Special values of L-functions 8

——— Iwasawa Main Conjecture

§1 "Dual Iwasawa cohomology"

Recall: Let F be a number field, $S :=$ a finite set of places. Write Gal_F^{ur} for $\mathrm{Gal}_{F,\phi}$

$p \geq 3$ prime $S_p :=$ all p-adic places;

$V \in \mathrm{Rep}_{\mathbb{Z}_p}(\mathrm{Gal}_{F,S})$, $\Gamma_F = \mathrm{Gal}(F(\mu_{p^\infty})/F)$ $\quad \Delta_F := \mathrm{Gal}(F(\mu_p)/F)$

Define $H^1_{Iw}(\mathrm{Gal}_{F,S}, V) := \varprojlim_n H^1(\mathrm{Gal}_{F(\mu_{p^n}),S}, V)$

if $S \supseteq S_p$ $\quad \cong \varprojlim_n H^1(\mathrm{Gal}_{F,S}, V \otimes \mathbb{Z}_p[\mathrm{Gal}(F(\mu_{p^n})/F)])$ $\circlearrowleft \mathbb{Z}_p[\![\Gamma_F]\!]$

We need a "dual version": $V^\vee := \mathrm{Hom}_{\mathbb{Z}_p}(V, \mathbb{Q}_p/\mathbb{Z}_p)$ Pontryagin dual

Define $\check{H}^1_{Iw}(\mathrm{Gal}_{F,S}, V) := \varprojlim_n H^1(\mathrm{Gal}_{F_n,S}, V^\vee)^\vee$ $\circlearrowleft \mathbb{Z}_p[\![\Gamma_F]\!]$

The inverse limit is dual to the restriction map $H^1(\mathrm{Gal}_{F_n,S}, V^\vee) \xrightarrow{\mathrm{Res}} H^1(\mathrm{Gal}_{F_{n+1},S}, V^\vee)$

$$\check{H}^1_{Iw}(\mathrm{Gal}_{F,S}, V) = \varprojlim_n H^1(\mathrm{Gal}_{F,S}, V^\vee \otimes \mathbb{Z}_p[\mathrm{Gal}(F_n/F)])^\vee$$

If $S \supseteq S_p$

$$\cong H^1(\mathrm{Gal}_{F,S}, \mathrm{Hom}_{\mathbb{Z}_p}(V \otimes \mathbb{Z}_p[\![\Gamma_F]\!], \mathbb{Q}_p/\mathbb{Z}_p))^\vee$$

Heuristic expectation: For $n \geq n_0$, $H^1(\mathrm{Gal}_{F(\mu_{p^{n+1}}),S}, V^\vee)^\vee \approx \check{H}^1_{Iw}(\mathrm{Gal}_{F,S}, V)/(1-\gamma_{1+p^{n+1}})$.

Example (We have discussed the Iwasawa cohomology of $V = \mathbb{Z}_p(1)$ $\xleftrightarrow{\text{Kummer theory}}$ Cyclotomic units)

If $V = \mathbb{Z}_p$ and $V^\vee \cong \mathbb{Q}_p/\mathbb{Z}_p$, $S = \phi$

$$H^1(\mathrm{Gal}_F^{ur}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee \cong \mathrm{Hom}(\mathrm{Gal}_F^{ur}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee = Cl(F)\{p\}$$ ← p-part of ideal class group.

So $\check{H}^1_{Iw}(\mathrm{Gal}_F^{ur}, \mathbb{Z}_p) := \varprojlim(Cl(F_n) \otimes \mathbb{Z}_p) =$ Galois gp of max'l unramified p-abel. extn of F_∞.

$\check{H}^1_{Iw}(Gal_{F,\mathfrak{p}}, \mathbb{Z}_p)$ = Galois group of max'l p-abelian extn of F_∞ unramified outside $\mathfrak{p}$.

Today ① Relation between $\check{H}^1_{Iw}(Gal_{F,S}, V^\vee)/(1-\gamma_{1+p^{n+1}})$ and $H^1(Gal_{F(\mu_{p^{n+1}}),S}, V^\vee)$ (Control theorem)

and growth of $n \longmapsto \log_p \# H^1(Gal_{F(\mu_{p^{n+1}}),S}, V^\vee)$

② Size of $H^1_{Iw}(Gal^{ur}_{\mathbb{Q}}, \mathbb{Z}_p)$ versus p-adic L-function (Iwasawa Main Conjecture)

§2. Theory of characteristic ideals

Let $\mathcal{O}$ = ring of integer in a finite extn of $\mathbb{Q}_p$, $\varpi \in \mathcal{O}$ uniformizer, $\mathbb{F} = \mathcal{O}/(\varpi)$

Write $\mathbb{Z}_p^\times = \Delta \times (1+p\mathbb{Z}_p)^\times \simeq \Delta \times \mathbb{Z}_p$, where $\Delta \xrightarrow{\omega} \mathbb{Z}_p^\times$ is the Teichmüller lift

($\exp(p\,\cdot)$: $(1+p\mathbb{Z}_p)^\times \to \mathbb{Z}_p$)

Then $\mathcal{O}[\![\mathbb{Z}_p^\times]\!] \simeq \mathcal{O}[\Delta] \otimes \mathcal{O}[\![\mathbb{Z}_p]\!] \cong \prod_{i=0}^{p-2} \mathcal{O}[\![X]\!]$

$$a \otimes [g] \longmapsto \left(\omega^i(a)\cdot(1+X)^g\right)_{i=0,\cdots,p-2}$$

Remark: The ideal $(1-\gamma_{\exp(p^m)})$ corresponds to $(1+X)^{p^m}-1 = g^m(X)$ ← I don't like to call this $g^m(X)$ despite it is indeed shorter. (This is something on $\mathbb{Z}_p^\times$, nothing to do with g on T.)

Essentially, we need some commutative algebra on $\mathcal{O}[\![X]\!]$.

Definition-Lemma A polynomial $f(X) = a_0 + \cdots + a_n X^n \in \mathcal{O}[\![X]\!]$ is called distinguished if

$$\varpi \mid a_0, \ \cdots, \ \varpi \mid a_{n-1}, \ a_n \in \mathcal{O}^\times.$$

(Division algorithm) For $g \in \mathcal{O}[\![X]\!]$, $\exists!\ q \in \mathcal{O}[\![X]\!]$ and $r \in \mathcal{O}[X]$ polynomial of degree $r-1$

s.t. $g(X) = f(X)q(X) + r(X)$.

(Weierstrass Preparation Theorem) Every nonzero power series $g \in \mathcal{O}[\![X]\!]$ can be written uniquely as

$$g(X) = \varpi^r \cdot f(X) \cdot u(X) \quad \text{for } r \geq 0,\ f(X) \text{ distinguished monic},\ u(X) \in \mathcal{O}[\![X]\!]^\times.$$

Corollary All irreducible elements in $\mathcal{O}[\![X]\!]$ are essentially ϖ and distinguished polynomials.

Definition (with more general setup) Let R be a noetherian UFD (e.g. $\mathcal{O}[\![X]\!]$).

A homomorphism $\phi : M_1 \to M_2$ of finite R-modules is called a pseudo-isomorphism if

$\operatorname{codim} \operatorname{Supp}(\ker \phi) \geq 2$ and $\operatorname{codim} \operatorname{Supp}(\operatorname{coker} \phi) \geq 2$ (*)

(For this, just need $\phi: M_{1,\mathfrak{p}} \xrightarrow{\sim} M_{2,\mathfrak{p}}$ for all $\mathfrak{p}$ of ht 1.)

* When $R = \mathcal{O}[\![X]\!]$, (*) is equivalent to $\ker \phi$ and $\operatorname{coker} \phi$ being finite.

Definition. Call two such R-modules pseudo-isomorphic if $M_{1,\mathfrak{p}} \simeq M_{2,\mathfrak{p}}$ for all height 1 primes $\mathfrak{p}$.

Caution: $\exists$ pseudo-isomorphism $\phi: M_1 \longrightarrow M_2$ $\rightleftarrows$ M_1 is pseudo-isomorphic to M_2 (denoted by $M_1 \approx M_2$)

↑ Yes for torsion modules.

Big Theorem. Let M be a finite torsion R-module. Then $\exists$ a pseudo-isomorphism

$$\phi: M \xrightarrow{\approx} \bigoplus_{j=1}^{s} R/(f_j)^{m_j} \quad \text{for } f_j \text{ irreducible element and } m_j \in \mathbb{Z}_{\geq 1}$$

When $R = \mathcal{O}[\![X]\!]$, we have $\phi: M \xrightarrow{\approx} \bigoplus_{i=1}^{s} \frac{\mathcal{O}[\![X]\!]}{(\varpi^{l_i})} \oplus \bigoplus_{j=1}^{t} \frac{\mathcal{O}[\![X]\!]}{(f_j(X))^{m_j}}$ (*)

for some n_i, m_j and $f_j(X)$ distinguished.

Remark: A similar result holds without torsion hypothesis

Definition If M is a finite torsion R-module, define its characteristic ideal to be

$$\operatorname{Ch}(M) := \prod_{i=1}^{s} (\varpi^{l_i}) \cdot \prod_{j=1}^{t} (f_j(X))^{m_j} \subseteq R$$

Remark: $\operatorname{Ch}(M)$ is independent of the choice of (*).

Proof of Theorem. Since M is regular in codimension 1, $\forall \mathfrak{p} \subset R$ of ht 1, $R_{\mathfrak{p}}$ is a DVR.

Then for each such $\mathfrak{p}$, we have $M_{\mathfrak{p}} \simeq \bigoplus_i \left(R_{\mathfrak{p}}/\mathfrak{p}^{n_{\mathfrak{p},i}}\right)$

Consider $M \longrightarrow M_{\mathfrak{p}} \simeq \bigoplus_{\mathfrak{p}} \bigoplus_i \left(R_{\mathfrak{p}}/\mathfrak{p}^{n_{\mathfrak{p},i}}\right)$

$\phi_{\mathfrak{p},i}$ ⇢ ∪| $R/\mathfrak{p}^{n_{\mathfrak{p},i}}$

↑ The image lies in some $s_{\mathfrak{p},i}^{-1} R/\mathfrak{p}^{n_{\mathfrak{p},i}}$ with $s_{\mathfrak{p},i} \notin \mathfrak{p}$

Consider $M \xrightarrow{\oplus s_{p,i}\cdot\phi_{p,i}} \bigoplus_{p,i} R/p^{n_{p,i}}$ it is an isomorphism after localizing at each ht 1 prime.

Theorem is proved. $\square$

§3 Numerical information from characteristic ideal.

Theorem. Let $e :=$ ramification of $\mathcal{O}$ over $\mathbb{Z}_p$.

Let M be a finite torsion $\mathcal{O}[\![X]\!]$-mod s.t. $M \xrightarrow{\approx} \bigoplus_{i=1}^{s} \frac{\mathcal{O}[\![X]\!]}{(\varpi^{l_i})} \oplus \bigoplus_{j=1}^{t} \frac{\mathcal{O}[\![X]\!]}{f_j(X)^{m_j}}$

Suppose that none of f_j is a factor of some $\varphi^n(X) := (1+X)^{p^n} - 1$.

Then $\exists\, n_0, \lambda, \mu, \nu \in \mathbb{Z}_{\geq 0}$ s.t. when $n \geq n_0$, $\operatorname{length}_{\mathcal{O}}\left(M/\varphi^n(X)M\right) = \mu p^n + \lambda n + \nu$

Explicitly, $\mu = \sum l_i$, $\lambda = \sum m_j \deg(f_j) \cdot e$ ↳ or $\#\left(M/((1+X)^{p^n}-1)\right) = p^{\mu p^n + \lambda n + \nu}$.

Proof: **Step 0** (Cheating step) If $\mathcal{O}'$ is a finite (normal) extension of $\mathcal{O}$ of ramification degree e',

then $\operatorname{length}_{\mathcal{O}'}(M\mathcal{O}'/\varphi^n(X)M\mathcal{O}') = e' \cdot \operatorname{length}_{\mathcal{O}} M/\varphi^n(X)M$.

May assume that all f_j's are linear polynomials.

Consider $0 \to \mathrm{Ker} \to M \xrightarrow{\phi} N \to \mathrm{Coker} \to 0$

$$N = \bigoplus_{i=1}^{s} \frac{\mathcal{O}[\![X]\!]}{\varpi^{l_i}} \oplus \bigoplus_{j=1}^{t} \frac{\mathcal{O}[\![X]\!]}{f_j(X)^{m_j}}$$

Step 1: Reduction from M to N.

Since Ker and Coker is support in codim 2 $\Rightarrow$ killed by $(\varpi, X)^{n_0'}$.

For $n \geq n_0'$ which we assume now, multiplication by $\varphi^n(X)$ is the zero map on Ker & Coker.

Also $f_j(X) \nmid \varphi^n(X) \Rightarrow$ multiplication by $\varphi^n(X)$ is injective on N.

(because $\mathcal{O}[\![X]\!]$ is a UFD.)

$$\begin{array}{ccccc}
\ker\phi & \xrightarrow{\cdot\varphi^n(X)=0} & \ker\phi & \longrightarrow & \ker' \\
\downarrow & & \downarrow & & \downarrow \\
M & \xrightarrow{\cdot\varphi^n(X)} & M & \longrightarrow & M/\varphi^n(X)M \longrightarrow 0 \\
\downarrow\phi & & \downarrow\phi & & \downarrow \\
\end{array}$$

$$0 \longrightarrow N \xrightarrow{\cdot \varphi^n(x)} N \longrightarrow N/\varphi^n(x)N \longrightarrow 0$$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$\mathrm{coker}\phi \xrightarrow[0]{\cdot \varphi^n(x)} \mathrm{coker}\phi \longrightarrow \mathrm{coker}'$$

$$\Rightarrow \mathrm{length}_{\mathcal{O}} M/\varphi^n(x)M - \mathrm{length}_{\mathcal{O}} N/\varphi^n(x)N = \mathrm{length}_{\mathcal{O}} \ker\phi + \mathrm{length}_{\mathcal{O}} \mathrm{coker}\phi - \mathrm{length}_{\mathcal{O}} \mathrm{coker}\phi$$

Step 2. Compute ① $\mathrm{length}_{\mathcal{O}}\left(\mathcal{O}[\![X]\!]/(\varpi^l, \varphi^n(X))\right)$

② $\mathrm{length}_{\mathcal{O}}\left(\mathcal{O}[\![X]\!]/(f(X)^m, \varphi^n(X)\right) \quad f(X) \nmid \varphi^n(X)$

① Use $0 \to \mathcal{O}[\![X]\!]/\varpi^{l-1} \to \mathcal{O}[\![X]\!]/\varpi^l \to \mathcal{O}[\![X]\!]/\varpi \to 0$

$\varphi^n(X)$ $\varphi^n(X)$ $\varphi^n(X)$

$0 \to \mathcal{O}[\![X]\!]/\varpi^{l-1} \to \mathcal{O}[\![X]\!]/\varpi^l \to \mathcal{O}[\![X]\!]/\varpi \to 0$

By induction, $\mathrm{length}_{\mathcal{O}}\left(\mathcal{O}[\![X]\!]/(\varpi^l, \varphi^n(X))\right) = l \cdot \mathrm{length}_{\mathcal{O}}\left(\mathbb{F}_q[\![X]\!]/\underbrace{\varphi^n(X)}_{\| X^{p^n}}\right) = l \cdot p^n$

② Similarly, $\mathrm{length}_{\mathcal{O}}\left(\mathcal{O}[\![X]\!]/(f(X)^m, \varphi^n(X)\right) = m \cdot \mathrm{length}_{\mathcal{O}}\left(\mathcal{O}[\![X]\!]/(f(X), \varphi^n(X))\right)$

But $f(X) = X - \alpha$ is linear with $\alpha \in \mathfrak{M}$. $= m \cdot v_{\varpi}\left(\varphi^n(X)|_{X=\alpha}\right)$

Consider $v_{\varpi}\left(\dfrac{\varphi^{n+1}(X)}{\varphi^n(X)}\Big|_{X=\alpha}\right) = \sum_{\substack{j=0 \\ p \nmid j}}^{p^{n+1}-1} v_{\varpi}\left(\alpha - \left(\zeta_{p^{n+1}}^{j} - 1\right)\right) = v_{\varpi}(p) = e.$

whenever $v_{\varpi}(\alpha) > v_{\varpi}\left(\zeta_{p^{n+1}} - 1\right)$. $\square$

§4 Control theorem of Iwasawa-Mazur (in cyclotomic case)

$\Gamma_F := \mathrm{Gal}\left(F(\mu_{p^\infty})/F\right) \subseteq \mathbb{Z}_p^\times \quad F_n := F(\mu_{p^n})$.

Assume $1 + p^{n_0}\mathbb{Z}_p \subseteq \Gamma_F^+$.

Interested in the trivial rep'n $V = \mathbb{Z}_p$. (possibly generalizable to other cases.)

Theorem. Suppose all p-adic places of F_{n_0} is totally ramified in F_∞/F_{n_0}.

For any $n \geq n_0$, we have $\check{H}^1_{Iw}\left(\mathrm{Gal}_{F,\phi}, \mathbb{Z}_p\right)/(\gamma_{1+p^m} - 1) \cong H^1\left(\mathrm{Gal}^{ur}_{F_{n+1}}, \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee$

Corollary: (As each $H^1(\mathrm{Gal}_{F_n,\Phi}^{ur}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee = Cl(F_n)\{p\}$ is finite $\Rightarrow \check{H}^1_{Iw}(\mathrm{Gal}_{F,\Phi}, \mathbb{Z}_p)$ is torsion).

$\Rightarrow \exists\, n_0$ s.t. when $n \geq n_0$, $\#Cl(F_n)\{p\} = p^{\mu \cdot p^n + \lambda p + \nu}$ for some $\mu, \lambda, \nu \in \mathbb{Z}$.

Write $\Delta = \mathbb{F}_p^\times \subseteq \mathbb{Z}_p^\times$, characters of Δ are ω^i for $i = 0, \cdots, p-2$

$$\mathbb{Z}_p[\![\Gamma_{\mathbb{Q}}]\!] = \bigoplus_{i=0}^{p-2} \mathbb{Z}_p[\![X]\!]_{\omega^i}$$

Iwasawa Main Conjecture: When $F = \mathbb{Q}$,

$$Ch_{\mathbb{Z}_p[\![X]\!]_{\omega^i}}\left(\check{H}^1_{Iw}\left(\mathrm{Gal}_{\mathbb{Q},\Phi}^{ur}, \mathbb{Z}_p\right)_{\omega^i}\right) \simeq \mathcal{L}_{p,i}$$

($\mathcal{L}_{p,i}$: Kubota-Leopoldt p-adic L-function)

when i odd and $i \neq 1$.

where $\int_{\Gamma_{\mathbb{Q}}} \eta_p(x) x^s \mathcal{L}_{p,i}(x) = L^{\{p\}}(0, \tilde{\eta}_p \chi_{cyc}^s)$ if $\tilde{\eta}_p|_\Delta = \omega^{i-s}$

When i is even, Vandiver's conjecture predicts that $p \nmid \#Cl(\mathbb{Q}(\zeta_p + \zeta_p^{-1}))$

and that $Ch_{\mathbb{Z}_p[\![X]\!]_{\omega^i}}\left(\check{H}^1_{Iw}(\mathrm{Gal}_{\mathbb{Q}}^{ur}, \mathbb{Z}_p)_{\omega^i}\right) = 0$ if i is even.

Proof: Recall the general Hoshchild-Serre spectral sequence: for $V \in \mathrm{Rep}(\mathrm{Gal}_K)$

$$E_2^{ij} := H^i\left(\mathrm{Gal}(L/K), H^j(\mathrm{Gal}_L, V)\right) \Rightarrow H^{i+j}(\mathrm{Gal}_K, V)$$

Gal_K ($\bar{K}$ | Gal_L | L | $\mathrm{Gal}(L/K)$ | K)

$H^2(\mathrm{Gal}_L, V)^{\mathrm{Gal}(L/K)}$		
$H^1(\mathrm{Gal}_L, V)^{\mathrm{Gal}(L/K)}$	$\xrightarrow{d_2}$	
$(V^{\mathrm{Gal}_L})^{\mathrm{Gal}(L/K)}$	$H^1(\mathrm{Gal}(L/K), V^{\mathrm{Gal}_L})$	$H^2(\mathrm{Gal}(L/K), V^{\mathrm{Gal}_L})$

Get a five term exact sequence:

$$0 \to H^1(\mathrm{Gal}(K/L), V^{\mathrm{Gal}_L}) \to H^1(\mathrm{Gal}_K, V) \to H^1(\mathrm{Gal}_L, V)^{\mathrm{Gal}(L/K)} \to H^2(\mathrm{Gal}(L/K), V^{\mathrm{Gal}_L})$$
$$\to H^2(\mathrm{Gal}_K, V).$$

The condition implies that if $\mathbb{I} := \langle I_v : v|p \rangle$, then $\dfrac{\mathbb{I} \cap \mathrm{Gal}_{F_m,S}}{\mathbb{I} \cap \mathrm{Gal}_{F_n,S}} \simeq \mathrm{Gal}(F_m/F_n)$

$$\text{Also } H^1(\mathrm{Gal}_{F_n,\Phi}, \mathbb{Q}_p/\mathbb{Z}_p) = \ker\left(H^1(\mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(\mathbb{I} \cap \mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p)\right)$$

Applying this to F_m/F_n for $m \geq n$, we get

$$H^1(\mathrm{Gal}_{F_n,\phi}, \mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\sim} H^1(\mathrm{Gal}_{F_m,\phi}, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(F_m/F_n)}$$

$$\begin{array}{ccccccccc}
0 & \to & H^1(\mathrm{Gal}(F_m/F_n), \mathbb{Q}_p/\mathbb{Z}_p) & \to & H^1(\mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p) & \to & H^1(\mathrm{Gal}_{F_m,p}, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(F_m/F_n)} & \to & H^2(\mathrm{Gal}(F_m/F_n), \mathbb{Q}_p/\mathbb{Z}_p) \\
 & & \| & & \downarrow & & \downarrow & & \| \\
0 & \to & H^1(\mathrm{Gal}(F_m/F_n), \mathbb{Q}_p/\mathbb{Z}_p) & \to & H^1(I \cap \mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p) & \to & H^1(I \cap \mathrm{Gal}_{F_m,p}, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{Gal}(F_m/F_n)} & \to & H^2(\mathrm{Gal}(F_m/F_n), \mathbb{Q}_p/\mathbb{Z}_p)
\end{array}$$

$$\Rightarrow \quad H^1(\mathrm{Gal}^{ur}_{F_n}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee = H^1(\mathrm{Gal}^{ur}_{F_m}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee_{\Gamma_m/\Gamma_n} \simeq \check{H}^1_{Iw}(\mathrm{Gal}^{ur}_F, \mathbb{Q}_p/\mathbb{Z}_p)\Big/(1-\gamma_{1+p^n}).$$