Note : Axiomatic Lattice Construction

2023/11/3

We will start with Ribet's lattice construction and then move to Wiles' generalization (actually due to Urban, ...).

§1 Lattice construction à la Ribet

The so-called lattice construction is the following theorem in the manner of Urban.

Theorem A Let $\rho : \mathrm{Gal}_{\mathbb{Q}} \to GL_2(K)$ be an irreducible Galois rep'n with

$$\mathrm{tr}\,\rho \equiv \chi_1 + \chi_2 \mod \varpi_K$$

for characters $\chi_i : \mathrm{Gal}_{\mathbb{Q}} \to O_K^\times$ that are distinct modulo ϖ_K. Then $\exists$ a lattice $M \subseteq K^2$ s.t.

(i) M is $\mathrm{Gal}_{\mathbb{Q}}$-stable

(ii) The lattice $\overline{M} := M \bmod \varpi_K$ is a nonsplit extension between χ_1 and $\chi_2 \bmod \varpi_K$.

Proof : Diagonalize :

Observe $\det(\rho(\sigma_1)) = \frac{1}{2}\left(\mathrm{tr}(\rho(\sigma_1)^2 - \mathrm{tr}(\rho(\sigma_1^2))\right)$, we see (exercise)

$$\det(XI - \rho(\sigma)) \equiv (X - \chi_1(\sigma))(X - \chi_2(\sigma)) \mod \varpi_K \quad -(*)$$

Since χ_1 and χ_2 are distinct mod ϖ_K, $\exists\, \sigma_0 \in \mathrm{Gal}_{\mathbb{Q}}$ such that the charpoly $\det(XI - \rho(\sigma_0))$ has distinct roots mod ϖ_K by $(*)$. Using Hensel's lemma, the roots lift to distinct eigenvalues in O_K.

$\Longrightarrow \exists$ a basis $\{v_1, v_2\}$ of K^2 such that

$$\rho(\sigma_0) = \begin{pmatrix} \alpha_1 & \\ & \alpha_2 \end{pmatrix}, \quad \alpha_i \in O_K, \quad \alpha_i \equiv \chi_i(\sigma_0) \mod \varpi_K.$$

Under this basis, for $\sigma \in O_K[\mathrm{Gal}_{\mathbb{Q}}]$, we write $\rho(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$.

Then we claim : (note : $a_\sigma, b_\sigma, c_\sigma, d_\sigma$ a priori lies in K, but they are not group homomorphisms $\mathrm{Gal}_{\mathbb{Q}} \to K$ in general).

① for all $\sigma, \tau \in O_K[\mathrm{Gal}_{\mathbb{Q}}]$, $a_\sigma, d_\sigma, b_\sigma c_\tau \in O_K$, and

$$a_\sigma \equiv \chi_1(\sigma), \quad d_\sigma \equiv \chi_2(\sigma), \quad b_\sigma c_\tau \equiv 0 \mod \varpi_K.$$

② $\mathcal{C}$ be the O_K-submodule of K generated by all $c_\sigma \in K$.
Then $\mathcal{C}$ is a nonzero fractional ideal of K.

Proof of claim 1 :

- Start with an observation : $\forall\ \sigma \in \mathrm{Gal}_{\mathbb{Q}}$, $\mathrm{tr}(\rho(\sigma)) \in \mathcal{O}_K$.

  b/c : $\mathrm{tr}(\rho(\mathrm{Frob}_\ell)) = a_\ell(F) \in \mathcal{O}_K$ for $\ell \neq p$. As $\{\mathrm{Frob}_\ell\}_{\ell \neq p}$ is a dense subset of $\mathrm{Gal}_{\mathbb{Q}}$. by continuity $\mathrm{tr}(\rho(\sigma)) \in \mathcal{O}_K$.

  Or from the assumption : $\mathrm{tr}\,\rho \equiv \chi_1 + \chi_2 \bmod \varpi_K$. By assumption, $\chi_i : \mathrm{Gal}_{\mathbb{Q}} \to \mathcal{O}_K^\times$ so it inexplicitly implies $\mathrm{tr}\rho(\sigma) \in \mathcal{O}_K$ for any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$.

- Then we realize a_σ, d_σ, $b_\sigma c_\tau$ as traces of particular elements in $\mathcal{O}_K[\mathrm{Gal}_{\mathbb{Q}}]$

  Take
  $$\mathcal{E}_1 = \frac{1}{\alpha_1 - \alpha_2}(\sigma_0 - \alpha_2) \in \mathcal{O}_K[\mathrm{Gal}_{\mathbb{Q}}]$$
  $$\mathcal{E}_2 = \frac{1}{\alpha_2 - \alpha_1}(\sigma_0 - \alpha_1) \in \mathcal{O}_K[\mathrm{Gal}_{\mathbb{Q}}].$$

  ? linear-algebraic interpretation of $\mathcal{E}_1$ and $\mathcal{E}_2$.

  Then one checks
  $$\rho(\mathcal{E}_1) = \frac{1}{\alpha_1 - \alpha_2}\left(\begin{pmatrix}\alpha_1 & \\ & \alpha_2\end{pmatrix} - \begin{pmatrix}\alpha_2 & \\ & \alpha_2\end{pmatrix}\right) = \begin{pmatrix}1 & 0 \\ 0 & 0\end{pmatrix}$$
  $$\rho(\mathcal{E}_2) = \frac{1}{\alpha_2 - \alpha_1}\left(\begin{pmatrix}\alpha_1 & \\ & \alpha_2\end{pmatrix} - \begin{pmatrix}\alpha_1 & \\ & \alpha_1\end{pmatrix}\right) = \begin{pmatrix}0 & 0 \\ 0 & 1\end{pmatrix}$$

  Then we see

  * $\rho(\mathcal{E}_1\sigma) = \rho(\mathcal{E}_1)\rho(\sigma) = \begin{pmatrix}1 & 0 \\ 0 & 1\end{pmatrix}\begin{pmatrix}a_\sigma & b_\sigma \\ c_\sigma & d_\sigma\end{pmatrix} = \begin{pmatrix}a_\sigma & b_\sigma \\ 0 & 0\end{pmatrix}$

    hence $a_\sigma = \mathrm{tr}(\rho(\mathcal{E}_1\sigma)) \in \mathcal{O}_K$
    $$\equiv \chi_1(\mathcal{E}_1\sigma) + \chi_2(\mathcal{E}_1\sigma) \bmod \varpi_K$$
    $$\equiv \chi_1(\sigma) \bmod \varpi_K$$

    as $\chi_1(\mathcal{E}_1) = \frac{1}{\alpha_1 - \alpha_2}(\chi_1(\sigma_0) - \alpha_2) \equiv \frac{1}{\alpha_1 - \alpha_2}(\alpha_1 - \alpha_2) = 1 \bmod \varpi_K$

    $\chi_2(\mathcal{E}_1) = \frac{1}{\alpha_2 - \alpha_1}(\chi_2(\sigma_0) - \alpha_2) \equiv 0 \bmod \varpi_K$

  * Similarly consider $\rho(\mathcal{E}_2\sigma)$, we obtain results on d_σ. (exercise)

- Moreover, as $\rho(\sigma)\rho(\tau) = \rho(\sigma\tau)$,
  $$\begin{pmatrix}a_\sigma & b_\sigma \\ c_\sigma & d_\sigma\end{pmatrix}\begin{pmatrix}a_\tau & b_\tau \\ c_\tau & d_\tau\end{pmatrix} = \begin{pmatrix}a_{\sigma\tau} & b_{\sigma\tau} \\ c_{\sigma\tau} & d_{\sigma\tau}\end{pmatrix}.$$

  hence $a_{\sigma\tau} = a_\sigma a_\tau + b_\sigma c_\tau$. This implies
  $$b_\sigma c_\tau = a_{\sigma\tau} - a_\sigma a_\tau \in \mathcal{O}_K \quad \text{since } a_\sigma \in \mathcal{O}_K,\ \forall \sigma \in \mathcal{O}_K[\mathrm{Gal}_{\mathbb{Q}}].$$
  $$\equiv \chi_1(\sigma\tau) - \chi_1(\sigma)\chi_1(\tau) \bmod \varpi_K$$
  $$= 0 \bmod \varpi_K.$$
  □

Proof of claim 2 :

- $\mathfrak{C}$ is nonzero because ρ is irreducible.
- $\mathfrak{C}$ is a fractional ideal since $\mathrm{Gal}_{\mathbb{Q}}$ is compact.

  Pourquoi? Suffices to consider $c : \mathrm{Gal}_{\mathbb{Q}} \to K$. This is a continuous map (even though c is not a group homomorphism). So $\mathrm{im}(c) \subseteq K$ is compact since $\mathrm{Gal}_{\mathbb{Q}}$ is compact. Therefore it is possible to find (?) some $a \in \varpi^N \mathcal{O}_K$ s.t. $a \cdot \mathrm{im}(c) \subseteq \mathcal{O}_K$, making $\mathfrak{C}$ a fractional ideal of $\mathcal{O}_K \subseteq K$.

Back to the construction of the lattice

Consider M to be the $\mathcal{O}_K[\mathrm{Gal}_{\mathbb{Q}}]$-lattice generated by v_1. We compute

$$\rho(\sigma) v_1 = (v_1, v_2) \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (v_1, v_2) \begin{pmatrix} a_\sigma \\ c_\sigma \end{pmatrix} = a_\sigma v_1 + c_\sigma v_2$$

So actually $M \simeq \mathcal{O}_K v_1 \oplus \mathfrak{C} v_2$. (recall Claim① $\Rightarrow a_\sigma \in \mathcal{O}_K$). Then we have

☹ — $0 \longrightarrow M_2 := \mathfrak{C} v_2 \longrightarrow M \longrightarrow M/M_2 \simeq \mathcal{O}_K v_1 =: M_1 \longrightarrow 0$.

1° For $m_2 = c_\tau v_2 \in M_2$, we compute

- $\rho(\sigma) m_2 = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \begin{pmatrix} 0 \\ c_\tau \end{pmatrix} = \begin{pmatrix} b_\sigma c_\tau \\ d_\sigma c_\tau \end{pmatrix} = b_\sigma c_\tau v_1 + d_\sigma c_\tau v_2 \in M$.

2° For $m_1 = a v_1 \in M_1$, we compute

- $\rho(\sigma) m_1 = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \begin{pmatrix} a \\ 0 \end{pmatrix} = a_\sigma \cdot a v_1 + a c_\sigma \cdot v_2 \in M$.

But everything gets better when we do reduction mod ϖ_K.

Note : (1) The sequence ☹ is ONLY a (of course split) extension of $\mathcal{O}_K$-modules, but it is NOT $\mathrm{Gal}_{\mathbb{Q}}$-equivariant, as we can see from the computation 1° and 2° that M_2 and M_1 are NOT $\mathrm{Gal}_{\mathbb{Q}}$-stable.

(2) By we say "mod ϖ_K", we do NOT mean mod ϖ_K directly on ☹ ($- \otimes_{\mathcal{O}_K} \mathcal{O}_K/\varpi$ may not be exact actually). We mean moding M_2 and M by ϖ_K, check $\overline{M}$ and $\overline{M}_2$ are $\mathrm{Gal}_{\mathbb{Q}}$-stable and form the quotient $\overline{M}/\overline{M}_2$.

Reduction mod ϖ_K : We claim :

③ $\overline{M_2} := M_2/\varpi_K M_2$ is a $\mathrm{Gal}_{\mathbb{Q}}$-stable $\Bbbk$-line with χ_2-action.

④ The quotient $\mathrm{Gal}_{\mathbb{Q}}$-module $\overline{M}/\overline{M_2}$ is a $\Bbbk$-line with χ_1-action.

Along the proof of the above two claims, we will see $\overline{M}$ is $\mathrm{Gal}_{\mathbb{Q}}$-stable.

Proof of claim ③ : $\forall\, m_2 = c_\tau v_2 \in M_2$, $c_\tau \in \mathcal{O}$ for some $\tau \in \mathrm{Gal}_{\mathbb{Q}}$.

Then written in coordinates

$$\rho(\sigma) m_2 = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \begin{pmatrix} 0 \\ c_\tau \end{pmatrix} = \begin{pmatrix} b_\sigma c_\tau \\ d_\sigma c_\tau \end{pmatrix} = b_\sigma c_\tau v_1 + d_\sigma c_\tau v_2 \in M_2$$

hence modulo ϖ_K,

$$\rho(\sigma) m_2 = b_\sigma c_\tau v_1 + d_\sigma m_2 \equiv 0 + \chi_2(\sigma) m_2 = \chi_2(\sigma) m_2 \mod \varpi_K,$$

by Claim ①. The claim then follows. □

Proof of claim ④ : $\forall\, m_1 = \bar{a} v_1 \in \overline{M}/\overline{M_2} \simeq \mathcal{O}_K/\varpi_K v_1$ for some $a \in \mathcal{O}_K$. Then similarly

$$\rho(\sigma) m_1 = a_\sigma \cdot \bar{a} v_1 + \bar{a} c_\sigma \cdot v_2 \overset{\text{"mod } v_2\text{"}}{=\!=} a_\sigma \cdot a v_1 \text{ in } M_1$$

hence modulo ϖ_K, $\rho(\sigma) m_1 \equiv \chi_1(\sigma) m_1 + 0 = \chi_1(\sigma) m_1 \mod \varpi_K$, by Claim ①. □

The reduction mod ϖ_K gives $\overline{M}$ over $\mathcal{O}_K/\varpi_K =: \Bbbk$.

Now as $\mathcal{O}_K/\varpi_K \simeq \mathcal{O}/\varpi_K \mathcal{O} \simeq \Bbbk$, we obtain an extension

$$0 \to \Bbbk(\chi_2) \to \overline{M} \to \Bbbk(\chi_1) \to 0 \quad \circlearrowleft \mathrm{Gal}_{\mathbb{Q}} \qquad \text{— (}\ast\ast\text{)}$$

from modulo ϖ_K from $0 \to M_2 \to M \to M_1 \to 0$ (of course split). We claim :

(∗∗) is nonsplit.

b/c : Suppose otherwise there were a splitting $s : \overline{M} \to \Bbbk(\chi_2)$:

$$0 \to \Bbbk(\chi_2) \underset{s}{\leftarrow} \overline{M} \to \Bbbk(\chi_1) \to 0 \quad \circlearrowleft \mathrm{Gal}_{\mathbb{Q}}.$$

Let $\bar{v}_1 := v_1 \mod \varpi_K$. Then

- $\rho(\sigma_b) s(\bar{v}_1) \equiv \chi_2(\sigma_b) s(\bar{v}_1) \equiv \alpha_2 s(\bar{v}_1) \mod \varpi_K$.
- Since s is $\mathrm{Gal}_{\mathbb{Q}}$-equivariant,

$$\rho(\sigma_b) s(\bar{v}_1) = s(\rho(\sigma_b)\bar{v}_1) \overset{\text{by definition}}{=} s(\overline{\rho(\sigma_b) v_1}) = s(\alpha_1 \bar{v}_1) = \alpha_1 s(\bar{v}_1) \mod \varpi_K.$$

Since $\alpha_1 \neq \alpha_2 \mod \varpi_K$, they force $s(\bar{v}_1) = 0$ in $\Bbbk(\chi_2)$. This is absurd as $\bar{v}_1$ generates $\overline{M}$ over $\mathcal{O}_K[\mathrm{Gal}_{\mathbb{Q}}]$. □

By the construction, we have obtained a nonsplit Galois-extension

$$0 \longrightarrow \Bbbk(\chi_2) \longrightarrow \bar{M} \longrightarrow \Bbbk(\chi_1) \longrightarrow 0 .$$

Twisted by χ_1^{-1}, we get a nonsplit Galois-extension

$$0 \longrightarrow \Bbbk(\chi_2\chi_1^{-1}) \longrightarrow \bar{M}(\chi_1^{-1}) \longrightarrow \Bbbk \longrightarrow 0 .$$

It gives a nontrivial cohomology class in $H^1(\mathbb{Q}, \Bbbk(\chi_2\chi_1^{-1}))$.

Remark :

(1) We can replace "mod ϖ_K" by "mod ϖ_K^n" for some $n \in \mathbb{N}$ everywhere in the statement and the proof. This viewpoint is adopted in Wiles' generalization.
(Then of course $\Bbbk$ should be replaced by $\Bbbk := \mathcal{O}_K/\varpi_K^n$)

(2) The theorem can further be generalized by Bellaïche & Chenevier to :

- $\mathcal{O}_K$ is a local Henselian ring
- $\bar{\rho}^{ss}$ is the sum of mutually nonisomorphic irreducible repns

See Bellaïche & Chenevier "Families of Galois repns and Selmer groups".

Local Property: Let p be a fixed prime.

The background of this part is the following theorem of Mazur–Wiles:

Theorem (Mazur–Wiles) For an ordinary form f, $\exists$ a basis $\{w_1, w_2\}$ of K^2 such that

$$\rho_f\big|_{\mathrm{Gal}_{\mathbb{Q}_p}} = \begin{pmatrix} \beta^{-1}\omega^{k-1} & * \\ 0 & \beta \end{pmatrix}$$

where β is the unramified character $\beta : \mathrm{Gal}_{\mathbb{Q}_p} \longrightarrow \overline{\mathbb{Q}}_p^{\times}$ such that $\beta(\mathrm{Frob}_p)$ is the unit root of $X^2 - a_p(f)X + p^{k-1}$.

In particular, we further restrict ρ_f to the inertia I_p,

$$\rho_f\big|_{I_p} = \begin{pmatrix} \omega^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

Note: Even in Ribet's case, we may be oversimplified: in general ρ_f is unramified outside Np for f of level N. One cheating way is to construct f of level p. This is what Ribet did.

Recall in Theorem A, a KEY assumption is that

$$\mathrm{tr}\,\rho \equiv \chi_1 + \chi_2 \mod \varpi_K$$

for distinct characters $\chi_i : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow \mathcal{O}_K^{\times} \mod \varpi_K$. This is called the "distinguished property", i.e. $\exists\, \sigma_0 \in \mathrm{Gal}_{\mathbb{Q}}$ s.t.

$$\chi_1(\sigma_0) \not\equiv \chi_2(\sigma_0) \mod \varpi_K \qquad -(*)$$

To get local properties, we require further

(a) "distinguished at p": which means $\exists\, \sigma_0 \in \mathrm{Gal}_{\mathbb{Q}_p} \subseteq \mathrm{Gal}_{\mathbb{Q}}$ s.t. $(*)$ holds.

⇓ seems to have no implication !

(b) "upper triangular at p": then as the above argument goes, we get a basis $\{v_1, v_2\}$ s.t. $\rho(\sigma_0) = \begin{pmatrix} \alpha_1 & \\ & \alpha_2 \end{pmatrix} \equiv \begin{pmatrix} \chi_1(\sigma_0) & \\ & \chi_2(\sigma_0) \end{pmatrix}$. We further require that under this basis,

$$\rho(\sigma) = \begin{pmatrix} \chi_1'(\sigma) & * \\ 0 & \chi_2'(\sigma) \end{pmatrix} \quad \text{for } \sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$$

for some characters $\chi_1', \chi_2' : \mathrm{Gal}_{\mathbb{Q}_p} \longrightarrow \mathcal{O}_K^{\times}$ s.t. for $\sigma \in \mathrm{Gal}_{\mathbb{Q}_p}$, $\chi_i(\sigma) \equiv \chi_i'(\sigma) \mod \varpi_K$ for $i = 1, 2$.

(c) ρ is unramified outside p, i.e. I_ℓ acts trivially for $\ell \neq p$.

Then by the above three assumptions, we see the extension class $[\overline{M}]$ splits everywhere locally, i.e. restricting to I_v-actions for all places v of $\mathbb{Q}$, $\overline{M}$ splits:

- 1° is stated to guarantee the existence of the basis $\{v_1, v_2\}$ to claim 2°. And 2° implies $c_\sigma = 0$ for all $\sigma \in I_p$.
- 3° implies that $c_\sigma = 0$ for all $\sigma \in I_\ell$, $\ell \neq p$.

So altogether $c|_{I_v} = 0$ for all places v of $\mathbb{Q}$. Then dating back to M_1, we see $M_1 = \mathcal{O}_K v_1$ with I_v-action on $m_1 = a v_1 \in M_1$

$$\begin{pmatrix} a_\sigma & b_\sigma \\ 0 & d_\sigma \end{pmatrix} \begin{pmatrix} a \\ 0 \end{pmatrix} = a_\sigma \cdot a v_1 = a_\sigma m_1$$

is I_v-stable for any $\sigma \in I_v$ (v any place of $\mathbb{Q}$). So M_1 itself is a submodule of M. Hence $[\overline{u}]$ splits everywhere locally.

§2 Lattice Construction à la Wiles

Upshot : Ribet's argument is the "local picture" of Wiles' approach !

Setup :

- $\Lambda := $ cyclotomic Iwasawa algebra $\cong \mathbb{Z}_p[\![T]\!]$.
- $\mathbb{I}$: a reduced ring which is a finite Λ-module.
- $I \subseteq \mathbb{I}$, $J \subseteq \Lambda$ be two ideals such that $\Lambda \longrightarrow \mathbb{I} \twoheadrightarrow \mathbb{I}/I$ induces $\Lambda/J \xrightarrow{\sim} \mathbb{I}/I$

~~(Question : Does this implies that for any $t>0$, $\Lambda/J^t \xrightarrow{\sim} \mathbb{I}/I^t$? I'm afraid not necessarily. So do we need to modify the arguments ?)~~ ×

- We fix a height one prime $\mathfrak{p}$ of Λ such that $\mathrm{ord}_{\mathfrak{p}}(J) > 0$

§2.1 Some (vague) commutatie algebra

The first trouble is that $\mathbb{I}$ may not be an integral domain.

(1) Total ring of fractions :

Let $S := \{ f \in R \mid f \text{ is not a zero divisor in } R \}$.

Then this is a multiplicatie subset of R. We call $Q(R) := S^{-1}R$ the total ring of fractions. When R is an integral domain, $Q(R) = \mathrm{Frac}(R)$

For reduced rings R with finitely many minimal primes $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$,

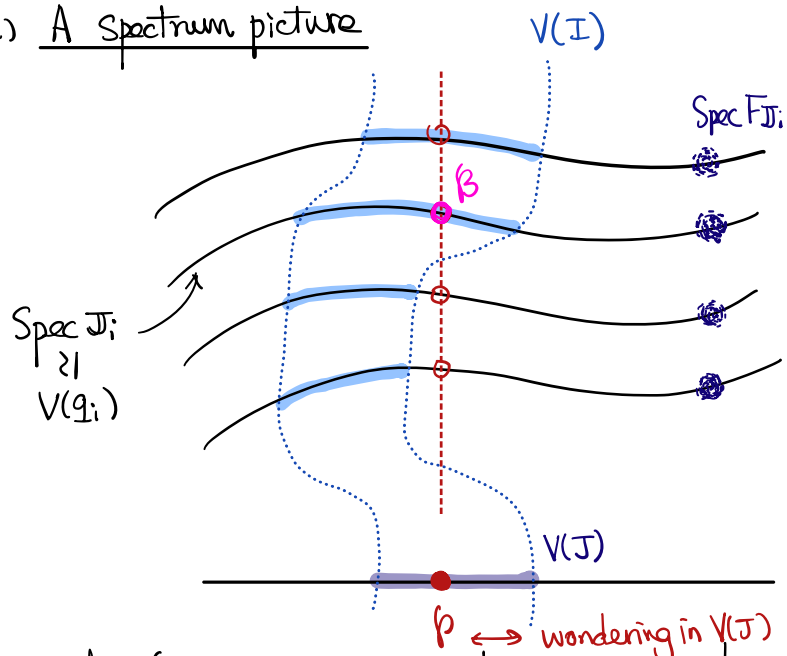
$$\mathbb{K} := Q(R) = R_{\mathfrak{q}_1} \times \cdots \times R_{\mathfrak{q}_t}$$

where the localizations $R_{\mathfrak{q}_i}$ are fields. Moreover, for minimal ideals $\mathfrak{q}$ in R,

$$R_{\mathfrak{q}} = \mathrm{Frac}(R/\mathfrak{q})$$ (Need to check this in more detail)

So we can also write $\mathbb{K} = Q(R) = F_{\mathbb{J}_1} \times \cdots \times F_{\mathbb{J}_t}$, where $\mathbb{J}_i = R/\mathfrak{q}_i$ and $F_{\mathbb{J}_i}$ is its fraction fields.

(2) A Spectrum picture



$= \{ \beta \in \operatorname{Spec} \mathbb{I} : \beta \supseteq I \}$

$\operatorname{Spec} \mathbb{I}/I \simeq V(I) \simeq \operatorname{Spec} \mathbb{I}/I$

$\downarrow$

$\operatorname{Spec} \mathbb{I} \hookleftarrow \operatorname{Spec} \mathfrak{J}_i = \operatorname{Spec} \mathbb{I}/q_i$ $\cong$

$\downarrow$

$\operatorname{Spec} \Lambda \hookleftarrow V(J) \simeq \operatorname{Spec} \Lambda/J$

Take $\beta \in \operatorname{Spec} \mathbb{I}$ as in the picture, then β is a prime ideal of $\mathbb{I}$ containing (p, I) of height one in $\operatorname{Spec} \mathbb{I}$.

Some commutatie algebra problem: $\forall\, i = 1, \dots, t$

- Lying over: $\Lambda \to \mathbb{I} \to \mathbb{I}/q_i$ is finite hence integral. As Λ and $\mathfrak{J}_i$ are integral domains, we see: $\exists\, \beta$ in $\operatorname{Spec} \mathfrak{J}_i$ s.t. $\beta \cap \Lambda = p$
- Going up: the going up property is satisfied, so $\operatorname{height}(\beta) \geq \operatorname{height}(p) = 1$.
- Going down: problem is the "going down" property: it is required that $\mathfrak{J}_i$ is integrally closed. Is it ok for us to take the integral closure of $\mathfrak{J}_i$? Should be ok!

  ↑ check: $K = Q(\mathbb{I}) = \prod_{i=1}^{t} F_{\mathfrak{J}_i} \overset{(?)}{=} \prod_{i=1}^{t} F_{\overline{\mathfrak{J}}_i}$, where $\overline{\mathfrak{J}}_i$ is the integral closure of $\mathfrak{J}_i$.

  $\Longrightarrow \operatorname{height}(\beta) \leq \operatorname{height}(p) = 1$.

So the prime β obtained by lying over satisfies $\operatorname{height}(\beta) = \operatorname{height}(p) = 1$.

- Irreducible decomposition: Actually $\operatorname{Spec} \mathbb{I} = \bigcup_{i=1}^{t} \operatorname{Spec} \mathfrak{J}_i$ is an irreducible decomposition. For the closed set $V(I)$, we do the samething, then $V(I) \cap \operatorname{Spec} \mathfrak{J}_i \neq \emptyset$ for some i. By that $\operatorname{ord}_p(J) > 0$, we can take $\beta_1 \in V(I) \cap \operatorname{Spec} \mathfrak{J}_i$ as above. (a little bit vague.)

From here we see that it's natural to focus on one single irreducible component $\mathrm{Spec}\,\mathbb{I}_i$, with $\mathbb{I}_i$ an integrally closed integral domain of fraction field K_i.

§2.2 Some "Axioms"

Let $\rho: G_{\mathbb{Q}} \longrightarrow GL(V)$. $V \simeq \mathbb{I}^{\oplus 2}$ and $\rho_{\mathbb{I}_i}: G_{\mathbb{Q}} \to GL(V_i)$, $V_i \simeq F_{\mathbb{I}_i}$ be the projection via $\mathbb{I} \hookrightarrow Q(I) = F_{\mathbb{I}_1} \times \cdots \times F_{\mathbb{I}_t} \twoheadrightarrow F_{\mathbb{I}_i}$

(LC.1) Each $\rho_{\mathbb{I}_i}$ on $F_{\mathbb{I}_i}^{\oplus 2}$ is irreducible. $i = 1, \cdots, t$.

(LC.2) There are $\Lambda^\times$-valued characters χ_1, χ_2 of $G_{\mathbb{Q}}$ such that

$$\mathrm{tr}\,\rho(\sigma) \equiv \chi_1(\sigma) + \chi_2(\sigma) \mod J.$$

(LC.3) There are $\mathbb{I}^\times$-valued characters χ_1', χ_2' of $G_{\mathbb{Q}_p}$ such that

$$\rho|_{G_{\mathbb{Q}_p}} \simeq \begin{pmatrix} \chi_1' & * \\ 0 & \chi_2' \end{pmatrix}$$

and some $\sigma_0 \in G_{\mathbb{Q}_p}$ s.t. $\chi_1'(\sigma_0) \not\equiv \chi_2'(\sigma_0) \mod \mathfrak{p}$.

(LC.4) For each $\sigma \in \mathbb{I}[\mathrm{Gal}_{\mathbb{Q}_p}]$, $\chi_1(\sigma) \equiv \chi_1'(\sigma) \mod I$ for $i = 1, 2$.

(LC.5) ρ is unramified outside p.

Then we define the Selmer module $X := H^1_{ur}(\mathbb{Q}, \Lambda^*(\chi_2^{-1}\chi_1))^*$, where $(-)^*$ means the Pontragin dual, i.e. $M^\times := \mathrm{Hom}_{cts}(M, \mathbb{Q}_p/\mathbb{Z}_p)$.

Main result: For the fixed height one prime $\mathfrak{p}$, $\mathrm{ord}_{\mathfrak{p}}\left(\mathrm{char}_\Lambda(X)\right) \geq \mathrm{ord}_{\mathfrak{p}}(J)$.

Remark: Actually in the proof (of Wan in his course or his Iwasawa 2012 article, I guess), people inexplicitly replaced $\mathbb{I}$ by $\mathbb{I}_i$ and require it to be integrally closed, and $\mathfrak{p} \in \mathbb{I}_i$ is a height one prime of $\mathbb{I}_i$ containing (I, p). Then $\mathbb{I}_{i,\mathfrak{p}}$ is a DVR ($\mathbb{I}_i$ is an integrally closed noetherian domain, so as $\mathfrak{p}$ is a height one prime, $\dim \mathbb{I}_{i,\mathfrak{p}} = \mathrm{height}(\mathfrak{p}) = 1$. So $\mathbb{I}_{i,\mathfrak{p}}$ is a DVR). In other words, WMA $\mathbb{I}$ itself is an integral domain over Λ that is integrally closed.

§2.3 Proof of main result

(1) Diagonalize : Take the $\sigma_0 \in \mathrm{Gal}_{\mathbb{Q}_p}$ in (LC.3). Then as in Ribet's proof of the Hensel-like argument (so we do need $\mathbb{I}$ is ~~complete~~ henselian under $\mathfrak{p}$-adic topology for the height one prime $\mathbb{I}$? Does it follow from that Λ is complete under the (p,T)-topology hence the p-topology and note $\mathbb{I}$ is finite over Λ ? Here is a GAP ! [Hsieh2014, P90] : finite + reduced Λ-alg $\overset{(?)}{\Longrightarrow}$ Henselian)

$\exists$ a basis $\{v_1, v_2\}$ of V s.t.

$$\rho(\sigma_0) = \begin{pmatrix} \alpha_1 & \\ & \alpha_2 \end{pmatrix} \qquad \alpha_i \equiv \chi_i(\sigma_0) \bmod \mathfrak{p}, \quad i=1,2. \qquad \alpha_1, \alpha_2 \in \mathbb{I}$$

We write $\rho(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$ for any $\sigma \in \mathbb{K}[\mathrm{Gal}_{\mathbb{Q}}]$ wrt the basis $\{v_1, v_2\}$.

Denote $r = \alpha_1 - \alpha_2$. Then $r \equiv \chi_1'(\sigma_0) - \chi_2'(\sigma_0) \neq 0 \bmod \mathfrak{p}$, hence $r \notin \mathfrak{p}$.

(2) We claim ① $r a_\sigma,\ r d_\sigma,\ r^2 b_\sigma c_\tau \in \mathbb{I}$ for any $\sigma, \tau \in \mathbb{I}[\mathrm{Gal}_{\mathbb{Q}}]$.

$$r a_\sigma \equiv r\chi_1'(\sigma), \quad r d_\sigma \equiv r\chi_2'(\sigma), \quad r^2 b_\sigma c_\tau \equiv 0 \bmod I.$$

② $\mathcal{C} = \{ c_\sigma : \sigma \in \mathbb{I}[\mathrm{Gal}_{\mathbb{Q}}] \}$ is a finite faithful Λ-module.

③ $c_\sigma = 0$ for any $\sigma \in I_p$.

Proof of claim ① : again note that $\mathrm{tr}(\rho(\sigma)) \in \mathbb{I}$.

- Let $\delta_1 = \sigma_0 - \alpha_2 \in \mathbb{I}[\mathrm{Gal}_{\mathbb{Q}}]$.

(Compare : in Ribet's proof, we set $\varepsilon_1 = \frac{1}{\alpha_1 - \alpha_2}(\sigma_0 - \alpha_2) \in \mathcal{O}_K[\mathrm{Gal}_{\mathbb{Q}}]$
There, $r = \alpha_1 - \alpha_2$ is invertible in $\mathcal{O}_K$ since $\alpha_1 - \alpha_2 \equiv \chi_1(\sigma) - \chi_2(\sigma) \neq 0 \bmod w$
Here through, $r \notin \mathfrak{p}$ but we cannot see r is invertible. This can be settled by localizing $\mathbb{I}$ at $\mathfrak{p}$.)

Then $\rho(\delta_1) = \rho(\sigma_0) - \rho(\sigma_2) = \begin{pmatrix} \alpha_1 & \\ & \alpha_2 \end{pmatrix} - \begin{pmatrix} \alpha_2 & \\ & \alpha_2 \end{pmatrix} = \begin{pmatrix} r & \\ & 0 \end{pmatrix}$.

Then $\rho(\delta_1\sigma) = \rho(\delta_1)\rho(\sigma) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} = \begin{pmatrix} r a_\sigma & r b_\sigma \\ 0 & 0 \end{pmatrix}$

so $\mathrm{tr}(\rho(\delta_1\sigma)) = r a_\sigma \in \mathbb{I}$. and moding I,

$\Big\|$ (LC.2)

$$\chi_1(\delta_1\sigma) + \chi_2(\delta_1\sigma) \equiv r\chi_1'(\sigma) \bmod I \qquad (*)$$

here (*) because $\chi_1(\delta_1) = \chi_1(\sigma_0) - \alpha_2 \overset{(LC.4)}{\equiv} \alpha_1 - \alpha_2 \equiv r \mod I$

$\chi_2(\delta_1) = \chi_2(\sigma_0) - \alpha_2 \overset{(LC.4)}{=} 0 \mod I$.

So we see the proof is essentially the same as Ribet's. So we omit the proof here.

Ribet's

Proof of Claim② : (I'm confused here)

- (LC1) (irreducibleness) $\Longrightarrow$ faithfulness of $\mathcal{C}$. $\overset{\text{compare}}{\longleftrightarrow}$ $\mathcal{C}$ is nonzero.
- $\mathrm{Gal}_{\mathbb{Q}}$ is compact $\Longrightarrow$ finiteness of $\mathcal{C}$. $\overset{\text{compare}}{\longleftrightarrow}$ $\mathcal{C}$ is a fractional ideal of O_K

Proof of Claim③ : follows directly from (LC.3).

(3) Back to the construction of the lattice

- Define $M = \mathbb{I}_\beta[\mathrm{Gal}_{\mathbb{Q}}]v_1$. Then $M \simeq \mathcal{C}_\beta v_2 \oplus \mathbb{I}_\beta v_1$.

  Let $M_2 := \mathcal{C}_\beta v_2$. Then

$$0 \to M_2 \to M \to M/M_2 =: M_1 \simeq \mathbb{I}_\beta v_1 \to 0$$

  but not as $\mathbb{I}_\beta[\mathrm{Gal}_{\mathbb{Q}}]$-module, instead only as $\mathbb{I}_\beta$-modules.

- Things again get better by moding out I_β in $\mathbb{I}_\beta$. Write $\Bbbk = \mathbb{I}_\beta / I\mathbb{I}_\beta$.

$$0 \to \overline{M_2} \to \overline{M} \to \overline{M_1} \to 0. \quad - (*)$$

  Then as in Ribet's claim③ and ④, note here $r \in \mathbb{I}_\beta$ is invertible (!), we see:

  ③ $\overline{M_2}$ is a $\Bbbk$-line with $\mathrm{Gal}_{\mathbb{Q}}$-action by χ_2'.

  ④ $\overline{M_1}$ is a $\Bbbk$-line with $\mathrm{Gal}_{\mathbb{Q}}$-action by χ_1'.

  Note: In [Wan. Iwasawa2012 article, p50], he claimed $\overline{M_2}$ is a direct summand of $\overline{M}$. This is quite absurd? Especially compared with Ribet's argument. Actually next we would like to show that (*) is nonsplit.

  Moreover, by the same proof as Ribet's, we see that (*) does not split!

Now except the "local property", we have imitated Ribet's proof above.

Next: after all, $\mathbb{I}_\beta$ is not we really want. We try to lift the story over $\mathbb{I}$!

(4) Lift to $\mathbb{I}$

Recall previously we obtained $0 \to \Bbbk(\chi_2) \to \overline{\mathcal{M}} \to \Bbbk(\chi_1) \to 0$ a short exact sequence of $\mathrm{Gal}_{\mathbb{Q}}$-modules over $\Bbbk$. Then we try to lift it to $\mathbb{I}$. This is not as difficult as we may think.

- Define $\mathcal{M} :=$ the $\mathbb{I}[\mathrm{Gal}_{\mathbb{Q}}]$-module generated by v_1. Then we lift:

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & \mathcal{M}_2 & \longrightarrow & \mathcal{M} = \mathbb{I}[\mathrm{Gal}_{\mathbb{Q}}]v_1 & \longrightarrow & \mathcal{M}_1 & \to & 0 \quad / \mathbb{I} \\
0 & \longrightarrow & \mathcal{M}_2 & \longrightarrow & M = \mathbb{I}_\beta[\mathrm{Gal}_{\mathbb{Q}}]v_1 & \longrightarrow & M_1 & \to & 0 \quad / \mathbb{I}_\beta \\
0 & \longrightarrow & \overline{\mathcal{M}}_2 & \longrightarrow & \overline{\mathcal{M}} = \Bbbk[\mathrm{Gal}_{\mathbb{Q}}]v_1 & \longrightarrow & \overline{\mathcal{M}}_1 & \to & 0 \quad / \Bbbk, \circlearrowleft \mathrm{Gal}_{\mathbb{Q}} \\
 & & \circlearrowleft \chi_2 & & & & \circlearrowleft \chi_1 & &
\end{array}
$$

i.e. let $\mathcal{M}_2 := \mathcal{M} \cap \overline{\mathcal{M}}_2$, $\mathcal{M}_1 = \mathcal{M}/\mathcal{M}_2 \subseteq \overline{\mathcal{M}}_1$, (The precise meaning should be reflected as in the diagram above.) and the $\mathrm{Gal}_{\mathbb{Q}}$-action on $\mathcal{M}_i$ is χ_i' for $i = 1, 2$.

- By definition, $\mathcal{M}_{2,\beta} = \overline{\mathcal{M}}_2$ — Goal (i)
- By Claim ③ and (LC.5), ※ splits under I_ℓ-action for any prime ℓ of $\mathbb{Q}$.
- Note: In [Wan, Iwasawa 2012, p50], he said
  - "$\overline{\mathcal{M}}_1$ is isomorphic to $\Lambda/\mathfrak{p}^t$". This should be incorrect. $\overline{\mathcal{M}}_1$ is localized so it should be $\Lambda_{\mathfrak{p}}/\mathfrak{p}^t$. Note that $t = \mathrm{ord}_{\mathfrak{p}}(J)$. We are in the case $\Lambda_{\mathfrak{p}}$ is a DVR, so $\Lambda_{\mathfrak{p}}/J\Lambda_{\mathfrak{p}} \simeq \Lambda_{\mathfrak{p}}/\mathfrak{p}^t$. This is under the condition that $\Lambda/J \simeq \mathbb{I}/I$, so no problem using Λ not $\mathbb{I}$.
  - Then he said "it is easy to see $\mathcal{M}_1 \simeq \Lambda/\mathfrak{p}^t$". Why it is easy since localization $(-) \otimes_{\Lambda} \Lambda_{\mathfrak{p}}$ may not be "faithfully flat"? And even more importantly, where did we used this description?

So twisting by χ_1^{-1}, this gives us a useful extension

※' — $0 \to \mathcal{M}_2(\chi_2\chi_1^{-1}) \to \mathcal{M}(\chi_1^{-1}) \to \mathcal{M}_1 \to 0 \quad \in H^1_{ur}\left(\mathbb{Q}, \mathcal{M}_2(\chi_2\chi_1^{-1})\right)$.

(5) End of the proof : connection to the Selmer module.

Compare with Theorem A, actually we have ended in gaining a desired extension. Next the problem is how to apply it to bound the Selmer module.

Claim | Goal (ii) | There exists a Λ-linear map $X \to \mathfrak{M}_2$, that is a surjection after localizing at $\mathfrak{p}$.

Proof of the claim :

(a) Construct such a map :

- Let $[\mathfrak{M}] :=$ the extension (※)'. Then by functoriality, we immediately get

$$\theta : \mathrm{Hom}_\Lambda(\mathfrak{M}_2, \Lambda^*) \longrightarrow H^1_{ur}(\mathbb{Q}, \Lambda^*(\chi_2\chi_1^{-1}))$$
$$\varphi \longmapsto \varphi_*[\mathfrak{M}],$$

where φ_* is the induced $H^1_{ur}(\mathbb{Q}, \mathfrak{M}_2(\chi_2\chi_1^{-1})) \longrightarrow H^1_{ur}(\mathbb{Q}, \Lambda^*(\chi_2\chi_1^{-1}))$.

- Take the Pontryagin dual of θ :

$$\theta^* : X = H^1_{ur}(\mathbb{Q}, \Lambda^*(\chi_2\chi_1^{-1}))^* \longrightarrow \mathrm{Hom}_\Lambda(\mathfrak{M}_2, \Lambda^*)^* \xrightarrow[(\star)]{\simeq} \mathfrak{M}_2$$

Here (★) is some "linear algebra" :

$$\mathrm{Hom}_\Lambda(\mathfrak{M}_2, \Lambda^*)^* = \mathrm{Hom}_\Lambda\left(\mathfrak{M}_2, \mathrm{Hom}_{cts}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)\right)^*$$
$$\overset{(?)}{=} \mathrm{Hom}_{cts}\Big(\underbrace{\mathfrak{M}_2 \otimes_\Lambda \Lambda}_{\simeq \mathfrak{M}_2}, \mathbb{Q}_p/\mathbb{Z}_p\Big)^* \quad \text{"some adjointness"}$$
$$= (\mathfrak{M}_2)^{**} \overset{(?)}{=} \mathfrak{M}_2.$$

We need to find references to support the (?) here !

Here the θ^* is the Λ-linear map we want. So we need to show θ^* is surjective after localizing at $\mathfrak{p}$. By Pontragin duality, it suffices to show θ is injective after localizing at $\mathfrak{p}$. i.e. Let $\mathcal{R} := \ker\theta$, then we show $\mathcal{R}_\mathfrak{p} = 0$.

(b) Show $R_{\mathfrak{p}} = 0$. I'm confused here (?)

- Let S be any finite subset of $R \subseteq \mathrm{Hom}_{\Lambda}(M_2, \Lambda^*)$. Then consider $M_S = \bigcap_{\varphi \in S} \ker\varphi \subseteq M_2$. Naturally we have

$$0 \longrightarrow \frac{M_2}{M_S} \xrightarrow{\prod_{\varphi\in S}\varphi} \prod_{\varphi\in S} \Lambda^* \longrightarrow \text{the quotient} \longrightarrow 0 \qquad /\Lambda$$

and equip each term a $\mathrm{Gal}_{\mathbb{Q}}$-action by $\chi_2\chi_1^{-1}$

- Take the Galois cohomology long exact sequence.

$$\mathcal{K} := \ker\left(H^1\left(\mathbb{Q}, \frac{M_2}{M_S}(\chi_2\chi_1^{-1})\right) \longrightarrow H^1\left(\mathbb{Q}, \left(\prod_{\varphi\in S}\Lambda^*\right)(\chi_2\chi_1^{-1})\right)\right)$$

we see $\mathcal{K}$ is a quotient of $\left(\dfrac{\left(\prod_{\varphi\in S}\Lambda^*\right)(\chi_2\chi_1^{-1})}{\left(\frac{M_2}{M_S}\right)(\chi_2\chi_1^{-1})} \right)^{\mathrm{Gal}_{\mathbb{Q}}}$. Observe:

- By definition, the image of $[M]$ in $H^1\left(\mathbb{Q}, \frac{M_2}{M_S}(\chi_2\chi_1^{-1})\right)$ lies in $\mathcal{K}$.
- $\mathcal{K}$ is killed by $1-\chi_2\chi_1^{-1}(\sigma_0) \notin \mathfrak{p}$. (By (LC.4), $\chi_i(\sigma_0) \equiv \chi_i'(\sigma_0)$, $i=1,2$. so actually we argue $1-\chi_2'(\chi_1')^{-1}(\sigma_0) \notin \mathfrak{p}$, so go back we see that)

So $[M] \in H^1\left(\mathbb{Q}, \frac{M_2}{M_S}(\chi_2\chi_1^{-1})\right)$ is killed by an element outside $\mathfrak{p}$. This implies that the extension

$$0 \longrightarrow \frac{M_2}{M_S}(\chi_2\chi_1^{-1}) \longrightarrow \frac{M}{M_S}(\chi_1^{-1}) \longrightarrow M_1 \longrightarrow 0$$

splits after localizing at $\mathfrak{p}$, ie. (omitting the bracket indicating Galois action),

$$0 \longrightarrow \frac{M_{2,\mathfrak{p}}}{M_{S,\mathfrak{p}}} \longrightarrow \frac{M_{\mathfrak{p}}}{M_{S,\mathfrak{p}}} \longrightarrow M_{1,\mathfrak{p}} \longrightarrow 0$$

splits as $\Lambda_{\mathfrak{p}}[\mathrm{Gal}_{\mathbb{Q}}]$-modules.

- Then this implies that $M_{2,\mathfrak{p}} = M_{S,\mathfrak{p}}$, since (Pourquoi ?) otherwise it would contradicts to that M is generated by v_1 over $\mathbb{I}[\mathrm{Gal}_{\mathbb{Q}}]$.
- Therefore by arbitarity of S, "$M_{2,\mathfrak{p}} = M_{S,\mathfrak{p}}$" implies that $R_{\mathfrak{p}} = 0$, this proves the claim.

(6) Finally final :

- Preparation : Fitting ideals (cf. [Mazur-Wiles, Appendix])
  - Let R be a ring, M be a finitely presented R-module. Then we can define an ideal $\mathrm{Fitt}_R^0(M)$ of R. (Omit the defintion but only list some properties)
    ① $M \twoheadrightarrow M'$ a surjection, then $\mathrm{Fitt}_R(M) \subseteq \mathrm{Fitt}_R(M')$
    ② $I \subseteq R$ any ideal, then $\mathrm{Fitt}_{R/I}(M/IM) = \mathrm{Fitt}_R M$ in R/I.
    More generally, for $R \to S$, $\mathrm{Fitt}_S(M \otimes_R S) = \mathrm{Fitt}_R(M)$ in S.
    ③ Let M be a direct sum of cyclic R-modules $M = R/\pi_1 \times \cdots \times R/\pi_s$. Then
    $$\mathrm{Fitt}_R(M) = \pi_1 \cdot \cdots \cdot \pi_s .$$
  - Suppose R is a DVR of uniformizer ϖ and M is finitely generated torsion R-mod then by the structure theorem,
    $$M \simeq R/\varpi^{n_1} \times \cdots \times R/\varpi^{n_s} \qquad \text{④}$$
    So by ③, $\mathrm{Fitt}_R(M) = \varpi^{\sum_{i=1}^s n_i}$. So coincidentally, $\mathrm{Fitt}_R(M) = \mathrm{char}_R(M)$.
  - Exercise : In general, including the Iwasawa module case, the two are not the same :
    1° Find examples s.t. $\mathrm{char}_R(-)$ does not respect base change.
    2° See [Ochiai, p36] for the "$\neq$"-example.
    3° Let M be a finitely generated torsion Λ-module, then
    $$\mathrm{char}_\Lambda(M) = \mathrm{Fitt}_\Lambda(M)^{\vee\vee}, \text{ where } (-)^{\vee\vee} \text{ is the double } \Lambda\text{-dual}.$$

- So now we are ready !
$$\begin{aligned}
\mathrm{ord}_p(\mathrm{char}_\Lambda(X)) &= \mathrm{ord}_p(\mathrm{char}_{\Lambda_p}(X_p)) \\
&= \mathrm{ord}_p(\mathrm{Fitt}_{\Lambda_p}(X_p)) && \text{by ④} \\
&\leq \mathrm{ord}_p(\mathrm{Fitt}_{\Lambda_p}(M_{2,p})) && \text{by ① + Goal (ii)} \\
&= \mathrm{ord}_p(\mathrm{Fitt}_{\Lambda_p}(\overline{M_2})) && \text{by Goal (i)}
\end{aligned}$$

Moreover,
$$\mathrm{Fitt}_{\Lambda_p}(\overline{M_2}) \bmod J \overset{②}{=} \mathrm{Fitt}_{\Lambda_p/J\Lambda_p}(\overline{M_2}) = \mathrm{Fitt}_{\mathbb{I}_\beta/I\mathbb{I}_\beta}(\overline{M_2}) \overset{②}{=} \mathrm{Fitt}_{\mathbb{I}_\beta} M_2 \bmod I = 0$$

The last equality follows from the previous claim ② that $\mathfrak{u}_2$ is a finite faithful $\mathbb{I}_\beta$-module. Hence $\mathrm{Fitt}_{\Lambda_\beta}(\overline{\mathfrak{u}}_2) \subseteq J$.

- Putting these altogether, we see $\mathrm{ord}_\beta(\mathrm{char}_\Lambda(X)) \leq \mathrm{ord}_\beta(J)$, as desired.

□

§ Appendix : Some background on Hecke algebras

In Wiles' axiomatic proof, one might be confused at what $\mathbb{T}, I, J$ really is.
In this appendix, I hope to provide some background.

§ A.1 Hecke algebras and congruence of modular forms

Let $S_k(\Gamma_1(N), \mathbb{C})$ be the space of weight k, level N holomorphic cusp forms.

Recall : The Hecke $\mathbb{Z}$-algebra $\mathbb{T}_{\mathbb{Z}}$ is defined as the subring inside $\mathrm{End}_{\mathbb{C}}(S_k(\Gamma_1(N), \mathbb{C}))$ generated by all Hecke operators. Similar for cusp forms.

Let R be a ring (i.e. $\mathbb{Z}$-algebra), define Hecke R-algebra as $\mathbb{T}_R := \mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R$.
Then by the q-expansion principle (see Talk 2), we have

$$\begin{array}{ccc} S_k(\Gamma_1(N), R) & \xrightarrow{1:1} & \mathrm{Hom}_{R\text{-Mod}}(\mathbb{T}_R, R) \\ f & \longmapsto & (T \mapsto a_1(Tf)) \\ f(q) = \sum_{n \geq 1} \Phi(T_n) q^n & \longleftarrow & \Phi \end{array}$$

moreover, the normalized eigenform in $S_k(\Gamma_1(N), R)$ are precisely corresponds to the R-algebra homomorphisms $\Phi : \mathbb{T}_R \to R$, called the eigensystem of f.

Case 1 : $R = K$ is a field with fixed seperable closure $\overline{K}$.
Then we have the bijective correspondence

$$\mathrm{Spec}(\mathbb{T}_K) \xleftrightarrow{1:1} \mathrm{Hom}_{K\text{-alg}}(\mathbb{T}_K, \overline{K}) / \mathrm{Gal}_K \xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{normalized eigenforms} \\ \text{in } S_k(N, \overline{K}) \end{array} \right\} / \mathrm{Gal}_K$$

In particular when $K = \overline{K}$,

$$\mathrm{Spec}(\mathbb{T}_K) \xleftrightarrow{1:1} \mathrm{Hom}_{K\text{-alg}}(\mathbb{T}_K, \overline{K}) \xleftrightarrow{1:1} \left\{ \begin{array}{c} \text{normalized eigenforms} \\ \text{in } S_k(N, \overline{K}) \end{array} \right\}$$

Case 2 : Let $\mathcal{O}$ be a finitely generated $\mathbb{Z}$-module, an integral domain of char zero.
Consider $\widehat{\mathcal{O}}$: completion of $\mathcal{O}$ at a maximal prime of $\mathcal{O}$.
(What in mind : $\mathcal{O} = \mathbb{Z}$ or integer ring $\mathcal{O}_K$ of number fields.
$\widehat{\mathcal{O}} = \mathbb{Z}_p$ or completion of $\mathcal{O}_K$ at a finite place)

Then we have :

- $K := $ fraction field of $\widehat{\mathcal{O}}$.
- $\mathbb{F} := $ residue field of $\widehat{\mathcal{O}}$

Fact ① : $\mathbb{T}_{\widehat{\mathcal{O}}}$ is a free $\widehat{\mathcal{O}}$-module of finite rank.

Fact ② : $\operatorname{Kdim}(\mathbb{T}_{\widehat{\mathcal{O}}}) = 1$.

So we decompose $\operatorname{Spec}\mathbb{T}_{\widehat{\mathcal{O}}} = \operatorname{MinSpec}\mathbb{T}_{\widehat{\mathcal{O}}} \sqcup \operatorname{MaxSpec}\mathbb{T}_{\widehat{\mathcal{O}}}$ where :

- $\operatorname{MinSpec}\mathbb{T}_{\widehat{\mathcal{O}}} =$ minimal primes.
- $\operatorname{MaxSpec}\mathbb{T}_{\widehat{\mathcal{O}}} =$ maximal primes.

(note : inexplicitly, every minimal prime is properly contained in a maximal prime)

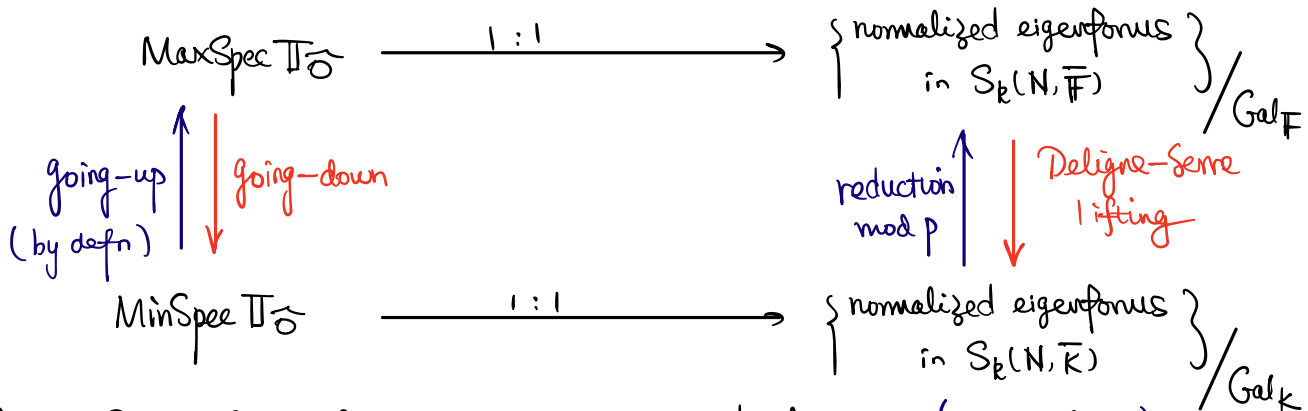
Fact ③ : Consider $\widehat{\mathcal{O}} \xrightarrow{\pi} \mathbb{F}$, inducing $\mathbb{T}_{\widehat{\mathcal{O}}} \xrightarrow{\pi} \mathbb{T}_{\mathbb{F}}$, then

$$\begin{array}{ccccc} \operatorname{MaxSpec}\mathbb{T}_{\widehat{\mathcal{O}}} & \xrightarrow{1:1} & \operatorname{Spec}\mathbb{T}_{\mathbb{F}} & \xrightarrow[1:1]{\text{Fact ①}} & \left\{\text{normalized eigenforms in } S_k(N,\overline{\mathbb{F}})\right\}/\mathrm{Gal}_{\mathbb{F}} \\ \mathfrak{m}^c = \pi^{-1}(\mathfrak{m}) & \longleftarrow & \mathfrak{m} & & \end{array}$$

Fact ④ : Consider $\widehat{\mathcal{O}} \hookrightarrow K$, inducing $\mathbb{T}_{\widehat{\mathcal{O}}} \hookrightarrow \mathbb{T}_K$, then

$$\begin{array}{ccccc} \operatorname{MinSpec}\mathbb{T}_{\widehat{\mathcal{O}}} & \xrightarrow{1:1} & \operatorname{Spec}\mathbb{T}_K & \xrightarrow[1:1]{\text{Fact ①}} & \left\{\text{normalized eigenforms in } S_k(N,\overline{K})\right\}/\mathrm{Gal}_K \\ \mathfrak{p} & \longmapsto & \iota(\mathfrak{p})\mathbb{T}_K = \mathfrak{p}^e & & \end{array}$$

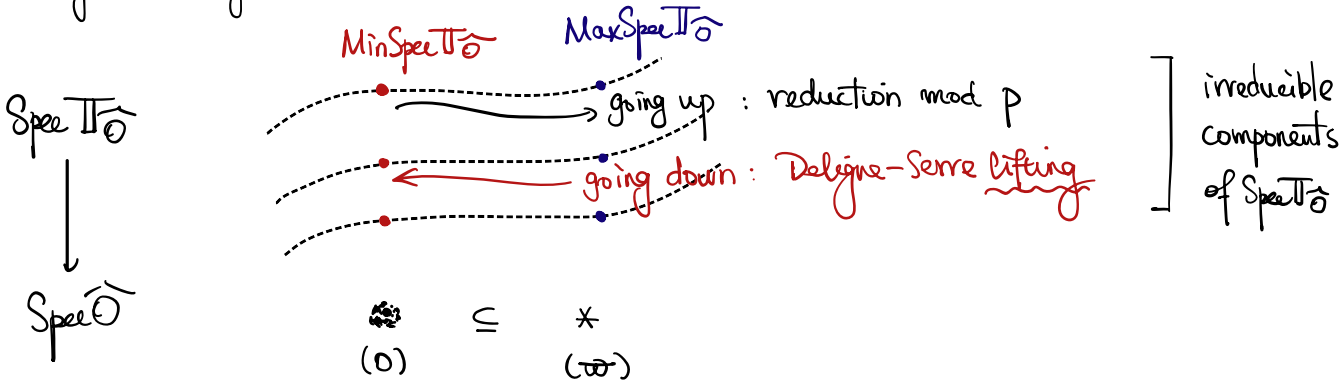
$\Longrightarrow$ Combining **Fact ③** & **Fact ④**, the spectrum of $\mathbb{T}_{\widehat{\mathcal{O}}}$ allows us to phrase elegantly when (conjugacy classes of) normalized eigenforms are congruence modulo (a prime lying above) $\mathfrak{p}$.



So the Deligne-Serre lifting theorem is equivalent to the (particular) going-down property of $\mathbb{T}_{\widehat{\mathcal{O}}}$: this follows easily by the flatness of $\mathbb{T}_{\widehat{\mathcal{O}}}$ over $\widehat{\mathcal{O}}$.

Proof: By Fact①, $\mathbb{T}_{\widehat{\mathcal{O}}}$ is flat over $\widehat{\mathcal{O}}$. The result follows when observing $(0) \subsetneq \mathfrak{m}\widehat{\mathcal{O}}$ is a proper chain of prime ideals, where $\widehat{\mathcal{O}}$ is the completion of $\widehat{\mathcal{O}}$ wrt. $\mathfrak{m}$. □

So topologically drawing a picture:



So geometrically speaking, we see "Hecke algebra" $\mathbb{T}_{\widehat{\mathcal{O}}}$ is quite a "universal object"

Then question: a "universal" Galois representation?

i.e. we hope to see a "Hecke algebra-valued" Galois representation

$$\rho_{\mathbb{T}} : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow GL_2\left((\mathbb{T}_{\widehat{\mathcal{O}}})_{\mathrm{red}}\right)$$

s.t. for any normalized eigenform $f \in S_k(\Gamma_1(N), \bar{K})$ corresponding to the minimal prime $\mathfrak{q}_f$, the projection of $\rho_{\mathbb{T}}$ to the component of $\mathfrak{q}_f$ induces

$$\rho_f : \mathrm{Gal}_{\mathbb{Q}} \longrightarrow GL_2\left((\mathbb{T}_{\widehat{\mathcal{O}}})_{\mathrm{red}}\right) \xrightarrow[\text{total ring of fractions}]{\text{first pass to its}} GL_2\left((\mathbb{T}_{\widehat{\mathcal{O}}})_{\mathrm{red}}, \mathfrak{q}_f\right)$$

that is the usual Galois representation attached to f, i.e. Deligne's construction.

Remark: Since the Galois rep is "determined" by the characteristic poly of $\mathrm{Frob}_{\mathbb{Q}}$-action, the "coincides with Deligne" fact is not hard to verify once we know the corresponding information of $\rho_{\mathbb{T}}$.

Actually this is how Deligne constructed the Galois rep if we really dive into details. The "$GL_2((\mathbb{T}_{\widehat{\mathcal{O}}})_{\mathrm{red}})$" maybe weird b/c we are secretely taking a basis. The rep space is actually the "(étale) parabolic coh. space" with Galois action!

— See 李文威《模形式初步》第十章的细节.

§ A.2. Wiles' case

(1) We expect the similar description on $\mathrm{Spec}(\mathbb{T}_N^{\circ})$. but I cannot found any reference.

(2) We have similar machinary for Galois representations : [Hida, GME 2ed, §4.2.2] especi [Thm.4.2.2, Cor0.4.2.3, loc.cit].