



# Cyclotomic Extensions and Iwasawa Theory

Institute of Mathematics, Eötvös  
Loránd Tudományegyetem

Ritoprovo Roy

May 30, 2024





## Cyclotomic Fields

- Let  $p$  be an odd prime. Let  $\mu_p$  denote the group of  $p$ -th roots of unity.



## Cyclotomic Fields

- Let  $p$  be an odd prime. Let  $\mu_p$  denote the group of  $p$ -th roots of unity.
- Let  $\mu_p$  denote the group of  $p$ -th roots of unity and we put

$$\mathcal{F} = \mathbb{Q}(\mu_p), \quad \bar{\omega} = \text{Gal}(\mathcal{F}/\mathbb{Q})$$



## Cyclotomic Fields

- Let  $p$  be an odd prime. Let  $\mu_p$  denote the group of  $p$ -th roots of unity.
- Let  $\mu_p$  denote the group of  $p$ -th roots of unity and we put

$$\mathcal{F} = \mathbb{Q}(\mu_p), \quad \bar{\omega} = \text{Gal}(\mathcal{F}/\mathbb{Q})$$

- We observe that  $\bar{\omega}$  acts on  $\mu_p$ , and thus gives an injective homomorphism (embedding)

$$\theta : \bar{\omega} \rightarrow \text{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^\times$$



## Cyclotomic Fields (Continued)

### Bernoulli Numbers

The  $n^{\text{th}}$  Bernoulli number is defined as  $B_n$  are defined as

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$



## Cyclotomic Fields (Continued)

### Bernoulli Numbers

The  $n^{\text{th}}$  Bernoulli number is defined as  $B_n$  are defined as

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

### Irregular Primes

A prime number  $p$  is irregular if  $p$  divides the order of the ideal class group of  $\mathcal{F}$ .



## Cyclotomic Fields (Continued)

### Bernoulli Numbers

The  $n^{\text{th}}$  Bernoulli number is defined as  $B_n$  are defined as

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

### Irregular Primes

A prime number  $p$  is irregular if  $p$  divides the order of the ideal class group of  $\mathcal{F}$ .

- We denote  $\mathcal{C}$  as the ideal class group of  $\mathcal{F}$ . The order of  $\mathcal{C}$  is called the class number. We should note that class numbers are computationally difficult to find out for larger primes.



## An Important Criterion

### Kummer's Criterion

The prime  $p$  is irregular if and only if  $p$  divides the numerator of at least one of  $\zeta(i)$  where  $i = -1, -2, -3, \dots, (4 - p)$



## An Important Criterion

### Kummer's Criterion

The prime  $p$  is irregular if and only if  $p$  divides the numerator of at least one of  $\zeta(i)$  where  $i = -1, -2, -3, \dots, (4 - p)$

### Kummer's Congruences

Let  $n$  and  $m$  be odd positive integers such that

$$n \equiv m \equiv (-1) \pmod{p-1}$$

then the rational numbers  $\zeta(-n)$  and  $\zeta(-m)$  are  $p$ -integral and

$$\zeta(-n) \equiv \zeta(-m) \pmod{p}$$



## Iwasawa's Main Conjecture

*Herbrand Ribet's Theorem, The Cyclotomic Tower, Main Conjecture and related stuff*





## Herbrand Ribet's Theorem

- We consider  $\mathfrak{B} = \mathcal{C}/\mathcal{C}^p$ , which is finite dimensional vector space over  $\mathbb{F}_p$ , on which the Galois group  $\bar{\omega}$  acts naturally.



## Herbrand Ribet's Theorem

- We consider  $\mathfrak{B} = \mathcal{C}/\mathcal{C}^p$ , which is finite dimensional vector space over  $\mathbb{F}_p$ , on which the Galois group  $\bar{\omega}$  acts naturally.
- We observe that the action is semi-simple since the order of  $\bar{\omega}$  is prime to  $p$ .



## Herbrand Ribet's Theorem

- We consider  $\mathfrak{B} = \mathfrak{C}/\mathfrak{C}^p$ , which is finite dimensional vector space over  $\mathbb{F}_p$ , on which the Galois group  $\bar{\omega}$  acts naturally.
- We observe that the action is semi-simple since the order of  $\bar{\omega}$  is prime to  $p$ .

### Question

Which of the characters  $\theta^n$ , where  $n = 1, 2, 3, \dots, p - 1$ , occur in  $\mathfrak{B}$ , and what is their multiplicity of occurrence ?

### Herbrand-Ribet's Theorem

Assume that  $n$  is an odd integer with  $3 \leq n \leq p - 2$ . Then  $\theta^n$  occurs in  $\mathfrak{B} = \mathfrak{C}/\mathfrak{C}^p$  if and only if  $p$  divides the numerator of  $\zeta(n + 1 - p)$



## Varandiver's Conjecture

- The above theorem however partially answers our questions without multiplicities.



## Varandiver's Conjecture

- The above theorem however partially answers our questions without multiplicities.
- The problem of multiplicities is however still unsolved.



## Varandiver's Conjecture

- The above theorem however partially answers our questions without multiplicities.
- The problem of multiplicities is however still unsolved.

### Varandiver's Conjecture

A prime  $p$  does not divide the class number  $h(R)$  of the maximal real subfield  $R$  of the  $p$ -th cyclotomic field.

- We shall see result that Main Conjecture would have been an easy conjecture of Iwasawa if the Varandiver's conjecture is assumed to be true.
- Numerical evidences can be found at [1].



## Iwasawa Algebras

- The theory of commutative Iwasawa algebras were first introduced by the Japanese mathematician Kenkichi Iwasawa.
- Let  $\Gamma = \mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ , where the inverse limit is taken on  $n$ , where  $\Gamma$  is compact and pro-cyclic as a profinite group.
- Let  $\gamma$  be a topological generator of  $\Gamma$  and hence  $\Gamma = \langle \bar{\gamma} \rangle$ .
- Let  $\Gamma_n$  be generated by  $\gamma^{p^n}$ , and this be the unique closed group of index  $p^n$  of  $\Gamma$ , then  $\Gamma/\Gamma_n$  is cyclic of order  $p^n$  generated by  $r + \Gamma_n$ .



## Iwasawa Algebras - The Setup

- One has isomorphism

$$\begin{aligned} O_K[\Gamma/\Gamma_n] &\cong O_K[\Gamma]/((1+T)^{p^n} - 1) \\ \gamma \bmod \Gamma_n &\rightarrow (1+T) \bmod ((1+T)^{p^n} - 1) \end{aligned}$$

- Moreover, if  $m \geq n \geq 0$ , the natural map of  $\Gamma/\Gamma_m \rightarrow \Gamma/\Gamma_n$  induces a natural map,

$$\phi_{m,n} : O_K[\Gamma/\Gamma_m] \rightarrow O_K[\Gamma/\Gamma_n]$$

- We let

$$O_K[[\Gamma]] = \varprojlim O_K[\Gamma/\Gamma_n] = \varprojlim O_K[\Gamma]/((1+T)^{p^n} - 1)$$

where the limits are taken on  $n$ .



## Iwasawa Algebras - The Setup

- We finally note that  $O_K$  is a topological ring which is compact and complete with the  $\pi$ -adic topology, so are  $O_K[\Gamma/\Gamma_n]$  and thus  $O_K[[\Gamma]]$  is the endowed with the product topology of  $\pi$ -adic topology. It is also compact and complete in this topology.
- We are now in a position to define what Iwasawa Algebras are,

### Iwasawa Algebras

$$\Lambda = \Lambda(\Gamma) = O_K[[\Gamma]]$$

is called the Iwasawa Algebra over  $\Gamma$ .



# Iwasawa Algebra

- An important thing to note is that,

## Iwasawa Algebra on Profinite Group

Let  $G$  be a profinite abelian group, then Iwasawa algebra over  $G$  is given by,

$$\Gamma(G) = \varprojlim O_K[G/H]$$

when limit is taken over all  $H \triangleleft G$ .

- In fact we are able to identify the rings  $O_K[[\Gamma]]$  and  $O_K[[T]]$ .

$$\begin{aligned} O_K[[T]] &\cong O_K[[\Gamma]] \\ T &\rightarrow \gamma - 1 \end{aligned}$$



## The Main Conjecture of Iwasawa

- We consider larger abelian extensions of  $\mathcal{F}_\infty$  and  $F_\infty$ .



## The Main Conjecture of Iwasawa

- We consider larger abelian extensions of  $\mathcal{F}_\infty$  and  $F_\infty$ .
- We let  $\mathcal{M}_\infty$  be the maximal abelian  $p$ -extension of  $\mathcal{F}_\infty$  which is unramified outside the unique prime above  $p$  in  $\mathcal{F}_\infty$ .



## The Main Conjecture of Iwasawa

- We consider larger abelian extensions of  $\mathcal{F}_\infty$  and  $F_\infty$ .
- We let  $\mathcal{M}_\infty$  be the maximal abelian  $p$ -extension of  $\mathcal{F}_\infty$  which is unramified outside the unique prime above  $p$  in  $\mathcal{F}_\infty$ .

- We consider

$$\mathcal{X}_\infty = \text{Gal}(\mathcal{M}_\infty/\mathcal{F}_\infty)$$

- $\mathcal{X}_\infty$  via inner automorphisms, making it a module over Iwasawa Algebra.



# The Main Conjecture of Iwasawa

## Theorem

The module  $X_\infty$  is a finitely generated torsion  $\Lambda(G)$ -module.

- Before going to the main conjecture directly we state the following theorems

## Ferro-Washington's Theorem

Iwasawa's  $\mu$ -invariant vanishes for cyclotomic  $\mathbb{Z}_p$  extensions for abelian algebraic number fields.

- This implies that  $X_\infty$  is a finitely generated  $\mathbb{Z}_p$ -module.



## The Main Conjecture of Iwasawa (Contd.)

### Iwasawa's Theorem

$X_\infty$  has no non-zero finite  $\Lambda(\Gamma_0)$ -submodule, where  $\Gamma_0 = \text{Gal}(F_\infty/F_0)$

- $X_\infty$  has no non-zero  $\mathbb{Z}_p$ -torsion.
- Together they imply that  $X_\infty$  is a free finitely generated  $\mathbb{Z}_p$ -module, on which the group  $G$ , which topologically generated by one element acting continuously.
- There is an intimate connection between generator of the group  $ch_G(X_\infty)$



## The Main Conjecture of Iwasawa

### Relating $p$ -adic measures to Iwasawa Algebras

There exists a unique pseudo-measure  $\zeta_p$  on  $G$  such that

$$\int_G \chi(g)^k d\zeta_p = (1 - p^{k-1})\zeta(1 - k)$$

for all even integers  $k \geq 2$ .



## The Main Conjecture of Iwasawa

### Relating $p$ -adic measures to Iwasawa Algebras

There exists a unique pseudo-measure  $\zeta_p$  on  $G$  such that

$$\int_G \chi(g)^k d\zeta_p = (1 - p^{k-1})\zeta(1 - k)$$

for all even integers  $k \geq 2$ .



## The Main Conjecture of Iwasawa

- We let  $I(G)$  denote the kernel of the augmentation map (homomorphism) from  $\Lambda(G)$  to  $\mathbb{Z}_p$ . As  $\zeta_p$  is a pseudo-measure,  $I(G)\zeta_p$  is an ideal of  $\Lambda(G)$ .



## The Main Conjecture of Iwasawa

- We let  $I(G)$  denote the kernel of the augmentation map (homomorphism) from  $\Lambda(G)$  to  $\mathbb{Z}_p$ . As  $\zeta_p$  is a pseudo-measure,  $I(G)\zeta_p$  is an ideal of  $\Lambda(G)$ .

### Iwasawa Main Conjecture

We have

$$ch_G(X_\infty) = I(G)\zeta_p$$



## The Main Conjecture of Iwasawa

- We let  $I(G)$  denote the kernel of the augmentation map (homomorphism) from  $\Lambda(G)$  to  $\mathbb{Z}_p$ . As  $\zeta_p$  is a pseudo-measure,  $I(G)\zeta_p$  is an ideal of  $\Lambda(G)$ .

### Iwasawa Main Conjecture

We have

$$ch_G(X_\infty) = I(G)\zeta_p$$

- The first complete proof was given by Mazur and Wiles.



# Iwasawa's Theorem

*Iwasawa's Theorem and its  
proof overview*





## Iwasawa's Theorem

- For each  $n \geq 0$ , consider now the local field

$$K_n = \mathbb{Q}_p(\mu_{p^{n+1}})^+$$

- We denote  $U_n^1$  for the group of units of  $K_n$ , which are  $\equiv 1 \pmod{\mathfrak{p}_n}$ , where  $\mathfrak{p}_n$  is the maximal ideal of the ring of integers of  $K_n$ . Also we let  $D_n$  be the group of cyclotomic units of  $F_n$ .
- We see that  $D_n$  is generated by all Galois conjugates of

$$\pm \frac{\zeta_n^{-e/2} - \zeta_n^{e/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}}$$

$e$  is primitive root modulo  $p$  such that  $e^{p-1} \not\equiv (1 \pmod{p^2})$



## Iwasawa's Theorem

- We define  $D_n^1$  to be the subgroup of all elements of  $D_n$  which are  $\equiv 1 \pmod{\mathfrak{p}_n}$ . And we let  $C_n^1$  to be the closure of  $D_n^1$  in  $U_n^1$  with respect to  $\mathfrak{p}_n$ -adic topology.

- We define

$$U_\infty^1 = \varprojlim U_n^1, \quad C_\infty^1 = \varprojlim C_n^1$$

where limits are taken with respect to norm maps.

- We now state Iwasawa's Theorem.



# Iwasawa's Theorem

## Iwasawa's Theorem

The  $\Lambda(G)$ -module  $U_\infty^1/C_\infty^1$  is canonically isomorphic to  $\Lambda(G)/I(G) \cdot \zeta_p$ , where  $\zeta_p$  is the  $p$ -adic zeta function, and  $I(G)$  the canonical ideal.

We give a brief elementary proof of the theorem without local class field theory due to Wiles and Coates. We state some results without proofs



## Proof of Iwasawa's Theorem

### Brief Overview of the Proof

- We have an exact sequences of  $\mathcal{G}$ -modules

$$0 \rightarrow \mu_{p-1} \times T_p(\mu) \rightarrow \mathcal{U}_\infty \rightarrow \Lambda(\mathcal{G}) \rightarrow T_p(\mu) \rightarrow 0$$

where the kernel of the left is the natural inclusion, and the map  $\beta$  on the right is given by  $\beta(\lambda) = (\zeta_n)^{\int_G \chi^{d\lambda}}$

- Since the norm map from  $K_n$  to  $K_{n-1}$  induces the identity map on the residue fields, we must have

$$\mathcal{U}_\infty = \mu_{p-1} \times \mathcal{U}_\infty^1$$



## Proof of Iwasawa's Theorem

### Brief Overview of the Proof

- and hence the previous line maybe rewritten as

$$0 \rightarrow T_p(\mu) \rightarrow \mathcal{U}_\infty^1 \rightarrow \Lambda(\mathcal{G}) \rightarrow T_p(\mu) \rightarrow 0$$

As our prime is odd our sequence remains exact after taking invariants under  $J = \{1, \iota\}$ .

- Since we have  $T_p(\mu)^J = 0$ , there is a canonical  $\Lambda(G)$ -isomorphism

$$\mathcal{L}^\infty : U_\infty \cong \Lambda(G)$$



## Proof of Iwasawa's Theorem

### Brief Overview of the Proof

- We have  $C_\infty = \Lambda(G).\mathbf{b}$  where  $\mathbf{b} = (b_n) = (uc_n(e, 1))$  and  $u$  is the unique  $(p - 1)$ -th root of unity in  $\mathbb{Q}_p$  such that  $eu \equiv 1 \pmod{p}$  so that  $\mathcal{L}^1(C_\infty^1) = \Lambda(G)\mathcal{L}^1(\mathbf{b})$ .
- But we also know that  $\mathcal{L}^1(\mathbf{b}) = \zeta_p\theta^+(e, 1)$  where  $\theta^+(e, 1)$  is the image of  $\theta(e, 1)$  in  $\Lambda(G)$ . However we also have  $\Lambda(G)\theta^+(e, 1) = I(G)$  and we finish the proof.



**THANK YOU**

*I thank everyone for their valuable attention!*

