Horizontal Iwasawa theory

Alberto Angurel Andrés

University of Nottingham

June 29, 2026

$\mathbb{Z}_p$-extensions

Idea of K. Iwasawa

Certain arithmetic objects that are difficult to compute individually, such as class groups or ranks of elliptic curves, are more approachable through their growth along certain tower of number fields.

$\mathbb{Z}_p$-extensions

Fix an odd prime p. A $\mathbb{Z}_p$-extension K_∞/K is a Galois extension of fields satisfying that

$$\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p.$$

By Galois theory, for each $n \in \mathbb{N}$, it admits a unique subextension K_n such that

$$[K_n : K] = p^n.$$

Then K_∞ can be recovered as the union

$$K_\infty = \bigcup_{n=1}^{\infty} K_n.$$

Cyclotomic $\mathbb{Z}_p$-extension

Roots of unity

For any $n \in \mathbb{N}$, let μ_{p^n} denote the set of roots of unity of order p^n.

The field $\mathbb{Q}_n$

There is an isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^{n+1}})/\mathbb{Q}) = (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

By Galois theory, there is a unique subfield $\mathbb{Q}_n \subset \mathbb{Q}(\mu_{p^{n+1}})$ such that

$$[\mathbb{Q}_n : \mathbb{Q}] = p^n$$

Cyclotomic $\mathbb{Z}_p$-extension

We can consider

$$\mathbb{Q}_\infty := \bigcup_{n=1}^{\infty} \mathbb{Q}_n.$$

Since $\mathbb{Q}_n \subset \mathbb{Q}_{n+1}$ for all $n \in \mathbb{N}$, we can conclude that

$$\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p.$$

Iwasawa theory

BSD conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$. Then

$$\mathrm{rank}\ E(\mathbb{Q}) = \mathrm{ord}_{s=1}\ L(E,s).$$

Points over $\mathbb{Q}_\infty$

The group of points $E(\mathbb{Q}_\infty)$ has a natural structure of a module over the ring

$$\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty)/\mathbb{Q}]] = \mathbb{Z}_p[[T]].$$

p-adic L-function

There is an element $\mathcal{L}_p(E) \in \Lambda$ that interpolates the twisted L-values $L(E,\chi,1)$ for all characters χ of $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$.

$$
\begin{tikzcd}
\boxed{\text{rank } E(\mathbb{Q})} \arrow[r, dashed, leftrightarrow, "BSD(?)"] \arrow[d, "\text{Iwasawa modules}"] & \boxed{\begin{array}{c} L(E,s) \\ \text{at } s=1 \end{array}} \arrow[d, "\text{Interpolation}"] \\
\boxed{E(\mathbb{Q}_\infty) \otimes \mathbb{Z}_p} & \boxed{\mathcal{L}_p(E)} \arrow[d, "\text{Cohomology}"] \\
\boxed{\text{Kolyvagin system}} \arrow[u] & \boxed{\begin{array}{c} \text{Euler system} \\ \text{(Kato)} \end{array}} \arrow[l, "\text{Derivative}"]
\end{tikzcd}
$$

Other abelian extensions

Horizontal Iwasawa theory

Iwasawa theory

Ultrafilters

Selmer groups

Kronecker-Weber theorem

The maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$ is

$$\mathbb{Q}^{\mathrm{ab}} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\mu_n) = \prod_{\ell \text{ prime}} \left(\bigcup_{k=1}^{\infty} \mathbb{Q}(\mu_{\ell^k}) \right)$$

Maximal abelian p-extension

The maximal abelian p-extension $\mathbb{Q}^{\mathrm{ab},p}$ of $\mathbb{Q}$ is

$$\mathbb{Q}^{\mathrm{ab},p} = \mathbb{Q}_\infty \cdot \prod_{\ell \neq p} \mathbb{Q}(\ell),$$

where $\mathbb{Q}(\ell)$ denotes the maximal p-extension inside $\mathbb{Q}(\mu_\ell)$, which is cyclic of degree

$$[\mathbb{Q}(\ell) : \mathbb{Q}] = p^{v_p(\ell-1)}$$

Chebotarev density theorem

For every $n \in \mathbb{N}$, $\mathbb{Q}$ admits infinitely many cyclic extensions of degree n.
However, $\mathbb{Q}_\infty$ is the only $\mathbb{Z}_p$-extension.

Euler and Kolyvagin systems

Euler system

An Euler system is an object living in Galois cohomology that behaves like an equivariant p-adic L-function. It does not only interpolate the characters in $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ but all the characters in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$.

Kolyvagin derivative

The Euler system relations along p-extensions of $\mathbb{Q}$ lead to other cohomological relations, known as Kolyvagin systems. They can be used to compute $E(\mathbb{Q}_\infty)$.

Lack of $\mathbb{Z}_p$-extensions

One technical obstruction to the method of Kolyvagin systems is the lack of more $\mathbb{Z}_p$-extensions, which forces us to work in the Galois cohomology with finite coefficients. Having more $\mathbb{Z}_p$-extensions would allow us to avoid this step and work with modules over the Iwasasa algebra $\Lambda := \mathbb{Z}_p[[X]]$.

Ultrafilters

Ultrafilter

An ultrafilter $\mathcal{U}$ is a collection of subsets of the natural numbers satisfying the following axioms:

- $\emptyset \notin \mathcal{U}$.
- $S, T \in \mathcal{U} \Rightarrow S \cap T \in \mathcal{U}$.
- $S \subset T,\ S \in \mathcal{U} \Rightarrow T \in \mathcal{U}$.
- For any $S \in \mathcal{P}(\mathbb{N})$, either $S \in \mathcal{U}$ or $(\mathbb{N} \setminus S) \in \mathcal{U}$.

Key property

If we have a partition $\{S_1, \ldots, S_n\}$ of $\mathbb{N}$, there is exactly one i such that $S_i \in \mathcal{U}$.

Ultraproducts

Ultraproduct

Let $(M_n)_{n\in\mathbb{N}}$ be a sequence of groups. An ultrafilter defines an equivalence relation in $\prod_{n\in\mathbb{N}} M_n$:

$$(\alpha_n)_{n\in\mathbb{N}} \sim (\beta_n)_{n\in N} \Leftrightarrow \{n \in \mathbb{N} :\ \alpha_n = \beta_n\} \in \mathcal{U}.$$

The ultraproduct is defined as

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

Proposition

Assume that M is a finite group and $M_n = M$ for each $n \in \mathbb{N}$. Then $\mathcal{U}(M_n) = M$.
Proof: Let $(\alpha_n) \in \prod M_n$ and for each $m \in M$, define the set

$$S_m := \{n \in \mathbb{N} :\ \alpha_n = m\}.$$

Then

$$\bigsqcup_{m\in M} S_m = \mathbb{N}.$$

By the key property, there exists a unique $m_0 \in M$ such that $S_{m_0} \in \mathcal{U}$.
If we set $\beta_n = m_0$ for all n, then $(\alpha_n) \sim (\beta_n)$.

Ultraprimes

Ultraprimes

An ultraprime $\mathfrak{u}$ is a sequence of primes

$$\mathfrak{u} = (\ell_n)_{n \in \mathbb{N}}.$$

We say that two sequences represent the same ultraprime if they are in the same class of the ultrafilter equivalence relation.

Constructing $\mathbb{Z}_p$-extensions

- For every $n \in \mathbb{N}$, choose a prime $\ell_i \in 1 + p^i\mathbb{Z}$ and let $\mathfrak{u} = (\ell_i)_{i \in \mathbb{N}}$.
- Consider the ultraproduct $\mathcal{G}_\mathfrak{u} = \mathcal{U}(\mathrm{Gal}(\mathbb{Q}(\ell_i)/\mathbb{Q}))$.
- This ultraproduct itself is a huge group but I can study its finite quotients.
- For each $k \in \mathbb{N}$, whenever $i \geq k$, $\mathrm{Gal}(\mathbb{Q}(\ell_i)/\mathbb{Q})$ admits a (unique) subgroup $H_i^{(k)}$ such that
$$\mathrm{Gal}(\mathbb{Q}(\ell_i)/\mathbb{Q}) \Big/ H_i^{(k)} \cong \mathbb{Z}/p^k.$$
- The ultraproduct $\mathcal{H}^{(k)} := \mathcal{U}\left(H_i^{(k)}\right)$ is a subgroup of $G_\mathfrak{u}$ such that $\mathcal{G}_\mathfrak{u}/\mathcal{H}^{(k)} \cong \mathbb{Z}/p^k$.
- By considering $\mathcal{H} := \bigcap_{k \in \mathbb{N}} \mathcal{H}^{(k)}$, we obtain that $\mathcal{G}_\mathfrak{u}/\mathcal{H} \cong \mathbb{Z}_p$.

Hyperrationals

Ultrapower of the absolute Galois group

The ultrapower $\mathcal{U}(G_{\mathbb{Q}})$ of the absolute Galois group of the rationals contains infinitely many $\mathbb{Z}_p$-quotients.

Hyperrationals

These quotients can be seen as $\mathbb{Z}_p$-extensions of a bigger field: the hyperrationals,

$$\mathbb{Q}^* = \mathcal{U}(\mathbb{Q}),$$

which is the ultrapower of the rational numbers.
Its absolute Galois group is the (internal) profinite completion of the ultrapower $\mathcal{U}(G_{\mathbb{Q}})$.

Remark

Most aspects of the algebraic theory of number fields can be generalised to the Galois theory of $\mathbb{Q}^*$.

Ultra-Euler and ultra-Kolyvagin systems

Generalisations

There is a natural generalisation of Euler and Kolyvagin systems on the Galois cohomology of the hyperrationals. We call them ultra-Euler and ultra-Kolyvagin systems.

Construction

If you are given an Euler system in the rational Galois cohomology, you can use it to have an ultra-Euler system.

$\mathbb{Z}_p$-extensions associated with Kolyvagin ultraprimes

The existence of new $\mathbb{Z}_p$-extensions allows more powerful applications of the method.

Structure of Iwasawa Selmer groups

Goal: compute the structure of Selmer groups as modules over Λ

- $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]) \sim E(\mathbb{Q}_\infty)$,
- $\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty]) \sim \ker\Big(E(\mathbb{Q}_\infty) \to E(\mathbb{Q}_\infty)\Big)$,

$(*)$ $\sim$ denotes "equality" up to some "small" factor due to Tate-Shafarevich groups.

Assumptions on E

- The image of the Galois representation is large enough.
- E has good ordinary reduction at p.

Analytic ideals (after Sweeting, Loeffler-Zerbes)

If we look at the ultra-Euler system (resp. Greenberg p-adic L-function) along a $\mathbb{Z}_p$-extension generated by some well behaved ultraprime, we can generalise the construction of the Kolyvagin derivative. With this process, we obtain a sequence of ideals

$$\Theta_i(\kappa) \ (\mathrm{resp.}\ \Theta_i(\delta)) \ \forall i \in \mathbb{Z}_{\geq 0}.$$

Main theorems

Theorem 1(A.)

$$\Theta_i(\kappa) = \mathrm{Fitt}^i_\Lambda\left(\mathrm{Sel}_0(\mathbb{Q}_\infty, E[p^\infty]^\vee)\right) \; \forall i \in \mathbb{Z}_{\geq 0}$$

Theorem 2 (A., in progress)

$$\Theta_i(\delta) = \mathrm{Fitt}^i_\Lambda\left(\mathrm{Sel}(\mathbb{Q}_\infty, E[p^\infty])^\vee\right) \; \forall i \in 2\mathbb{Z}$$

Remarks

- The sequence ideals $\Theta_i(\kappa)$ and $\Theta_i(\delta)$ describe the Selmer group up to pseudo-isomorphism of Iwasawa modules.
- The theorems apply in more generality, to arbitrary Galois representations satisfying certain mild big image assumptions.

Thank you!