Entering the tower with Iwasawa theory

Marta Sánchez Pavón

Seminari Informal de Matemàtiques de Barcelona

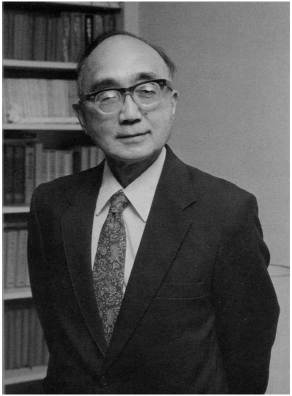
April 21st 2021

General idea about Iwasawa theory

Iwasawa theory was born as the study of the growth of the ideal class group of $\mathbb{Q}(\zeta_{p^n})$ over towers of numbers fields.

The three main characteristics of (general) Iwasawa theory:

- Studying the growth of objects of arithmetic nature...
- ...over infinite towers of fields....
- ... which are built using p-adic extensions.



Kenkichi Iwasawa. 1917-1998

Fermat's Last Theorem (Wiles, 1995)

The equation $x^n + y^n = z^n$ has no non-trivial solutions for every integer $n \geq 3$.

Around 1840, Kummer developed his theory of cyclotomic fields trying to prove nice properties of the complex factorization of

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y)$$

in the ring $\mathbb{Z}[\zeta_p]$, where ζ_p is the p-th root of unity.

Ernst Kummer. 1810-1893

Problem: $\mathbb{Z}[\zeta_p]$ is not a principal ideal domain in general!

- Kummer defines the **ideal class group** $Cl(K)$ of a number field K, which measures the failure of the ring of integers $\mathcal{O}_K$ of K to be a PID.

$$Cl(K) = (\text{Fractional ideals})/(\text{Principal fractional ideals})$$

- Kummer defines the **ideal class group** $Cl(K)$ of a number field K, which measures the failure of the ring of integers $\mathcal{O}_K$ of K to be a PID.

$$Cl(K) = (\text{Fractional ideals})/(\text{Principal fractional ideals})$$

- $Cl(K)$ is a multiplicative **finite** abelian group.

- Kummer defines the **ideal class group** $Cl(K)$ of a number field K, which measures the failure of the ring of integers $\mathcal{O}_K$ of K to be a PID.

$$Cl(K) = (\text{Fractional ideals})/(\text{Principal fractional ideals})$$

- $Cl(K)$ is a multiplicative **finite** abelian group.
- $\mathcal{O}_K$ is a PID $\iff |Cl(K)| = 1$.

- Kummer defines the **ideal class group** $Cl(K)$ of a number field K, which measures the failure of the ring of integers $\mathcal{O}_K$ of K to be a PID.

$$Cl(K) = (\text{Fractional ideals})/(\text{Principal fractional ideals})$$

- $Cl(K)$ is a multiplicative **finite** abelian group.
- $\mathcal{O}_K$ is a PID $\iff |Cl(K)| = 1$.
- Case of interest: $K = \mathbb{Q}(\zeta_p)$, since $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.

- Kummer defines the **ideal class group** $Cl(K)$ of a number field K, which measures the failure of the ring of integers $\mathcal{O}_K$ of K to be a PID.

$$Cl(K) = (\text{Fractional ideals})/(\text{Principal fractional ideals})$$

- $Cl(K)$ is a multiplicative **finite** abelian group.
- $\mathcal{O}_K$ is a PID $\iff |Cl(K)| = 1$.
- Case of interest: $K = \mathbb{Q}(\zeta_p)$, since $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- A prime p is **regular** if p does not divide the order of the ideal class group of $\mathbb{Q}(\zeta_p)$ (i.e. the p-Sylow subgroup of $Cl(\mathbb{Q}(\zeta_p))$ is trivial); and **irregular** otherwise.

- Kummer defines the **ideal class group** $Cl(K)$ of a number field K, which measures the failure of the ring of integers $\mathcal{O}_K$ of K to be a PID.

$$Cl(K) = (\text{Fractional ideals})/(\text{Principal fractional ideals})$$

- $Cl(K)$ is a multiplicative **finite** abelian group.
- $\mathcal{O}_K$ is a PID $\iff |Cl(K)|= 1$.
- Case of interest: $K = \mathbb{Q}(\zeta_p)$, since $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$.
- A prime p is **regular** if p does not divide the order of the ideal class group of $\mathbb{Q}(\zeta_p)$ (i.e. the p-Sylow subgroup of $Cl(\mathbb{Q}(\zeta_p))$ is trivial); and **irregular** otherwise.
- Reminder: A finite group G has a p-Sylow subgroup for every prime p, which consists of all the elements of G whose order is a power of p.

A miraculous connection!

Theorem. Kummer, 1846

If p is a regular prime then Fermat's Last Theorem holds for exponent p.

A miraculous connection!

Theorem. Kummer, 1846

If p is a regular prime then Fermat's Last Theorem holds for exponent p.

How many regular primes are there?

A miraculous connection!

Theorem. Kummer, 1846

If p is a regular prime then Fermat's Last Theorem holds for exponent p.

How many regular primes are there?

The Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\ell \text{ prime}} \frac{1}{1-\ell^{-s}},$$

and the p-Sylow subgroup of the ideal class group are deeply related!

Kummer's criterion

A prime p is irregular (i.e. the p-Sylow subgroup of $Cl(\mathbb{Q}(\zeta_p))$ *is non-trivial) if and only if p divides the numerator of at least one of* $\zeta(-1), \zeta(-3), \ldots, \zeta(4-p)$.

Kummer's criterion

A prime p is irregular (i.e. the p-Sylow subgroup of $Cl(\mathbb{Q}(\zeta_p))$ is non-trivial) if and only if p divides the numerator of at least one of $\zeta(-1), \zeta(-3), \ldots, \zeta(4-p)$.

Example: 691 is irregular since it divides the numerator of

$$\zeta(-11) = \frac{691}{32760}.$$

So $|Cl(\mathbb{Q}(\zeta_{691}))|$ is multiple of 691.

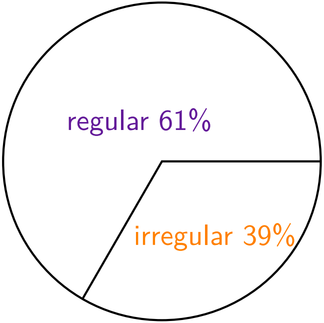
Kummer's criterion

A prime p is irregular (i.e. the p-Sylow subgroup of $Cl(\mathbb{Q}(\zeta_p))$ is non-trivial) if and only if p divides the numerator of at least one of $\zeta(-1), \zeta(-3), \ldots, \zeta(4-p)$.

Example: 691 is irregular since it divides the numerator of

$$\zeta(-11) = \frac{691}{32760}.$$

So $|Cl(\mathbb{Q}(\zeta_{691}))|$ is multiple of 691.



First irregular primes: 37, 59, 67, 101, 103...

Kummer congruences

Let $n, m \in \mathbb{Z}$ odd positive such that $n \equiv m \not\equiv -1 \bmod p-1$. Then

$$\zeta(-n) \equiv \zeta(-m) \bmod p.$$

Kummer congruences

Let $n, m \in \mathbb{Z}$ odd positive such that $n \equiv m \not\equiv -1 \bmod p-1$. Then

$$\zeta(-n) \equiv \zeta(-m) \bmod p.$$

This congruence relations can be generalized to congruences modulo p^n for $n \geq 1$.

Kummer congruences

Let $n, m \in \mathbb{Z}$ odd positive such that $n \equiv m \not\equiv -1 \bmod p-1$. Then

$$\zeta(-n) \equiv \zeta(-m) \bmod p.$$

This congruence relations can be generalized to congruences modulo p^n for $n \geq 1$.

Kubota-Leopoldt p-adic L-function, 1964

Fix $k \in \mathbb{Z}$. There exists a continuous $\mathbb{Z}_p$-valued function $L_p(\omega^k, s)$ of p-adic variable $s \in \mathbb{Z}_p$ satisfying

$$L_p(\omega^k, 1-n) = (1-p^{n-1})\zeta(1-n)$$

for all $n \equiv k \bmod p-1$, where ω is the p-adic character

$$\omega \colon (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{Z}_p.$$

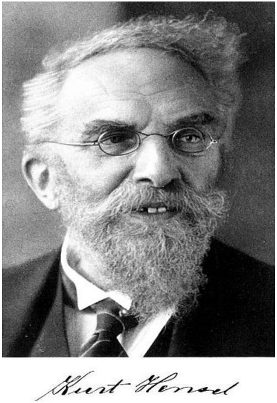
p-adic world

- We define the p-**adic integers** as an inverse limit

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p,$$

with respect to the reduction maps

$$\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$$
$$a \bmod p^n \mapsto a \bmod p^{n-1}.$$

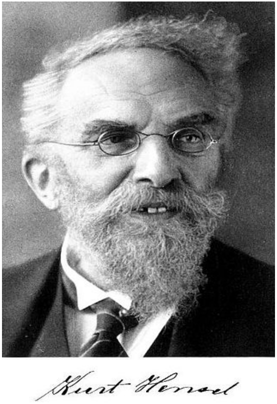


p-adic numbers were introduced by Kurt Hensel around 1897.

p-adic world

- We define the p-**adic integers** as an inverse limit
$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p,$$
with respect to the reduction maps
$$\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$$
$$a \bmod p^n \mapsto a \bmod p^{n-1}.$$

- $(a \bmod p, a \bmod p^2, a \bmod p^3, \dots) \in \mathbb{Z}_p$



p-adic numbers were introduced by Kurt Hensel around 1897.

p-adic world

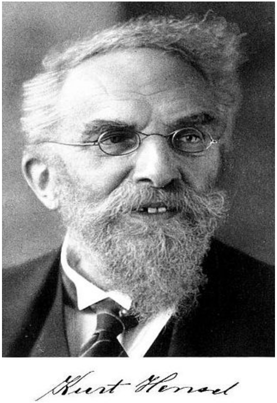
- We define the p-**adic integers** as an inverse limit

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} = \mathbb{Z}_p,$$

with respect to the reduction maps

$$\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$$
$$a \bmod p^n \mapsto a \bmod p^{n-1}.$$

- $(a \bmod p, a \bmod p^2, a \bmod p^3, \dots) \in \mathbb{Z}_p$
- Taking the fraction field of $\mathbb{Z}_p$, we get the p-**adic field** $\mathbb{Q}_p$.



p-adic numbers were introduced by Kurt Hensel around 1897.

p-adic world

Setting: $x \in \mathbb{Q}$ non-zero, $p \in \mathbb{Z}$ prime, $a, b \in \mathbb{Z}$ coprime with p.

p-adic world

Setting: $x \in \mathbb{Q}$ non-zero, $p \in \mathbb{Z}$ prime, $a, b \in \mathbb{Z}$ coprime with p.

- Write
$$x = p^n \frac{a}{b}.$$

p-adic world

Setting: $x \in \mathbb{Q}$ non-zero, $p \in \mathbb{Z}$ prime, $a, b \in \mathbb{Z}$ coprime with p.

- Write
$$x = p^n \frac{a}{b}.$$
- Define the p-**adic absolute value** of x as
$$|x|_p = p^{-n}.$$

p-adic world

Setting: $x \in \mathbb{Q}$ non-zero, $p \in \mathbb{Z}$ prime, $a, b \in \mathbb{Z}$ coprime with p.

- Write
$$x = p^n \frac{a}{b}.$$

- Define the p-**adic absolute value** of x as
$$|x|_p = p^{-n}.$$

- Ultrametric condition: $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.

p-adic world

Setting: $x \in \mathbb{Q}$ non-zero, $p \in \mathbb{Z}$ prime, $a, b \in \mathbb{Z}$ coprime with p.

- Write
$$x = p^n \frac{a}{b}.$$
- Define the p-**adic absolute value** of x as
$$|x|_p = p^{-n}.$$
- Ultrametric condition: $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.
- Completing $\mathbb{Q}$ with respect to the p-adic absolute value, we obtain a complete local field $\mathbb{Q}_p$.

p-adic world

Setting: $x \in \mathbb{Q}$ non-zero, $p \in \mathbb{Z}$ prime, $a, b \in \mathbb{Z}$ coprime with p.

- Write
$$x = p^n \frac{a}{b}.$$
- Define the p-**adic absolute value** of x as
$$|x|_p = p^{-n}.$$
- Ultrametric condition: $|x + y|_p \leq \max\{|x|_p, |y|_p\}$.
- Completing $\mathbb{Q}$ with respect to the p-adic absolute value, we obtain a complete local field $\mathbb{Q}_p$.
- Now, the p-adic integers are
$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

Why should we care about the p-adics?

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p$$

Why should we care about the p-adics?

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p$$

- **(Ostrowski's theorem)** There are only two non-trivial non-equivalent ways of completing $\mathbb{Q}$: one with respect to the real absolute value, and the other with respect to the p-adic absolute value.

Why should we care about the p-adics?

$$\mathbb{C} \supset \mathbb{R} \supset \mathbb{Q} \subset \mathbb{Q}_p$$

- **(Ostrowski's theorem)** There are only two non-trivial non-equivalent ways of completing $\mathbb{Q}$: one with respect to the real absolute value, and the other with respect to the p-adic absolute value.

- **(Hasse principle or local-to-global principle)** An equation has a solution over $\mathbb{Q}$ if and only if it has a solution over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all primes p. Not true in general!

$\mathbb{Z}_p$-extensions

- Take all extensions K_n/K such that

$$\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

$\mathbb{Z}_p$-extensions

- Take all extensions K_n/K such that

$$\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

- A $\mathbb{Z}_p$-**extension** of a K is a Galois extension K_∞/K such that

$$K_\infty = \bigcup_n K_n.$$

$\mathbb{Z}_p$-extensions

- Take all extensions K_n/K such that

$$\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

- A $\mathbb{Z}_p$-**extension** of a K is a Galois extension K_∞/K such that

$$K_\infty = \bigcup_n K_n.$$

- $\mathrm{Gal}(K_\infty/K) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p.$

$\mathbb{Z}_p$-extensions

- Take all extensions K_n/K such that

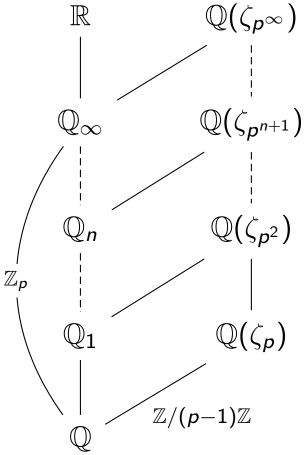
$$\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}.$$

- A $\mathbb{Z}_p$-**extension** of a K is a Galois extension K_∞/K such that

$$K_\infty = \bigcup_n K_n.$$

- $\mathrm{Gal}(K_\infty/K) \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}_p$.

- $\mathbb{Q}_\infty$ is the *only* $\mathbb{Z}_p$-extension of $\mathbb{Q}$, called the **cyclotomic** $\mathbb{Z}_p$-extension.



Question: how many linearly independent $\mathbb{Z}_p$-extensions can we get from K?

Question: how many linearly independent $\mathbb{Z}_p$-extensions can we get from K?

1. The cyclotomic $\mathbb{Z}_p$-extension always exists: $K_\infty^{\text{cyc}} = K\mathbb{Q}_\infty$.

Question: how many linearly independent $\mathbb{Z}_p$-extensions can we get from K?

1. The cyclotomic $\mathbb{Z}_p$-extension always exists: $K_\infty^{\text{cyc}} = K\mathbb{Q}_\infty$.
2. Using class field theory, we can show that the number of linearly independent $\mathbb{Z}_p$-extensions of K is a finite number d, which is **at least** $r_2 + 1$, where r_2 is the number of complex embeddings $K \hookrightarrow \mathbb{C} - \mathbb{R}$.

Question: how many linearly independent $\mathbb{Z}_p$-extensions can we get from K?

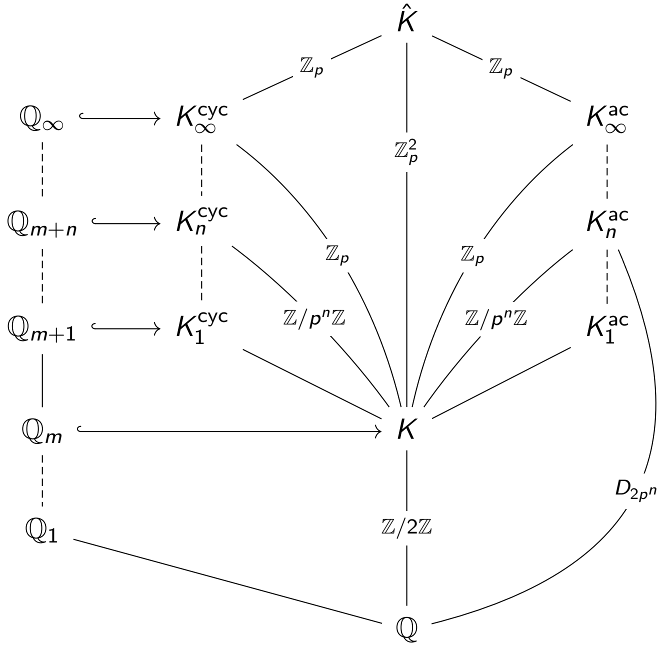
1. The cyclotomic $\mathbb{Z}_p$-extension always exists: $K_\infty^{\text{cyc}} = K\mathbb{Q}_\infty$.
2. Using class field theory, we can show that the number of linearly independent $\mathbb{Z}_p$-extensions of K is a finite number d, which is **at least** $r_2 + 1$, where r_2 is the number of complex embeddings $K \hookrightarrow \mathbb{C} - \mathbb{R}$.

Leopoldt's conjecture

With the same notation as above, $d = r_2 + 1$.

Proven for abelian extensions $K/\mathbb{Q}$ by Brumer in 1976.

Example: K imaginary quadratic field.



Fix a $\mathbb{Z}_p$-extension K_∞ of K. Let A_n denote the p-Sylow subgroup of the ideal class group of K_n.

Fix a $\mathbb{Z}_p$-extension K_∞ of K. Let A_n denote the p-Sylow subgroup of the ideal class group of K_n.

Theorem. Iwasawa, 1959

There are non-negative $\lambda, \mu, \nu \in \mathbb{Z}$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

for sufficiently large n.

Fix a $\mathbb{Z}_p$-extension K_∞ of K. Let A_n denote the p-Sylow subgroup of the ideal class group of K_n.

Theorem. Iwasawa, 1959

There are non-negative $\lambda, \mu, \nu \in \mathbb{Z}$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

for sufficiently large n.

Conjecture: if K_∞ is the cyclotomic $\mathbb{Z}_p$-extension, $\mu = 0$.
Proven for abelian extensions $K/\mathbb{Q}$ by a theorem of Ferrero and Washington.

Fix a $\mathbb{Z}_p$-extension K_∞ of K. Let A_n denote the p-Sylow subgroup of the ideal class group of K_n.

Theorem. Iwasawa, 1959

There are non-negative $\lambda, \mu, \nu \in \mathbb{Z}$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

for sufficiently large n.

Conjecture: if K_∞ is the cyclotomic $\mathbb{Z}_p$-extension, $\mu = 0$. Proven for abelian extensions $K/\mathbb{Q}$ by a theorem of Ferrero and Washington.

- $A_\infty = \varprojlim_n A_n$ is p-group, so it is a $\mathbb{Z}_p$-module.

Fix a $\mathbb{Z}_p$-extension K_∞ of K. Let A_n denote the p-Sylow subgroup of the ideal class group of K_n.

Theorem. Iwasawa, 1959

There are non-negative $\lambda, \mu, \nu \in \mathbb{Z}$ such that

$$|A_n| = p^{\lambda n + \mu p^n + \nu}$$

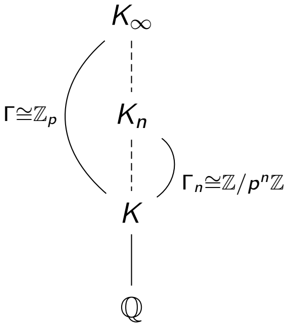
for sufficiently large n.

Conjecture: if K_∞ is the cyclotomic $\mathbb{Z}_p$-extension, $\mu = 0$. Proven for abelian extensions $K/\mathbb{Q}$ by a theorem of Ferrero and Washington.

- $A_\infty = \varprojlim_n A_n$ is p-group, so it is a $\mathbb{Z}_p$-module.
- Stronger: it is a module over the Iwasawa algebra Λ.

Iwasawa algebra

Notation: $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, $\Gamma_n = \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

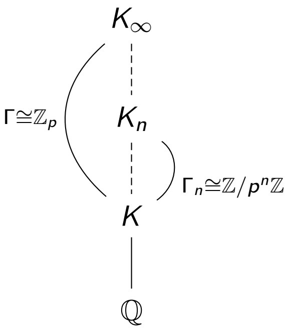


Iwasawa algebra

Notation: $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, $\Gamma_n = \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

- Define the **Iwasawa algebra**

$$\Lambda := \varprojlim_n \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[\![\Gamma]\!].$$



Iwasawa algebra

Notation: $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, $\Gamma_n = \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

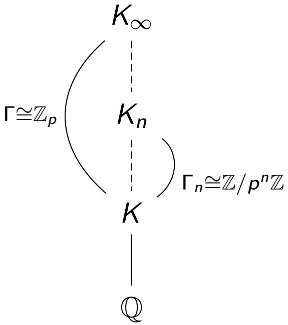
- Define the **Iwasawa algebra**

$$\Lambda := \varprojlim_{n} \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[\![\Gamma]\!].$$

- There is an isomorphism

$$\begin{aligned} \Lambda &\to \ \mathbb{Z}_p[\![T]\!] \\ \gamma &\mapsto 1 + T \end{aligned}$$

where γ is a topological generator of Γ.



Iwasawa algebra

Notation: $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, $\Gamma_n = \mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$.

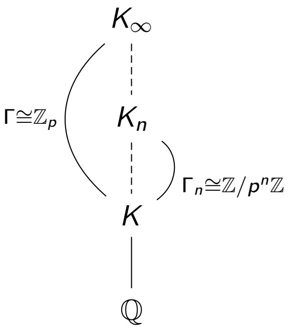
- Define the **Iwasawa algebra**

$$\Lambda := \varprojlim_n \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[\![\Gamma]\!].$$

- There is an isomorphism

$$\begin{aligned} \Lambda \to \ & \mathbb{Z}_p[\![T]\!] \\ \gamma \mapsto & \ 1 + T \end{aligned}$$

where γ is a topological generator of Γ.



A monic polynomial $f(T) \in \mathbb{Z}_p[T]$ is called *distinguished* if all its coefficients (except the leading) are divisible by p.

Structure theorem for f.g. Λ-modules. Iwasawa, Serre.

Let M be a finitely generated Λ-module. Then

$$M \sim \Lambda^{rank} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

where f_i are distinguished irreducible polynomials.

Structure theorem for f.g. Λ-modules. Iwasawa, Serre.

Let M be a finitely generated Λ-module. Then

$$M \sim \Lambda^{rank} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

where f_i are distinguished irreducible polynomials.

$$\lambda(M) = \sum_{i=1}^{r} k_i \deg f_i, \quad \mu(M) = \sum_{j=1}^{s} m_j.$$

Structure theorem for f.g. Λ-modules. Iwasawa, Serre.

Let M be a finitely generated Λ-module. Then

$$M \sim \Lambda^{rank} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

where f_i are distinguished irreducible polynomials.

$$\lambda(M) = \sum_{i=1}^{r} k_i \deg f_i, \quad \mu(M) = \sum_{j=1}^{s} m_j.$$

Fact: A_∞ becomes a finitely-generated *torsion* Λ-module.

Structure theorem for f.g. Λ-modules. Iwasawa, Serre.

Let M be a finitely generated Λ-module. Then

$$M \sim \Lambda^{rank} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

where f_i are distinguished irreducible polynomials.

$$\lambda(M) = \sum_{i=1}^{r} k_i \deg f_i, \quad \mu(M) = \sum_{j=1}^{s} m_j.$$

Fact: A_∞ becomes a finitely-generated *torsion* Λ-module.

Iwasawa's Main Conjecture. Theorem by Mazur-Wiles.

$$\mathrm{char}(A_\infty) = (L_p).$$

arithmetic objects $\leftrightsquigarrow$ L-functions

Elliptic curves

- An **elliptic curve** $E/\mathbb{Q}$ is a smooth, projective curve of genus 1 with a marked point.

$$E : y^2 = x^3 + Ax + B.$$

Elliptic curves

- An **elliptic curve** $E/\mathbb{Q}$ is a smooth, projective curve of genus 1 with a marked point.

$$E : y^2 = x^3 + Ax + B.$$

- **Mordell-Weil theorem**: $E(\mathbb{Q})$ is a *finitely generated* abelian group,

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}} \oplus \mathbb{Z}^{R_E}.$$

Elliptic curves

- An **elliptic curve** $E/\mathbb{Q}$ is a smooth, projective curve of genus 1 with a marked point.

$$E : y^2 = x^3 + Ax + B.$$

- **Mordell-Weil theorem**: $E(\mathbb{Q})$ is a *finitely generated* abelian group,

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_E}.$$

- **Problem**: the local-to-global principle does not hold in general.

Elliptic curves

- An **elliptic curve** $E/\mathbb{Q}$ is a smooth, projective curve of genus 1 with a marked point.

$$E : y^2 = x^3 + Ax + B.$$

- **Mordell-Weil theorem**: $E(\mathbb{Q})$ is a *finitely generated* abelian group,

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_E}.$$

- **Problem**: the local-to-global principle does not hold in general.
- A theorem of Mazur classifies the possibilities for $E(\mathbb{Q})_{\text{tors}}$.

Elliptic curves

- An **elliptic curve** $E/\mathbb{Q}$ is a smooth, projective curve of genus 1 with a marked point.

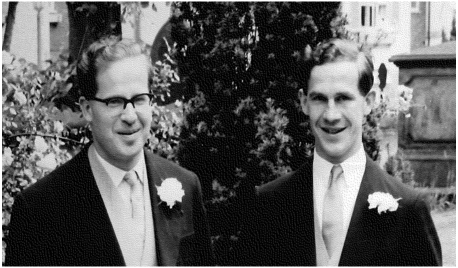
$$E : y^2 = x^3 + Ax + B.$$

- **Mordell-Weil theorem**: $E(\mathbb{Q})$ is a *finitely generated* abelian group,

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^{R_E}.$$

- **Problem**: the local-to-global principle does not hold in general.
- A theorem of Mazur classifies the possibilities for $E(\mathbb{Q})_{\text{tors}}$.
- **Open question**: possibilities for $\text{rank}(E(\mathbb{Q}))$?

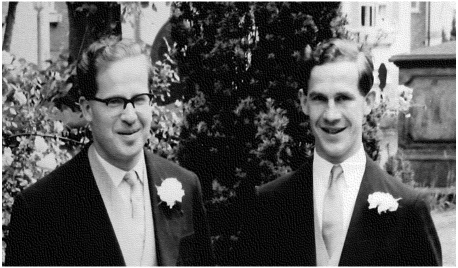
A Millennium Prize Problem...



Birch and Swinnerton-Dyer conjecture

Let $E/\mathbb{Q}$ be an elliptic curve and $L(E,s)$ be its L-function.

A Millennium Prize Problem...

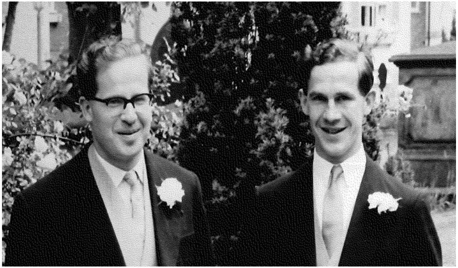


Birch and Swinnerton-Dyer conjecture

Let $E/\mathbb{Q}$ be an elliptic curve and $L(E,s)$ be its L-function.

- *Rank conjecture:* $\mathrm{rank}(E(\mathbb{Q})) = \mathrm{ord}_{s=1} L(E,s)$.

A Millennium Prize Problem...



Birch and Swinnerton-Dyer conjecture

Let $E/\mathbb{Q}$ be an elliptic curve and $L(E,s)$ be its L-function.

- *Rank conjecture:* $\operatorname{rank}(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E,s)$.
- *Residue of $L(E,s)$ at $s=1$:*

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^{R_E}} = \frac{|Ш_E| \cdot \Omega_E \cdot \operatorname{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E_{\text{tors}}(\mathbb{Q})|^2}.$$

Selmer groups

Setting: E/K elliptic curve with good ordinary reduction at all primes above p, where $K_\infty = \bigcup_n K_n$ is the *cyclotomic* $\mathbb{Z}_p$-extension of K. Assume that the Tate-Shafarevich group $\text{Ш}_E(K)$ is finite.

Selmer groups

Setting: E/K elliptic curve with good ordinary reduction at all primes above p, where $K_\infty = \bigcup_n K_n$ is the *cyclotomic* $\mathbb{Z}_p$-extension of K. Assume that the Tate-Shafarevich group $\text{Ш}_E(K)$ is finite.

- Global:

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathrm{Sel}_E(K) \twoheadrightarrow \text{Ш}_E(K) \to 0$$

Selmer groups

Setting: E/K elliptic curve with good ordinary reduction at all primes above p, where $K_\infty = \bigcup_n K_n$ is the *cyclotomic* $\mathbb{Z}_p$-extension of K. Assume that the Tate-Shafarevich group $Ш_E(K)$ is finite.

- Global:

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathrm{Sel}_E(K) \twoheadrightarrow Ш_E(K) \to 0$$

- Local:

$$0 \to E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathrm{Sel}_E(K_n)_p \twoheadrightarrow Ш_E(K_n)_p \to 0$$

Selmer groups

Setting: E/K elliptic curve with good ordinary reduction at all primes above p, where $K_\infty = \bigcup_n K_n$ is the *cyclotomic* $\mathbb{Z}_p$-extension of K. Assume that the Tate-Shafarevich group $Ш_E(K)$ is finite.

- Global:

$$0 \to E(K) \otimes \mathbb{Q}/\mathbb{Z} \hookrightarrow \mathrm{Sel}_E(K) \twoheadrightarrow Ш_E(K) \to 0$$

- Local:

$$0 \to E(K_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathrm{Sel}_E(K_n)_p \twoheadrightarrow Ш_E(K_n)_p \to 0$$

Idea: study the growth of $\mathrm{Sel}_E(K_n)_p$ over K_∞.

Consider $\mathrm{Sel}_E(K_\infty)_p := \varinjlim \mathrm{Sel}_E(K_n)_p$.

Consider $\mathrm{Sel}_E(K_\infty)_p := \varinjlim \mathrm{Sel}_E(K_n)_p$.

Mazur's Control theorem

The natural maps

$$\mathrm{Sel}_E(K_n)_p \to \mathrm{Sel}_E(K_\infty)_p^{\mathrm{Gal}(K_\infty/K_n)}$$

have finite kernel and cokernel, of bounded order as $n \to \infty$.

Consider $\mathrm{Sel}_E(K_\infty)_p := \varinjlim \mathrm{Sel}_E(K_n)_p$.

Mazur's Control theorem

The natural maps

$$\mathrm{Sel}_E(K_n)_p \to \mathrm{Sel}_E(K_\infty)_p^{\mathrm{Gal}(K_\infty/K_n)}$$

have finite kernel and cokernel, of bounded order as $n \to \infty$.

Corollary: Assume that $E(K_n)$ is finite for all n. There are non-negative $\lambda, \mu, \nu \in \mathbb{Z}$ such that

$$|\mathrm{Sel}_E(K_n)_p| = |\text{Ш}_E(K_n)_p| = p^{\lambda n + \mu p^n + \nu},$$

for sufficiently large n.

Consider $\mathrm{Sel}_E(K_\infty)_p := \varinjlim \mathrm{Sel}_E(K_n)_p$.

Mazur's Control theorem

The natural maps

$$\mathrm{Sel}_E(K_n)_p \to \mathrm{Sel}_E(K_\infty)_p^{\mathrm{Gal}(K_\infty/K_n)}$$

have finite kernel and cokernel, of bounded order as $n \to \infty$.

Corollary: Assume that $E(K_n)$ is finite for all n. There are non-negative $\lambda, \mu, \nu \in \mathbb{Z}$ such that

$$|\mathrm{Sel}_E(K_n)_p| = |\text{Ш}_E(K_n)_p| = p^{\lambda n + \mu p^n + \nu},$$

for sufficiently large n.

Theorem. Kato, Rohrlich

Assume $K = \mathbb{Q}$. Then rank$(E(K_n))$ is bounded and independent of n.

- **Pontryagin dual** of $\mathrm{Sel}_E(K_\infty)_p$:

$$X_E(K_\infty) := \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

- **Pontryagin dual** of $\mathrm{Sel}_E(K_\infty)_p$:

$$X_E(K_\infty) := \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

- $X_E(K_\infty)$ becomes a finitely generated Λ-module, so we can apply the structure theorem!

$$X_E(K_\infty) \sim \Lambda^{\mathrm{rank}} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

- **Pontryagin dual** of $\mathrm{Sel}_E(K_\infty)_p$:

$$X_E(K_\infty) := \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

- $X_E(K_\infty)$ becomes a finitely generated Λ-module, so we can apply the structure theorem!

$$X_E(K_\infty) \sim \Lambda^{\mathrm{rank}} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

- **Conjecture**: $X_E(K_\infty)$ is *torsion*.

- **Pontryagin dual** of $\mathrm{Sel}_E(K_\infty)_p$:

$$X_E(K_\infty) := \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

- $X_E(K_\infty)$ becomes a finitely generated Λ-module, so we can apply the structure theorem!

$$X_E(K_\infty) \sim \Lambda^{\mathrm{rank}} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

- **Conjecture**: $X_E(K_\infty)$ is *torsion*.
- Mazur and Swinnerton-Dyer constructed a p-**adic analogue** $L_p(E,s)$ of $L(E,s)$ using interpolation.

- **Pontryagin dual** of $\mathrm{Sel}_E(K_\infty)_p$:

$$X_E(K_\infty) := \mathrm{Hom}(\mathrm{Sel}_E(K_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p).$$

- $X_E(K_\infty)$ becomes a finitely generated Λ-module, so we can apply the structure theorem!

$$X_E(K_\infty) \sim \Lambda^{\mathrm{rank}} \oplus \bigoplus_{i=1}^{r} \Lambda/(f_i^{k_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{m_j})$$

- **Conjecture**: $X_E(K_\infty)$ is *torsion*.

- Mazur and Swinnerton-Dyer constructed a p-**adic analogue** $L_p(E,s)$ of $L(E,s)$ using interpolation.

Main Conjecture for Elliptic Curves

$$\mathrm{char}(X_E(K_\infty)) = (L_p(E,s)).$$

References

- Ralph Greenberg's Research Page about Iwasawa theory
- *Desde Fermat, Lamé y Kummer hasta Iwasawa: Una introducción a la teoría de Iwasawa* - Álvaro Lozano-Robledo
- *Structure of Mordell-Weil groups over $\mathbb{Z}_p$-extensions* - Jaehoon Lee
- *Cyclotomic Fields and Zeta Values* - John Coates and Sujatha Ramdorai
- *Introduction to Cyclotomic Fields* - Lawrence C. Washington
- Trilogy *Number Theory* by Kazuya Kato, Nobushige Kurokawa, Takeshi Saito and Masato Kurihara

Thank you!!