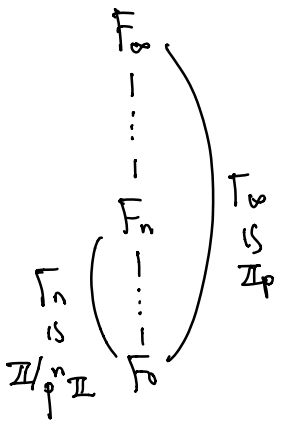
Introduction to Iwasawa theory

Liang Xiao

p prime. $F = F_0$ number field (e.g. $\mathbb{Q}$).

Consider a $\mathbb{Z}_p$-ext'n F_∞ of F_0



(Gal ext'n w/ Galois grp $\Gamma_\infty \simeq \mathbb{Z}_p$)

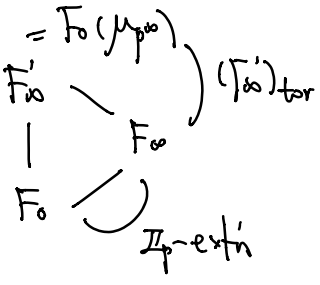
$\uparrow$ abstract isom

WLOG: Fix a top gen γ of Γ_∞

s.t. $\Gamma_\infty \xrightarrow{\sim} \mathbb{Z}_p$

$\gamma \longmapsto 1$.

<u>Typical example</u>



$\mu_{p^\infty} = \{$all (p-power)th roots of unity$\}$.

Γ'_∞

$=$

$\mathrm{Gal}(F'_\infty/F_0) \hookrightarrow \mathbb{Z}_p^\times$

$g \longmapsto (a$ s.t. $g(\zeta_{p^n}) = \zeta_{p^n}^a)$.

Call the F_∞ the p-adic cycl ext'n of F_0.

<u>Goal</u> Understand how the ideal class grp

$Cl_{F_n}\{p\}$ (p-sylow subgrp of Cl_{F_n})

grows as $n \to \infty$.

Theorem (Iwasawa) $\exists \lambda, \mu \in \mathbb{Z}_{\geq 0}$, $\nu \in \mathbb{Z}$ s.t.

for $n \gg 0$, $\quad h_{F_n}^{(p)} := \#\mathrm{Cl}_{F_n}\{p\} = p^{p^n\mu + n\lambda + \nu}$.

Conj (Iwasawa μ-invariant conj)

For cycl ext'n $F_\infty / F_n / F_0$, $\mu = 0$.

Rmk By Ferrero-Washington:

true if F is an ab ext'n of $\mathbb{Q}$.

Key idea of Iwasawa's thm

Consider $\Gamma_n \curvearrowright \mathrm{Cl}_{F_n}\{p\}$.

$\searrow \quad \circlearrowright$

$\mathbb{Z}_p[\Gamma_n]$

Take lim as $n \to \infty$:

$\varprojlim_n \mathbb{Z}_p[\Gamma_n] \curvearrowright \varprojlim_n \mathrm{Cl}_{F_n}\{p\} =: X_\infty$ — inverse lim w.r.t. $\mathrm{Cl}_{F_{n+n}} \xrightarrow{\text{norm}} \mathrm{Cl}_{F_n}$

w.r.t. $\Gamma_{n+1} \to \Gamma_n$ — compatible with $\circlearrowright \Gamma_{n+1} \to \Gamma_n \circlearrowright$

$\| \qquad \|$

$\mathbb{Z}/p^{n+1} \to \mathbb{Z}/p^n$ natural.

Recall $\Gamma_\infty \xrightarrow{\sim} \mathbb{Z}_p^\times$, $\quad \gamma \mapsto 1$

$\mathbb{Z}_p[\![\Gamma_\infty]\!] := \varprojlim_n \mathbb{Z}_p[\Gamma_n]$

$\|$

$\varprojlim_n \mathbb{Z}_p[\mathbb{Z}/p^n\mathbb{Z}]$

$\|$

$\varprojlim_n \mathbb{Z}_p[x]/(x^{p^n}-1)$

w.r.t. $\mathbb{Z}_p[x]/(x^{p^{n+1}}-1) \twoheadrightarrow \mathbb{Z}_p[x]/(x^{p^n}-1)$.

Take $x = T+1$

$$\rightsquigarrow \varprojlim_r \mathbb{Z}_p[x]/(x^{p^n}-1) = \varprojlim_n \mathbb{Z}_p[T]/\underbrace{((T+1)^{p^n}-1)}_{\| \; T^n + \cdots \in (p,T)^n}$$

$$= \varprojlim_n \varprojlim_m \mathbb{Z}_p[T]/(p^m, (1+T)^{p^n}-1)$$

$$\cong \mathbb{Z}_p[\![T]\!].$$

So $\mathbb{Z}_p[\![T]\!] \simeq \varprojlim_n \mathbb{Z}_p[\Gamma_n] \hookrightarrow X_\infty$.

$T = [\gamma]-1$ — called Iwasawa alg.

Rmk Can define Iwasawa alg for all pro-finite grps G.

$$\mathbb{Z}_p[\![G]\!] := \varprojlim_{\substack{H \lhd G \\ \text{open}}} \mathbb{Z}_p[G/H].$$

- If G is pro-p, $\mathbb{Z}_p[\![G]\!]$ is a (possibly non-comm) local ring.

Two main "lemmas" in Iwasawa theory

(1) Control theorem

X_∞ is a torsion fin gen $\mathbb{Z}_p[\![\Gamma_\infty]\!]$-mod.

& $\exists N_0$ s.t. when $n \geq N_0$, the natural map

$$\varphi_n : X_\infty \longrightarrow Cl_{F_n}\{p\} \text{ is surj}$$

& $$\ker \varphi_n = \frac{(1+T)^{p^n}-1}{(1+T)^{p^N}-1} \ker \varphi_N.$$

Hope $X_\infty \otimes_{\mathbb{Z}_p[\![\Gamma_\infty]\!]} \mathbb{Z}_p[\Gamma_n] = X_\infty \otimes_{\mathbb{Z}_p[\![T]\!]} \mathbb{Z}_p[T]/((1+T)^{p^n}-1)$

$\simeq Cl_{F_n}\{p\}$ a priori.

(2) For every f.g. torsion $\mathbb{Z}_p[\![T]\!]$-mod M,

there exists (abstractly) a homomorph

$$M \longrightarrow \bigoplus_{i=1}^{s} \frac{\mathbb{Z}_p[\![T]\!]}{(f_i(T))^{k_i}} \oplus \bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[\![T]\!]}{(p^{l_j})}$$

with finite kernel & cokernel

for some s.t. $s,t \in \mathbb{Z}_{\geq 0}$, irred $f_i(T) \in \mathbb{Z}_p[T]$

s.t. $f_i(T) \equiv T^{\deg f_i} \bmod p$.

Pf keys · For $g \in \mathbb{Z}_p[T]$, note that $\frac{\mathbb{Z}_p[\![T]\!]}{(p^k, g(T))}$ is finite.

· When $g = f_1 f_2$, have

$$\frac{\mathbb{Z}_p[\![T]\!]}{(g)} \longrightarrow \frac{\mathbb{Z}_p[\![T]\!]}{(f_1)} \oplus \frac{\mathbb{Z}_p[T]}{(f_2)}.$$

Put $\mu(X_\infty) := \sum_{j=1}^{t} l_j$, $\lambda(X_\infty) := \sum_{i=1}^{s} k_i \cdot \deg(f_i)$,

$\nu(X_\infty)$ = error term $\longleftrightarrow$ finite ker / coker.

"Proof" of Iwasawa's thm

$n \geq N_0$. $\operatorname{length}(Cl_{F_n}\{p^\infty\}) \overset{O(1)}{=} \operatorname{length}(X_\infty / \ker \varphi_n)$

$= \operatorname{length}(Y_\infty / \omega_{n,N_0}(T))$

where $Y_\infty := X_\infty / \ker \varphi_{N_0}$, $\omega_{n,N_0}(T) := \frac{(1+T)^{p^n} - 1}{(1+T)^{p^{N_0}} - 1}$

Have exact sequence:

$$0 \longrightarrow \frac{\ker \varphi_{N_0}}{\omega_{n,N_0} \ker \varphi_{N_0}} \longrightarrow \frac{Cl_{F_n}\{p\}}{\underbrace{X_\infty}_{\omega_{n,N_0}\cdot \ker \varphi_{N_0}}} \longrightarrow \frac{Cl_{F_{N_0}}\{p\}}{X_\infty} \longrightarrow 0$$

$$\ker \varphi_n$$

A more refined str

$$\mathrm{char}(M) := \left(\pi(f_i)^{k_i} \cdot \pi p^{l_j} \right) \subseteq \mathbb{Z}_p[\![T]\!] .$$

characteristic ideal.

* What is $\mathrm{char}(X_\infty)$?

Consider the case $F = \mathbb{Q}(\mu_p)$. then $F_n = \mathbb{Q}(\mu_{p^{n+1}})$.

$$F_\infty = \mathbb{Q}(\mu_{p^\infty}).$$

$$\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong \varprojlim_n Cl_{F_n}\{p\} =: X_\infty$$

$$\| \quad \Rightarrow \quad X_\infty \simeq \bigoplus_{i=1}^{p-1} X_\infty^{(i)}.$$

$\mathbb{F}_p^\times$

s.t. on each $X_\infty^{(i)}$, $a \in \mathbb{F}_p^\times$ acts by $\omega(a)^i$,

$$\omega : \mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p^\times$$
$$a \longmapsto [a]$$

Teichmüller lift.

Theorem (Iwasawa main conj for cyc ext'ns)

(proved by Mazur-Wiles, Kolyvagin (?))

Let k = an even integer $\in 2\mathbb{Z}$. Then

$$\mathrm{char}(X_\infty^{(1-k)}) = (\underbrace{L_{p,k}}) \text{ in } \mathbb{Z}_p[\![T]\!]$$

(Kubota-Leopoldt p-adic L-fct.

Note "p-adic family version of analytic class number formula":
class grps $\longleftrightarrow$ special val of L-fcts.

Kubota-Leopoldt p-adic L-fct

"Origin" (Kummer congruence).

(1) $\zeta(1-n) = -\frac{B_n}{n}$, n even.

(2) if $m_1, m_2 \in 2\mathbb{Z}_{>0}$, not divisible by $p-1$, then

$$(1-p^{m_1-1})\frac{B_{m_1}}{m_1} \equiv (1-p^{m_2-1})\frac{B_{m_2}}{m_2} \mod p^a$$

(1) $\Updownarrow$ if $m_1 \equiv m_2 \mod \underbrace{(p-1)p^{a-1}}_{\varphi(p^a)}$.

$$(1-p^{m_1-1})\zeta(1-m_1) \equiv (1-p^{m_2-1})\zeta(1-m_2) \mod p^a.$$

Put $\zeta^{(p)}(s) := \prod_{\substack{\ell \neq p \\ \text{prime}}} \frac{1}{1-\ell^{-s}} = \zeta(s)\cdot(1-p^{-s})$.

Then: Kummer congruence says

$$\zeta^{(p)}(1-m_1) \equiv \zeta^{(p)}(1-m_2) \mod p^a$$
$$\text{if } m_1 \equiv m_2 \mod (p-1)\cdot p^{a-1}.$$

Expect $\exists$ "p-adic fct" interpolates values of $\zeta^{(p)}$.

Want a more general theory:

$$\chi : (\mathbb{Z}/p^m\mathbb{Z})^\times \longrightarrow \bar{\mathbb{Q}}^\times \subseteq \mathbb{C}^\times \quad \text{nontriv.}$$

$\rightsquigarrow L^{(p)}(s,\chi) = \prod_{\substack{q \neq p \\ \text{prime}}} \frac{1}{1-\chi(q)\cdot q^{-s}}$ Dirichlet L-fct.

interested in $L^{(p)}(n,\chi)$, $n \leq 0$.

p-adic chars

- $n \in \mathbb{Z} \rightsquigarrow$ char of $\mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$
  $x \longmapsto x^n$.
- a char $\chi : (\mathbb{Z}/p^m\mathbb{Z})^\times \to \mathbb{Q}^\times \subseteq \mathbb{C}^\times$
  $\cong$
  $\mathbb{Q}_p^\times$

  $\rightsquigarrow$ char of $\mathbb{Z}_p^\times \longrightarrow \mathbb{Q}_p^\times$
  $x \longmapsto \chi(x \bmod p^m)$.

Note $\{\mathbb{Z}_p^\times \longrightarrow \mathbb{Q}_p^\times$ cont p-adic char$\}$
$\cup$
$(n,\chi) : x \longmapsto x^n \chi(x \bmod p^m)$.

Rmk Why do this?

$\chi \hookleftarrow \chi : \mathrm{Gal}(\mathbb{Q}(\mu_{p^m})/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_{p^m})/\mathbb{Q})$
$\cong$
$(\mathbb{Z}/p^m\mathbb{Z})^\times \longrightarrow \mathbb{Q}_p^\times$.

$n \longleftrightarrow \underline{\mathbb{Q}_p(n)} : \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}_p^\times \longrightarrow \mathbb{Z}_p^\times$
$x \longmapsto x^n$

Normalization $L^{(p)}(s, \underline{\mathbb{Q}_p(n)}) = L^{(p)}(s+n, \mathrm{triv})$.

Upshot a cont char $\eta : \mathbb{Z}_p^\times \to \mathbb{Q}_p^\times$ extends "by continuity"
to a cont homo $\eta : \mathbb{Z}_p \amalg \mathbb{Z}_p^\times \amalg \mathbb{Z} \longrightarrow \mathbb{Q}_p$.

Thm (modern ver of KL p-adic L-fct)

$\forall\, k \not\equiv 1 \bmod p-1$, $\exists!\ \mathcal{L}_{p,k} \in \mathbb{I}_p[\![T]\!]$ s.t.

$\forall$ char $\chi : (\mathbb{Z}/p^m\mathbb{Z})^\times \longrightarrow \mathbb{C}_p^\times$. $n \in \mathbb{Z}_{<0}$.

$$\mathbb{F}_p^\times \times (\mathbb{Z}/p^{m-1}\mathbb{Z}, +),$$

$\chi = \omega^a \times (\ )$

s.t. $a+n \equiv k \pmod{p-1}$,

we have

$$\mathcal{L}_{p,k}\big|_{T=(1+p)^n \cdot \chi(1+p)-1} = L^{(p)}(n,\chi).$$

<u>More general Iwasawa theory</u>

V a cont p-adic rep of $\mathrm{Gal}_{F,S}$ (S finite set of places)

$\mathrm{Gal}_{F,S}$ = Gal grp of max'l ext'n of F unram outside S.

(e.g. arising from ell curve E/F).

<u>Selmer grp</u> $H^1_f(F,V) := \left\{ x \in H^1(\mathrm{Gal}_{F,S}, V) \;\middle|\; \forall\, v \in S,\ \mathrm{loc}_v(x) \in H^1_f(F_v,V) \right\}$.

$\mathrm{loc}_v \downarrow$; $H^1_f(F_v,V) \subseteq H^1(F_v,V)$

$H^1(F_v,V)$

if $v \nmid p$, typically, $H^1_f(F_v,V) = H^1(k_v, V^{I_v}) \subseteq H^1(F_v,V)$

$v \mid p$, more complicated.

<u>Natural obj in Iwasawa theory</u>

$X_\infty := \varprojlim_n H^1_f(F_n,V)$

$\circlearrowright$

$\mathbb{I}_p[\![\Gamma_\infty]\!]$ $\rightsquigarrow$ <u>ask</u>: $\mathrm{char}(X_\infty)$ v.s. $\mathcal{L}_{p,V}$.