①

LECTURE II – "Iwasawa Theory".

Let $p \neq 2$ be a prime number.
The p-adic integers are equal to

$$\mathbb{Z}_p := \left\{ \sum_{n \geq 0} a_n p^n \;\middle|\; 0 \leq a_n < p \right\}$$

while

$$\mathbb{Q}_p := \mathrm{Frac}(\mathbb{Z}_p).$$

<u>Def:</u> We call $\Lambda = \mathbb{Z}_p[\![X]\!]$ the Iwasawa algebra.

<u>Weierstraß Preparation Theorem:</u>
If $\mathcal{Y}(X) \in \mathbb{Z}_p[\![X]\!]$ is non-zero, then

$$\mathcal{Y}(X) = p^{\mu} \times \prod_{i=1}^{n} f_i(X)^{e_i} \times (\text{a unit})$$

where $\mu \geq 0$, $e_i > 0$ and the $f_i(X) \in \mathbb{Z}_p[X]$ are distinguished polynomials

(so that $f_i(X) = X^{d_i} + c_{d_i-1} X^{d_i-1} + \ldots + c_0$ with $p \mid c_0, \ldots, c_{d_i-1}$.)

<u>Notation:</u> $\mu = \mu(\mathcal{Y})$ "μ-invariant of $\mathcal{Y}$"

and $\lambda = \sum_{i=1}^{n} e_i \times \deg(f_i)$ "λ-invariant of $\mathcal{Y}$"

Structure Theorem:

If M is a finitely-generated compact Λ-module, there is a short exact sequence

$$0 \longrightarrow \text{finite} \longrightarrow M$$
$$\longrightarrow \Lambda^{\oplus r} \oplus \bigoplus_{j=1}^{m} \frac{\Lambda}{p^{\mu_j}} \oplus \bigoplus_{i=1}^{n} \frac{\Lambda}{f_i^{e_i}} \longrightarrow \text{finite} \rightarrow 0$$

of Λ-modules.

<u>N.B.</u> Here • $r \geq 0$ "rank of M"

• $\mu(M) = \sum_{j=1}^{m} \mu_j \geq 0$

• $\lambda(M) = \sum_{i=1}^{n} e_i \times \deg(f_i) \geq 0.$

<u>Def:</u> If $rk_\Lambda(M) = 0$ then we define

$$\text{char}_\Lambda(M) := \prod_{j=1}^{m} p^{\mu_j} \times \prod_{i=1}^{n} f_i(X)^{e_i}.$$

"characteristic series of M"

<u>Fact:</u> If $\mathcal{S}$ is a discrete f.g. Λ-module then $\hat{\mathcal{S}} := \text{Hom}_{\text{cont}}(\mathcal{S}, \mathbb{Q}_p/\mathbb{Z}_p)$ is a compact f.g. Λ-module, and vice versa.

Cyclotomic Fields.

$$
\begin{tikzcd}
 & \mathbb{Q}^{cyc} = \bigcup_{n\geq 1} \mathbb{Q}(e^{2\pi i/p^n}) \arrow[d, dash] \\
\mathbb{Q}_\infty \arrow[ur, dash, "\mathbb{F}_p^\times"] \arrow[d, dash] & \mathbb{Q}(e^{2\pi i/p^n}) \arrow[d, dash] \\
\mathbb{Q} \arrow[r, phantom, "="] & \mathbb{Q}
\end{tikzcd}
$$

$(\mathbb{Z}/p^n\mathbb{Z})^\times$

$\mathbb{Z}_p^\times \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times$

Here $\mathbb{Q}_\infty = H^0(\mathbb{F}_p^\times, \mathbb{Q}^{cyc})$ is the so-called cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

Then $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \cong 1 + p\mathbb{Z}_p$ (multiplicatively)

Remark:

If we fix a topological generator of Γ, say that $\Gamma = \langle \gamma \rangle$, then

$$
\begin{array}{ccc}
\Lambda = \mathbb{Z}_p[[X]] & \xrightarrow{\sim} & \mathbb{Z}_p[[\Gamma]]. \\
\cup\!\!\!\downarrow & & \cup\!\!\!\downarrow \\
1+X & \longmapsto & \gamma
\end{array}
$$

This is an IM of topological rings.

④

$$G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \left(\begin{array}{c} \overline{\mathbb{Q}} \\ | \\ \mathbb{Q}_\infty \\ | \\ \mathbb{Q} \end{array} \right. \begin{array}{l} \left.\begin{array}{c} \\ \\ \end{array}\right\} \mathcal{H}_\infty \\ \left.\begin{array}{c} \\ \\ \end{array}\right\} \Gamma \end{array}$$

Note that $\Gamma \cong G_{\mathbb{Q}} / \mathcal{H}_\infty$.

Clearly Γ acts on $\mathcal{H}_\infty$ via conjugation

$\Longrightarrow$ Γ acts on $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) \subset H^1(\mathcal{H}_\infty, E_{p^\infty})$.

This extends to an action of $\Lambda \cong \mathbb{Z}_p[[\Gamma]]$ by linearity and continuity.

<u>Def:</u> We introduce the compact Λ-module

$$\mathcal{X}_E := \mathrm{Hom}_{\mathrm{cont}}\left(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p\right)$$

for any elliptic curve $E/\mathbb{Q}$.

<u>Hypothesis:</u> From now on we assume that E has good ordinary reduction at p, so that $p \nmid N_E \times a_p(E)$.

⑤ Recall from last lecture the L-function

$$L(E,\chi,s) = \sum_{n\geq 1}^{\infty} a_n(E)\cdot\chi(n)\cdot n^{-s}$$

for $\mathrm{Re}(s) > \frac{3}{2}$.

<u>Theorem:</u> (Mazur–Tate–Teitelbaum)

There exists an $\mathcal{L}_E \in \Lambda[\frac{1}{p}]$ such that

$$\mathcal{L}_E(\chi(\gamma)-1) = * \times \frac{L(E,\chi,1)}{\Omega_E}$$

for each finite order character $\chi : \Gamma \to \mathbb{C}^\times$.

<u>Q1:</u> Is $\mathcal{X}_E$ finitely-generated over Λ?

<u>Q2:</u> Does $\mathrm{rk}_\Lambda(\mathcal{X}_E) = 0$?

<u>Q3:</u> If so, what is the link between $\mathrm{char}_\Lambda(\mathcal{X}_E)$ and $\mathcal{L}_E$?

⑥ Using results of Poitou & Tate, there is a commutative diagram

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] \\
\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \arrow[r, "\alpha_E"] \arrow[d] & \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty) \arrow[d] \\
H^1(G_{\mathbb{Q}}, E_{p^\infty}) \arrow[r, "\beta_E"] \arrow[d, "\prod \mathrm{res}_\ell"] & H^1(\mathcal{H}_\infty, E_{p^\infty}) \arrow[d, "\prod \mathrm{res}_w"] \\
\prod_\ell \dfrac{H^1(G_{\mathbb{Q}_\ell}, E_{p^\infty})}{\delta^{\mathrm{Kum}}(E(\mathbb{Q}_\ell)\otimes \mathbb{Q}_p/\mathbb{Z}_p)} \arrow[r, "\prod \delta_{E,\ell}"] \arrow[d] & \prod_\ell \prod_{w|\ell} \dfrac{H^1(\mathcal{H}_{\infty,w}, E_{p^\infty})}{\delta^{\mathrm{Kum}}(E(\mathbb{Q}_{\infty,w})\otimes \mathbb{Q}_p/\mathbb{Z}_p)} \arrow[d] \\
\vdots & \vdots
\end{tikzcd}$$

with exact columns.

<u>Control Theorem:</u> (Mazur)

The mapping

$$\alpha_E : \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \longrightarrow H^0(\Gamma, \mathrm{Sel}(E/\mathbb{Q}_\infty))$$

has finite kernel & cokernel.

⑦

As a corollary,

$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ cofinitely generated over $\mathbb{Z}_p$

Mazur

$\Rightarrow$ $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^\Gamma$ cofinitely-generated over $\mathbb{Z}_p$

$\Rightarrow$ $(\mathcal{X}_E)_\Gamma$ is finitely-generated over $\mathbb{Z}_p$

$\Rightarrow$ $\mathcal{X}_E$ is a finitely-generated Λ-module.

Nakayama's Lemma

Interlude – the Riemann zeta-function.

Let χ be a Dirichlet character of conductor f_χ, so that

$$\chi : (\mathbb{Z}/f_\chi\mathbb{Z})^\times \longrightarrow \overline{\mathbb{Q}}^\times.$$

Consider the L-function

$$L(\chi, s) = \sum_{n=1}^{\infty} \chi(n)\cdot n^{-s}, \quad \mathrm{Re}(s) > 1.$$

Then

$$L(\chi,1) = \begin{cases} \pi i \dfrac{\mathcal{G}_\chi}{f_\chi^2} \times \displaystyle\sum_{a=1}^{f_\chi} \overline{\chi}(a)\, a & \text{if } \chi(-1) = -1 \\[2ex] -\dfrac{\mathcal{G}_\chi}{f_\chi} \times \displaystyle\sum_{a=1}^{f_\chi} \overline{\chi}(a) \log\left|1 - e^{2\pi i a/f_\chi}\right| & \text{if } \chi(-1) = +1. \end{cases}$$

8

Let $\zeta_m = e^{2\pi i/m}$ at any $m \geq 1$.

For even characters χ, there is a link

$$L(\chi, 1) \xleftrightarrow[\text{formula}]{\text{Euler's}} \log|1-\zeta_m| \quad \text{with } m = f_\chi.$$

Nice Properties:

(a) The units of $\mathbb{Q}(\zeta_{p^n}) \cap \mathbb{R}$ are generated by -1 and $\zeta_{p^n}^{\frac{1-a}{2}} \times \dfrac{1-\zeta_{p^n}^a}{1-\zeta_{p^n}}$ with $\text{g.c.d.}(a,p) = 1$.

(b) Let ℓ be a prime, $\ell \neq p$. Then

$$\mathrm{Norm}_{\mathbb{Q}(\zeta_{m\ell})/\mathbb{Q}(\zeta_m)}(1-\zeta_{m\ell}) = \begin{cases} \dfrac{1-\zeta_m}{1-\zeta_m^{\mathrm{Frob}_\ell^{-1}}} & \text{if } \ell \nmid m \\ 1-\zeta_m & \text{if } \ell \mid m \end{cases}$$

where $\mathrm{Frob}_\ell : x \mapsto x^\ell$.

"Sideways Compatibility"

ⓒ R. Coleman devised a mapping on $\varprojlim_n \mathcal{O}^\times_{\mathbb{Q}(\mu_{p^n})}$ which converted the elements $\left(\frac{1-\zeta_{p^n}^a}{1-\zeta_{p^n}}\right)_{n\geq 1}$ into the p-adic Riemann zeta-function

$$\zeta_{p\text{-adic}}(\chi\omega^j, X) \in \tilde{\Lambda}.$$

ⓓ Finally, using the analytic class no. formula and ⓐ – ⓒ, K. Rubin proved for even characters $\chi\omega^j$:

$$\mathrm{char}_\Lambda\left(A_\infty^{(\chi\omega^j)}\right) = (\gamma_0^a - 1)\cdot \zeta_{p\text{-adic}}(\chi\omega^j, -)$$

where $A_\infty = \varprojlim_n$ class gp. of $\mathbb{Q}(\zeta_{p^n})$.

"Classical Iwasawa Main Conjecture"