb{Z}_p$-extension, $\mu = 0$.

Classical $\mu = 0$ Conjecture

Conjecture (Iwasawa)

In a cyclotomic $\mathbb{Z}_p$-extension, $\mu = 0$.

This is known only when $F/\mathbb{Q}$ is an Abelian extension. This was proved by Ferrero-Washington (1979).

Selmer Groups of Elliptic Curves

Consider an elliptic curve E/F and p be an odd prime.

Selmer Groups of Elliptic Curves

Consider an elliptic curve E/F and p be an odd prime. Let S be a finite set of primes containing the primes above p, the Archimedean primes and the primes of bad reduction of E.

Selmer Groups of Elliptic Curves

Consider an elliptic curve E/F and p be an odd prime. Let S be a finite set of primes containing the primes above p, the Archimedean primes and the primes of bad reduction of E.
Let F_S/F be the maximal extension unramified outside S.

Selmer Groups of Elliptic Curves

Consider an elliptic curve E/F and p be an odd prime. Let S be a finite set of primes containing the primes above p, the Archimedean primes and the primes of bad reduction of E.
Let F_S/F be the maximal extension unramified outside S.
The p**-primary Selmer group** of E/L for a finite Galois extension L/F contained in F_S is given by the exact sequence

$$0 \to \mathrm{Sel}(E/L) \to H^1\left(\mathrm{Gal}\left(F_S/L\right),\ E[p^\infty]\right) \to \bigoplus_{v \in S} \bigoplus_{w|v} H^1\left(L_w,\ E\right)[p^\infty].$$

Selmer Groups of Elliptic Curves

Consider an elliptic curve E/F and p be an odd prime. Let S be a finite set of primes containing the primes above p, the Archimedean primes and the primes of bad reduction of E.
Let F_S/F be the maximal extension unramified outside S.
The p**-primary Selmer group** of E/L for a finite Galois extension L/F contained in F_S is given by the exact sequence

$$0 \to \mathrm{Sel}(E/L) \to H^1\left(\mathrm{Gal}\left(F_S/L\right),\ E[p^\infty]\right) \to \bigoplus_{v \in S} \bigoplus_{w|v} H^1\left(L_w,\ E\right)[p^\infty].$$

We have,

$$\mathrm{Sel}\left(E/F_\infty\right) = \varinjlim_{L} \mathrm{Sel}\left(E/L\right)$$

where L runs over all finite extensions of F contained in the $\mathbb{Z}_p$-extension F_∞/F.

Iwasawa Theory of Elliptic Curves: The Work of Mazur

When the Galois module M is a discrete p-primary Abelian group or a compact pro-p Abelian group, its **Pontryagin dual** is defined as

$$M^{\vee} := \mathrm{Hom}\left(M,\ \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Iwasawa Theory of Elliptic Curves: The Work of Mazur

When the Galois module M is a discrete p-primary Abelian group or a compact pro-p Abelian group, its **Pontryagin dual** is defined as

$$M^\vee := \mathrm{Hom}\left(M,\ \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Theorem (Mazur)

The Pontryagin dual of $\mathrm{Sel}\left(E/F_{cyc}\right)$*, denoted by* $X\left(E/F_{cyc}\right)$*, is a finitely generated* $\Lambda(\Gamma)$*-module.*

Iwasawa Theory of Elliptic Curves: The Work of Mazur

When the Galois module M is a discrete p-primary Abelian group or a compact pro-p Abelian group, its **Pontryagin dual** is defined as

$$M^{\vee} := \mathrm{Hom}\left(M,\ \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Theorem (Mazur)

The Pontryagin dual of $\mathrm{Sel}\left(E/F_{cyc}\right)$*, denoted by* $X\left(E/F_{cyc}\right)$*, is a finitely generated* $\Lambda(\Gamma)$*-module.*

Conjecture (Mazur)

At primes of good ordinary reduction, $X\left(E/F_{cyc}\right)$ *is* $\Lambda(\Gamma)$*-torsion.*

Iwasawa Theory of Elliptic Curves: The Work of Mazur

When the Galois module M is a discrete p-primary Abelian group or a compact pro-p Abelian group, its **Pontryagin dual** is defined as

$$M^\vee := \mathrm{Hom}\left(M,\ \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Theorem (Mazur)

The Pontryagin dual of $\mathrm{Sel}\left(E/F_{cyc}\right)$*, denoted by* $X\left(E/F_{cyc}\right)$*, is a finitely generated* $\Lambda(\Gamma)$*-module.*

Conjecture (Mazur)

At primes of good ordinary reduction, $X\left(E/F_{cyc}\right)$ *is* $\Lambda(\Gamma)$*-torsion.*

If $X\left(E/F_{cyc}\right)$ is $\Lambda(\Gamma)$-torsion, the Structure Theorem holds as in the classical case.

Iwasawa Theory of Elliptic Curves: The Work of Mazur

When the Galois module M is a discrete p-primary Abelian group or a compact pro-p Abelian group, its **Pontryagin dual** is defined as

$$M^{\vee} := \mathrm{Hom}\left(M,\ \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Theorem (Mazur)

The Pontryagin dual of $\mathrm{Sel}\left(E/F_{cyc}\right)$*, denoted by* $X\left(E/F_{cyc}\right)$*, is a finitely generated* $\Lambda(\Gamma)$*-module.*

Conjecture (Mazur)

At primes of good ordinary reduction, $X\left(E/F_{cyc}\right)$ *is* $\Lambda(\Gamma)$*-torsion.*

If $X\left(E/F_{cyc}\right)$ is $\Lambda(\Gamma)$-torsion, the Structure Theorem holds as in the classical case. There are examples (over $\mathbb{Q}$) where $\mu(X) > 0$.

Coates-Sujatha Conjecture A

The right analogue of class groups in the elliptic curve setting (for $\mathbb{Z}_p$-extensions) is a subgroup of the Selmer group, called the **fine Selmer group**.

Coates-Sujatha Conjecture A

The right analogue of class groups in the elliptic curve setting (for $\mathbb{Z}_p$-extensions) is a subgroup of the Selmer group, called the **fine Selmer group**.

Conjecture (Coates-Sujatha (2005))

Let p be any odd prime and $Y(E/F_{cyc})$ be the Pontryagin dual of the fine Selmer group. Then,
$Y(E/F_{cyc})$ is $\Lambda(\Gamma)$-torsion and $\mu(Y) = 0$.

$Y(E/F_{cyc})$ is expected to be $\Lambda(\Gamma)$-torsion independent of the reduction type at p.

Coates-Sujatha Conjecture A

The right analogue of class groups in the elliptic curve setting (for $\mathbb{Z}_p$-extensions) is a subgroup of the Selmer group, called the **fine Selmer group**.

Conjecture (Coates-Sujatha (2005))

Let p be any odd prime and $Y(E/F_{cyc})$ be the Pontryagin dual of the fine Selmer group. Then,
$Y(E/F_{cyc})$ is $\Lambda(\Gamma)$-torsion and $\mu(Y) = 0$.

$Y(E/F_{cyc})$ is expected to be $\Lambda(\Gamma)$-torsion independent of the reduction type at p. This is the elliptic curve analogue of the *weak Leopoldt conjecture*. It is known for elliptic curves over $\mathbb{Q}$ by a deep result of Kato.

Fine Selmer Group

We define

$$R(E/L) := \ker\left(H^1\left(\mathrm{Gal}\left(F_S/L\right), E[p^\infty]\right) \to \bigoplus_{v \in S} \bigoplus_{w|v} H^1\left(L_w,\ E[p^\infty]\right)\right).$$

Fine Selmer Group

We define

$$R(E/L) := \ker\left(H^1\left(\mathrm{Gal}\left(F_S/L\right), E[p^\infty]\right) \to \bigoplus_{v \in S} \bigoplus_{w|v} H^1\left(L_w,\ E[p^\infty]\right)\right).$$

Taking direct limits as before, define

$$R(E/F_\infty) := \varinjlim_{L} R(E/L)$$

where L runs over all finite extensions of F contained in F_∞.

Evidence for Conjecture A

Theorem (K.-Sujatha)

Let F be a number field and E be an elliptic curve of rank 0 over F. Assume that the Shafarevich-Tate group of the elliptic curve E over F is finite. Varying over all primes of good ordinary reduction, $\mathrm{Sel}(E/F_{cyc})$ is trivial outside a set of density 0. In particular, Conjecture A holds for $Y(E/F_{cyc})$.

Relating the Two Conjectures

Briefly recall the two conjectures discussed so far

Conjecture (Iwasawa)

In a cyclotomic $\mathbb{Z}_p$-extension, $\mu = 0$.

Conjecture (Coates-Sujatha (2005))

Let p be any odd prime and $Y(E/F_{cyc})$ be the Pontryagin dual of the fine Selmer group. Then,
$Y(E/F_{cyc})$ is $\Lambda(\Gamma)$-torsion and $\mu(Y) = 0$.

Relating the Two Conjectures

A priori, it is not obvious that the two conjectures are related to each other. But,

Relating the Two Conjectures

A priori, it is not obvious that the two conjectures are related to each other. But,

Theorem (Coates-Sujatha, 2005; Lim-Murty 2016)

Let $F/\mathbb{Q}$ be a number field and $p \neq 2$ such that $E[p] \subset E(F)$. Then Conjecture A for $Y(E/F_{cyc})$ is equivalent to the classical $\mu = 0$ Conjecture.

Relating the Two Conjectures

A priori, it is not obvious that the two conjectures are related to each other. But,

Theorem (Coates-Sujatha, 2005; Lim-Murty 2016)

Let $F/\mathbb{Q}$ be a number field and $p \neq 2$ such that $E[p] \subset E(F)$. Then Conjecture A for $Y(E/F_{cyc})$ is equivalent to the classical $\mu = 0$ Conjecture.

It is natural to ask the following question:

Question

Are (fine) Selmer groups closely related to the class group in other p-adic Lie extensions (in particular, other $\mathbb{Z}_p$ extensions)?

Known Cases of Similar Growth Pattern

The similarity in the growth pattern of the class groups and fine Selmer groups are observed in the following cases

Known Cases of Similar Growth Pattern

The similarity in the growth pattern of the class groups and fine Selmer groups are observed in the following cases

- (multiple) $\mathbb{Z}_p$-extensions

Known Cases of Similar Growth Pattern

The similarity in the growth pattern of the class groups and fine Selmer groups are observed in the following cases

- (multiple) $\mathbb{Z}_p$-extensions
- False Tate curve extensions *or* Kummer extensions

Known Cases of Similar Growth Pattern

The similarity in the growth pattern of the class groups and fine Selmer groups are observed in the following cases

- (multiple) $\mathbb{Z}_p$-extensions
- False Tate curve extensions *or* Kummer extensions
- non-Abelian non p-adic analytic extensions

Known Cases of Similar Growth Pattern

The similarity in the growth pattern of the class groups and fine Selmer groups are observed in the following cases

- (multiple) $\mathbb{Z}_p$-extensions
- False Tate curve extensions *or* Kummer extensions
- non-Abelian non p-adic analytic extensions
- quadratic extensions

Known Cases of Similar Growth Pattern

The similarity in the growth pattern of the class groups and fine Selmer groups are observed in the following cases

- (multiple) $\mathbb{Z}_p$-extensions
- False Tate curve extensions *or* Kummer extensions
- non-Abelian non p-adic analytic extensions
- quadratic extensions
- cyclic $\mathbb{Z}/p\mathbb{Z}$ extensions

Non-Cyclotomic $\mathbb{Z}_p$-Extensions

Theorem (Iwasawa)

Let F be the cyclotomic field of p-th or 4-th roots of unity according as $p > 2$ or $p = 2$. For any given integer $N \geq 1$, there exists a cyclic extension L/F of degree p and a $\mathbb{Z}_p$-extension L_∞/L such that

$$\mu \geq N.$$

Theorem (K. 2020)

Let F be the cyclotomic field of p-th roots of unity for $p > 2$. Let E/F be an elliptic curve such that $E(F)[p] \neq 0$. Suppose the analogue of the Weak Leopoldt Conjecture holds. Given an integer $N \geq 1$, there exists a cyclic extension L/F of degree p and a $\mathbb{Z}_p$-extension L_∞/L such that

$$\mu(Y(E/L_\infty)) \geq N.$$

Outline of the Proof

- Let F_+ be the maximal totally real subfield of F. Construct a (non-)cyclotomic $\mathbb{Z}_p$-extension F_∞/F which is Galois over F_+.

Outline of the Proof

- Let F_+ be the maximal totally real subfield of F. Construct a (non-)cyclotomic $\mathbb{Z}_p$-extension F_∞/F which is Galois over F_+.
- Show there are infinitely many prime ideals $\mathfrak{l}$ in F which split completely in F_∞/F.

Outline of the Proof

- Let F_+ be the maximal totally real subfield of F. Construct a (non-)cyclotomic $\mathbb{Z}_p$-extension F_∞/F which is Galois over F_+.
- Show there are infinitely many prime ideals $\mathfrak{l}$ in F which split completely in F_∞/F.
- Choose prime ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, $t \geq 1$, in F which are prime to p and are totally split in F_∞/F. Let η be a non-zero element of F which is divisible exactly by the first power of $\mathfrak{l}_i$ for $1 \leq i \leq t$. Set $L = F\left(\sqrt[p]{\eta}\right)$ and $L_\infty = LF_\infty$.

Outline of the Proof

- Let F_+ be the maximal totally real subfield of F. Construct a (non-)cyclotomic $\mathbb{Z}_p$-extension F_∞/F which is Galois over F_+.
- Show there are infinitely many prime ideals $\mathfrak{l}$ in F which split completely in F_∞/F.
- Choose prime ideals $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$, $t \geq 1$, in F which are prime to p and are totally split in F_∞/F. Let η be a non-zero element of F which is divisible exactly by the first power of $\mathfrak{l}_i$ for $1 \leq i \leq t$. Set $L = F\left(\sqrt[p]{\eta}\right)$ and $L_\infty = LF_\infty$.
- Relate the (p-rank of) fine Selmer groups to the (p-rank of) class groups.

Outline of the Proof

- Let F_+ be the maximal totally real subfield of F. Construct a (non-)cyclotomic $\mathbb{Z}_p$-extension F_∞/F which is Galois over F_+.
- Show there are infinitely many prime ideals $\mathfrak{l}$ in F which split completely in F_∞/F.
- Choose prime ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_t$, $t \geq 1$, in F which are prime to p and are totally split in F_∞/F. Let η be a non-zero element of F which is divisible exactly by the first power of $\mathfrak{l}_i$ for $1 \leq i \leq t$. Set $L = F\left(\sqrt[p]{\eta}\right)$ and $L_\infty = LF_\infty$.
- Relate the (p-rank of) fine Selmer groups to the (p-rank of) class groups.
- Finally using Iwasawa's result show

$$\mu\left(Y\left(E/L_\infty\right)\right) \geq c_1 t + c_2(E/F).$$

More General Results

In pro-*p* *p*-adic Lie extensions, there is now a general strategy to show that the μ-invariant of (fine) Selmer groups can be arbitrarily large in extensions where it is known that the μ-invariant associated to the class group is arbitrarily large.

More General Results

In pro-p p-adic Lie extensions, there is now a general strategy to show that the μ-invariant of (fine) Selmer groups can be arbitrarily large in extensions where it is known that the μ-invariant associated to the class group is arbitrarily large.

More precisely, using the work of Hajir-Maire (2019), it is possible to show that there are nilpotent, uniform, pro-p, p-adic Lie extensions of number fields with arbitrarily large μ-invariant of (fine) Selmer groups.

Thank you!!