Iwasawa theory – a brief introduction

Jeanine Van Order

Fakultät für Mathematik
Universität Bielefeld

Sage Days 71, Oxford 03/2016

Historical overview

- Iwasawa theory is a collection of techniques developed since the 1950s to the study the behaviour of certain arithmetic groups (such as ideal class groups) in towers of number fields.

Historical overview

- Iwasawa theory is a collection of techniques developed since the 1950s to the study the behaviour of certain arithmetic groups (such as ideal class groups) in towers of number fields.
- The topic is named in honour of Japanese mathematician Kenkichi Iwasawa (1917-1998), who initiated the study for class groups of number fields.

Historical overview

- Iwasawa theory is a collection of techniques developed since the 1950s to the study the behaviour of certain arithmetic groups (such as ideal class groups) in towers of number fields.
- The topic is named in honour of Japanese mathematician Kenkichi Iwasawa (1917-1998), who initiated the study for class groups of number fields. Iwasawa's seminal construction of p-adic L-functions as characteristic polynomials of Frobenius of cyclotomic extensions was inspired by Weil's theory of zeta functions of algebraic curves over finite fields.

Historical overview

- Iwasawa theory is a collection of techniques developed since the 1950s to the study the behaviour of certain arithmetic groups (such as ideal class groups) in towers of number fields.
- The topic is named in honour of Japanese mathematician Kenkichi Iwasawa (1917-1998), who initiated the study for class groups of number fields. Iwasawa's seminal construction of p-adic L-functions as characteristic polynomials of Frobenius of cyclotomic extensions was inspired by Weil's theory of zeta functions of algebraic curves over finite fields. Weil in fact anticipated this idea himself, as seen in written correspondence to Borel in 1941.

Historical overview

- Iwasawa theory is a collection of techniques developed since the 1950s to the study the behaviour of certain arithmetic groups (such as ideal class groups) in towers of number fields.
- The topic is named in honour of Japanese mathematician Kenkichi Iwasawa (1917-1998), who initiated the study for class groups of number fields. Iwasawa's seminal construction of p-adic L-functions as characteristic polynomials of Frobenius of cyclotomic extensions was inspired by Weil's theory of zeta functions of algebraic curves over finite fields. Weil in fact anticipated this idea himself, as seen in written correspondence to Borel in 1941.
- Most of what we understand today about the behaviour of class groups or Mordell-Weil ranks in towers of number fields (and even the conjecture of Birch-Swinnerton-Dyer) has come about through these so-called Iwasawa theoretic techniques.

Iwasawa's theorem on $\mathbf{Z}_p$-extensions

- Consider a tower of number fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_\infty = \bigcup_{n \geq 0} F_n$ with Galois groups $\mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}/p^n\mathbf{Z}$ and profinite limit $\mathrm{Gal}(F_\infty/F) = \varprojlim \mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}_p$.

Iwasawa's theorem on $\mathbf{Z}_p$-extensions

- Consider a tower of number fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_\infty = \bigcup_{n \geq 0} F_n$ with Galois groups $\mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}/p^n\mathbf{Z}$ and profinite limit $\mathrm{Gal}(F_\infty/F) = \varprojlim \mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}_p$.
- Let e_n denote the exponent of p in the class number of F_n.

Iwasawa's theorem on $\mathbf{Z}_p$-extensions

- Consider a tower of number fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_\infty = \bigcup_{n \geq 0} F_n$ with Galois groups $\mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}/p^n\mathbf{Z}$ and profinite limit $\mathrm{Gal}(F_\infty/F) = \varprojlim \mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}_p$.
- Let e_n denote the exponent of p in the class number of F_n.

- Theorem (Iwasawa, 1958)

  There exist integers $\mu \geq 0$, $\lambda \geq 0$, and ν such that for all sufficiently large integers $n \geq 1$, we have $e_n = \mu p^n + \lambda n + \nu$.

Iwasawa's theorem on $\mathbf{Z}_p$-extensions

- Consider a tower of number fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_\infty = \bigcup_{n \geq 0} F_n$ with Galois groups $\mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}/p^n\mathbf{Z}$ and profinite limit $\mathrm{Gal}(F_\infty/F) = \varprojlim \mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}_p$.
- Let e_n denote the exponent of p in the class number of F_n.

- Theorem (Iwasawa, 1958)

  There exist integers $\mu \geq 0$, $\lambda \geq 0$, and ν such that for all sufficiently large integers $n \geq 1$, we have $e_n = \mu p^n + \lambda n + \nu$.

  - These invariants μ, λ, and ν are the so-called Iwasawa invariants associated to the $\mathbf{Z}_p$-extension F_∞/F_0.

Iwasawa's theorem on $\mathbf{Z}_p$-extensions

- Consider a tower of number fields $F_0 \subseteq F_1 \subseteq \cdots \subseteq F_\infty = \bigcup_{n \geq 0} F_n$ with Galois groups $\mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}/p^n\mathbf{Z}$ and profinite limit $\mathrm{Gal}(F_\infty/F) = \varprojlim \mathrm{Gal}(F_n/F_0) \approx \mathbf{Z}_p$.
- Let e_n denote the exponent of p in the class number of F_n.

- Theorem (Iwasawa, 1958)

  There exist integers $\mu \geq 0$, $\lambda \geq 0$, and ν such that for all sufficiently large integers $n \geq 1$, we have $e_n = \mu p^n + \lambda n + \nu$.

  - These invariants μ, λ, and ν are the so-called Iwasawa invariants associated to the $\mathbf{Z}_p$-extension F_∞/F_0.

The (cyclotomic) μ-invariant and class numbers

- Iwasawa conjectured that $\mu = 0$ for cyclotomic extensions (i.e. for $F_\infty \subseteq \bigcup_{n \geq 0} F_0(\zeta_{p^n})$).

The (cyclotomic) μ-invariant and class numbers

- Iwasawa conjectured that $\mu = 0$ for cyclotomic extensions (i.e. for $F_\infty \subseteq \bigcup_{n\geq 0} F_0(\zeta_{p^n})$). His conjecture was based on calculations for primes $p < 4000$ in the case of $F_0 = \mathbf{Q}$.

The (cyclotomic) μ-invariant and class numbers

- Iwasawa conjectured that $\mu = 0$ for cyclotomic extensions (i.e. for $F_\infty \subseteq \bigcup_{n\geq 0} F_0(\zeta_{p^n})$). His conjecture was based on calculations for primes $p < 4000$ in the case of $F_0 = \mathbf{Q}$.
- This conjecture has been proven for F_0 abelian by a landmark theorem of Ferrero-Washington, and later by Sinnott using a different method.

The (cyclotomic) μ-invariant and class numbers

- Iwasawa conjectured that $\mu = 0$ for cyclotomic extensions (i.e. for $F_\infty \subseteq \bigcup_{n \geq 0} F_0(\zeta_{p^n})$). His conjecture was based on calculations for primes $p < 4000$ in the case of $F_0 = \mathbf{Q}$.
- This conjecture has been proven for F_0 abelian by a landmark theorem of Ferrero-Washington, and later by Sinnott using a different method. The general case remains open.

The (cyclotomic) μ-invariant and class numbers

- Iwasawa conjectured that $\mu = 0$ for cyclotomic extensions (i.e. for $F_\infty \subseteq \bigcup_{n\geq 0} F_0(\zeta_{p^n})$). His conjecture was based on calculations for primes $p < 4000$ in the case of $F_0 = \mathbf{Q}$.
- This conjecture has been proven for F_0 abelian by a landmark theorem of Ferrero-Washington, and later by Sinnott using a different method. The general case remains open.
- One implication of this type of result is the following well-known estimate for p-parts of class numbers:

The (cyclotomic) μ-invariant and class numbers

- Iwasawa conjectured that $\mu = 0$ for cyclotomic extensions (i.e. for $F_\infty \subseteq \bigcup_{n \geq 0} F_0(\zeta_{p^n})$). His conjecture was based on calculations for primes $p < 4000$ in the case of $F_0 = \mathbf{Q}$.
- This conjecture has been proven for F_0 abelian by a landmark theorem of Ferrero-Washington, and later by Sinnott using a different method. The general case remains open.
- One implication of this type of result is the following well-known estimate for p-parts of class numbers:

- Corollary

  Let e_n be the exponent of p dividing the class number of the cyclotomic field $\mathbf{Q}(\zeta_{p^{n+1}})$ ($p > 2$). Then, there exist integers $\lambda \geq 0$ and ν such that for all sufficiently large n, $e_n = \lambda n + \nu$.

The underlying idea: Iwasawa algebras

- Suppose that G is a profinite group (such as $\mathbf{Z}_p^d$ for $d \geq 1$), and that $\mathcal{O}$ is a complete local ring (such as $\mathbf{Z}_p$).

The underlying idea: Iwasawa algebras

- Suppose that G is a profinite group (such as $\mathbf{Z}_p^d$ for $d \geq 1$), and that $\mathcal{O}$ is a complete local ring (such as $\mathbf{Z}_p$).
- The $\mathcal{O}$-Iwasawa algebra of G, often denoted $\Lambda = \Lambda_{\mathcal{O}}(G)$ or $\mathcal{O}[[G]]$, is the profinite limit over open normal subgroups

$$\Lambda = \Lambda_{\mathcal{O}}(G) = \mathcal{O}[[G]] = \varprojlim_{U \subseteq G} \mathcal{O}[G/U].$$

The underlying idea: Iwasawa algebras

- Suppose that G is a profinite group (such as $\mathbf{Z}_p^d$ for $d \geq 1$), and that $\mathcal{O}$ is a complete local ring (such as $\mathbf{Z}_p$).
- The $\mathcal{O}$-Iwasawa algebra of G, often denoted $\Lambda = \Lambda_{\mathcal{O}}(G)$ or $\mathcal{O}[[G]]$, is the profinite limit over open normal subgroups

$$\Lambda = \Lambda_{\mathcal{O}}(G) = \mathcal{O}[[G]] = \varprojlim_{U \subseteq G} \mathcal{O}[G/U].$$

- If G is abelian (and finitely generated), then the elements of this $\Lambda = \Lambda_{\mathcal{O}}(G)$ can be viewed in a natural way as $\mathcal{O}$-valued measures on G.

The underlying idea: Iwasawa algebras

- Suppose that G is a profinite group (such as $\mathbf{Z}_p^d$ for $d \geq 1$), and that $\mathcal{O}$ is a complete local ring (such as $\mathbf{Z}_p$).
- The $\mathcal{O}$-Iwasawa algebra of G, often denoted $\Lambda = \Lambda_{\mathcal{O}}(G)$ or $\mathcal{O}[[G]]$, is the profinite limit over open normal subgroups

$$\Lambda = \Lambda_{\mathcal{O}}(G) = \mathcal{O}[[G]] = \varprojlim_{U \subseteq G} \mathcal{O}[G/U].$$

- If G is abelian (and finitely generated), then the elements of this $\Lambda = \Lambda_{\mathcal{O}}(G)$ can be viewed in a natural way as $\mathcal{O}$-valued measures on G.
- Suppose that $G \approx \mathbf{Z}_p^d$ for $d \geq 1$. Fix a system of topological generators $(\gamma_i)_{i=1}^d$ of G. We then have an isomorphism

$$\varphi : \Lambda_{\mathcal{O}}(G) \longrightarrow \mathcal{O}[[T_1, \ldots, T_d]], \quad \gamma_i \longmapsto T_i + 1$$

for $\mathcal{O}[[T_1, \ldots, T_d]]$ the $\mathcal{O}$-power series ring in $(T_i)_{i=1}^d$.

Iwasawa's structure theory

- Theorem (Iwasawa, 1958)

  Suppose that $G \approx \mathbf{Z}_p$ and that $\mathcal{O} = \mathbf{Z}_p$. Let M be a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G) \approx \mathbf{Z}_p[[T]]$-module. Then, there is a pseudo-isomorphism of Λ-modules

$$M \longrightarrow \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda / p^{m_i} \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda / f_j(T)^{l_j} \right)$$

  for non-negative integers r, m_i, and l_j, where the $f_j(T)$ correspond (under φ) to irreducible, distinguished polynomials in $\mathcal{O}[[T]] \approx \Lambda$.

Iwasawa's structure theory

- Theorem (Iwasawa, 1958)

  Suppose that $G \approx \mathbf{Z}_p$ and that $\mathcal{O} = \mathbf{Z}_p$. Let M be a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G) \approx \mathbf{Z}_p[[T]]$-module. Then, there is a pseudo-isomorphism of Λ-modules

$$M \longrightarrow \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/p^{m_i} \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/f_j(T)^{l_j} \right)$$

  for non-negative integers r, m_i, and l_j, where the $f_j(T)$ correspond (under φ) to irreducible, distinguished polynomials in $\mathcal{O}[[T]] \approx \Lambda$.

  - When $r = 0$, we define the Λ-characteristic power series of M:

$$\mathrm{char}_\Lambda(M) = \prod_{i=1}^{s} p^{m_i} \prod_{j=1}^{t} f_j(T)^{l_j},$$

    with (familiar!) invariants $\mu = \mu_\Lambda(M) = \sum_{i=1}^{s} m_i$ and $\lambda = \lambda_\Lambda(M) = \sum_{j=1}^{t} \deg(f_j) \cdot l_j$.

Iwasawa's structure theory

- Theorem (Iwasawa, 1958)

  Suppose that $G \approx \mathbf{Z}_p$ and that $\mathcal{O} = \mathbf{Z}_p$. Let M be a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G) \approx \mathbf{Z}_p[[T]]$-module. Then, there is a pseudo-isomorphism of Λ-modules

$$M \longrightarrow \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/p^{m_i} \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/f_j(T)^{l_j} \right)$$

  for non-negative integers r, m_i, and l_j, where the $f_j(T)$ correspond (under φ) to irreducible, distinguished polynomials in $\mathcal{O}[[T]] \approx \Lambda$.

  - When $r = 0$, we define the Λ-characteristic power series of M:

$$\mathrm{char}_\Lambda(M) = \prod_{i=1}^{s} p^{m_i} \prod_{j=1}^{t} f_j(T)^{l_j},$$

    with (familiar!) invariants $\mu = \mu_\Lambda(M) = \sum_{i=1}^{s} m_i$ and $\lambda = \lambda_\Lambda(M) = \sum_{j=1}^{t} \deg(f_j) \cdot l_j$.

General structure theory (abelian setting)

- Theorem (Bourbaki, 1965)

  Let G be a pro-p p-adic Lie group with no element of order p. Suppose G is abelian. Let M be a finitely generated, torsion $\Lambda = \Lambda_{\mathcal{O}}(G)$-module. Then, there is a pseudo-isomorphism of Λ-modules

$$M \longrightarrow \bigoplus_{j=1}^{w} \Lambda/(f_j)$$

  for some nonzero elements $f_j \in \Lambda$.

General structure theory (abelian setting)

- Theorem (Bourbaki, 1965)

  Let G be a pro-p p-adic Lie group with no element of order p. Suppose G is abelian. Let M be a finitely generated, torsion $\Lambda = \Lambda_{\mathcal{O}}(G)$-module. Then, there is a pseudo-isomorphism of Λ-modules

$$M \longrightarrow \bigoplus_{j=1}^{w} \Lambda/(f_j)$$

  for some nonzero elements $f_j \in \Lambda$.

  - In this setting, we define the corresponding characteristic ideal

$$\mathrm{char}_\Lambda(M) := \prod_{j=1}^{w} f_j,$$

    which is well-defined up to a unit in Λ.

General structure theory (abelian setting)

- Theorem (Bourbaki, 1965)

  Let G be a pro-p p-adic Lie group with no element of order p. Suppose G is abelian. Let M be a finitely generated, torsion $\Lambda = \Lambda_{\mathcal{O}}(G)$-module. Then, there is a pseudo-isomorphism of Λ-modules

$$M \longrightarrow \bigoplus_{j=1}^{w} \Lambda/(f_j)$$

  for some nonzero elements $f_j \in \Lambda$.

  - In this setting, we define the corresponding characteristic ideal

$$\mathrm{char}_{\Lambda}(M) := \prod_{j=1}^{w} f_j,$$

    which is well-defined up to a unit in Λ.

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n \geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n \geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.
- Let M_∞ be the maximal abelian pro-p extension of F_∞ which is unramified outside of p, and $Y = \mathrm{Gal}(M_\infty / F_\infty)$.

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n \geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.
- Let M_∞ be the maximal abelian pro-p extension of F_∞ which is unramified outside of p, and $Y = \mathrm{Gal}(M_\infty/F_\infty)$.
- The group Y has the structure of a $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module via the action of $G = \mathrm{Gal}(F_\infty/F)$ by inner automorphisms.

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n \geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.
- Let M_∞ be the maximal abelian pro-p extension of F_∞ which is unramified outside of p, and $Y = \mathrm{Gal}(M_\infty / F_\infty)$.
- The group Y has the structure of a $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module via the action of $G = \mathrm{Gal}(F_\infty / F)$ by inner automorphisms. It can be shown to be finitely generated and torsion as a Λ-module.

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n \geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.
- Let M_∞ be the maximal abelian pro-p extension of F_∞ which is unramified outside of p, and $Y = \mathrm{Gal}(M_\infty / F_\infty)$.
- The group Y has the structure of a $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module via the action of $G = \mathrm{Gal}(F_\infty / F)$ by inner automorphisms. It can be shown to be finitely generated and torsion as a Λ-module.
- A construction of Deligne-Ribet and Cassou-Nougués (extending Kubota/Leopold) gives an element $L_p \in \Lambda$ which can be characterized as follows:

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n \geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.
- Let M_∞ be the maximal abelian pro-p extension of F_∞ which is unramified outside of p, and $Y = \mathrm{Gal}(M_\infty / F_\infty)$.
- The group Y has the structure of a $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module via the action of $G = \mathrm{Gal}(F_\infty / F)$ by inner automorphisms. It can be shown to be finitely generated and torsion as a Λ-module.
- A construction of Deligne-Ribet and Cassou-Nougués (extending Kubota/Leopold) gives an element $L_p \in \Lambda$ which can be characterized as follows: Fix a topological generator $\gamma \in G$, let $H = [\gamma] - 1 \in \Lambda$, and let $\nu_s : \Lambda \longrightarrow \mathbf{Z}_p, [\gamma] \to u^s$ (for u is the image of γ under the canonical map $G \to 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^\times$and $s \in \mathbf{Z}_p$) be the specialization map.

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n \geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.
- Let M_∞ be the maximal abelian pro-p extension of F_∞ which is unramified outside of p, and $Y = \mathrm{Gal}(M_\infty/F_\infty)$.
- The group Y has the structure of a $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module via the action of $G = \mathrm{Gal}(F_\infty/F)$ by inner automorphisms. It can be shown to be finitely generated and torsion as a Λ-module.
- A construction of Deligne-Ribet and Cassou-Nougués (extending Kubota/Leopold) gives an element $L_p \in \Lambda$ which can be characterized as follows: Fix a topological generator $\gamma \in G$, let $H = [\gamma] - 1 \in \Lambda$, and let $\nu_s : \Lambda \longrightarrow \mathbf{Z}_p, [\gamma] \to u^s$ (for u is the image of γ under the canonical map $G \to 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^\times$and $s \in \mathbf{Z}_p$) be the specialization map. Then for all integers $n \geq 1$ which satisfy $n \equiv 0 \mod p-1$, we have the interpolation formula $\nu_s(L_p)/\nu_s(H) = \zeta_F^{(p)}(1-n)$.

Main conjecture for (totally real) number fields

- Let $F = F_0$ be a totally real number field, $p > 2$ a fixed prime, and $F_\infty = \bigcup_{n\geq 0} F_n$ the cyclotomic $\mathbf{Z}_p$-extension of F.
- Let M_∞ be the maximal abelian pro-p extension of F_∞ which is unramified outside of p, and $Y = \mathrm{Gal}(M_\infty/F_\infty)$.
- The group Y has the structure of a $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module via the action of $G = \mathrm{Gal}(F_\infty/F)$ by inner automorphisms. It can be shown to be finitely generated and torsion as a Λ-module.
- A construction of Deligne-Ribet and Cassou-Nougués (extending Kubota/Leopold) gives an element $L_p \in \Lambda$ which can be characterized as follows: Fix a topological generator $\gamma \in G$, let $H = [\gamma] - 1 \in \Lambda$, and let $\nu_s : \Lambda \longrightarrow \mathbf{Z}_p, [\gamma] \to u^s$ (for u is the image of γ under the canonical map $G \to 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^\times$and $s \in \mathbf{Z}_p$) be the specialization map. Then for all integers $n \geq 1$ which satisfy $n \equiv 0 \mod p-1$, we have the interpolation formula $\nu_s(L_p)/\nu_s(H) = \zeta_F^{(p)}(1-n)$.

- Theorem (Mazur-Wiles, 1984 & Wiles, 1990; cf. Rubin 1990)

We have an equality of principal ideals $(\mathrm{char}_\Lambda(Y)) \doteq (L_p)$ *in* Λ.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K,

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.
- Let K_∞ be the $\mathbf{Z}_p^2$-extension of K.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.
- Let K_∞ be the $\mathbf{Z}_p^2$-extension of K. Let $G = \mathrm{Gal}(K_\infty/K) \approx \mathbf{Z}_p^2$ be its Galois group.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.
- Let K_∞ be the $\mathbf{Z}_p^2$-extension of K. Let $G = \mathrm{Gal}(K_\infty/K) \approx \mathbf{Z}_p^2$ be its Galois group.
- Let E be an elliptic curve defined over K with CM by $\mathcal{O}_K$.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.
- Let K_∞ be the $\mathbf{Z}_p^2$-extension of K. Let $G = \mathrm{Gal}(K_\infty/K) \approx \mathbf{Z}_p^2$ be its Galois group.
- Let E be an elliptic curve defined over K with CM by $\mathcal{O}_K$.
- Let $M = \mathrm{Gal}(M_\infty/K_\infty)$, where M_∞ is the maximal, abelian p-extension of K_∞ which is unramified outside of $\mathfrak{p}$.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.
- Let K_∞ be the $\mathbf{Z}_p^2$-extension of K. Let $G = \mathrm{Gal}(K_\infty/K) \approx \mathbf{Z}_p^2$ be its Galois group.
- Let E be an elliptic curve defined over K with CM by $\mathcal{O}_K$.
- Let $M = \mathrm{Gal}(M_\infty/K_\infty)$, where M_∞ is the maximal, abelian p-extension of K_∞ which is unramified outside of $\mathfrak{p}$. It has the structure of a finitely generated torsion $\Lambda = \Lambda_{\mathcal{O}}(G)$-module.

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.
- Let K_∞ be the $\mathbf{Z}_p^2$-extension of K. Let $G = \mathrm{Gal}(K_\infty/K) \approx \mathbf{Z}_p^2$ be its Galois group.
- Let E be an elliptic curve defined over K with CM by $\mathcal{O}_K$.
- Let $M = \mathrm{Gal}(M_\infty/K_\infty)$, where M_∞ is the maximal, abelian p-extension of K_∞ which is unramified outside of $\mathfrak{p}$. It has the structure of a finitely generated torsion $\Lambda = \Lambda_{\mathcal{O}}(G)$-module.
- The Hasse-Weil L-function $L(E/K, s)$ is known by a classical theorem of Deuring to be identified with the L-function of a Hecke Grössencharacter, and hence to have an analytic continuation and functional equation (relating $s \to 2 - s$).

Main conjecture for CM elliptic curves, setup

- Let K be an imaginary quadratic field with integers $\mathcal{O}_K$.
- Fix a prime $p \geq 5$. Assume for simplicity that p splits in K, and that K has class number 1. Fix a prime $\mathfrak{p}$ above p in K.
- Let K_∞ be the $\mathbf{Z}_p^2$-extension of K. Let $G = \mathrm{Gal}(K_\infty/K) \approx \mathbf{Z}_p^2$ be its Galois group.
- Let E be an elliptic curve defined over K with CM by $\mathcal{O}_K$.
- Let $M = \mathrm{Gal}(M_\infty/K_\infty)$, where M_∞ is the maximal, abelian p-extension of K_∞ which is unramified outside of $\mathfrak{p}$. It has the structure of a finitely generated torsion $\Lambda = \Lambda_{\mathcal{O}}(G)$-module.
- The Hasse-Weil L-function $L(E/K, s)$ is known by a classical theorem of Deuring to be identified with the L-function of a Hecke Grössencharacter, and hence to have an analytic continuation and functional equation (relating $s \to 2 - s$).

Main conjectures for CM elliptic curves, results

- Let ψ to denote the Hecke Grössencharacter associated to E.

Main conjectures for CM elliptic curves, results

- Let ψ to denote the Hecke Grössencharacter associated to E. Let L be the period lattice of the Weierstrass-$\mathcal{P}$ function associated to E, and $\Omega_\infty \in L$ an element such that $L = \Omega_\infty \mathcal{O}_K$.

Main conjectures for CM elliptic curves, results

- Let ψ to denote the Hecke Grössencharacter associated to E. Let L be the period lattice of the Weierstrass-$\mathcal{P}$ function associated to E, and $\Omega_\infty \in L$ an element such that $L = \Omega_\infty \mathcal{O}_K$. A theorem of Damerell shows the numbers $\mathcal{L}(\overline{\psi}, k, j) := (2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\overline{\psi}^{k+j}, k) \in \overline{\mathbf{Q}}$ and in fact lie in K for integers $0 \leq j < k$.

Main conjectures for CM elliptic curves, results

- Let ψ to denote the Hecke Grössencharacter associated to E. Let L be the period lattice of the Weierstrass-$\mathcal{P}$ function associated to E, and $\Omega_\infty \in L$ an element such that $L = \Omega_\infty \mathcal{O}_K$. A theorem of Damerell shows the numbers $\mathcal{L}(\overline{\psi}, k, j) := (2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\overline{\psi}^{k+j}, k) \in \overline{\mathbf{Q}}$ and in fact lie in K for integers $0 \le j < k$. Fixing an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$, one views these algebraic values as elements in $\overline{\mathbf{Q}}_p$.

Main conjectures for CM elliptic curves, results

- Let ψ to denote the Hecke Grössencharacter associated to E. Let L be the period lattice of the Weierstrass-$\mathcal{P}$ function associated to E, and $\Omega_\infty \in L$ an element such that $L = \Omega_\infty \mathcal{O}_K$. A theorem of Damerell shows the numbers $\mathcal{L}(\overline{\psi}, k, j) := (2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\overline{\psi}^{k+j}, k) \in \overline{\mathbf{Q}}$ and in fact lie in K for integers $0 \leq j < k$. Fixing an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$, one views these algebraic values as elements in $\overline{\mathbf{Q}}_p$.
- Construction(s) due to Manin-Visik, Katz, and Coates-Wiles give an element $L_p = L_p(\overline{\psi}) \in \Lambda_{\mathcal{O}}(G)$ determined uniquely by some interpolation formula relating specializations of L_p to the values $\mathcal{L}(\overline{\psi}, k, j)$.

Main conjectures for CM elliptic curves, results

- Let ψ to denote the Hecke Grössencharacter associated to E. Let L be the period lattice of the Weierstrass-$\mathcal{P}$ function associated to E, and $\Omega_\infty \in L$ an element such that $L = \Omega_\infty \mathcal{O}_K$. A theorem of Damerell shows the numbers $\mathcal{L}(\overline{\psi}, k, j) := (2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\overline{\psi}^{k+j}, k) \in \overline{\mathbf{Q}}$ and in fact lie in K for integers $0 \leq j < k$. Fixing an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$, one views these algebraic values as elements in $\overline{\mathbf{Q}}_p$.
- Construction(s) due to Manin-Visik, Katz, and Coates-Wiles give an element $L_p = L_p(\overline{\psi}) \in \Lambda_{\mathcal{O}}(G)$ determined uniquely by some interpolation formula relating specializations of L_p to the values $\mathcal{L}(\overline{\psi}, k, j)$. Here, $\mathcal{O}$ is ring of the integers of some unramified extension of $K_{\mathfrak{p}}$.

- Theorem (Coates-Wiles, 1977; Yager, 1980; cf. Rubin, 1991)
We have an equality of principal ideals $(\mathrm{char}_\Lambda(M)) = (L_p)$ *in* Λ.

Main conjectures for CM elliptic curves, results

- Let ψ to denote the Hecke Grössencharacter associated to E. Let L be the period lattice of the Weierstrass-$\mathcal{P}$ function associated to E, and $\Omega_\infty \in L$ an element such that $L = \Omega_\infty \mathcal{O}_K$. A theorem of Damerell shows the numbers $\mathcal{L}(\overline{\psi}, k, j) := (2\pi/\sqrt{d_K})^j \Omega_\infty^{-(k+j)} L(\overline{\psi}^{k+j}, k) \in \overline{\mathbf{Q}}$ and in fact lie in K for integers $0 \leq j < k$. Fixing an embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$, one views these algebraic values as elements in $\overline{\mathbf{Q}}_p$.
- Construction(s) due to Manin-Visik, Katz, and Coates-Wiles give an element $L_p = L_p(\overline{\psi}) \in \Lambda_{\mathcal{O}}(G)$ determined uniquely by some interpolation formula relating specializations of L_p to the values $\mathcal{L}(\overline{\psi}, k, j)$. Here, $\mathcal{O}$ is ring of the integers of some unramified extension of $K_{\mathfrak{p}}$.

- Theorem (Coates-Wiles, 1977; Yager, 1980; cf. Rubin, 1991)

  We have an equality of principal ideals $(\mathrm{char}_\Lambda(M)) = (L_p)$ *in* Λ.

  - This theorem can be used to derive strong results towards the conjecture of Birch-Swinnerton-Dyer in the rank zero case.

Main conjecture for non-CM elliptic curves, setup

- Let E be an elliptic curve defined over $F_0 = \mathbf{Q}$.

Main conjecture for non-CM elliptic curves, setup

- Let E be an elliptic curve defined over $F_0 = \mathbf{Q}$. Hence, E is modular by a fundamental theorem of Wiles, Taylor-Wiles, and Breuil-Conrad-Diamond-Taylor.

Main conjecture for non-CM elliptic curves, setup

- Let E be an elliptic curve defined over $F_0 = \mathbf{Q}$. Hence, E is modular by a fundamental theorem of Wiles, Taylor-Wiles, and Breuil-Conrad-Diamond-Taylor.
- In this setting, the Hasse-Weil L-function $L(E/F_0, s)$ can be identified with the (automorphic) L-function $L(f, s)$ of some associated eigenform $f \in S_2^{\mathrm{new}}(\mathrm{cond}(E))$, from which we derive the analytic continuation and functional equation.

Main conjecture for non-CM elliptic curves, setup

- Let E be an elliptic curve defined over $F_0 = \mathbf{Q}$. Hence, E is modular by a fundamental theorem of Wiles, Taylor-Wiles, and Breuil-Conrad-Diamond-Taylor.
- In this setting, the Hasse-Weil L-function $L(E/F_0, s)$ can be identified with the (automorphic) L-function $L(f, s)$ of some associated eigenform $f \in S_2^{\mathrm{new}}(\mathrm{cond}(E))$, from which we derive the analytic continuation and functional equation.
- Let $F_\infty = \mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $F_0 = \mathbf{Q}$, with profinite Galois group $G = \mathrm{Gal}(F_\infty/F_0) \approx \mathbf{Z}_p$.

Main conjecture for non-CM elliptic curves, setup

- Let E be an elliptic curve defined over $F_0 = \mathbf{Q}$. Hence, E is modular by a fundamental theorem of Wiles, Taylor-Wiles, and Breuil-Conrad-Diamond-Taylor.
- In this setting, the Hasse-Weil L-function $L(E/F_0, s)$ can be identified with the (automorphic) L-function $L(f, s)$ of some associated eigenform $f \in S_2^{\mathrm{new}}(\mathrm{cond}(E))$, from which we derive the analytic continuation and functional equation.
- Let $F_\infty = \mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $F_0 = \mathbf{Q}$, with profinite Galois group $G = \mathrm{Gal}(F_\infty/F_0) \approx \mathbf{Z}_p$.
- A theorem of Shimura shows that there exists a complex number Ω such that $\mathcal{L}(f \times \chi, 1) = L(f \times \chi, 1)/\Omega$ is an algebraic number for any (nontrivial) character χ of G.

Main conjecture for non-CM elliptic curves, setup

- Let E be an elliptic curve defined over $F_0 = \mathbf{Q}$. Hence, E is modular by a fundamental theorem of Wiles, Taylor-Wiles, and Breuil-Conrad-Diamond-Taylor.
- In this setting, the Hasse-Weil L-function $L(E/F_0, s)$ can be identified with the (automorphic) L-function $L(f, s)$ of some associated eigenform $f \in S_2^{\mathrm{new}}(\mathrm{cond}(E))$, from which we derive the analytic continuation and functional equation.
- Let $F_\infty = \mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $F_0 = \mathbf{Q}$, with profinite Galois group $G = \mathrm{Gal}(F_\infty/F_0) \approx \mathbf{Z}_p$.
- A theorem of Shimura shows that there exists a complex number Ω such that $\mathcal{L}(f \times \chi, 1) = L(f \times \chi, 1)/\Omega$ is an algebraic number for any (nontrivial) character χ of G.
- A construction due to Manin and Mazur-Swinnerton-Dyer (cf. Mazur-Tate-Teitelbaum) gives an element $L_p = L_p(f) \in \Lambda = \Lambda_{\mathbf{Z}_p}(G)$ characterized uniquely by an interpolation property of the form $\chi(L_p) = (*)\mathcal{L}(f \times \chi, 1)$ for finite-order characters χ of G (for $(*)$ some algebraic factor).

Main conjecture for non-CM elliptic curves, results

- Consider the p-primary Selmer group $\mathrm{Sel}(E/F_\infty)$ of E/F_∞.

Main conjecture for non-CM elliptic curves, results

- Consider the p-primary Selmer group $\mathrm{Sel}(E/F_\infty)$ of E/F_∞. Its Pontryayin dual $X(E/F_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$ has the structure of a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module.

Main conjecture for non-CM elliptic curves, results

- Consider the p-primary Selmer group $\mathrm{Sel}(E/F_\infty)$ of E/F_∞. Its Pontryayin dual $X(E/F_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$ has the structure of a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module.
- A deep theorem of Kato (+ Rohrlich) shows that $X(E/F_\infty)$ is Λ-torsion, and hence that we can define $\mathrm{char}_\Lambda(X(E/F_\infty))$.

Main conjecture for non-CM elliptic curves, results

- Consider the p-primary Selmer group $\mathrm{Sel}(E/F_\infty)$ of E/F_∞. Its Pontryayin dual $X(E/F_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$ has the structure of a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module.
- A deep theorem of Kato (+ Rohrlich) shows that $X(E/F_\infty)$ is Λ-torsion, and hence that we can define $\mathrm{char}_\Lambda(X(E/F_\infty))$. Kato's argument uses the construction of what is known as an Euler system – a certain system of compatible cohomology classes related (via so-called explicit reciprocity laws) to the algebraic L-values interpolated by $L_p(f) \in \Lambda$.

Main conjecture for non-CM elliptic curves, results

- Consider the p-primary Selmer group $\mathrm{Sel}(E/F_\infty)$ of E/F_∞. Its Pontryayin dual $X(E/F_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$ has the structure of a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module.
- A deep theorem of Kato (+ Rohrlich) shows that $X(E/F_\infty)$ is Λ-torsion, and hence that we can define $\mathrm{char}_\Lambda(X(E/F_\infty))$. Kato's argument uses the construction of what is known as an Euler system – a certain system of compatible cohomology classes related (via so-called explicit reciprocity laws) to the algebraic L-values interpolated by $L_p(f) \in \Lambda$. Note however that Kato requires Rohrlich's theorem to deduce nontriviality, and hence to deduce that the Λ-module $X(E/F_\infty)$ is torsion.

Main conjecture for non-CM elliptic curves, results

- Consider the p-primary Selmer group $\mathrm{Sel}(E/F_\infty)$ of E/F_∞. Its Pontryayin dual $X(E/F_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$ has the structure of a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module.
- A deep theorem of Kato (+ Rohrlich) shows that $X(E/F_\infty)$ is Λ-torsion, and hence that we can define $\mathrm{char}_\Lambda(X(E/F_\infty))$. Kato's argument uses the construction of what is known as an Euler system – a certain system of compatible cohomology classes related (via so-called explicit reciprocity laws) to the algebraic L-values interpolated by $L_p(f) \in \Lambda$. Note however that Kato requires Rohrlich's theorem to deduce nontriviality, and hence to deduce that the Λ-module $X(E/F_\infty)$ is torsion.

- Theorem (Kato, 2004 + Skinner-Urban, 2014)

  We have an equality of ideals $(\mathrm{char}_\Lambda(X(E/F_\infty))) = (L_p(f))$ *in* Λ.

Main conjecture for non-CM elliptic curves, results

- Consider the p-primary Selmer group $\mathrm{Sel}(E/F_\infty)$ of E/F_∞. Its Pontryayin dual $X(E/F_\infty) = \mathrm{Hom}(\mathrm{Sel}(E/F_\infty), \mathbf{Q}_p/\mathbf{Z}_p)$ has the structure of a finitely generated $\Lambda = \Lambda_{\mathbf{Z}_p}(G)$-module.
- A deep theorem of Kato (+ Rohrlich) shows that $X(E/F_\infty)$ is Λ-torsion, and hence that we can define $\mathrm{char}_\Lambda(X(E/F_\infty))$. Kato's argument uses the construction of what is known as an Euler system – a certain system of compatible cohomology classes related (via so-called explicit reciprocity laws) to the algebraic L-values interpolated by $L_p(f) \in \Lambda$. Note however that Kato requires Rohrlich's theorem to deduce nontriviality, and hence to deduce that the Λ-module $X(E/F_\infty)$ is torsion.

- Theorem (Kato, 2004 + Skinner-Urban, 2014)

  We have an equality of ideals $(\mathrm{char}_\Lambda(X(E/F_\infty)) = (L_p(f))$ *in* Λ.

- Corollary

  $E(F_\infty)$ *is finitely-generated.*

Other developments and open problems

- There have been many other developments, among them:

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticyclotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems
  - mysterious connections to ergodic/transcendence theory

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems
  - mysterious connections to ergodic/transcendence theory
- However, many open problems remain in this setting:

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticyclotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems
  - mysterious connections to ergodic/transcendence theory
- However, many open problems remain in this setting:
  - Iwasawa's conjecture on μ (as refined by Greenberg):

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticyclotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems
  - mysterious connections to ergodic/transcendence theory
- However, many open problems remain in this setting:
  - Iwasawa's conjecture on μ (as refined by Greenberg): Does the cyclotomic μ-invariant of a totally real number field not containing any p-th roots of unity necessarily vanish?

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems
  - mysterious connections to ergodic/transcendence theory
- However, many open problems remain in this setting:
  - Iwasawa's conjecture on μ (as refined by Greenberg): Does the cyclotomic μ-invariant of a totally real number field not containing any p-th roots of unity necessarily vanish?
  - Can we show main conjectures for CM abelian varieties?

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticyclotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems
  - mysterious connections to ergodic/transcendence theory
- However, many open problems remain in this setting:
  - Iwasawa's conjecture on μ (as refined by Greenberg): Does the cyclotomic μ-invariant of a totally real number field not containing any p-th roots of unity necessarily vanish?
  - Can we show main conjectures for CM abelian varieties? Or Hilbert modular forms in cyclotomic $\mathbf{Z}_p$-extensions of totally real fields?

Other developments and open problems

- There have been many other developments, among them:
  - non-commutative Iwasawa theory
  - anticylotomic main conjectures and CM fields
  - Iwasawa main conjectures for p-adic representations/motives
  - variation in Hida families
  - extensions to automorphic forms on higher-rank groups
  - the role/theory of the L-values and Euler systems
  - mysterious connections to ergodic/transcendence theory
- However, many open problems remain in this setting:
  - Iwasawa's conjecture on μ (as refined by Greenberg): Does the cyclotomic μ-invariant of a totally real number field not containing any p-th roots of unity necessarily vanish?
  - Can we show main conjectures for CM abelian varieties? Or Hilbert modular forms in cyclotomic $\mathbf{Z}_p$-extensions of totally real fields? Or stronger (p-adic) Birch-Swinnerton-Dyer results, even just for higher-rank CM elliptic curves?

Some references – the classical setup

N. Bourbaki,
Élements de mathématique, Fasc. XXXI, Alg. comm., Ch. VII, *Act. Scientifiques et Industrielles* **1314**, Hermann, (1965).

B. Ferrero and L. Washington,
The Iwasawa μ_p invariant vanishes for abelian number fields, *Ann. of Math.* **109** (1979), 377-396.

K. Iwasawa,
On $\mathbf{Z}_l$-extentensions of number fields, *Ann. of Math.* **98** (1973), 246-323.

K. Iwasawa and C. Sims,
Computation of invariants in the theory of cyclotomic fields, *J. Math. Soc. Japan* **18** (1966), 86-96.

W. Sinnott
On the μ-invariant of the Γ transform of a rational function, *Invent. math.* **75** (1984), 273-282.

Some references – totally real fields

P. Deligne and K. Ribet,
Values of abelian L-functions at negative integers over totally real fields, *Invent. math.* **59** (1980), 227-286.

R. Greenberg,
On the Iwasawa invariants of totally real number fields, *Amer. J. Math.* **98** (1976), 263-284.

B. Mazur and A. Wiles,
Class fields of abelian extensions of $\mathbf{Q}$, *Invent. math.* **76** (1984), 179-330.

K. Rubin,
The main conjecture. Appendix to: Cyclotomic Fields I and II by S. Lang, *Graduate Texts in Math.* **121**, Springer (1990) 397419.

A. Wiles,
The Iwasawa Conjecture for Totally Real Fields, *Ann. of Math.* **131** no. 3 (1990), 493-540.

Some references – CM elliptic curves

J. Coates,
Elliptic curves with complex multiplication and Iwasawa theory, *Bull. London Math. Soc.* **23** (1991), 321-350.

J. Coates and A. Wiles,
On the conjecture of Birch and Swinnerton-Dyer, *Invent. math.* **39** (1977), 223-251.

B. Mazur,
Rational points of abelian varieties with values in towers of number fields, *Invent. math.* **18** (1972), 183-266.

E. de Shalit,
Iwasawa theory for elliptic curves with complex multiplication, *Perspectives in Math.*, Academic Press Boston (1987).

K. Rubin,
The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. math.* **103** (1991) 25-68.

Some references – modular elliptic curves

K. Kato,
p-adic Hodge theory and values of zeta functions of modular forms, *Astérisque* **295** (2004), 117-290.

B. Mazur and P. Swinnerton-Dyer,
Arithmetic of Weil curves, *Invent. math.* **25** (174), 1-61.

B. Mazur, J. Tate, and J. Teitelbaum,
On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Invent. math.* **84** (1986), 1-48.

D. Rohrlich,
On L-functions of elliptic curves and cyclotomic towers, *Invent. math.* **75** (1984), 409-423.

C. Skinner and E. Urban,
The Iwasawa main conjecture for GL(2), *Invent. math.* **195** (2014), 1-277.