Special values of L-functions 9

—— Euler system proof of Iwasawa Main Conjecture

Goal today: Prove the Iwasawa Main Conjecture using Euler system argument.

§1. What is Iwasawa Main Conjecture?

Notation p odd prime. $\Delta = \mathbb{F}_p^\times$, Teichmüller character $\omega : \mathbb{F}_p^\times \longrightarrow \mathbb{Z}_p^\times$

If M is a $\mathbb{Z}_p[\Delta]$-module, $M = M^\Delta \oplus \underset{\underset{i \text{ odd}}{\bigoplus} M^{\Delta = \omega^i}}{\underset{\parallel}{M^{\text{odd}}}} \oplus \underset{\underset{\substack{i \text{ even} \\ i \neq 0}}{\bigoplus} M^{\Delta = \omega^i}}{\underset{\parallel}{M^{\text{even}}}}$

Write $F_n = \mathbb{Q}(\zeta_{p^n})$ and $F_n^+ = \mathbb{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1})$ $\Lambda := \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$

Put $A_n := Cl(F_n)\{p\} = H^1(\mathrm{Gal}_{F_n}^{ur}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$, $\mathcal{A}_n := H^1(\mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p)^\vee$

$X_\infty := \varprojlim_n A_n$ by norm/cores. $\mathcal{X}_\infty := \varprojlim_n \mathcal{A}_n$ by corestriction

$A_\infty := \varinjlim_n A_n$. Both X_∞, $A_\infty^\vee$ are torsion Λ-modules

Lemma. Let $\imath : \Lambda \longrightarrow \Lambda$ be the map induced by $-1 : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$,

Then (as X_∞ is Λ-torsion), $Ch(X_\infty) = \imath(Ch(A_\infty^\vee))$.

(This follows from Iwasawa adjoint)

Recall For F a number field, analytic class number formula says

$$\lim_{s\to 1} (s-1)\zeta_F(s) = \frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot \mathrm{Reg}_F \cdot \# Cl(F)}{w_F \cdot \sqrt{|D_F|}}, \quad \lim_{s \to 0} s^{-r_1 - r_2 + 1} \zeta_F(s) = -\frac{\mathrm{Reg}_F \cdot \# Cl(F)}{w_F}$$

Separating Δ-action by even/odd

① (odd side) $\left.\dfrac{\zeta_{F_n}(s)}{\zeta_{F_n^+}(s)}\right|_{s=0} = \dfrac{\# Cl(F_n) / \# Cl(F_n^+)}{p^n}$ (**Fact**: $\mathcal{O}_{F_n}^\times = \langle \zeta_{p^n} \rangle \cdot \mathcal{O}_{F_n^+}^\times$.)

at $s=0$

② (even side) $\left.\dfrac{\zeta_{F_n^+}(s)}{\zeta_{\mathbb{Q}}(s)}\right|_{s=1} = \dfrac{2^{\varphi(p^n)/2} \cdot \mathrm{Reg}_{F_n^+} \cdot \#Cl(F_n^+)}{\sqrt{|D_{F_n^+}|} = p^{?}}$

at s=1

LHS and RHS can be both "spread out" over $\mathbb{Z}_p[(\mathbb{Z}_p/p^n\mathbb{Z}_p)^\times]$ by controlling sizes.

<u>Interpretation of ①</u> $\zeta_p^{odd} = Ch(X_\infty^{odd})$

<u>Interpretation of ②</u> : $\zeta_p^{odd}(1) = Ch\left(\dfrac{H^1_{Iw}(\mathrm{Gal}_{\mathbb{Q}_p}, \mathbb{Z}_p(1))}{H^1_{Iw}(\mathrm{Gal}_{\mathbb{Q},p}, \mathbb{Z}_p(1))}\right)^{even} + Ch(X_\infty^{even})$

twist by 1

} Iwasawa Main Conjecture

<u>Observation</u>: LHS of ①② concerns different types of Dirichlet L-values

① for odd Dirichlet L-function at s=0 (even point)

② – even ———————— s=1 (odd point)

} but they give rise to the same p-adic L-function

Will explain ①⇔② & then use Euler system method to prove version

§2 Some more Kummer theory.

- F number field, $S \supseteq S_p$.

$$0 \to \mu_{p^n} \to \mathcal{O}_F^S[\tfrac{1}{S}]^\times \xrightarrow{x^{p^n}} \mathcal{O}_F^S[\tfrac{1}{S}]^\times \to 0$$

$$\Rightarrow \quad 0 \to \mathcal{O}_F[\tfrac{1}{S}]^\times/(\mathcal{O}_F[\tfrac{1}{S}]^\times)^{p^n} \to H^1(\mathrm{Gal}_{F,S}, \mu_{p^n}) \to \underbrace{H^1(\mathrm{Gal}_{F,S}, \mathcal{O}_F^S[\tfrac{1}{S}]^\times)[p^n]}_{\substack{\| \\ \mathrm{Pic}(\mathcal{O}_F[\frac{1}{S}])}} \to 0$$

* <u>Inverse limit</u>: Since $\mathrm{Pic}(\mathcal{O}_F[\frac{1}{S}])$ is finite, $\varprojlim_n \mathrm{Pic}(\mathcal{O}_F[\frac{1}{S}])[p^n] = 0$

$$\mathcal{O}_F[\tfrac{1}{S}]^\times \hat{\otimes} \mathbb{Z}_p \simeq H^1(\mathrm{Gal}_{F,S}, \mathbb{Z}_p(1)). \qquad (*)$$

* <u>Direct limit</u>: Will study this in a special case $F = F_n = \mathbb{Q}(\zeta_{p^n})$ and $S = \{p\}$.

* <u>Key</u>: $\mathrm{Pic}(\mathcal{O}_{F_n}[\frac{1}{p}]) = \mathrm{Pic}(\mathcal{O}_{F_n})$ b/c $(\zeta_{p^n} - 1)$ is a principal ideal.

Get $0 \to \mathcal{O}_F[\frac{1}{\ }]^\times \otimes \mathbb{Q}_p/\mathbb{Z} \to H^1(\mathrm{Gal}_{F}, \mu) \to Cl(F)\{p\} \to 0$

$$0 \to \mathcal{O}_{F_n}[\tfrac{1}{p}]^\times \otimes \mathbb{Q}_p/\mathbb{Z}_p \to H^1(\mathrm{Gal}_{F_n,p}, \mu_{p^\infty}) \to \underset{\overset{\parallel}{A_n}}{Cl(F_n)[p^\infty]} \to 0$$

Take the "odd" part for Δ-action $\Rightarrow$ $H^1(\mathrm{Gal}_{F_n,p}, \mu_{p^\infty})^{\mathrm{odd}} \simeq A_n^{\mathrm{odd}}$

Take $\varinjlim_n$ $\Rightarrow$ $\left(\varinjlim_n A_n\right)^{\mathrm{odd}} \cong \varinjlim_n H^1(\mathrm{Gal}_{F_n,p}, \mu_{p^\infty})^{\mathrm{odd}} = H^1(\mathrm{Gal}_{F_\infty,p}, \mu_{p^\infty})^{\mathrm{odd}}$.

$$= H^1(\mathrm{Gal}_{F_\infty,p}, \mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{even}}(1) = \left(\varprojlim_n A_n^{\mathrm{even}}\right)^\vee(1)$$

Take Pontryagin dual $\Rightarrow$ $A_\infty^{\mathrm{odd},\vee} \cong \mathfrak{X}_\infty^{\mathrm{even}}(1)$

Combining earlier $\Rightarrow$ $\mathrm{Ch}(X_\infty^{\mathrm{odd}}) = \iota(\mathrm{Ch}(A_\infty^{\mathrm{odd},\vee})) = \iota(\mathrm{Ch}(\mathfrak{X}_\infty^{\mathrm{even}})(1))$

§3 Poitou-Tate duality

Let F be a number field. $p \geq 3$ prime. S = finite set of places $\supseteq S_p$.

Theorem (Poitou-Tate) Let $V \in \mathrm{Rep}^{\mathrm{fr}}_{\mathbb{Z}_p}(\mathrm{Gal}_{F,S})$. We have an exact sequence

$$\begin{tikzcd}
0 \arrow[r] & H^0(\mathrm{Gal}_{F,S}, V) \arrow[r, "\oplus \mathrm{loc}_v"] & \bigoplus_{v\in S} H^0(\mathrm{Gal}_{F_v}, V) \arrow[r, "\oplus \mathrm{loc}_v^\vee"] & H^2(\mathrm{Gal}_{F,S}, V^\vee(1))^\vee \arrow[dll, bend left] \\
& H^1(\mathrm{Gal}_{F,S}, V) \arrow[r, "\oplus \mathrm{loc}_v"] & \bigoplus_{v\in S} H^1(\mathrm{Gal}_{F_v}, V) \arrow[r, "\oplus \mathrm{loc}_v^\vee"] & H^1(\mathrm{Gal}_{F,S}, V^\vee(1))^\vee \arrow[dll, bend left] \\
& H^2(\mathrm{Gal}_{F,S}, V) \arrow[r, "\oplus \mathrm{loc}_v"] & \bigoplus_{v\in S} H^2(\mathrm{Gal}_{F_v}, V) \arrow[r, "\oplus \mathrm{loc}_v^\vee"] & H^0(\mathrm{Gal}_{F,S}, V^\vee(1))^\vee \arrow[r] & 0
\end{tikzcd}$$

Here the map $\bigoplus_{v\in S} H^{2-i}(\mathrm{Gal}_{F_v}, V) \longrightarrow H^i(\mathrm{Gal}_{F,S}, V^\vee(1))^\vee$ is the Pontryagin dual of the localization map $H^i(\mathrm{Gal}_{F,S}, V^\vee(1)) \xrightarrow{\oplus \mathrm{loc}_v} \bigoplus_{v\in S} H^{2-i}(\mathrm{Gal}_{F_v}, V)^\vee \simeq \bigoplus_{v\in S} H^i(\mathrm{Gal}_{F_v}, V^\vee(1))$.

Consider $F_n = F(\mu_{p^n})$ and $F_\infty = \bigcup_n F_n$. Taking inverse limit $\Rightarrow$

exact sequence $\cdots \to H^1_{Iw}(\mathrm{Gal}_{F,S}, V) \xrightarrow{\oplus \mathrm{loc}_v} \bigoplus_{v\in S} H^1_{Iw}(\mathrm{Gal}_{F_v}, V) \xrightarrow{\oplus \mathrm{loc}_v^\vee} \check{H}^1_{Iw}(\mathrm{Gal}_{F,S}, V) \to \cdots$

Here we have Iwasawa duality

$$H^1_{Iw}(\mathrm{Gal}_{F_v}, V) = \varprojlim_n H^1(F_v(\mu_{p^n}), V) \simeq \varprojlim_n H^1(F_v(\mu_{p^n}), V^\vee(1))^\vee = \check{H}^1_{Iw}(\mathrm{Gal}_{F_v}, V)$$

<u>Special case</u>: $V = \mathbb{Z}_p(1)$, $F = \mathbb{Q}$, $S = \{p\}$

$$\begin{tikzcd}
H^1_{\mathrm{Iw}}(\mathrm{Gal}_{\mathbb{Q},p}, \mathbb{Z}_p(1)) \arrow[r, "\mathrm{loc}_p"] \arrow[d, equal] & H^1_{\mathrm{Iw}}(\mathrm{Gal}_{\mathbb{Q}_p}, \mathbb{Z}_p(1)) \arrow[r, "\mathrm{loc}_p^{\vee}"] \arrow[d, equal] & \check{H}^1_{\mathrm{Iw}}(\mathrm{Gal}_{\mathbb{Q},p}, \mathbb{Z}_p(1)) \quad (\star) \\
\varprojlim_n \left(\mathcal{O}_{F_n}[\tfrac{1}{p}]^{\times} \hat{\otimes} \mathbb{Z}_p\right) \arrow[r, hook] & \varprojlim_n F_{n,v}^{\times} \hat{\otimes} \mathbb{Z}_p & \\
H^1_{\mathrm{Iw},f}(\mathrm{Gal}_{\mathbb{Q}}, \mathbb{Z}_p(1)) = \varprojlim_n \left(\mathcal{O}_{F_n}^{\times} \hat{\otimes} \mathbb{Z}_p\right) \arrow[r, hook] \arrow[u, phantom, sloped, "\subseteq"] & \varprojlim_n \mathcal{O}_{F_{n,v}}^{\times} \hat{\otimes} \mathbb{Z}_p \arrow[u, phantom, sloped, "\subseteq"] \arrow[uur] &
\end{tikzcd}$$

still exact in the middle.

On the dual side, $\boxed{\quad\quad}$ becomes

$$\begin{tikzcd}
H^1(I_{F_{n,v}}, \mathbb{Q}_p/\mathbb{Z}_p) \arrow[d, equal] & H^1(\mathrm{Gal}_{F_{n,v}}, \mathbb{Q}_p/\mathbb{Z}_p) \arrow[l] \arrow[d, equal] & H^1(\mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p) \arrow[l, "\mathrm{loc}_p"'] \arrow[ll, bend left, "\mathrm{sing}_p"] \\
\mathrm{Hom}(\mathcal{O}_{F_{n,v}}^{\times} \hat{\otimes} \mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) & \mathrm{Hom}(F_{n,v}^{\times} \hat{\otimes} \mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \arrow[l, two heads] &
\end{tikzcd}$$

$$\mathrm{Ker}(\mathrm{sing}_p) = \mathrm{Coker}(\mathrm{sing}_p^{\vee}) = H^1(\mathrm{Gal}_{F_n}^{ur}, \mathbb{Q}_p/\mathbb{Z}_p)$$

Taking limit now gives

$$\begin{tikzcd}
0 \arrow[r] & H^1_{\mathrm{Iw},f}(\mathrm{Gal}_{\mathbb{Q}}, \mathbb{Z}_p(1)) \arrow[r] \arrow[d, phantom, sloped, "\cong"] & H^1_{\mathrm{Iw},f}(\mathrm{Gal}_{\mathbb{Q}_p}, \mathbb{Z}_p(1)) \arrow[r] \arrow[d, phantom, sloped, "\cong"] & \check{H}^1_{\mathrm{Iw}}(\mathrm{Gal}_{\mathbb{Q},p}, \mathbb{Z}_p(1)) \arrow[r] \arrow[d, phantom, sloped, "\cong"] & \check{H}^1_{\mathrm{Iw}}(\mathrm{Gal}_{\mathbb{Q}}^{ur}, \mathbb{Z}_p(1)) \arrow[r] \arrow[d, phantom, sloped, "\cong"] & 0 \\
0 \arrow[r] & \varprojlim_n \mathcal{O}_{F_n}^{\times} \hat{\otimes} \mathbb{Z}_p \arrow[r] & \varprojlim_n \mathcal{O}_{F_{n,v}}^{\times} \hat{\otimes} \mathbb{Z}_p \arrow[r] & \varprojlim_n A_n \arrow[r] & \varprojlim_n A_n = X_\infty \arrow[r] & 0 \\
 & \left(\frac{\zeta_p^a - 1}{\zeta_p - 1}\right) \arrow[u, phantom, sloped, "\in"] \arrow[r, mapsto] & \zeta_{p,a} \in \mathbb{Z}_p[[\mathbb{Z}_p^{\times}]] = \Lambda \arrow[u, phantom, sloped, "\cong"] & \mathfrak{X}_\infty \arrow[u, phantom, sloped, "="] & &
\end{tikzcd}$$

↑ This is called the fundamental exact sequence of IMC.

Write $\mathcal{U}_\infty := \varprojlim_n \mathcal{O}_{F_n}^{\times} \hat{\otimes} \mathbb{Z}_p$,

$\mathcal{C}yc_\infty :=$ sub-Λ-mod generated by all $\frac{\zeta_p^a - 1}{\zeta_p - 1}$

$$\Rightarrow \quad 0 \longrightarrow \frac{\mathcal{U}_\infty}{\mathcal{C}yc_\infty} \longrightarrow \frac{\Lambda}{\iota(\zeta_p)(1)} \longrightarrow \mathfrak{X}_\infty \longrightarrow X_\infty \longrightarrow 0$$

<u>Sum up</u>: <u>IMC 1</u>: $\zeta_p^{odd} = \mathrm{Ch}(X_\infty^{odd})$

Have proved $\mathrm{Ch}(X_\infty^{odd}) = \iota\left(\mathrm{Ch}(\mathfrak{X}_\infty^{even})\right)(1)$

<u>Equivalent version</u> <u>IMC 2</u>: $\mathrm{Ch}(\mathfrak{X}_\infty^{even}) = \iota(\zeta_p^{odd})(1)$

<u>IMC 3</u>: $\mathrm{Ch}(\mathcal{U}_\infty/\mathcal{C}yc_\infty)^{even} = \mathrm{Ch}(X_\infty)^{even}$.

Remark: Using analytic class number formula,

$$\#\left(\Lambda^{odd}/\zeta_p^{odd}, \varphi^n(X)\right) / \#\left(X_\infty^{odd}/\varphi^n(X)\right)$$ is bounded independent of n.

So suffices to prove one divisibility of characteristic classes

Method 1: Constructing Selmer class $\Rightarrow \zeta_p^{odd} \mid \mathrm{Ch}(X_\infty^{odd})$

Method 2: Using Euler system $\Rightarrow \mathrm{Ch}(X_\infty)^{even} \mid \mathrm{Ch}\left(\mathcal{U}_\infty/\mathcal{C}yc_\infty\right)^{even}$

§4 Essential part of the Euler system construction

Rough idea: Want to prove $\mathrm{Ch}(\mathcal{X}_\infty^{even}) \mid \iota(\zeta_p)(1)$.

Fix $i \in \{2, 4, \dots, p-2\}$ $\rightsquigarrow \mathrm{Ch}(\mathcal{X}_\infty^i) \mid \iota(\zeta_{p,1-i})$ over $\mathbb{Z}_p[[X]]$

Suffices to show, $\exists M > 0$, s.t $\forall n$, $``\underbrace{\iota(\zeta_{p,1-i})}_{\zeta'_p} \cdot (p, X)^M" \subseteq ``\mathrm{Ch}(\mathcal{X}_\infty^i)"$ in $\underbrace{\mathbb{Z}_p[[X]]/\varphi^n(X)}_{\Lambda_{n,i}}$.

Return to the finite level:

$$\begin{tikzcd}
0 \arrow[r] & \left(\mathcal{O}_{F_n}^\times \hat{\otimes} \mathbb{Z}_p\right)_{\omega^i} \arrow[r] & \left(\mathcal{O}_{F_n,v}^\times \hat{\otimes} \mathbb{Z}_p\right)_{\omega^i} \arrow[r, "\mathrm{loc}_p^\vee"] & H^1\left(\mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee_{\omega^i} \arrow[r] & H^1\left(\mathrm{Gal}_{F_n}^{ur}, \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee_{\omega^i} \arrow[r] & 0 \\
& \mathrm{Cyc}_{F_n} \arrow[u, phantom, sloped, "\subseteq"] \arrow[r, mapsto] & \zeta'_p \in \Lambda_{n,i} \arrow[u, equal] & & &
\end{tikzcd}$$

If $\mathrm{loc}_p^\vee$ is surjective, done! b/c $H^1\left(\mathrm{Gal}_{F_n,p}, \mathbb{Q}_p/\mathbb{Z}_p\right)^\vee_{\omega^i}$ is a quotient of $\Lambda_{n,i}/\zeta'_p$

What if $\mathrm{loc}_p^\vee$ is not surjective? Add new primes $\ell_1, \dots, \ell_r$ (that splits completely in F_{n+1})

$$\begin{tikzcd}
H^1\left(\mathrm{Gal}_{\mathbb{Q},pq_1\cdots q_r}, \Lambda_n(1)\right) \arrow[r] \arrow[dr, "\mathrm{res}_{pq}"] & H^1\left(\mathrm{Gal}_{\mathbb{Q}_p}, \Lambda_n(1)\right) \oplus \bigoplus_{i=1}^r H^1\left(\mathrm{Gal}_{\mathbb{Q}_{q_i}}, \Lambda_n(1)\right) \arrow[r] \arrow[d] & H^1\left(\mathrm{Gal}_{F_n,pq_1\cdots q_r}, \Lambda_n^\vee\right)^\vee \arrow[d] \\
& H^1\left(\mathrm{Gal}_{\mathbb{Q}_p}, \Lambda_n(1)\right) \oplus \bigoplus_{i=1}^r H^1_{sing}\left(\mathrm{Gal}_{\mathbb{Q}_{q_i}}, \Lambda_n(1)\right) \arrow[r, "\mathrm{loc}_{pq}"] & H^1\left(\mathrm{Gal}_{F_n,pq_1\cdots q_r}, \Lambda_n^\vee\right)^\vee \\
& H^1_{ur}\left(\mathrm{Gal}_{\mathbb{Q}_{q_i}}, \Lambda_n^\vee\right)^\vee \arrow[u, phantom, sloped, "\cong"] &
\end{tikzcd}$$

localized at ω^i everywhere

Choose appropriate q_i s.t. $\mathrm{loc}_{pq}^\vee$ is surjective,

and try to show res_{pq} has large image by exhibiting elements

(1) Choice of q_i : by Chebotarev density theorem

(2) Construction of classes in $H^1(\mathrm{Gal}_{\mathbb{Q},pq_1,\dots,q_r}, \Lambda_n(1))$ <u>Kolyvagin's method</u>

<u>Subtlety</u>: Not known if $\mathrm{Cyc}_{F_n,\omega^i} \subseteq (\mathcal{O}_{F_n}^{\times} \hat{\otimes} \mathbb{Z}_p)_{\omega^i}$ is an equality in general

But some variant $\mathrm{Cyc}_{F_n,q_1\cdots q_n,\omega^i} \subseteq H^1(\mathrm{Gal}_{F_n,q_1\cdots q_n}, \Lambda_n/p^t)$ tend to be surj. $t>>0$

Too technical, may come back for this later.