Introduction to Iwasawa Theory

Anlun Li

USTC

February 23,2022

Plan

- Motivations and Backgrounds
- Basic Notations and Facts
- Iwasawa Main conjecture
- An easy application

Let $K/\mathbb{Q}$ be a finite extension. Then we may consider the distance between O_K and PID. We define $Cl(K)$ to be its ideal class group to measure its difference.

Definition

$Cl(K) =$
$\{\text{Invertible fractional ideal}\}/\{\text{ Principal fractional ideal}\}$
$h_K = \#Cl(K)$

There is a theorem showing that h_K is finite in general. We omit the proof.

Kummer's two propositions

In fact, Kummer has developed serveral propositions that makes h_K be powerful.

Proposition (Relating to Fermat's Last Theorem)

If $p \nmid h_{\mathbb{Q}(\mu_p)}$, then $x^p + y^p = z^n$ has no solutions in $\mathbb{Z}^3$.

Proposition

$p \mid h_{\mathbb{Q}(\mu_p)} \iff \exists$ *positive even integer r, such that $p \mid \zeta(1-r)$*

We will briefly prove the latter proposition at the end of this talk.

Notations

Henceforth, we assume p is an odd prime. And

$$K := \mathbb{Q}(\mu_p), K_n := \mathbb{Q}(\mu_{p^n}), K_\infty := \mathbb{Q}(\mu_{p^\infty}) = \bigcup_n \mathbb{Q}(\mu_{p^n}).$$

As we mentioned above, it's improtant to discuss the p part of $Cl(K)$. In general, we should focus on the p-sylow subgroup of $Cl(K_n)$.

Let $Cl(K_n) = A_{K_n} \oplus A'_{K_n}$, where A_{K_n} is its p-sylow subgroup.

Maps between $Cl(K_n)$ and $Cl(K_m)$

Suppose n>m, then for $x \in \mathbb{Q}(\mu_{p^n})$, we know

$$N(x) = \prod_{\sigma \in Gal(K_n/K_m)} \sigma x \in K_m.$$

Therefore, we have

$$N: \ Cl(K_n) \to Cl(K_m)$$

$$[I] \mapsto [N(I)].$$

Similarily, we can restrict N to A_{K_n}. And these maps define an inverse limit.
Let $X = \lim_{\leftarrow} A_{K_n}$. Next we will talk about its structure.

X,A_{K_n} are $\mathbb{Z}_p[[G]]$ modules

Let G =Gal(K_∞/Q). Since for any $\sigma \in G$, $\sigma\mu_{p^n} = \mu_{p^n}^{s_n}$, where $s_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. And for n>m, s_m is defined by s_n. Therefore,

$$\begin{aligned} G \cong & \lim_{\leftarrow} \mathrm{Gal}(K_n/\mathbb{Q}) \cong \lim_{\leftarrow}(\mathbb{Z}/p^n\mathbb{Z})^\times \\ \cong & (\mathbb{Z}/p\mathbb{Z})^\times \times \lim_{\leftarrow}(\mathbb{Z}/p^{n-1}\mathbb{Z}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p. \end{aligned}$$

We write $G = \Delta \times \Gamma$, where $\Gamma \cong \mathbb{Z}_p$, the p adic integer.

Since A_{K_n} is finite p group, it is $\mathbb{Z}_p$ module. And for $\sigma \in G$, it can act on $Cl(K_n)$ by $\sigma([I]) = [\sigma(I)]$, so does A_{K_n}.

In Conclusion, X and A_{K_n} are $\mathbb{Z}_p[[G]]$ modules.

A lemma for Decomposition

Here is a lemma to help us decomposite X and A_{K_n}.

Lemma

If R is a commutative ring containing $< \mu_n >$, Δ *is an abelian group, with order=n. Let* $\widehat{\Delta}$ *=Hom(*Δ*,R), then set*

$$e_\chi = \frac{1}{n} \sum_{\sigma \in \Delta} \chi(\sigma)\sigma^{-1}.$$

It's obvious to calcuate that

$$\sum_{\chi \in \widehat{\Delta}} e_\chi = 1, \;\; e_\chi e'_\chi = 0, \;\; e_\chi e_\chi = e_\chi.$$

Therefore, for $R[\Delta]$ *mod M, we have the decomposition:*

$$M = \oplus_{\chi \in \widehat{\Delta}} e_\chi M.$$

Decomposition for X and A_{K_n}

Since G, A_{K_n} are $\mathbb{Z}_p[[G]] = \mathbb{Z}_p[\Delta][[\Gamma]]$ mod, they are $\mathbb{Z}_p[\Delta]$ mod. Notice that $\widehat{\Delta} = \{\omega^i\}_{0 \leq i \leq p-2}$, Hence,

$$X = \oplus_{0 \leq i \leq p-2} X^{\omega^i}, A_{K_n} = \oplus_{0 \leq i \leq p-2} A_{K_n}^{\omega^i}.$$

We can prove that $X^{\omega^i}, A_{K_n}^{\omega^i}$ are indeed $\Lambda = \mathbb{Z}_p[[\Gamma]]$ mod.

$\Lambda \cong \mathbb{Z}_p[[T]]$

It is sufficient to prove that

$$\mathbb{Z}_p[\mathbb{Z}/p^n] \cong \mathbb{Z}_p[T]/((1+T)^{p^n} - 1)$$

and

$$\varprojlim \mathbb{Z}_p[T]/((1+T)^{p^n} - 1) \cong \mathbb{Z}_p[[T]].$$

For the former, only need to verify that the map $\bar{1} \to T+1$ is a bijective.
For the latter, we need to use the fact that $\mathbb{Z}_p$ is p-adic complete.

Pseudo-isomorphism and Char(X)

An important theorem tells us that X is a finitely generated tortion Λ mod. So

$$X \sim \Lambda/f_1^{n_1} \oplus \cdots \oplus \Lambda/f_r^{n_r}.$$

We say $M \sim N$, meaning that there exists Λ mod $\phi : M \to N$, such that $\ker(\phi)$, $coker(\phi)$ have finite length as $\mathbb{Z}_p$ mod.

Definition

$$Char(X) := \prod_{i=1}^{r} f_i^{n_i}$$

Note that this definition is independent of the choice of pseudo-isomorphism.

P-adic L function

Before we introduce p adic L function, I should mention a proposition proved by Kummer, which states there exists a form of ζ whcih has a good property in p adic number field.

Proposition (Kummer)

If n_1, n_2 are positive integers and $n_1 \equiv n_2 \neq 0 \pmod{\text{p-1}}$, then

$$(1-p^{n_1-1})\zeta(1-n_1) \equiv (1-p^{n_2-1})\zeta(1-n_2)\ (mod p).$$

More generally, if $p-1 \nmid n_1$ and $n_1 \equiv n_2\ (mod (p-1)p^{n-1})$, then

$$(1-p^{n_1-1})\zeta(1-n_1) \equiv (1-p^{n_2-1})\zeta(1-n_2)\ (mod p^n).$$

P-adic L function

We should define a function which has good property of continuous, or even holomorphic. Thanks to the proposition above, we can define p-adic L function as follows:

$$L_p(1-n,\chi) := (1-\chi\omega^{-n}(p))L(1-n,\chi\omega^{-n})$$

Using Euler-product we can show that the right hand side is well defined. Since $\mathbb{Z}_{\leq 0}$ is dense in $\mathbb{Z}_p$, if we assume L_p function is continuous, then we have defined a function in $\mathbb{Z}_p$.

Properties of P-adic L function

Here we list the properties of p adic L function.

- Continuous
- P adic holomorphic
- Iwasawa power series

We say a function is p adic holomorphic, means that

$$\forall \alpha \in \mathbb{Z}_p, \exists a_n \in \overline{\mathbb{Q}_p}, L_p(s, \chi) = \sum_{n=0}^{\infty} a_n (s-\alpha)^n, \forall s \in \mathbb{Z}_p$$

In the next page we will introduce Iwasawa power series.

Iwasawa power series

Let $\mathcal{O}_\chi := \mathbb{Z}_p[\mathrm{Im}\chi]$.

Theorem (Iwasawa Theorem)

- *$\exists G_\chi(T) \in Frac(\mathcal{O}_\chi[[T]])$, such that,*

$$G_\chi((1+p)^s - 1) = L_p(s, \chi).$$

- *If the conductor of $\chi \neq 1$ or $p^n \quad (n \geq 2)$, then G_χ defined above is in $\mathcal{O}_\chi[[T]]$.*

For example, $\chi = \omega^i$ satisfies the second condition.

Statement of Main Conjecture

Indeed, this main conjecture is a theorem now.

Theorem (Iwasawa Main Conjecture)

Let X, G_χ as defined above, then the following two ideals in $\mathbb{Z}_p[[T]] \cong \Lambda$ is equal:

$$(Char(X^{\omega^i})) = (G_{\chi^{1-i}}(T)).$$

This theorem connects an algebraic structure to an analytic object.

If we assume the following proposition is true, then we can prove Kummer's second proposition mentinoed in our motivation section.

Proposition (Duduced from Iwasawa Theory)

Suppose $1 < i < p-1$*, i is an odd integer. Then*

$$\#A^{\omega^i}_{\mathbb{Q}(\mu_p)} = \#\mathbb{Z}_p/L(0,\omega^{-i}) = \#\mathbb{Z}_p/L_p(0,\omega^{1-i}) = \#\mathbb{Z}_p/G_{\omega^{1-i}}(0).$$

Corollary (Kummer, Herbrand)

$$A^{\omega^i}_{\mathbb{Q}(\mu_p)} \neq \varnothing \iff \exists r > 0, 1-i \equiv r \ (mod\ p\text{-}1), p|\zeta(1-r).$$

If we assume the proposition above is true, we can prove the corollary, using basic properties of p-adic L function.

Proof of the Corollary

By the definition of $L_p(s,\chi)$, we can show that

$$\zeta(1-r) \equiv L_p(1-r,\omega^r)(\text{mod p}).$$

On the other hand, notice that $Im(\omega^i) \in \mathbb{Z}_p$, and

$$G_{\omega^r}(T) = \sum_{n=0}^{\infty} a_n T^n, \text{where } a_n \in \mathbb{Z}_p;$$

$$L_p(s,\omega^r) = G_{\omega^r}((1+p)^s - 1) = \sum_{n=0}^{\infty} a_n((1+p)^s - 1)^n.$$

Since

$$(1+p)^{1-r} - 1 = \sum_{n=0}^{\infty} p^n \binom{1-r}{n} - 1 \equiv 0(\text{mod p}),$$

therefore, $\zeta(1-r) \equiv L_p(1-r,\omega^r) \equiv a_0 \equiv L_p(0,\omega^r)$ (mod p). By using the proposition above, we are done.

- *Number Theory II Iwasawa Theory and Automorphic Form*
- Lawerence C. Washington, *Introduction to Cyclotomic Fields*