04 August 2023 14:55

Cyclotomic Units & Iwasawa Theory

Cyclotomic - GL_1 Euler System

Iwasawa Theory:

- Study L-functions associated to arithmetic objects

e.g. $E/\mathbb{Q}$ ell. curve

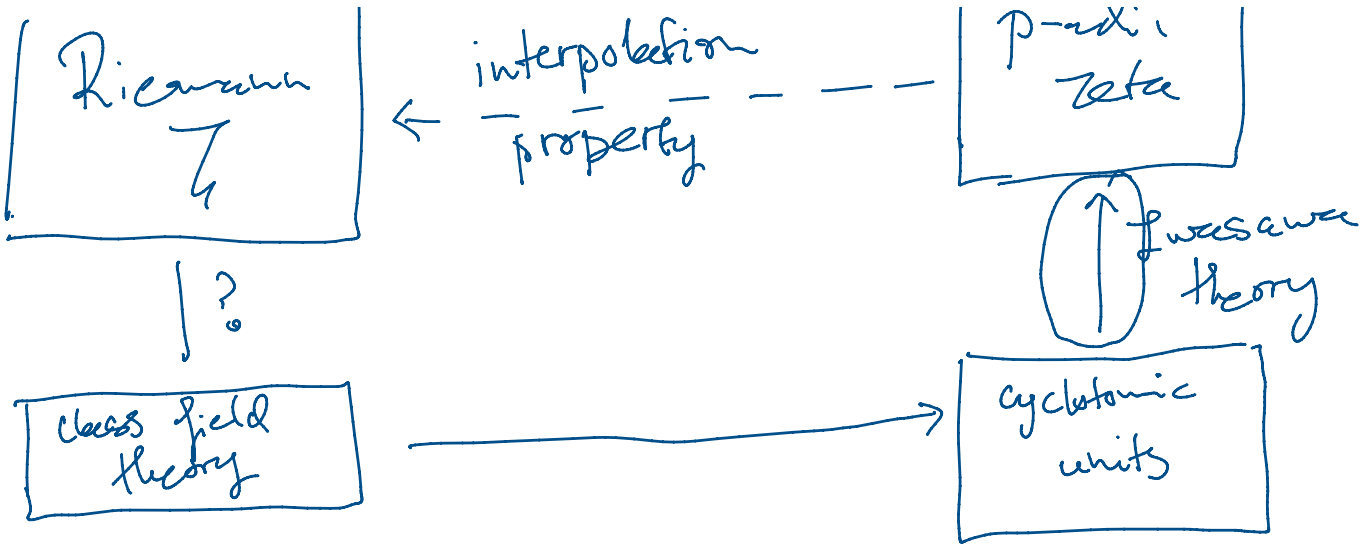
$\operatorname{ord}_{s=1} L(E,s) = \operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q})$

$\mathbb{C}$-analytic — algebraic

p-adic L-function is more algebraic!

This talk ζ_p p-adic zeta "measure" which sees values of Riemann zeta

Riemann — interpolation — — — p-adic zeta



Algebraicity of ζ_p:

ζ_p "$\in$" $\Lambda := \mathbb{Z}_p[\![\mathbb{Z}_p^\times]\!]$ Iwasawa algebra

$= \bigoplus_{\text{finite}} \mathbb{Z}_p[\![T]\!]^{\frac{p-1}{2}}$

(almost)

We understand well!

- What is a Euler system?

"cohomological incarnation of a p-adic L-function"

i.e. well chosen class in a cohomology group $\{Cn CH^i(-,-)\}_n$

$c \in H^1_{Iw}(G_{\mathbb{Q}}, -)$

s.t. under Perrin-Riou regulator

$\ell \cdot H^1_{\ell}(G_{\mathbb{Q}}, -) \longrightarrow \Lambda \otimes D_{cris}(-)$

$$\mathcal{I} : H^1_{Iw}(G_{\mathbb{Q}}, -) \longrightarrow \Lambda \otimes \mathbb{D}_{cris}(-)$$

$$c \longmapsto L_p$$

Euler system of cyclotomic units $\longmapsto$ ζ_p

Conjecture: There is a Λ-module $\boxed{X_\infty}$ s.t.

$$\underline{\mathrm{char}_\Lambda}(X_\infty) = \mathcal{I} \cdot \zeta_p$$

// augmentation ideal

$1 \cdot (\mathbb{Z}_p[[T]] \longrightarrow \mathbb{Z}_p)$

$T \longmapsto 1$

- What is X_∞?
- What is char_Λ?
- What are cyclotomic units?
- How do we prove IMC?

§1. Cyclotomic Units

Fix system $\{\mu_m\}_{m \in \mathbb{N}}$ of prim. mth roots of units

s.t. $(\mu_{mn})^n = \mu_m \quad \forall\, m, n \geq 1$.

Then $\mathcal{O}_{\mathbb{Q}(\mu_m)} = \mathbb{Z}[\mu_m]$

$\mathcal{L} = \mathbb{Z}[\mu_m]^\times$

$$E_m = \mathbb{Z}[\mu_m]^\times$$

cyclotomic units $C_m = E_m \cap \langle \pm \mu_m, 1-\mu_m^a : 1 \le a \le \frac{m}{2} \rangle$

for general $K/\mathbb{Q}$ abelian:

$K \subseteq \mathbb{Q}(\mu_m)$ some m

let $E_K = \mathcal{O}_K^\times \cap E_m$

$C_K = \mathcal{O}_K^\times \cap C_m$

Apply this to $K_n = \mathbb{Q}(\mu_{p^n})^+ := \mathbb{Q}(\mu_{p^n}) \cap \mathbb{R}$

Lemma: (a) $C_{K_n} = \langle -1, \zeta_a \rangle$

units will be useful later ← $\zeta_a = \mu_{p^n}^{(1-\sigma_a^{-1})} \cdot \frac{1-\mu_{p^n}^a}{1-\mu_{p^n}}$

$1 < a < \frac{1}{2}p^n \quad (a,p)=1$

(b) $C_{\mathbb{Q}(\mu_{p^n})} = \langle C_{K_n}, \mu_{p^n} \rangle$

Theorem: $[\mathbb{Z}[\mu_{p^n}]^\times \cap \mathbb{R} : C_{K_n}] = \#Cl(K_n)$

[Proof comes from analytic class # formula]

Euler system of cyclotomic units

$$u_{\mathbb{Q}} = 1 - \mu_m$$

Claim: $N_{\mathbb{Q}(\mu_{\ell m})/\mathbb{Q}(\mu_m)}(u_{\ell m}) = \begin{cases} u_m & \text{if } \ell \mid m \\ (1-\sigma_\ell^{-1}) \cdot u_m & \ell \nmid m \\ \ell & m = 1 \end{cases}$

ℓ prime odd

Proof of claim: $m = 1$ easy

$m > 1$, $[\mathbb{Q}(\mu_{\ell m}) : \mathbb{Q}(\mu_m)] = \begin{cases} \ell - 1 & \ell \nmid m \\ \ell & \ell \mid m \end{cases}$

$\ell \nmid m$: min poly of $\mu_{\ell m}$ over μ_m

is $f(X) = \dfrac{X^\ell - \mu_m}{X - \mu_m^{\ell-1}}$

min poly of $u_{\ell m}$ over u_m

is $f(1-X)$

Constant term:

$$\frac{1-\mu_m}{1-\mu_m^{\ell-1}} = \frac{u_m}{\sigma_\ell^{-1}(u_m)} = (1-\sigma_\ell^{-1}) \cdot u_m$$

---

② $\ell \mid m$ $\quad (1-X)^\ell - \mu_m$

constant term is $1 - \mu_m = u_m$.

Let $v_m = \begin{cases} u_m & p \mid m \end{cases}$

Let $V_m = \begin{cases} U_m & p \mid m \\ N_{\mathbb{Q}(\mu_{pm})/\mathbb{Q}(\mu_m)}(U_{pm}) & p \nmid m \end{cases}$

Claim: These form an Euler system.

(Exercise)

Remark: Apply Kummer map

$\kappa_p : K^\times \hookrightarrow H^1(K, \mathbb{Z}_p(1))$

$\{V_m\} \longmapsto \{c_m^\psi\}_m$ Euler system

comes from $K^\times/(K^\times)^{p^n} \xrightarrow{\sim} H^1(K, \mu_{p^n})$

and $\varprojlim_n$

§. Towers of Extensions

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

$G_n = \mathrm{Gal}(K_n/\mathbb{Q})$

$K_\infty = \bigcup_n K_n$ $\quad G = \mathrm{Gal}(K_\infty/\mathbb{Q})$

$\cong \mathbb{Z}_p \times \Delta$ ← finite gp of size $\frac{p-1}{2}$

$\mathbb{Z}_p$-extension

$U_n' = \{u \in \mathbb{Q}_p(\mu_{p^n})^\times$ s.t. $u \equiv 1 \bmod \mathfrak{m}_{\mathbb{Q}_p(\mu_{p^n})}\}$

E_n' = completion of $E_{K_n^+} \cap U_n'$

U_n' = " " $C_{K_n^+} \cap U_n'$

C_n' =

take $U_\infty' = \varprojlim_n U_n'$

$E_\infty' = \varprojlim_n E_n'$

$C_\infty' = \varprojlim_n C_n'$

Iwasawa algebra $\Lambda = \mathbb{Z}_p[\![G]\!] = \mathbb{Z}_p[\![T]\!]$

completed gp ring

$\gamma - 1 \longleftrightarrow T$

γ = top gen of $\mathbb{Z}_p \subseteq G$

U_∞', C_∞', E_∞' are all Λ-modules!

Lemma: C_∞' is a free Λ-module of rank 1

M_n = max ab. p-ext of K_n, unramified away from p

L_n = max ab p-ext of K_n, unramified anywhere.

$$M_\infty = \bigcup_n M_n \qquad L_\infty = \bigcup_n L_n$$

X_∞ = $\mathrm{Gal}(M_\infty/K_\infty)$

M_∞ | L_∞ | K_∞

$\mathrm{Gal}(L_\infty/K_\infty) = Y_\infty$

both Λ-modules (Selmer groups in disguise)

Theorem: There is an exact sequence of Λ-mods

$$(*) \quad 0 \to E'_\infty/C'_\infty \hookrightarrow U'_\infty/C'_\infty \to X_\infty \twoheadrightarrow Y_\infty \to 0$$

ξ_p

Theorem: $\exists$ Λ-morphism $\mathcal{L}' : U'_\infty \xrightarrow{\sim} \Lambda$

$\mathcal{L}'$ is an example of PR regulator map!

ER - $\mathcal{L}'(C'_\infty) = \underbrace{I(G)}_{\text{forget!}} \cdot \xi_p$

(Euler systems lives in U'_∞/C'_∞)

$\mathcal{L}'$ "=" $1-\phi$

ϕ = crystalline Frobenius

ξ_p = Kubota-Leopoldt p-adic L-function

Corollary: $U'_\infty/C'_\infty \simeq \Lambda/\mathcal{L}(G)\cdot\xi_p$

is a Λ-module!

torsion Λ-module !

$\longrightarrow$ all modules in $\circledast$ are torsion Λ-modules

Def: For a torsion Λ-module M, define characteristic ideal

$$\underline{\mathrm{char}_\Lambda(M) = (f_1 \cdots f_r) \subseteq \Lambda}$$

where $0 \to P \to \bigoplus_{i=1}^{r} \Lambda/f_i \to M \to Q \to 0$]

and Q finite Λ-module

(pseudo-null i.e. localizations of Q at ht 1 primes of Λ are 0)

Structure theorem of Iwasawa theory

M "pseudo-isomorphic" to $\bigoplus_{i=1}^{r} \Lambda/f_i$

Work of Iwasawa late 50s / early 60s

$\longrightarrow \mathrm{char}_\Lambda(M)$ well defined!

§. The Main Conjecture

Recall: $\mathrm{char}_\Lambda(X_\infty) = \overline{I(G_1) \cdot \zeta_p}$ (ideal of Λ)

char_Λ is multiplicative in exact

Fact: char_Λ is multiplicative in exact sequences!

$$0 \to A \to B \to C \to 0$$

torsion Λ-modules

then $\mathrm{char}_\Lambda(A)\,\mathrm{char}_\Lambda(C) = \mathrm{char}_\Lambda(B)$.

$$\mathrm{char}_\Lambda\left(\mathcal{X}_\infty / C_\infty'\right) = \mathrm{char}_\Lambda\left(\Lambda / I(G_1)\cdot \zeta_p\right)$$
$$= I(G_1)\cdot \zeta_p$$

Equivalent to show:

$$\longrightarrow \quad \mathrm{char}_\Lambda\left(E_\infty'/C_\infty'\right) \mid \mathrm{char}_\Lambda\left(Y_\infty\right)$$

"IMC without p-adic ζ"

Sketch of proof of $\longrightarrow$ direction:

Steps:

(1) Control theorem comparing $(Y_\infty)_{\Gamma_n}$ with $\mathrm{Gal}\left(L_n/K_n\right)$, $\Gamma_n = \mathrm{Gal}\left(K_\infty/K_n\right)$

(2) Reducing the problem into a divisibility in some small quotient of Λ

(3) Euler system argument

(3) Euler system argument (in disguise) to prove the reduced problem.

(1) Control theorem (Iwasawa 1959)

A_n = p-part of class group of K_n

= $\mathrm{Gal}(L_n/K_n)$

Then $|A_n| = p^{p^n\mu + n\lambda + \nu}$ ideal $\mu = 0$

for $\mu, \lambda, \nu \in \mathbb{Z}_{\geq 0}$

$n >> 0$

Understand how A_n grow as $n \to \infty$

$(Y_\infty)_{\Gamma_n} = \mathrm{Gal}(L_n/K_n)$

$0 \to \oplus \Lambda/(f_i) \to Y_\infty \to Q \to 0$

(2) Recall $\mathrm{char}_\Lambda(Y_\infty) = (f_1 \cdot \ldots \cdot f_r)$

Fact: $E_\infty^1/C_\infty^1 = \Lambda/(\beta)$ some $\beta \in \Lambda$

$\Rightarrow \mathrm{char}_\Lambda\left(E_\infty^1/C_\infty^1\right) = (\beta)$ (β multiple of ξ_p)

RTP: $\Pi f_i \mid \beta$

Proved to finite level K_n

Project to finite level K_m

$$R_m = \mathbb{Z}_p[\mathrm{Gal}(K_m/\mathbb{Q})]$$

$$pr : \Lambda \longrightarrow R_m$$

(Then $R_m/pr(\beta)$ finite

Fix annihilator of Q, σ,

S = p-power annihilating both $R_m/pr(\beta)$ & $R_m/pr(\sigma)$

($t = p^r$, $r \gg 0$)

$$t = \#A_m \#Q \cdot p^m \cdot S^{r+1}$$ p-power

$$\overline{R}_m = \mathbb{Z}/t\mathbb{Z}[\mathrm{Gal}(K_m/\mathbb{Q})]$$

$$\Lambda \longrightarrow \overline{R}_m$$

$$x \longmapsto \bar{x}$$

[Claim: For $i = 1, \dots, r$

$(\bar{f}_1 \dots \bar{f}_r) \mid \overline{((\gamma-1)\beta\,\sigma^{i+1})}$ in $\overline{R}_m$

$m \longrightarrow \infty$

$f_1 \dots f_r \mid (\gamma-1)\beta\,\sigma^{r+1}$ in Λ

Since Q is finite and $(\gamma_\infty)_{\mathfrak{m}}$

$\mathrm{char}_\Lambda(\gamma_\infty)$ coprime to $\gamma - 1$

and σ

$\Rightarrow$ $f_1 \dots f_r \mid p$ in Λ

(3) An Euler system argument in disguise to prove claim.

This makes use of

- Filtration on A_m
- 'induction argument on i
- Image of Euler system in $K^\times/(K^\times)^{p^t}$ satisfying norm relation

---

Prove that $\mathrm{char}_\Lambda(X_\infty) \mid \#(G) \cdot \xi_p$

§. General picture

$(\tilde{H}^1(V)^*) = (L_p(V,S))$ dual

$\mathrm{char}_\Lambda\left(H^1(V)^\vee\right) = (L_p(V,\dots))$

↑ Selmer group ↑ p-adic L-function

V p-adic Galois rep attached to some automorphic rep of a L-A-G- G_L

Issues in more general case:

- Ordinary of aut rep ($L_p \in \Lambda \iff$ rep is ordinary)
- Constructing of p-adic L-function
- Constructing of Euler systems are rare & non-explicit
- May have to replace $\Lambda = \mathbb{Z}_p[[T]]$
- Explicit Reciprocity Law.