Iwasawa Theory of Fine Selmer Groups

R. Sujatha

Mini Course-CMS Winter Meet 2019
Toronto

December 6, 2019

IWASAWA THEORY OF CLASS GROUPS

Iwasawa Theory

We will fix a number field $F/\mathbb{Q}$ and an odd prime p for simplicity.

We will fix a number field $F/\mathbb{Q}$ and an odd prime p for simplicity.

A $\mathbb{Z}_p$-extension of F is a Galois extension F_∞/F such that

$$F_\infty = \bigcup_n F_n$$

with each F_n/F a cyclic extension, $\mathrm{Gal}\,(F_n/F) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Example $F = \mathbb{Q}$

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 $\mathbb{Q}(\zeta_{p^n})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Example $F = \mathbb{Q}$

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 $\mathbb{Q}(\zeta_{p^n})$ such that $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

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

Example $F = \mathbb{Q}$

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 $\mathbb{Q}(\zeta_{p^n})$ 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 $\mathbb{Z}_p$-extension* is the *unique* $\mathbb{Z}_p$ extension of $\mathbb{Q}$. It is contained inside $\mathbb{Q}(\zeta_{p^\infty})$.

Example $F = \mathbb{Q}$

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 $\mathbb{Q}(\zeta_{p^n})$ 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 $\mathbb{Z}_p$-extension* is the *unique* $\mathbb{Z}_p$ extension of $\mathbb{Q}$. It is contained inside $\mathbb{Q}(\zeta_{p^\infty})$.

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

Field Diagram

$$
\begin{tikzcd}
\mathbb{Q}(\zeta_{p^\infty}) \arrow[d, dash, "\mathbb{Z}/(p-1)"'] \arrow[ddr, dash, "\mathbb{Z}_p"] & \\
\mathbb{Q}_{cyc} \arrow[dd, dash, "\mathbb{Z}_p"'] & \\
 & \mathbb{Q}(\zeta_p) \arrow[dl, dash, "\mathbb{Z}/(p-1)"] \\
\mathbb{Q} &
\end{tikzcd}
$$

For a number field F, the cyclotomic $\mathbb{Z}_p$-extension always exists.

$$F_{cyc} = F \cdot \mathbb{Q}_{cyc}.$$

Leopoldt Conjecture

Let r_1 denote the number of real places of F and r_2 the number of (non-conjugate) complex places.

Leopoldt Conjecture

Let r_1 denote the number of real places of F and r_2 the number of (non-conjugate) complex places.

Therefore,

$$[F : \mathbb{Q}] = r_1 + 2r_2.$$

Conjecture (Leopoldt Conjecture)

Let F be a number field. Then F admits $r_2 + 1$ independent $\mathbb{Z}_p$-extensions.
In particular, if F is totally real, F_{cyc} is the unique $\mathbb{Z}_p$-extension of F.

Leopoldt Conjecture

Let r_1 denote the number of real places of F and r_2 the number of (non-conjugate) complex places.

Therefore,

$$[F : \mathbb{Q}] = r_1 + 2r_2.$$

Conjecture (Leopoldt Conjecture)

Let F be a number field. Then F admits $r_2 + 1$ independent $\mathbb{Z}_p$-extensions.
In particular, if F is totally real, F_{cyc} is the unique $\mathbb{Z}_p$-extension of F.

Brumer proved the Leopoldt Conjecture for Abelian extensions $F/\mathbb{Q}$.

Anti-Cyclotomic $\mathbb{Z}_p$-Extension

If $F/\mathbb{Q}$ is an imaginary quadratic field, then F admits *two* linearly independent $\mathbb{Z}_p$-extensions.

Anti-Cyclotomic $\mathbb{Z}_p$-Extension

If $F/\mathbb{Q}$ is an imaginary quadratic field, then F admits *two* linearly independent $\mathbb{Z}_p$-extensions.

One of them is the cyclotomic $\mathbb{Z}_p$-extension.

Anti-Cyclotomic $\mathbb{Z}_p$-Extension

If $F/\mathbb{Q}$ is an imaginary quadratic field, then F admits *two* linearly independent $\mathbb{Z}_p$-extensions.

One of them is the cyclotomic $\mathbb{Z}_p$-extension. The other is the anti-cyclotomic $\mathbb{Z}_p$-extension.

Anti-Cyclotomic $\mathbb{Z}_p$-Extension

If $F/\mathbb{Q}$ is an imaginary quadratic field, then F admits *two* linearly independent $\mathbb{Z}_p$-extensions.

One of them is the cyclotomic $\mathbb{Z}_p$-extension. The other is the anti-cyclotomic $\mathbb{Z}_p$-extension.

The *anti-cyclotomic* $\mathbb{Z}_p$-extension (denoted F_{ac}/F) is the unique $\mathbb{Z}_p$-extension of F which is Galois over $\mathbb{Q}$ but not Abelian over $\mathbb{Q}$.

Field Diagram

Denote $\widetilde{F}$ to be the composite of *all* $\mathbb{Z}_p$-extensions of F.

Field Diagram

Denote $\widetilde{F}$ to be the composite of *all* $\mathbb{Z}_p$-extensions of F.
If $F/\mathbb{Q}$ is an imaginary quadratic extension, then

Denote $\widetilde{F}$ to be the composite of *all* $\mathbb{Z}_p$-extensions of F.
If $F/\mathbb{Q}$ is an imaginary quadratic extension, then

$$\begin{tikzcd}[arrows=dash]
 & \widetilde{F} & \\
F_{cyc} \arrow[ur, "\mathbb{Z}_p"] & & F_{ac} \arrow[ul, "\mathbb{Z}_p"'] \\
 & F \arrow[ul, "\mathbb{Z}_p"] \arrow[ur, "\mathbb{Z}_p"'] & \\
 & \mathbb{Q} \arrow[u, "\mathbb{Z}/2"] &
\end{tikzcd}$$

Equivalent Formulation of the Leopoldt Conjecture

Let $F_{\{p\}}/F$ be the maximal extension of F unramified outside primes above p.

Equivalent Formulation of the Leopoldt Conjecture

Let $F_{\{p\}}/F$ be the maximal extension of F unramified outside primes above p.

Theorem

The Leopoldt Conjecture is equivalent to the following assertion:

$$H^2\left(\mathrm{Gal}\left(F_{\{p\}}/F\right),\ \mathbb{Q}_p/\mathbb{Z}_p\right) = 0$$

Some Properties of $\mathbb{Z}_p$-Extensions

Let F_∞/F be a $\mathbb{Z}_p$-extension. Then

1. Any prime $\mathfrak{q} \nmid p$ is unramified in F_∞/F.

Some Properties of $\mathbb{Z}_p$-Extensions

Let F_∞/F be a $\mathbb{Z}_p$-extension. Then

1. Any prime $\mathfrak{q} \nmid p$ is unramified in F_∞/F. At least one prime $\mathfrak{p} \mid p$ ramifies in this extension.

Some Properties of $\mathbb{Z}_p$-Extensions

Let F_∞/F be a $\mathbb{Z}_p$-extension. Then

1. Any prime $\mathfrak{q} \nmid p$ is unramified in F_∞/F. At least one prime $\mathfrak{p} \mid p$ ramifies in this extension.
2. For $F_\infty = F_{cyc}$, the extension ramifies at *every prime* $\mathfrak{p} \mid p$.

Some Properties of $\mathbb{Z}_p$-Extensions

Let F_∞/F be a $\mathbb{Z}_p$-extension. Then

1. Any prime $\mathfrak{q} \nmid p$ is unramified in F_∞/F. At least one prime $\mathfrak{p} \mid p$ ramifies in this extension.
2. For $F_\infty = F_{cyc}$, the extension ramifies at *every prime* $\mathfrak{p} \mid p$.
3. $\mathbb{Q}_{cyc}/\mathbb{Q}$ is totally ramified at p.

Iwasawa algebra

Let G be a profinite group.

Iwasawa algebra

Let G be a profinite group.

Define 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.

Define 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.

Define 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

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

Pseudo-Isomorphism and Pseudo-Nullity

Let M and N be finitely generated $\Lambda(\Gamma)$-modules.

Pseudo-Isomorphism and Pseudo-Nullity

Let M and N be finitely generated $\Lambda(\Gamma)$-modules.

We say, M is *pseudo-isomorphic* to N (denoted $M \sim N$) if there exists a $\Lambda(\Gamma)$-homomorphism $\varphi : M \to N$ such that both $\mathrm{ker}(\varphi)$ and $\mathrm{coker}(\varphi)$ are finite.

Pseudo-Isomorphism and Pseudo-Nullity

Let M and N be finitely generated $\Lambda(\Gamma)$-modules.

We say, M is *pseudo-isomorphic* to N (denoted $M \sim N$) if there exists a $\Lambda(\Gamma)$-homomorphism $\varphi : M \to N$ such that both $\ker(\varphi)$ and $\mathrm{coker}(\varphi)$ are finite.

The (Krull) dimension of $\Lambda(\Gamma) = 2$.

Pseudo-Isomorphism and Pseudo-Nullity

Let M and N be finitely generated $\Lambda(\Gamma)$-modules.

We say, M is *pseudo-isomorphic* to N (denoted $M \sim N$) if there exists a $\Lambda(\Gamma)$-homomorphism $\varphi : M \to N$ such that both $\ker(\varphi)$ and $\mathrm{coker}(\varphi)$ are finite.

The (Krull) dimension of $\Lambda(\Gamma) = 2$. A finitely generated $\Lambda(\Gamma)$-module M is called *pseudo-null* if

Pseudo-Isomorphism and Pseudo-Nullity

Let M and N be finitely generated $\Lambda(\Gamma)$-modules.

We say, M is *pseudo-isomorphic* to N (denoted $M \sim N$) if there exists a $\Lambda(\Gamma)$-homomorphism $\varphi : M \to N$ such that both $\mathrm{ker}(\varphi)$ and $\mathrm{coker}(\varphi)$ are finite.

The (Krull) dimension of $\Lambda(\Gamma) = 2$. A finitely generated $\Lambda(\Gamma)$-module M is called *pseudo-null* if

$$M \text{ is finite (equivalently has Krull dimension 0).}$$

Structure Theorem: Iwasawa and Serre

Theorem

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

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

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

Invariants for M

The $\Lambda(\Gamma)$-rank of M is r.

Invariants for M

The $\Lambda(\Gamma)$-rank of M is r.
The μ-invariant is defined

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

Invariants for M

The $\Lambda(\Gamma)$-rank of M is r.
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 λ, μ, ν are all independent of n.

Iwasawa's Conjecture: Setting up the Diagram

Let F_∞/F be *any* $\mathbb{Z}_p$-extension.

Iwasawa's Conjecture: Setting up the Diagram

Let F_∞/F be *any* $\mathbb{Z}_p$-extension.
M_n/F_n is the maximal unramified p-extension.

$$H_n = \mathrm{Gal}\left(M_n^{ab}/F_n\right) = p - \text{Hilbert class field of } F_n$$
$$\mathcal{H} = \varprojlim_n H_n$$
$$\mathcal{L} = \varprojlim_n M_n^{ab}$$

Iwasawa's Conjecture: Setting up the Diagram

Let F_∞/F be *any* $\mathbb{Z}_p$-extension.
M_n/F_n is the maximal unramified p-extension.

$$H_n = \mathrm{Gal}\left(M_n^{ab}/F_n\right) = p - \text{Hilbert class field of } F_n$$
$$\mathcal{H} = \varprojlim_n H_n$$
$$\mathcal{L} = \varprojlim_n M_n^{ab}$$

M'_n/F_n is the maximal unramified p-extension completely decomposed at all primes above p.

$$H'_n = \mathrm{Gal}\left(M_n'^{ab}/F_n\right)$$
$$\mathcal{H}' = \varprojlim_n H'_n$$
$$\mathcal{L}' = \varprojlim_n M'_n$$

Field Diagram

$$
\begin{tikzcd}
\mathcal{L} \arrow[d, dash] & & \\
F_\infty \arrow[ddr, dash] \arrow[ddd, dash] & & M_n \arrow[d, dash] \\
& & M_n^{ab} \arrow[dl, dash] \\
& F_n \arrow[dl, dash] & \\
F & &
\end{tikzcd}
$$

Iwasawa's Conjecture: Defining the Modules

$\mathcal{L},\ \mathcal{L}'$ are Galois extensions over F_∞. Consider the $\Lambda(\Gamma)$-modules

Iwasawa's Conjecture: Defining the Modules

$\mathcal{L},\ \mathcal{L}'$ are Galois extensions over F_∞. Consider the $\Lambda(\Gamma)$-modules

$$X_{nr} = \mathrm{Gal}\left(\mathcal{L}/F_\infty\right)$$
$$X_{cs} = \mathrm{Gal}\left(\mathcal{L}'/F_\infty\right)$$

Iwasawa's Conjecture: Defining the Modules

$\mathcal{L},\ \mathcal{L}'$ are Galois extensions over F_∞. Consider the $\Lambda(\Gamma)$-modules

$$X_{nr} = \mathrm{Gal}\,(\mathcal{L}/F_\infty)$$
$$X_{cs} = \mathrm{Gal}\,\left(\mathcal{L}'/F_\infty\right)$$

Theorem (Iwasawa)

The modules X_{nr} and X_{cs} are finitely generated, torsion $\Lambda(\Gamma)$-modules.

Iwasawa's Conjecture: Defining the Modules

$\mathcal{L}, \ \mathcal{L}'$ are Galois extensions over F_∞. Consider the $\Lambda(\Gamma)$-modules

$$X_{nr} = \mathrm{Gal}\left(\mathcal{L}/F_\infty\right)$$
$$X_{cs} = \mathrm{Gal}\left(\mathcal{L}'/F_\infty\right)$$

Theorem (Iwasawa)

The modules X_{nr} and X_{cs} are finitely generated, torsion $\Lambda(\Gamma)$-modules.

Therefore, by the Structure Theorem, one can define the μ, λ-invariants.

Iwasawa's Conjecture

Conjecture

For the cyclotomic $\mathbb{Z}_p$-extension,

$$\mu(X_{nr}) = 0.$$

Iwasawa's Conjecture

Conjecture

For the cyclotomic $\mathbb{Z}_p$-extension,

$$\mu(X_{nr}) = 0.$$

Iwasawa proved that when $F = \mathbb{Q}$, $\mu = \lambda = \nu = 0$.

Iwasawa's Conjecture

Conjecture

For the cyclotomic $\mathbb{Z}_p$-extension,

$$\mu(X_{nr}) = 0.$$

Iwasawa proved that when $F = \mathbb{Q}$, $\mu = \lambda = \nu = 0$.
More generally, this holds when $F/\mathbb{Q}$ is an Abelian extension by the work of Ferrero-Washington (1979).
Another proof was given by Sinnott (1984).

Iwasawa's Conjecture: Equivalent Formulation

Let F be a number field that contains ζ_p.

Iwasawa's Conjecture: Equivalent Formulation

Let F be a number field that contains ζ_p.

Theorem

Iwasawa $\mu = 0$ Conjecture is equivalent to the following two assertions combined:

1. $H^2\left(\mathrm{Gal}\left(F_{\{p\}}/F\right), \mathbb{Q}_p/\mathbb{Z}_p\right) = 0$ *and*
2. $H^2\left(\mathrm{Gal}\left(F_{\{p\}}/F\right), \mathbb{Z}/p\right) = 0.$

Vandiver's Conjecture

A closely related conjecture is the following:

Vandiver's Conjecture

A closely related conjecture is the following:

Conjecture (Vandiver's Conjecture)

A prime p does not divide the class number of the maximal real sub-field of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$.

Vandiver's Conjecture

A closely related conjecture is the following:

Conjecture (Vandiver's Conjecture)

A prime p does not divide the class number of the maximal real sub-field of the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$*.*

It is known for primes less than 163 million (2008) and in particular is known for all *regular primes*.

A generalization due to Greenberg

Conjecture (Greenberg(1971, 1976))

Let F be a totally real field and F_{cyc}/F be the cyclotomic $\mathbb{Z}_p$-extension. Then

$$\mu(X_{nr}) = \lambda(X_{nr}) = 0.$$

In particular, X_{nr} is finite.

A generalization due to Greenberg

Conjecture (Greenberg(1971, 1976))

Let F be a totally real field and F_{cyc}/F be the cyclotomic $\mathbb{Z}_p$-extension. Then

$$\mu(X_{nr}) = \lambda(X_{nr}) = 0.$$

In particular, X_{nr} is finite.

This conjecture was further generalized (2001). We will study this conjecture in the next few slides.

Greenberg's Pseudonullity Conjecture: Setting up the notation

Let $\widetilde{F}$ be the compositum of all $\mathbb{Z}_p$-extensions of F.

Greenberg's Pseudonullity Conjecture: Setting up the notation

Let $\widetilde{F}$ be the compositum of all $\mathbb{Z}_p$-extensions of F.
Let L/F be a finite Galois extension contained in $\widetilde{F}$. Write

$$A(L) = p - \text{Sylow subgroup of } \mathrm{Cl}(L).$$

Greenberg's Pseudonullity Conjecture: Setting up the notation

Let $\widetilde{F}$ be the compositum of all $\mathbb{Z}_p$-extensions of F.
Let L/F be a finite Galois extension contained in $\widetilde{F}$. Write

$$A(L) = p - \text{Sylow subgroup of } \mathrm{Cl}(L).$$

Consider

$$\mathcal{A} := \varprojlim_{norm} A(L).$$

This can be identified with the maximal Abelian unramified p-extension of $\widetilde{F}$.

Greenberg's Pseudonullity Conjecture: Setting up the notation

Let $\widetilde{F}$ be the compositum of all $\mathbb{Z}_p$-extensions of F.
Let L/F be a finite Galois extension contained in $\widetilde{F}$. Write

$$A(L) = p - \text{Sylow subgroup of } \mathrm{Cl}(L).$$

Consider

$$\mathcal{A} := \varprojlim_{norm} A(L).$$

This can be identified with the maximal Abelian unramified p-extension of $\widetilde{F}$. It is a $\Lambda(\mathcal{G})$-module where $\mathcal{G} = \mathrm{Gal}\left(\widetilde{F}/F\right) \simeq \mathbb{Z}_p^d$. Here, $d \leq r_1 + r_2 - 1$ (equality iff the Leopoldt Conjecture is true).

Greenberg's Pseudonullity Conjecture

With notation as introduced in the last slide,

$$\Lambda(\mathcal{G}) \simeq \mathbb{Z}_p[\![T_1, \ldots, T_d]\!].$$

Greenberg's Pseudonullity Conjecture

With notation as introduced in the last slide,

$$\Lambda(\mathcal{G}) \simeq \mathbb{Z}_p[\![T_1, \ldots, T_d]\!].$$

Theorem (Greenberg)

$\mathcal{A}$ is a finitely generated torsion $\Lambda(\mathcal{G})$-module.

Greenberg's Pseudonullity Conjecture

With notation as introduced in the last slide,

$$\Lambda(\mathcal{G}) \simeq \mathbb{Z}_p[\![T_1, \ldots, T_d]\!].$$

Theorem (Greenberg)

$\mathcal{A}$ is a finitely generated torsion $\Lambda(\mathcal{G})$-module.

Conjecture (Pseudonullity Conjecture)

$\mathcal{A}$ is pseudonull, equivalently

$$\dim \mathcal{A} \leq d - 1.$$

Iwasawa Theory of Elliptic Curves

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 *Selmer group* of E/L for a finite Galois extension L/F contained in F_S is given by the exact sequence

$$0 \to \mathrm{Sel}(E/L) \to H^1\left(\mathrm{Gal}\left(F_S/L\right), E_{p^\infty}\right) \xrightarrow{\lambda_L} \bigoplus_{v \in S} J_v\left(E_{p^\infty}/L\right)$$

where

$$J_v\left(E_{p^\infty}/L\right) = \bigoplus_{w|v} H^1\left(L_w,\ E\right)(p).$$

Comments

1. The Galois group $\mathrm{Gal}(L/F)$ acts on $H^1\left(\mathrm{Gal}\left(F_S/L\right), E_{p^\infty}\right)$ and $J_v\left(E_{p^\infty}/L\right)$.

Comments

1. The Galois group $\mathrm{Gal}(L/F)$ acts on $H^1\left(\mathrm{Gal}\left(F_S/L\right), E_{p^\infty}\right)$ and $J_v\left(E_{p^\infty}/L\right)$. Therefore, the Selmer group is endowed with a natural Galois action.

Comments

1. The Galois group $\mathrm{Gal}(L/F)$ acts on $H^1\left(\mathrm{Gal}\left(F_S/L\right), E_{p^\infty}\right)$ and $J_v\left(E_{p^\infty}/L\right)$. Therefore, the Selmer group is endowed with a natural Galois action.
2. There is an analogous exact sequence by taking direct limits

Comments

1. The Galois group $\mathrm{Gal}(L/F)$ acts on $H^1(\mathrm{Gal}(F_S/L), E_{p^\infty})$ and $J_v(E_{p^\infty}/L)$. Therefore, the Selmer group is endowed with a natural Galois action.
2. There is an analogous exact sequence by taking direct limits

$$0 \to \mathrm{Sel}(E/F_\infty) \to H^1(\mathrm{Gal}(F_S/F_\infty), E_{p^\infty}) \xrightarrow{\lambda_\infty} \bigoplus_{v \in S} J_v(E_{p^\infty}/F_\infty).$$

Fine Selmer Groups

Fine Selmer Group

We define

$$R(E/L) := \ker\left(H^1\left(\mathrm{Gal}\left(F_S/L\right), E_{p^\infty}\right) \to \bigoplus_{v\in S} K_v^1\left(E_{p^\infty}/L\right)\right)$$

where

$$K_v^1\left(E_{p^\infty}/L\right) = \bigoplus_{w|v} H^1\left(L_w,\ E_{p^\infty}\right).$$

Fine Selmer Group

We define

$$R(E/L) := \ker\left(H^1\left(\mathrm{Gal}\left(F_S/L\right), E_{p^\infty}\right) \to \bigoplus_{v\in S} K_v^1\left(E_{p^\infty}/L\right)\right)$$

where

$$K_v^1\left(E_{p^\infty}/L\right) = \bigoplus_{w|v} H^1\left(L_w,\ E_{p^\infty}\right).$$

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_∞.

Some important sequences

1. $$0 \to E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa} \mathrm{Sel}(E/L) \xrightarrow{\lambda} Ш(E/L)(p) \to 0$$

Some important sequences

1. $$0 \to E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\kappa} \mathrm{Sel}(E/L) \xrightarrow{\lambda} Ш(E/L)(p) \to 0$$

2. $$0 \to R(E/L) \to \mathrm{Sel}(E/L) \to \bigoplus_{w|p} E(L_w)_{p^\infty} \otimes \mathbb{Q}_p/\mathbb{Z}_p$$

Pontryagin dual

Let $G = \mathrm{Gal}\,(F_\infty/F)$ be *any* pro-p, p-adic Lie group and $\Lambda(G)$ be the corresponding Iwasawa algebra.

Pontryagin dual

Let $G = \mathrm{Gal}\,(F_\infty/F)$ be *any* pro-p, p-adic Lie group and $\Lambda(G)$ be the corresponding Iwasawa algebra. For example, $G = \Gamma$ as before.

Pontryagin dual

Let $G = \mathrm{Gal}\,(F_\infty/F)$ be *any* pro-p, p-adic Lie group and $\Lambda(G)$ be the corresponding Iwasawa algebra. For example, $G = \Gamma$ as before.

$\mathrm{Sel}(E/F_\infty)$ and $R(E/F_\infty)$ are finitely generated *discrete* $\Lambda(G)$-modules.

Pontryagin dual

Let $G = \mathrm{Gal}\,(F_\infty/F)$ be *any* pro-p, p-adic Lie group and $\Lambda(G)$ be the corresponding Iwasawa algebra. For example, $G = \Gamma$ as before.

$\mathrm{Sel}(E/F_\infty)$ and $R(E/F_\infty)$ are finitely generated *discrete* $\Lambda(G)$-modules. We work with the Pontryagin duals which makes them compact. These are denoted $X(E/F_\infty)$ and $Y(E/F_\infty)$, respectively.

Pontryagin dual

Let $G = \mathrm{Gal}(F_\infty/F)$ be *any* pro-p, p-adic Lie group and $\Lambda(G)$ be the corresponding Iwasawa algebra. For example, $G = \Gamma$ as before.

$\mathrm{Sel}(E/F_\infty)$ and $R(E/F_\infty)$ are finitely generated *discrete* $\Lambda(G)$-modules. We work with the Pontryagin duals which makes them compact. These are denoted $X(E/F_\infty)$ and $Y(E/F_\infty)$, respectively.

The Pontryagin dual of a p-primary module M is defined as

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

CONJECTURES

Conjecture of Mazur

Conjecture

Suppose E/F is an elliptic curve with good ordinary reduction at all primes above p. Then $X(E/F_{cyc})$ is a finitely generated torsion $\Lambda(\Gamma)$-module.

Conjecture of Mazur

Conjecture

Suppose E/F is an elliptic curve with good ordinary reduction at all primes above p. Then $X(E/F_{cyc})$ is a finitely generated torsion $\Lambda(\Gamma)$-module.

By a deep result of Kato, this is now known in some cases such as when $F = \mathbb{Q}$ or an Abelian extension.

Conjecture of Mazur

Conjecture

Suppose E/F is an elliptic curve with good ordinary reduction at all primes above p. Then $X(E/F_{cyc})$ is a finitely generated torsion $\Lambda(\Gamma)$-module.

By a deep result of Kato, this is now known in some cases such as when $F = \mathbb{Q}$ or an Abelian extension.

For dual Selmer groups of elliptic curves over $\mathbb{Q}$, we therefore have the structure theorem.

Conjecture of Mazur

Conjecture

Suppose E/F is an elliptic curve with good ordinary reduction at all primes above p. Then $X(E/F_{cyc})$ is a finitely generated torsion $\Lambda(\Gamma)$-module.

By a deep result of Kato, this is now known in some cases such as when $F = \mathbb{Q}$ or an Abelian extension.

For dual Selmer groups of elliptic curves over $\mathbb{Q}$, we therefore have the structure theorem. But there are lots of examples of elliptic curves with *positive* μ-invariant.

Analogue of the Weak Leopoldt Conjecture

Conjecture

Let E/F be an elliptic curve and p be an odd prime. For any $\mathbb{Z}_p$-extension F_∞/F,

$$H^2\left(F_S/F_\infty,\ E_{p^\infty}\right) = 0.$$

Equivalently, the (dual) fine Selmer group is $\Lambda(\Gamma)$-torsion.

Analogue of the Weak Leopoldt Conjecture

Conjecture

Let E/F be an elliptic curve and p be an odd prime. For any $\mathbb{Z}_p$-extension F_∞/F,

$$H^2\left(F_S/F_\infty,\ E_{p^\infty}\right) = 0.$$

Equivalently, the (dual) fine Selmer group is $\Lambda(\Gamma)$-torsion.

The equivalence of the two statements was shown by Perrin-Riou.

Conjecture A

Conjecture (Coates-S.)

Let E be an elliptic curve over F and p be an odd prime. $Y(E/F_{cyc})$ is finitely generated as a $\mathbb{Z}_p$-module.

Conjecture A

Conjecture (Coates-S.)

Let E be an elliptic curve over F and p be an odd prime. $Y(E/F_{cyc})$ is finitely generated as a $\mathbb{Z}_p$-module.
Equivalently, the elliptic curve analogue of the weak Leopoldt Conjecture holds and $\mu(Y(E/F_{cyc})) = 0$.

Conjecture A

Conjecture (Coates-S.)

Let E be an elliptic curve over F and p be an odd prime. $Y(E/F_{cyc})$ is finitely generated as a $\mathbb{Z}_p$-module.
Equivalently, the elliptic curve analogue of the weak Leopoldt Conjecture holds and $\mu(Y(E/F_{cyc})) = 0$.

This conjecture is to be viewed as an analogue of Iwasawa's $\mu = 0$ Conjecture for the case of elliptic curves.

Conjecture B

Let F_∞/F be an *admissible* p-adic Lie extension, i.e.

Conjecture B

Let F_∞/F be an *admissible* p-adic Lie extension, i.e.

1. $F_{cyc} \subset F_\infty \subset F_S$.
2. $\mathrm{Gal}(F_S/F) = G$ is pro-p with no elements of order p.

Conjecture B

Let F_∞/F be an *admissible* p-adic Lie extension, i.e.

1. $F_{cyc} \subset F_\infty \subset F_S$.
2. $\mathrm{Gal}(F_S/F) = G$ is pro-p with no elements of order p.

Conjecture (Coates-S.)

Suppose Conjecture A holds for E/F_{cyc} and G has dimension strictly larger than 1 as a p-adic Lie group, then $Y(E/F_\infty)$ is a pseudonull $\Lambda(G)$-module.

Conjecture B

Let F_∞/F be an *admissible* p-adic Lie extension, i.e.

1. $F_{cyc} \subset F_\infty \subset F_S$.
2. $\mathrm{Gal}(F_S/F) = G$ is pro-p with no elements of order p.

Conjecture (Coates-S.)

Suppose Conjecture A holds for E/F_{cyc} and G has dimension strictly larger than 1 as a p-adic Lie group, then $Y(E/F_\infty)$ is a pseudonull $\Lambda(G)$-module.

This echoes Greenberg's pseudonullity conjecture in the context of elliptic curves.

Recent Results

Recent Evidence towards Conjecture A

Theorem (K.-S.)

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

Recent Evidence towards Conjecture A

Theorem (K.-S.)

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

This result was first proven for $F = \mathbb{Q}$ by Greenberg. To extend this to the general number fields case it was necessary to use an effective Chebotarev density result of Kumar Murty.

Evidence for Conjecture B: CM case

Theorem (K.-S.)

Let E be a CM elliptic curve defined over a number field F and p be an odd prime of good ordinary reduction.

Evidence for Conjecture B: CM case

Theorem (K.-S.)

Let E be a CM elliptic curve defined over a number field F and p be an odd prime of good ordinary reduction.
Let $F_\infty = F(E_{p^\infty})$. In this case, $\mathrm{Gal}(F_\infty/F)$ contains an open subgroup which is Abelian and isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Further, assume $G = \mathrm{Gal}(F_\infty/F)$ is pro-p.

Evidence for Conjecture B: CM case

Theorem (K.-S.)

Let E be a CM elliptic curve defined over a number field F and p be an odd prime of good ordinary reduction.
Let $F_\infty = F(E_{p^\infty})$. In this case, $\mathrm{Gal}(F_\infty/F)$ contains an open subgroup which is Abelian and isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$. Further, assume $G = \mathrm{Gal}(F_\infty/F)$ is pro-p.
If $Y(E/F_{cyc})$ is finite, $Y(E/F_\infty)$ is a pseudonull $\Lambda(G)$-module.

Evidence for Conjecture B: non-CM case for regular primes

Theorem (K.-S.)

Let E be an elliptic curve defined over $\mathbb{Q}$. Set $F = \mathbb{Q}(\mu_p)$ such that p is a regular prime. Then Conjecture B is true for $Y(E/\mathbb{Q}(E_{p^\infty}))$.

Specific Example

Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + xy = x^3 - 3x - 3.$$

Specific Example

Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + xy = x^3 - 3x - 3.$$

This is an elliptic curve of conductor 150 without CM.

Specific Example

Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + xy = x^3 - 3x - 3.$$

This is an elliptic curve of conductor 150 without CM. With $p = 5$, $F_\infty = \mathbb{Q}(E_{5^\infty})$ is a pro-5 extension of $F = \mathbb{Q}(\mu_5)$.

Specific Example

Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + xy = x^3 - 3x - 3.$$

This is an elliptic curve of conductor 150 without CM. With $p = 5$, $F_\infty = \mathbb{Q}(E_{5^\infty})$ is a pro-5 extension of $F = \mathbb{Q}(\mu_5)$.

It was shown in Coates-S. (2005) that either Conjecture B holds or there is no point of infinite order over F_∞. The latter possibility was not ruled out in the intervening years, despite advances in computational methods.

Specific Example

Consider the elliptic curve $E/\mathbb{Q}$ defined by

$$E : y^2 + xy = x^3 - 3x - 3.$$

This is an elliptic curve of conductor 150 without CM. With $p = 5$, $F_\infty = \mathbb{Q}(E_{5^\infty})$ is a pro-5 extension of $F = \mathbb{Q}(\mu_5)$.

It was shown in Coates-S. (2005) that either Conjecture B holds or there is no point of infinite order over F_∞. The latter possibility was not ruled out in the intervening years, despite advances in computational methods.
Our theorem settles this example theoretically.

Relating Greenberg's Conjecture with Conjecture B

Theorem (K.-S.)

Let E/F be an elliptic curve and p be a fixed odd prime.

Relating Greenberg's Conjecture with Conjecture B

Theorem (K.-S.)

Let E/F be an elliptic curve and p be a fixed odd prime. Let $\mathcal{L} = F_\infty = F(E_{p^\infty})$ or $\widetilde{F}$ be an admissible extension of F.

Relating Greenberg's Conjecture with Conjecture B

Theorem (K.-S.)

Let E/F be an elliptic curve and p be a fixed odd prime. Let $\mathcal{L} = F_\infty = F(E_{p^\infty})$ or $\widetilde{F}$ be an admissible extension of F. Then $X_{nr}^{\mathcal{L}}$ is pseudonull (i.e. Greenberg's Conjecture holds) if and only if Conjecture B holds for $Y(E/\mathcal{L})$.