* Cyclicity of adjoint Selmer groups and fundamental units

Haruzo Hida
Department of Mathematics, UCLA,
Los Angeles, CA 90095-1555, U.S.A.

A talk in Iwasawa 2017
at University of Tokyo.

*The author is partially supported by the NSF grant: DMS 1464106.

Generalizing a result of Cho–Vatsal (Crelle, 2003), we prove cyclicity over the Hecke algebra of the adjoint Selmer group of each modular deformation of an induced irreducible representation of a finite order character $\mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{F}}_p$ for a real quadratic field F under mild conditions.

A conjecture.
Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(W)$ be an odd absolutely irreducible Artin representation with coefficients in a complete discrete valuation ring W with finite residue field $\mathbb{F}$ of characteristic $p \nmid |\mathrm{Im}(\rho)|h$ for the class number h of the splitting field of $Ad(\rho)$. Suppose $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} = \left(\begin{smallmatrix}\epsilon & * \\ 0 & \delta\end{smallmatrix}\right)$ with unramified δ. Let $\overline{\rho} := \rho \mod \mathfrak{m}_W$.

Conjecture: *Suppose $p > 3$ and $\epsilon \not\equiv \delta \mod \mathfrak{m}_W$. For the minimal p-ordinary universal deformation $\rho_{\mathbb{T}}$ of $\overline{\rho}$ with values in $\mathrm{GL}_2(\mathbb{T})$ for the universal ring $\mathbb{T}$, Pontyagin dual of $\mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee$ is pseudo isomorphic to $\mathbb{T}/(L_p)$ as $\mathbb{T}$-modules for a non-zero divisor $0 \neq L_p \in \mathbb{T}$.*

Here $Ad(\rho_{\mathbb{T}})$ acts on $\mathfrak{sl}_2(\mathbb{T})$ by $x \mapsto \rho_{\mathbb{T}}(\sigma)x\rho_{\mathbb{T}}(\sigma)^{-1}$. The algebra $\mathbb{T}$ is an algebra over the Iwasawa algebra $\Lambda = W[[\Gamma]] = W[[T]]$ (with $t = 1+T$) by $\det \rho_{\mathbb{T}}$ factoring through $\Gamma := \mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p(\mu_p))$, and the element $L_p \neq 0$ is the adjoint p-adic L-function $L_p(Ad(\rho_{\mathbb{T}}))$ interpolating $L(1, Ad(\rho_P))$ (for arithmetic points $P \in \mathrm{Spec}(\mathbb{T})$) up to units in $\mathbb{T}$.

§0. Setting over a real quadratic field.

In this lecture, we deal with the case where $\rho = \mathrm{Ind}_F^{\mathbb{Q}} \varphi$ for a real quadratic field F and a character $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W^{\times}$.

Here is our setting:

• F: a real quadratic field with discriminant D and a **fundamental unit** ε. Let ς be the generator of $\mathrm{Gal}(F/\mathbb{Q})$.

• Pick a character $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \overline{\mathbb{Q}}^{\times}$ with mod p reduction $\overline{\varphi}$ with values in $\mathbb{F}$ (and put $W = W(\mathbb{F})$). Let $\varphi^{-}(\sigma) = \varphi(\sigma\widetilde{\varsigma}\sigma^{-1}\widetilde{\varsigma}^{-1})$ and $\overline{\delta}(\sigma) = \overline{\varphi}(\widetilde{\varsigma}\sigma\widetilde{\varsigma}^{-1})$ for $\widetilde{\varsigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with $\widetilde{\varsigma}|_F = \varsigma$.

• Let K^{-}/F be the maximal p-abelian anticyclotomic extension unramified outside p. Anticyclotomy means that $\widetilde{\varsigma}\sigma\widetilde{\varsigma}^{-1} = \sigma^{-1}$ for $\sigma \in \mathrm{Gal}(K^{-}/F)$. Let $\Gamma_{-} := \mathrm{Gal}(K^{-}/F) \cong \mathrm{Gal}(K_{\mathfrak{p}}/F)$ (a finite group), where $K_{\mathfrak{p}}$ is the maximal p-abelian extension unramified outside $\mathfrak{p}$.

Assume

• $p \nmid h_F$ for the class numbe h_F of F and $(p) = \mathfrak{p}\mathfrak{p}^{\varsigma}$ in O with $\mathfrak{p} \neq \mathfrak{p}^{\varsigma}$ for the generator ς of $\mathrm{Gal}(F/\mathbb{Q})$.

§**1. Cyclicity theorem.** Write $\mathfrak{f}$ for the prime-to-p-conductor of $\overline{\varphi}$ and put $N = DN_{F/\mathbb{Q}}(\mathfrak{c})$ (the level). For the conductor $\mathfrak{c}$ of φ, we suppose $\mathfrak{f}|\mathfrak{c}|\mathfrak{f}\mathfrak{p}$. Suppose
(H1) $\mathfrak{f}|\mathfrak{c}|\mathfrak{c}\mathfrak{p}$ and $N_{F/\mathbb{Q}}(\mathfrak{c})$ is square-free (so, N is cube-free),
(H2) p is prime to $N\prod_{l|N}(l-1)$ for prime factors l of N,
(H3) φ^- has order at least 3 with $\varphi^-(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)) \neq \{1\}$,
(H4) the class number h_F of F is prime to p.
We describe a proof of

Theorem A: *Under* (H1–4), *if the class number* $h_{F(\varphi^-)}$ *of the splitting field* $F(\varphi^-)$ *of* φ^- *is prime to* p, $\mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee \cong \mathbb{T}/(L_p)$ *as* $\mathbb{T}$*-modules for a non-zero divisor* $L_p \in \mathbb{T}$*.*

Note that Γ_- is a finite cyclic p-group (under (H4)), and we see

$$W[\Gamma_-] \cong \Lambda/(\langle\varepsilon\rangle - 1) \quad \text{for } \langle\varepsilon\rangle := t^{\log_p(\varepsilon)/\log_p(1+p)}.$$

§2. **Cyclicity and Hecke algebra.** The cyclicity follows from a **ring theoretic assertion** on the big ordinary Hecke algebra $\mathbf{h}$ as Spec($\mathbb{T}$) is a **connected component** of Spec($\mathbf{h}$). We identify the Iwasawa algebra $\Lambda = W[[\Gamma]]$ with the one variable power series ring $W[[T]]$ by $\Gamma \ni \gamma = (1+p) \mapsto t = 1+T \in \Lambda$. Take a Dirichlet character $\psi : (\mathbb{Z}/Np\mathbb{Z})^\times \to W^\times$, and consider the big ordinary Hecke algebra $\mathbf{h}$ (over Λ) of prime-to-p level N and the character ψ. We just mention here the following three facts about $\mathbf{h}$ which has $\mathbb{T}$ as a local factor:

• $\mathbf{h}$ is an algebra flat over the Iwasawa (weight) algebra $\Lambda := W[[T]]$ **interpolating** p-ordinary Hecke algebras of level Np^{r+1}, of weight $k+1 \geq 2$ and of character $\epsilon\psi\omega^{-k}$, where $\epsilon : \mathbb{Z}_p^\times \to \mu_{p^r}$ ($r \geq 0$) and $k \geq 1$ vary. If N is cube-free, $\mathbf{h}$ is a **reduced** algebra;
• Each prime $P \in$ Spec($\mathbf{h}$) has a unique Galois representation

$$\rho_P : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\kappa(P)),\ \mathrm{Tr}\rho_P(\mathrm{Frob}_l) = T(l) \bmod P (l \nmid Np)$$

for the residue field $\kappa(P)$ of P;
• $\rho_P|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \begin{pmatrix} \epsilon_P & * \\ 0 & \delta_P \end{pmatrix}$ with unramified quotient character δ_P.

§3. **Ring theoretic setting.** Since $\mathbb{T}$ is universal among p-ordinary deformations of $\overline{\rho} := \rho \bmod \mathfrak{m}_W$ with certain extra properties insensitive to the twist $\rho \mapsto \rho \otimes \chi$ for $\chi = \left(\frac{F/\mathbb{Q}}{}\right)$, $\mathbb{T}$ has an **algebra involution** σ over Λ coming from the twist. For any ring A with an involution σ, we put $A_\pm = A^\pm := \{x \in A | \sigma(x) = \pm x\}$. Then $A_+ \subset A$ is a subring and A_- is an A_+-module.

• For the ideal $I := \mathbb{T}(\sigma - 1)\mathbb{T}$ of $\mathbb{T}$ generated by $\mathbb{T}_-$ (the "$-$" eigenspace), we have a canonical Λ-algebra isomorphism

$$\mathbb{T}/I \cong W[\Gamma_-]$$

of Cho–Vatsal, where the Λ-algebra structure is given by sending $u \in \Gamma$ naturally into $u \in O_{\mathfrak{p}}^\times = \mathbb{Z}_p^\times$ and then projecting the local Artin symbol $\tau = [u, F_{\mathfrak{p}}] = [u, \mathbb{Q}_p] \in \Gamma$ to $\sqrt{\tau\widetilde{\varsigma}\tau^{-1}\widetilde{\varsigma}^{-1}} = \tau^{(1-\varsigma)/2} \in \Gamma_-$. By this we have $\mathbb{T}/I \cong W[\Gamma_-] \cong \Lambda/(\langle\varepsilon\rangle - 1)$.

Question: *Under what condition, we have* $\mathbb{T} \cong \Lambda[\sqrt{\langle\varepsilon\rangle - 1}]$? The condition $p \nmid h_F$ is necessary for this by Cho–Vatsal.

§4. Known structure of $\mathbb{T}$.

- The fixed points

$$\mathrm{Spec}(\mathbb{T})^{\sigma=1} \cong \mathrm{Spec}(\mathbb{T}/\mathbb{T}(\sigma-1)\mathbb{T}) = \mathrm{Spec}(\mathbb{T}/I)$$

is therefore isomorphic to Spec($W[\Gamma_-]$); note that $\mathbb{T} \neq W[\Gamma_-]$ as $W[\Gamma_-]$ has finite rank over W, while $\mathbb{T}$ is free of finite rank over Λ.

- Since $\mathbb{T} \neq W[\Gamma_-]$, σ is non-trivial on $\mathbb{T}$.
- The ring $\mathbb{T}$ is reduced (as N is cube-free).

Plainly $\mathbb{T}$ is stable under σ, but

$$\mathrm{Spec}(\mathbb{T})^{\sigma=1} \text{ has codimension 1 in } \mathrm{Spec}(\mathbb{T}),$$

which does not therefore contain an irreducible component.

§**5. Galois deformation theory.** By irreducibility of $\overline{\rho}$, we have a Galois representation

$$\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}) \quad \text{with } \mathrm{Tr}(\rho_{\mathbb{T}}(\mathrm{Frob}_l)) = T(l)$$

for all primes $l \nmid Np$. By the celebrated $R = \mathbb{T}$ theorem of Taylor–Wiles, the couple $(\mathbb{T}, \rho_{\mathbb{T}})$ is universal among deformations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A)$ satisfying
(D1) $\rho \mod \mathfrak{m}_A \cong \overline{\rho} := \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}$.
(D2) $\rho|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \cong \left(\begin{smallmatrix} \epsilon & * \\ 0 & \delta \end{smallmatrix}\right)$ with δ unramified and $\overline{\delta} = (\delta \mod \mathfrak{m}_A)$.
(D3) $\det(\rho)|_{I_l} = \psi_l$ for the l-part ψ_l of ψ for each prime $l|N$.
(D4) $\det(\rho)|_{I_p} \equiv \psi|_{I_p} \mod \mathfrak{m}_A$ ($\Leftrightarrow \epsilon|_{I_p} \equiv \psi|_{I_p} \mod \mathfrak{m}_A$).
By the $R = \mathbb{T}$ theorem and a theorem of Mazur,

$$I/I^2 = \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} \mathbb{T}/I \cong \mathrm{Sel}(Ad(\mathrm{Ind}_F^{\mathbb{Q}} \Phi))^\vee$$
$$\Omega_{\mathbb{T}/\Lambda} \cong \mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee,$$

and principality of I implies cyclicity, where $\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W[\mathrm{Gal}(K_{\mathfrak{p}}/F)]^\times \cong W[\Gamma_-]^\times$ is a character sending σ to $\varphi(\sigma)\sigma|_{K_{\mathfrak{p}}}$.

§6. Ring theoretic theorem.

Theorem B: *Suppose* (H1–4). *Then if the class number* $h_{F(\varphi^-)}$ *of* $F(\varphi^-) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\varphi^-)}$ *is prime to* p*, the following* **equivalent** *statements hold true:*

(1) *The rings* $\mathbb{T}$ *and* $\mathbb{T}_+$ *are both local complete intersections free of finite rank over* Λ*.*

(2) *The* $\mathbb{T}$*-ideal* $I = \mathbb{T}(\sigma - 1)\mathbb{T} \subset \mathbb{T}$ *is principal and is generated by a non-zero-divisor* $\theta \in \mathbb{T}_-$ *with* $\theta^2 \in \mathbb{T}_+$*, and* $\mathbb{T} = \mathbb{T}_+[\theta]$ *is free of rank* 2 *over* $\mathbb{T}_+$*.*

The implication (1)⇒(2) follows from the lemma in the following slide.

§7. A key duality lemma

Here is a simplest case of the theory of dualizing modules by Grothendieck, Hartshorne and Kleiman (exploited by Cho–Vatsal):

Lemma 1 (Key lemma)**.** *Let S be a p-profinite* **Gorenstein integral domain** *and A be a* **reduced Gorenstein local S-algebra** *free of finite rank over S. Suppose*

- *A has a ring involution σ with $A_+ := \{a \in A | \sigma(a) = a\}$,*
- *A_+ is Gorenstein,*
- $\mathrm{Frac}(A)/\mathrm{Frac}(A_+)$ *is étale quadratic extension.*
- $\mathfrak{d}^{-1}_{A/A_+} := \{x \in \mathrm{Frac}(A) | \mathrm{Tr}_{A/A_+}(xA) \subset A_+\} \supsetneq A$,

Then A is free of rank 2 over A_+ and $A = A_+ \oplus A_+\theta$ for an element $\theta \in A$ with $\sigma(\theta) = -\theta$.

To see (1)⇒(2) of Theorem B, we apply the lemma to $A = \mathbb{T}$.

§8. Sketch of Theorem B ⇒ Theorem A.

Assuming (1), by Key lemma, $\mathfrak{d}_{\mathbb{T}/\mathbb{T}_+} = (\theta)$ for a non-zero divisor $\theta \in \mathbb{T}$. By "$R = T$" theorem, we see that $\mathbb{T}/I \cong W[\Gamma_-]$. Then by a theorem of Mazur, we have

$$\Omega_{\mathbb{T}/\Lambda} \cong \mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee \text{ and } I/I^2 \cong \Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} W[\Gamma_-](\cong \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \Phi)^\vee),$$

where $\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W[\Gamma_-]^\times$ is the universal character deforming φ unramified outside $\mathfrak{cp}$. Since $I/I^2 = (\theta)/(\theta^2)$ is cyclic, by Nakayama's lemma, $\Omega_{\mathbb{T}/\Lambda} \cong \mathrm{Sel}(Ad(\rho_{\mathbb{T}}))^\vee$ has one generator over $\mathbb{T}$. Later we will see the annihilator of the generator is a principal ideal (L_p) for a non-zero divisor $L_p \in \mathbb{T}$.

The proof of the adjoint class number formula by Wiles and myself (Pune IISER lecture notes Chap. 6) shows $L_p = L_p(Ad(\rho_{\mathbb{T}}))$ up to units for the adjoint p-adic L-function $L_p(Ad(\rho_{\mathbb{T}})) \in \mathbb{T}$.

(2)⇒(1) of Theorem B: We have $I = (\theta) \subset \mathbb{T}$ and $I_+ = (\theta^2) \subset \mathbb{T}_+$. Note that $\mathbb{T}/(\theta) \cong W[\Gamma_-] \cong \mathbb{T}_+/(\theta^2)$. Since θ is a non-zero divisor, the two rings $\mathbb{T}$ and $\mathbb{T}_+$ are local complete intersections since $W[\Gamma_-]$ is a local complete intersection.

§9. Presentation of $\mathbb{T}$ for the proof of (1) of Theorem B.

To see a possibility of applying the key lemma to $\mathbb{T}/\mathbb{T}_+$, we like to lift $\mathbb{T}$ to a power series ring $\mathcal{R} = \Lambda[[T_1, \ldots, T_r]]$ with an involution σ_∞ such that $\mathcal{R}^+ := \{x \in \mathcal{R} | \sigma_\infty(x) = x\}$ is Gorenstein and that $(\mathcal{R}/\mathfrak{A}, \sigma_\infty \bmod \mathfrak{A}) \cong (\mathbb{T}, \sigma)$ for an ideal $\mathfrak{A}$ stable under σ_∞.

Taylor and Wiles (with an improvement by Diamond and Fujiwara) found a pair $(\mathcal{R} := \Lambda[[T_1, \ldots, T_r]], (S_1, \ldots, S_r))$ with a regular sequence $S := (S_1, \ldots, S_r) \subset \Lambda[[T_1, \ldots, T_r]])$ such that

$$\Lambda[[T_1, \ldots, T_r]]/(S_1, \ldots, S_r) \cong \mathbb{T}$$

by their Taylor–Wiles system argument.

We need to lift σ somehow to an involution $\sigma_\infty \in \mathrm{Aut}(\mathcal{R})$ and show also that $\mathcal{R}^+$ is Gorenstein. If further $\mathcal{R} \cdot \mathcal{R}^- = (\theta_\infty)$, the image $\theta \in \mathbb{T}^-$ of θ_∞ in $\mathbb{T}$ generates I as desired.

§**10. Taylor–Wiles method.** Taylor–Wiles found an integer $r > 0$ and an infinite sequence of r-sets $\mathcal{Q} := \{Q_m | m = 1, 2, \dots\}$ of primes $q \equiv 1 \mod p^m$ such that for **the local ring** $\mathbb{T}^{Q_m}$ of $\overline{\rho}$ of the Hecke algebra $\mathbf{h}^{Q_m}$ of tame-level $N_m = N \prod_{q \in Q_m} q$. The pair $(\mathbb{T}^{Q_m}, \rho_{\mathbb{T}^{Q_m}})$ is universal among deformation satisfying (D1–4) but **ramification at** $q \in Q_m$ **is allowed**. Then $\rho \mapsto \rho \otimes \chi$ induces an involution σ_{Q_m}.

Actually they work with $\mathbb{T}_{Q_m} = \mathbb{T}^{Q_m}/(t - \gamma^k)\mathbb{T}^{Q_m}$ ($t = 1 + T$, $\gamma = 1 + p \in \Gamma$; the weight $k+1$ Hecke algebra of weight $k+1 \geq 2$ fixed). The product inertia group $I_{Q_m} = \prod_{q \in Q_m} I_q$ acts on $\mathbb{T}_{Q_m}$ by the p-abelian quotient Δ_{Q_m} of $\prod_{q \in Q_m} (\mathbb{Z}/q\mathbb{Z})^\times$. We choose an ordering of primes $Q_m = \{q_1, \dots, q_r\}$ and a generator $\delta_{i,m(n)}$ of the p-Sylow group of $(\mathbb{Z}/q_i\mathbb{Z})^\times$. The sequence $\mathcal{Q}$ is chosen so that for a given integer $n > 0$, we can find $m = m(n) > n$ so that we have ring projection maps $R_{n+1} \to R_n := \mathbb{T}_{Q_{m(n)}}/(p^n, \delta_{i,m(n)}^{p^n} - 1)_i$, and $R_\infty = \varprojlim_n R_n \cong W[[T_1, \dots, T_r]]$ and $S_i = \varprojlim_n (\delta_{i,m(n)} - 1)$.

§11. Lifting involution.

Write $\mathcal{D}_q$ for the local version of the deformation functor associated to (D1–4) adding a fixed determinant condition

(det) $\det(\rho) = \nu^k\psi$ for the chosen $k \geq 2$;

so, the Q_m-ramified universal ring is given by $\mathbb{T}_{Q_m}$.

Write $\overline{\mathcal{S}}_n$ for the image of $W[[S]]$ for $S = (S_1, \ldots, S_r)$ in R_n. We can add the involution to this projective system. Write σ_n for the involution of R_n induced by $\sigma_{Q_{m(n)}}$ to the Taylor-Wiles system, and get the lifting $\sigma_\infty \in \mathrm{Aut}(R_\infty)$. We can normalize the variable

$$\{T_1, \ldots, T_r\} = \{T_1^+, \ldots, T_{d_+}^+\} \sqcup \{T_1^-, \ldots, T_{d_-}^-\}$$

so that $\sigma_\infty(T_j^\pm) = \pm T_j^\pm$ (thus $r = d_+ + d_-$). Then we can further lift involution to $\mathcal{R} = \Lambda[[T_1^+, \ldots, T_{d_+}^+, T_1^-, \ldots, T_{d_-}^-]]$ as $\mathcal{R}/(t - \gamma^k) = R_\infty$ for $t = 1 + T$.

§12. Tangent space of $\mathbb{T}$.

Let $Y^-(\phi)$ (resp. $Y^-_{sp}(\phi)$) for a character $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to W^\times$ be the ϕ-eigenspace of the Galois group of the maximal p-abelian extension of the composite $K^-F(\phi)$ **unramified outside $\mathfrak{p}$ with total splitting of $\mathfrak{p}^\varsigma$ (resp. with total splitting at all prime factors of $\mathfrak{p}^\varsigma N$)**. The tangent space

$$t_{\mathbb{T}_{Qm}/W} = \mathrm{Hom}(\mathfrak{m}_{\mathbb{T}_{Qm}}/(\mathfrak{m}^2_{\mathbb{T}_{Qm}} + \mathfrak{m}_W), \mathbb{F})$$

is a Selmer group $\mathrm{Sel}(Ad)$ for $Ad = Ad(\overline{\rho}) = \mathfrak{sl}_2(\mathbb{F}) \cong \chi \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$. The involution σ acts on $t_{\mathbb{T}_{Qm}/W}$ and writing $t^{\pm}_{\mathbb{T}_{Qm}/W}$ for the "$\pm$" eigenspace of σ, we have $d_+ = \dim t^+_{\emptyset/W}$ and

$$t^+_{\mathbb{T}_\emptyset/W} = \mathrm{Sel}(\chi) = \mathrm{Hom}(Cl_F, \mathbb{F}) = 0$$

by a generalization of a result of Cho–Vatsal to the case $\mathfrak{f} \neq 1$:

$$t^-_{\mathbb{T}_{Qm}/W} = \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-) = \mathrm{Hom}_{W[\Gamma_-]}(Y^-(\varphi^-), \mathbb{F}).$$

§13. Dual Selmer groups as an index set for Q_m.

The index set of Q_m is any choice of $\mathbb{F}$-basis of a "dual" Selmer group. Regard $\mathcal{D}_q(\mathbb{F}[\epsilon])$ for the dual number ϵ as a subspace of $H^1(\mathbb{Q}_q, Ad)$ in the standard way: Thus we have the orthogonal complement $\mathcal{D}_q(\mathbb{F}[\epsilon])^\perp \subset H^1(\mathbb{Q}_q, Ad^*(1))$ under Tate local duality. The dual Selmer group $\mathrm{Sel}^\perp(Ad^*(1))$ is given by

$$\mathrm{Sel}^\perp(Ad^*(1)) := \mathrm{Ker}(H^1(\mathbb{Q}^{(Np)}/\mathbb{Q}, Ad^*(1)) \to \prod_{l|Np} \frac{H^1(\mathbb{Q}_l, Ad^*(1))}{\mathcal{D}_l(\mathbb{F}[\epsilon])^\perp}),$$

where $\mathbb{Q}^{(Np)}/\mathbb{Q}$ is the maximal extension of $\mathbb{Q}$ inside $\overline{\mathbb{Q}}$ unramified outside Np and ∞.

Then $r = \dim_{\mathbb{F}} \mathrm{Sel}^\perp(Ad^*(1))$ and choosing a basis $[c_j] \in \mathrm{Sel}^\perp(Ad^*(1))$ of Selmer classes, $q_j \in Q_m$ satisfies $c_j|_{\mathrm{Frob}_{q_j}^{\widehat{\mathbb{Z}}}}$ gives non-trivial local cohomology class.

§14. Interpretation of the dual Selmer group.

Define $Q_m^{\pm} := \{q \in Q_m | \chi(q) = \pm 1\}$. Then if S_q is the variable in $W[[S]]$ coming from $q \in Q_m^{\pm}$, then $\sigma(s_q) = s_q^{\pm 1}$ for $s_q := 1 + S_q$.

Since $Ad = \overline{\chi} \oplus \mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-$; so, for $Ad^*(1) = Ad(\overline{\rho})(1)$,

$$\mathrm{Sel}^{\perp}(Ad^*(1)) = \mathrm{Sel}^{\perp}(\overline{\chi}(1)) \oplus \mathrm{Sel}^{\perp}(\mathrm{Ind}_F^{\mathbb{Q}}(\overline{\varphi}^-(1))),$$

$$\mathrm{Sel}^{\perp}(\mathrm{Ind}_F^{\mathbb{Q}}(\overline{\varphi}^-(1))) \cong \mathrm{Hom}_{W[\Gamma_-]}(Y_{sp}^-(\varphi^-\omega), \mathbb{F}),$$

$$\mathrm{Sel}^{\perp}(\overline{\chi}(1)) \cong \mathrm{Hom}(O^{\times}, \mathbb{F}) \text{ (Kummer theory under } p \nmid h_F).$$

The choice of q_j with $c_j(\mathrm{Frob}_{q_j}) \neq 0$ forces us that Q_m^+ is indexed by a basis of $\mathrm{Sel}^{\perp}(\overline{\chi}(1))$ and Q_m^- is indexed by a basis of $\mathrm{Sel}^{\perp}(\mathrm{Ind}_F^{\mathbb{Q}}(\overline{\varphi}^-(1)))$; so,

$$r_+ := \dim \mathrm{Sel}^{\perp}(\overline{\chi}(1)) = |Q_m^+| \quad \text{and}$$
$$r_- := \dim \mathrm{Sel}^{\perp}(\mathrm{Ind}_F^{\mathbb{Q}}(\overline{\varphi}^-(1))) = |Q_m^-| \le d_- \quad \text{by } \sigma(s_q) = s_q^{\pm 1}.$$

§15. Determination of the dual induced Selmer group.

Write $\mathfrak{R}$ for the integer ring of $F(\varphi^-)$. For simplicity, assume that $\mathbb{F} = \mathbb{F}_p$. If $\phi \in \mathrm{Hom}_{W[\Gamma_-]}(Y_{sp}^-(\varphi^-\omega), \mathbb{F}_p)$, by Kummer theory (and $p \nmid h_{F(\varphi^-)}$),

$$\overline{\mathbb{Q}}^{\mathrm{Ker}(\phi)}[\mu_p] = F[\mu_p][\sqrt[p]{\epsilon}] \quad \text{for } \epsilon \in \mathfrak{R}[\frac{1}{p}]^\times$$

with the modulo p-power class $[\epsilon]$ in the $(\varphi^-)^{-1}$-eigenspace:

$$[\epsilon] \in (\mathfrak{R}[\frac{1}{p}]^\times/(\mathfrak{R}[\frac{1}{p}]^\times)^p)[(\overline{\varphi}^-)^{-1}].$$

Since $F(\varphi^-)$ is a CM field and $\varphi^-(c) = -1$ for complex conjugation c, $\mathfrak{R}^\times \otimes_{\mathbb{Z}} \mathbb{F}$ does not have $(\varphi^-)^{-1}$-eigenspace as φ^- is a totally odd character. The quotient p-divisor group $(\mathfrak{R}[\frac{1}{p}]^\times/\mathfrak{R}^\times) \otimes_{\mathbb{Z}} \mathbb{F}$ neither have $\overline{\varphi}^-$ eigenspace as $\overline{\varphi}^-(\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)) \neq 1$. Thus if $p \nmid h_{F(\varphi^-)}$,

$$r_- = \dim \mathrm{Sel}(\mathrm{Ind}_F^{\mathbb{Q}} \overline{\varphi}^-(1)) = \dim \mathrm{Hom}_{W[\Gamma_-]}(Y_{sp}^-(\varphi^-\omega), \mathbb{F}) = 0.$$

§16. Determination of the dual Selmer group of χ.

Write O for the integer ring of F. First assume that $\mathbb{F} = \mathbb{F}_p$. If $[c] \in \mathrm{Sel}^{\perp}_{\emptyset}(\overline{\chi}(1))$, taking $\Psi = c|_{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\chi\omega))}$, for $\mathbb{Q}(\Psi) = \overline{\mathbb{Q}}^{\mathrm{Ker}(\Psi)}$, the definition of the Selmer group tells us, by Kummer theory and $p \nmid h_F$,

$$\mathbb{Q}(\Psi)[\mu_p] = \mathbb{Q}[\mu_p][\sqrt[p]{\epsilon}]$$

for the fundamental unit ϵ. Thus we conclude

$$r_+ = \dim_{\mathbb{F}} \mathrm{Sel}(\overline{\chi}(1)) = 1.$$

Since $d_+ + d_- = r_+ + r_- = 1$ and $d_- > 0$ (as σ is non-trivial over $\mathbb{T}$), we conclude $d_- = 1$.

§17. QED.

Let $I_\infty = R_\infty(\sigma-1)R_\infty$, $I^Q = \mathbb{T}^Q(\sigma-1)\mathbb{T}^Q$. Then $R_\infty = W[[T_-]]$ with $S_+ \in W[[T_-^2]]$ and $\mathcal{R} = \Lambda[[T_-]]$ with $S_+ \in \Lambda[[T_-^2]]$. The image of T_- in $\mathbb{T}$ gives θ in Theorem B. By $\mathbb{T}/I \cong W = \Lambda/(\langle\varepsilon\rangle - 1)$, we get $\mathbb{T} = \Lambda[[T_-]]/(S_+)$, $\mathbb{T}_+ = \Lambda[[T_-^2]]/(S_+)$ and

$$\Omega_{\mathbb{T}/\Lambda} \otimes_{\mathbb{T}} W[\Gamma_-] = I/I^2 \cong (\theta)/(\theta)^2 \cong \Lambda/(\langle\varepsilon\rangle - 1).$$

This tells us that $\mathbb{T}$ is only ramified over $\mathbb{T}_+$ for the prime factor of $(\langle\varepsilon\rangle - 1)$ which supports my conjecture: $\mathbb{T} \stackrel{?}{=} \mathbb{T}_+[\sqrt{\langle\varepsilon\rangle - 1}]$ under (H1–4), generalizing a result of Cho–Vatsal who treated the case $\mathfrak{f} = 1$.

By Nakayama's lemma, $\Omega_{\mathbb{T}/\Lambda}$ is also cyclic.

§18. (L_p) is the different of $\mathbb{T}/\Lambda$.

Note that the ideal $(T_- - \theta) \supset (S_+)$ in $\mathbb{T}[[T_-]] = \Lambda[[T_-]] \otimes_\Lambda \mathbb{T}$. Write

$$(T_- - \theta)\mathcal{L}_p = S_+ \quad (\mathcal{L}_p \in \mathbb{T}[[T_-]])$$

with $L_p := (\mathcal{L}_p \bmod (T_- - \theta)) \in \mathbb{T}$. Then $\mathcal{L}_p dT_- + (T_- - \theta) d\mathcal{L}_p = dS_+$, and from the commutative diagram with exact rows

$$\begin{array}{ccccc}
(S_+)/(S_+)^2 & \xrightarrow{d} & \Omega_{\mathbb{T}[[T_-]]/\Lambda} \otimes_{\mathbb{T}[[T_-]]} \mathbb{T} & \xrightarrow{\twoheadrightarrow} & \Omega_{\mathbb{T}/\Lambda} \\
\wr\downarrow & & \wr\downarrow & & \| \downarrow \\
\mathbb{T}dS_+ & \xrightarrow[L_p]{} & \mathbb{T}dT_- & \xrightarrow[\twoheadrightarrow]{} & \Omega_{\mathbb{T}/\Lambda},
\end{array}$$

we conclude $\Omega_{\mathbb{T}/\Lambda} \cong \mathbb{T}/(L_p)$ for $L_p = L_p(Ad(\rho_{\mathbb{T}}))$.

In an appendix of a paper by Mazur–Roberts, Tate computed also the different $\mathfrak{d}_{\mathbb{T}/\Lambda}$ and showed $\mathfrak{d}_{\mathbb{T}/\Lambda} = (L_p)$.