2012/4/3 talk I

$p \geq 3$ prime fixed, $\overline{\mathbb{Q}} \overset{\iota_\infty}{\hookrightarrow} \mathbb{C}$, $\overline{\mathbb{Q}} \overset{\iota_p}{\hookrightarrow} \overline{\mathbb{Q}}_p$ fixed

<u>Recall</u> $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ is Galois

with $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \underset{\chi_{cyc}}{\xrightarrow{\sim}} \mathbb{Z}_p^\times$ (canonical)

$\mathbb{Q}_\infty$: unique subfield of $\mathbb{Q}(\mu_{p^\infty})$

s.t $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong \mathbb{Z}_p =: \Gamma_{cyc}$

<u>Def</u> For any fin. ext. $K/\mathbb{Q}$, we define

$K_\infty^{cyc} = \mathbb{Q}_\infty K$

and we call it the cyclo. $\mathbb{Z}_p$-ext. of K ⌟

From now on, we assume K : abel. ext of $\mathbb{Q}$ s.t $\mathbb{Q}_\infty \cap K = \mathbb{Q}$

We will formulate

alg. object$/K_\infty^{cyc}$ ① — ③ I.M.C — anal. obj$/K_\infty^{cyc}$ ②

$$\begin{tikzcd}
 & & M_\infty^{cyc} \\
 & L_\infty^{cyc} \arrow[ur, dash] & \\
K_\infty^{cyc} \arrow[uurr, dash, bend left, "\mathfrak{X}_K"] \arrow[ur, dash] \arrow[ur, dash, bend right, "X_K"'] & & \\
K \arrow[u, dash, "\Gamma_{cyc}"] & &
\end{tikzcd}$$

L_∞^{cyc} : max p-power abel. ext. over K_∞^{cyc} unramified everywhere

M_∞^{cyc} : max p-power abel. ext. over K_∞^{cyc} unramified outside p

By the exact seq.

$$\begin{array}{ccccccccc} 0 \to & X_K & \to & \mathrm{Gal}(L_\infty^{cyc}/K) & \longrightarrow & \Gamma_{cyc} & \to 0 \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} & \\ & x & & \tilde{g} & \longmapsto & g & \end{array}$$

$g \cdot x := \tilde{g} x \tilde{g}^{-1}$ (Note that the action is indep. of $\tilde{g}$ since X_K is abel.)

X_K is a compact module with $\mathbb{Z}_p$-linear cont. Γ_{cyc}-action
$\Rightarrow X_K$ is a compact $\mathbb{Z}_p[[\Gamma_{cyc}]]$-module

Similarly, $\mathfrak{X}_K$ is a compact $\mathbb{Z}_p[[\Gamma_{cyc}]]$-module.

Denote $\mathbb{Z}_p[[\Gamma_{cyc}]]$ by Λ.

<u>Thm</u> (Iwasawa) X_K is a fin. gen. torsion Λ-module. ┘

$\mathfrak{X}_K$ is a fin. gen. Λ-module, but not torsion over Λ.

($\mathfrak{X}_K \otimes_\Lambda \mathrm{Frac}(\Lambda) \cong \mathrm{Frac}(\Lambda)^{\oplus r_2(K)}$)

- M : module over $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty^{cyc}/\mathbb{Q})]] = \mathbb{Z}_p[\mathrm{Gal}(K/\mathbb{Q})][[\Gamma_{cyc}]]$

$M_\psi := M \otimes \mathbb{Z}_p[\psi][[\Gamma_{cyc}]]$

for any $\overline{\mathbb{Q}}_p^\times$-valued char. ψ on $\mathrm{Gal}(K/\mathbb{Q})$

- $\Lambda_\psi := \mathbb{Z}_p[\psi][[\Gamma_{cyc}]]$

Def For any f.g. torsion Λ_ψ-modules M, N, M is pseud-isom. to N if the following equivalent conditions hold:

(a) There exists a Λ_ψ-lin. map $M \to N$ whose kernel and cokernel are finite.

(b) For any height one prime $\mathfrak{P}$ of Λ_ψ, the localizations $M_\mathfrak{P}$ and $N_\mathfrak{P}$ at $\mathfrak{P}$ are isomorphic as $\Lambda_{\psi,\mathfrak{P}}$-module. $\lrcorner$

Thm (Kummer duality)

Let $\psi : \mathrm{Gal}(K/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times$ be a even Dirichlet char. We have a pseudo-isom $(X_K)_{\omega\psi^{-1}} \sim ((\mathfrak{X}_K)_\psi)^\iota(-1)$ where ι means twisting Γ_{cyc}-action via the involution $g \in \Gamma_{cyc} \mapsto g^{-1} \in \Gamma_{cyc}$ $\lrcorner$

By Class Field theory, we have the canonical identification

$\{$Dirichlet char. $\eta : \mathbb{Z} \to \overline{\mathbb{Q}}\}$

$\quad \xrightarrow{\sim} \{$Galois char. $G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^{\times}$ of finite order$\}$

Let $L(\eta, s)$ be Dirichlet L-function for any Dirichlet char η.

<u>Recall</u>

(1) $L(\eta, j) \in \mathbb{Q}[\eta]$ for $\forall j \in \mathbb{Z}_{\leq 0}$.

(2) $L(\eta, j) \neq 0$ iff $\eta(-1) = (-1)^{j-1}$ $\lrcorner$

<u>Thm</u> (Kubota-Leopoldt, Iwasawa, Coleman, etc)

Let N be an integer s.t $p^2 \nmid N$ and let ψ be a Dirichlet char. of conductor N s.t $\psi(-1) = 1$.

Then $\exists ! \, L_p(\psi) \in \begin{cases} \Lambda_{\psi} & \text{if } \psi \neq \mathbb{1} \\ \frac{1}{\gamma - 1} \Lambda & \text{if } \psi = \mathbb{1} \end{cases}$

s.t $\quad \kappa_{cyc}^{j} \phi (L_p(\psi)) = \left(1 - \frac{\psi \phi^{-1} \omega^{j-1}(p)}{p^j}\right) L(\psi \phi^{-1} \omega^{j-1}, j)$

for $\forall j \in \mathbb{Z}_{\leq 0}$, $\forall \phi$: finite order char. on Γ_{cyc}.
Here, $\varkappa_{cyc} = \chi_{cyc}|_{\Gamma_{cyc}}$ and ω is the Teichmüller char.
$(\omega : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^{\times} \hookrightarrow \mathbb{Z}_p^{\times})$ $\lrcorner$

For a fin. gen. torsion Λ_ψ-module N,
we put
$$\mathrm{char}_{\Lambda_\psi} N := \prod_{\mathfrak{p} : \mathrm{ht}\, 1 \text{ in } \Lambda_\psi} \mathfrak{p}^{\mathrm{length}_{\Lambda_{\psi,\mathfrak{p}}} N_{\mathfrak{p}}}$$
and we call it the char. ideal of N.

<u>I.M.C</u> ((−)-version)
Let N and ψ be as above. Then, we have:
$$\mathrm{char}_{\Lambda_\psi}(X_{K_{\omega\psi^{-1}}})_{\omega\psi^{-1}} = \begin{cases} (L_p(\psi)) \\ ((\gamma-1)L_p(\psi)) \end{cases}$$ $\lrcorner$

By Kummer theory introduced befone, the abore conj. is equivarent to:

<u>I.M.C</u> ((+)-version)
Let N and ψ be as above. Then, we have:
$$\mathrm{char}_{\Lambda_\psi}(\mathfrak{X}_{K_\psi})_\psi^{?}(-1) = \begin{cases} (L_p(\psi)) \\ ((\gamma-1)L_p(\psi)) \end{cases}$$ $\lrcorner$

Thm (Analytic class number formula)

Let $K = \mathbb{Q}(\zeta_{Np})$ $(N,p)=1$.

Then, we have

$$\prod_{\psi} \mathrm{char}_{\Lambda_{\mathcal{O}}} (X_K)_{\omega\psi^{-1}} = (\gamma - 1) \prod_{\psi} (L_p(\psi))$$

where ψ runs through even char's of $\mathrm{Gal}(K/\mathbb{Q})$

$\mathcal{O} \supset \mathbb{Z}_p[\psi]$ for these ψ's. $\lrcorner$

Rem A similar statement is true for $(\mathcal{X}_K)_\psi$.

Cor If $(\text{alg. ideal})_\psi \supset (\text{anal. ideal})_\psi$ is true for all even char ψ of $\mathrm{Gal}(\mathbb{Q}(\zeta_{Np})/\mathbb{Q})$,

$(\text{alg. ideal})_\psi = (\text{anal. ideal})_\psi$ is true for every ψ.

The same is true for "$\subset$". $\lrcorner$

Historical remark

modular method $\subset$	Euler system method $\supset$
Mazur-Wiles (1984) ($p \neq 2$, $p \nmid \mathrm{order}\ \psi$)	Rubin ($\psi = \omega^i$) appendix to "Lang"
	Rubin's book $p \nmid \mathrm{order}\ \psi$
Wiles (1990) any case	Greither any case