Hida family と Iwasawa main conjecture

千田 雅隆

これは Chris. Skinner 氏の中国での講演を青木美穂, 山上敦士両氏が非常に丁寧に記録されたノートを下に千田が勝手に編集して単に日本語訳しただけのノートです. *

1 Introduction

p を素数とし $\Lambda = \mathbb{Z}_p[[T]]$ とおく. 埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$, $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ を固定する. modular form の p-adic family とは大雑把に言って,

$$\mathcal{F} = \sum_{n=0}^{\infty} A_n q^n,\ A_n \in \Lambda$$

という形式的冪級数で, ほとんど全ての整数 $k \geq 2$ に対し

$$\mathcal{F}((1+p)^{k-1} - 1) = \sum_{n=0}^{\infty} A_n((1+p)^{k-1} - 1)q^n$$

が weight k の modular form の q-展開になっているようなもののことをいう. 正確な定義はあとで述べる (Section 2.5).

注 1.1 $k \equiv k' \mod (p-1)p^r$ ならば

$$\mathcal{F}((1+p)^{k-1} - 1) \equiv \mathcal{F}((1+p)^{k'-1} - 1) \mod p^{r+1}$$

が自動的に成り立つ.

1.1 p-adic family of Eisenstein series

$\omega : \mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \subset \mathbb{Z}_p^\times$ を Teichmüller 指標とし, $[x] = x \cdot \omega(x)^{-1}$ とおく. いま $p \nmid r \in \mathbb{Z}$ に対して $a_r \in \mathbb{Z}_p$ を $[r] = (1+p)^{a_r}$ によって定める. $\omega^i(-1) = (-1)^k$ のとき, つまり $i \equiv k \mod 2$ のとき, $E_k(\omega^i)$ を weight k, character ω^i の Eisenstein series とする. このとき L-関数は

$$L(E_k(\omega^i), s) = \zeta(s)L^{(p)}(s - k + 1, \omega^i)$$

となる. ここで $L^{(p)}$ は p での Euler factor を除いた L-関数をあらわす. Eisenstein series $E_k(\omega^i)$ は

$$E_k(\omega^i) = \frac{L^{(p)}(1-k, \omega^i)}{2} + \sum_{n=1}^{\infty} \left(\sum_{d|n,(d,p)=1} \omega^i(d)d^{k-1} \right) q^n \in M_k(p, \omega^i)$$

*Skinner 氏の講義ノートを快く見せていただきました青木, 山上両氏に感謝いたします.

によって定義される. いま,

$$A_n^{(i)}(T) := \sum_{d|n,(d,p)=1} \omega^i(d)(1+T)^{a_d}$$

とおけば

$$A_n^{(i)}((1+p)^{k-1}-1) = \sum_{d|n,(d,p)=1} \omega^i(d)((1+p)^{k-1})^{a_d} = \sum_{d|n,(d,p)=1} \omega^{i+1-k}(d)d^{k-1}$$

となり, これは $E_k(\omega^{i+1-k})$ の n 番目の Fourier 係数に等しい.

定理 1.2 (Kubota-Leopoldt, Iwasawa) ある $g_{\omega^i} \in \Lambda$ が存在して,

$$L_p(s,\omega^{i+1}) = \begin{cases} g_{\omega^{i+1}}((1+p)^s-1) & \text{if } i \not\equiv -1 \mod p-1, \\ \frac{g_{\omega^{i+1}}((1+p)^s-1)}{(1+p)^s-1} & \text{if } i \equiv -1 \mod p-1 \end{cases}$$

が成り立つ. ここで $L_p(s,\omega^{i+1})$ は Kubota-Leopoldt の p-進 L-関数.

いま $L_p(s,\omega^{i+1})$ は interpolation property により

$$L_p(1-n,\omega^{i+1}) = L^{(p)}(1-n,\omega^{i+1-n})$$

が成り立つ. よって,

$$A_0^{(i)} = \frac{1}{2} g_{\omega^{i+1}}((1+p)(1+T)-1) \in \Lambda$$

とおくと, $i \not\equiv -1 \mod (p-1)$ なら

$$A_0^{(i)}((1+p)^{k-1}-1) = 2 \cdot L^{(p)}(1-k,\omega^{i+1-k})$$

である. ここで

$$\mathcal{E}^{(i)}(T) = \sum_{n=0}^{\infty} A_n^{(i)}(T)q^n \ (\text{ if } i \not\equiv -1 \mod (p-1))$$

$$\mathcal{E}^{(i)}(T) = A_0^{(i)} + \sum_{n=1}^{\infty} ((1+p)(1+T)-1)A_n^{(i)}(T)q^n \ (\text{ if } i \equiv -1 \mod (p-1))$$

とおけば,

$$\mathcal{E}^{(i)}((1+p)^{k-1}-1) = E_k(\omega^{i+1-k}) \ (\text{ if } i \not\equiv -1 \mod (p-1))$$

$$\mathcal{E}^{(i)}((1+p)^{k-1}-1) = ((1+p)^k-1)E_k(\omega^{i+1-k}) \ (\text{ if } i \equiv -1 \mod (p-1))$$

となるので, これらは modular form の p-adic family となることがわかる.

1.2 岩澤理論との関係

$\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})$ とおくとき同型

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

が存在する. $L_\infty/\mathbb{Q}_\infty$ を maximal abelian unramified pro-p extension とするとき, $X_\infty = \mathrm{Gal}(L_\infty/\mathbb{Q}_\infty)$ は $\mathbb{Z}_p[[\Delta \times \Gamma]]$-module であり, $X_\infty = \oplus_{i=1}^{p-1} X_\infty^{(i)}$ と $\mathbb{Z}_p[[\Gamma]]$-module としての分解ができる. ただし, Δ は $X_\infty^{(i)}$ に ω^i によって作用しているものとする.

定理 1.3 (Iwasawa) i が odd のとき $X_\infty^{(i)}$ は有限位数の submodule を持たない有限生成 torsion Λ-module.

さらに Mazur-Wiles によって次が証明されている.

定理 1.4 (Iwasawa Main Conjecture, Mazur-Wiles) $f_i(T)$ を $X_\infty^{(-i)}$ の characteristic power series とするとき

$$f_i(T)\Lambda = g_{\omega^{i+1}}((1+p)(1+T)^{-1}-1)\Lambda = 2A_0^{(i)}((1+T)^{-1}-1)\Lambda$$

が成り立つ.

この定理の証明を Hida family を使って与えるのがこの note での目標となる.

注 1.5 Iwasawa Main Conjecture は Kolyvagin による Euler system の idea を用いて Rubin が純代数的に証明を与えている.

2 Modular form と Λ-form

2.1 Modular form と Hecke operator

$k \geq 1, N \geq 1$, χ を mod N の Dirichlet character とする. $M_k(N,\chi)$ を weight k, level N, character χ を持つ modular form の空間, $S_k(N,\chi)$ を weight k, level N, character χ を持つ cusp form の空間とする. いま, $\mathbb{C}$ の subring R に対して

$$M_k(N,\chi,R) := \{f = \sum_{n=0}^{\infty} a_n(f)q^n \in M_k(N,\chi) \,|\, a_n(f) \in R \text{ for any } n \geq 1\}$$
$$M'_k(N,\chi,R) := \{f = \sum_{n=0}^{\infty} a_n(f)q^n \in M_k(N,\chi) \,|\, a_n(f) \in R \text{ for any } n \geq 0\}$$
$$S_k(N,\chi,R) := \{f = \sum_{n=1}^{\infty} a_n(f)q^n \in S_k(N,\chi) \,|\, a_n(f) \in R \text{ for any } n \geq 1\}$$

とおく. 明らかに $S_k(N,\chi,R) \subset M'_k(N,\chi,R) \subset M_k(N,\chi,R)$ が成り立っている. $\Gamma = \Gamma_0(N)$ とおく.

$$\Delta_N := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \,\middle|\, ad-bc > 0,\ N|c,\ (a,c)=1 \right\}$$

とし, $g \in \Delta_N$ とすれば $\Gamma g \Gamma$ は $M_k(N,\chi)$, $S_k(N,\chi)$ に作用する. これを $f|\Gamma g\Gamma$ と書くことにする. また,

$$T(m) = \Gamma \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \Gamma,\ S(m) = \Gamma \begin{pmatrix} m & 0 \\ 0 & m \end{pmatrix} \Gamma$$

とおくことにする. 素数 ℓ に対しては

$$T(\ell) = \begin{cases} \bigcup_{a=0}^{\ell-1} \Gamma \begin{pmatrix} 1 & a \\ 0 & \ell \end{pmatrix} \coprod \Gamma \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} & \text{if } \ell \nmid N \\ \bigcup_{a=0}^{\ell-1} \Gamma \begin{pmatrix} 1 & a \\ 0 & \ell \end{pmatrix} & \text{if } \ell \mid N \end{cases}$$

であり

$$S(\ell) = \Gamma \begin{pmatrix} \ell & 0 \\ 0 & \ell \end{pmatrix} \text{ if } \ell \nmid N$$

であるから,

$$f|T(\ell) = \begin{cases} \sum_{n=0}^{\infty} a_{n\ell}(f)q^n + \chi(\ell)\ell^{k-1}\sum_{n=0}^{\infty} q^{n\ell} & \text{if } \ell \nmid N \\ \sum_{n=0}^{\infty} a_{n\ell}(f)q^n & \text{if } \ell \mid N \end{cases}$$

及び

$$f|S(\ell) = \chi(\ell)\ell^{k-2}f$$

となる.

注 2.1 *1.* $T(m)$, $S(m)$ の作用は $T(\ell)$, $S(\ell)$ の多項式で書ける.

2. $a_1(f|T(m)) = a_m(f)$ が成り立つ.

3. $k \geq 2$ で R が χ の値を全て含んでいるのなら $T(m)$, $S(m)$ の作用は $M_k(N, \chi, R)$ の中で stable である.

4.

$$\mathbb{H}_k(N, \chi, R) := \langle T(m), S(m) | m \geq 1 \rangle_R \subseteq \mathrm{End}(M_k(N, \chi, R))$$
$$\mathbb{T}_k(N, \chi, R) := \langle T(m), S(m) | m \geq 1 \rangle_R \subseteq \mathrm{End}(S_k(N, \chi, R))$$

とおくとき, 自然な全射 $\mathbb{H}_k(N, \chi, R) \twoheadrightarrow \mathbb{T}_k(N, \chi, R)$ がある.

2.2 Modular form と cohomology

A を $\mathbb{Z}$-algebra とし, $n \geq 1$ に対し $L_n(A) \subseteq A[X, Y]$ を n 次の A 係数斉次多項式全体とする. いま $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$, $P(X, Y) \in L_n(A)$ に対して

$$(gP)(X, Y) := P((X, Y)\begin{pmatrix} d & -c \\ -b & a \end{pmatrix}) = P(dX - bY, -cX + aY) = P((X, Y)^t g^\iota)$$

とおく. ただし, $g^\iota = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ とおいた. いま A は $\mathbb{Z}[\chi]$-algebra と仮定する. $L_n(A, \chi) = L_n(A) \otimes \chi$ とおき, $P \in L_n(A)$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_N$ に対して $g * P = \chi(a)gP$ とおく. $g \in \Delta_N$ に対し $\Gamma g \Gamma = \cup_i \Gamma g_i$, $g_i \in \Delta_N$ とし, $[c] \in H^1(\Gamma, L_n(A, \chi))$ に対して, $(c|\Gamma g\Gamma)(\gamma) := \sum_i g_i^\iota * c(\gamma_i)$ と定める. ただし $g_i\gamma = \gamma_i g_j$ とおいた. j は i に依存して決まる数である. このとき $[c|\Gamma g\Gamma]$ は $H^1(\Gamma, L_n(A, \chi))$ の中で well-defined な元になる.

定理 2.2 (Eichler-Shimura) $f \in M_k(N, \chi)$, $h \in S_k(N, \chi)$, $P \in \mathcal{H}$ に対して

$$c_f = \left[\gamma \mapsto \int_P^{\gamma P} f(z)(X - zY)^{k-2}\, dz\right],$$
$$\overline{c}_h = \left[\gamma \mapsto \int_P^{\gamma P} h(\overline{z})(X - \overline{z}Y)^{k-2}\, d\overline{z}\right]$$

とおくとき, $(f,g)\mapsto c_f+\bar{c}_h$ は Hecke equivariant な同型

$$M_k(N,\chi)\oplus S_k(N,\chi)\cong H^1(\Gamma,L_{k-2}(\mathbb{C},\chi))=H^1(\Gamma\backslash\mathcal{H},\widetilde{L_{k-2}(\mathbb{C},\chi)})$$

を与える. ここで $\widetilde{L_{k-2}(\mathbb{C},\chi)}$ は $L_{k-2}(\mathbb{C},\chi)$ から定まる modular curve $\Gamma\backslash\mathcal{H}$ 上の sheaf.

この定理より次のことが分かる.

1. $\mathbb{Z}[\chi]$-algebra $R\subseteq R'\subseteq\mathbb{C}$ に対して $M_k(N,\chi,R)$, $M'_k(N,\chi,R)$, $S_k(N,\chi,R)$ 及び $\mathbb{H}_k(N,\chi,R)$, $\mathbb{T}_k(N,\chi,R)$ は有限生成 R-module であり,

   $$M_k(N,\chi,R')=M_k(N,\chi,R)\otimes R'$$
   $$S_k(N,\chi,R')=S_k(N,\chi,R)\otimes R'$$

   が成り立つ.

2. $$M'_k(N,\chi,R)\times\mathbb{H}_k(N,\chi,R)\ni(f,T)\mapsto a_1(f|T)\in R$$

   及び

   $$S_k(N,\chi,R)\times\mathbb{T}_k(N,\chi,R)\ni(f,T)\mapsto a_1(f|T)\in R$$

   は perfect pairing.

2.3 Ordinary idempotent

p を odd prime, $N=p^rN_0\,(p\nmid N_0,r\geq 1)$ とし, $\chi=\chi_t\cdot\psi$ を $\mathrm{cond}(\chi_t)|pN_0$, $\mathrm{cond}(\psi)|p^r$ となるように分解する. (つまり tame part と wild part に分解する) また, O を $\mathbb{Q}_p$ の有限次拡大体の整数環で $\mathbb{Z}_p[\chi]$ を含むと仮定する. このとき $M_k(N,\chi,O)$ は有限生成 free O-module であり, $T(p)$-stable となる. このことから $T(p):M_k(N,\chi,O)\to M_k(N,\chi,O)$ は行列表示を使って

$$T(p)\sim\begin{pmatrix}\alpha_1 & & & *\\ & \alpha_2 & & \\ & & \ddots & \\ 0 & & & \alpha_n\end{pmatrix}$$

と書くことができる. いま Hida の idempotent を

$$e_k:=\lim_{n\to\infty}T(p)^{n!}\sim\begin{pmatrix}1 & & & & & 0\\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 0\end{pmatrix}\in\mathbb{H}_k(N,\chi,O)$$

と定める. このとき ${e_k}^2=e_k$ である. Eichler-Shimura の同型を用いて $H^1(\Gamma,L_{k-2}(O,\chi))$ 上の作用素としても $\lim_{n\to\infty}T(p)^{n!}$ が定義できるので, これも $e=e_k$ と書くことにする.

2.4 Ordinary form

$R \subseteq \mathbb{C}$ を O-algebra とし,

$$M_k^{\mathrm{ord}}(N,\chi,R) := e_k M_k'(N,\chi,R) \subseteq M_k'(N,\chi,R),$$
$$S_k^{\mathrm{ord}}(N,\chi,R) := e_k S_k(N,\chi,R) \subseteq S_k(N,\chi,R)$$

と定める. $f \in M_k^{\mathrm{ord}}(N,\chi,R)$ なら $e_k f = f$ である. ordinary の名前の由来は, $f = \sum_{n=1}^{\infty} a_n(f) q^n$ が level N の normalized eigenform のとき

$$e_k f = f \iff a_p(f) \text{ が } p\text{-adic unit}$$

となっているからである.

命題 2.3 $\mathrm{rank}_R\, M_k^{\mathrm{ord}}(Np^\alpha,\chi,R)$ は $k \geqq 2$, χ, $\alpha \geqq 1$ に依らず bounded.

証明の sketch

$$\mathrm{rank}_R\, e_k M_k^{\mathrm{ord}}(Np^\alpha,\chi,R) \leq \dim_{\mathbb{F}_p} e_k H^1(\Gamma_1(Np),\mathbb{F}_p)$$

を示す. 明らかに右辺は k, χ に依らない. $R = O = \mathbb{Z}_p[\chi]$ のときに言えば十分. π を O の素元とする.

$\mathbb{F}$ を O の剰余体とし $\Gamma = \Gamma_1(Np^\alpha)$ とおく. まず Γ-module の完全列

$$0 \to L_{k-2}(O) \xrightarrow{\pi} L_{k-2}(O) \to L_{k-2}(\mathbb{F})$$

より cohomology の完全列

$$H^1(\Gamma, L_{k-2}(O)) \xrightarrow{\pi} H^1(\Gamma, L_{k-2}(O)) \to H^1(\Gamma,\mathbb{F})$$

が得られるので $H^1(\Gamma, L_{k-2}(O)) \otimes_O \mathbb{F} \hookrightarrow H^1(\Gamma,\mathbb{F})$ となる. ゆえに $e_k H^1(\Gamma, L_{k-2}(\mathbb{F}))$ が k, α に依らずに有界であることを示せば良い. ここで

$$i : L_{k-2}(\mathbb{F}) \ni P(X,Y) \mapsto P(1,0) \in \mathbb{F},$$

とおく. これらの写像は群 cohomology の間の写像

$$i_* : H^1(\Gamma, L_{k-2}(\mathbb{F})) \to H^1(\Gamma,\mathbb{F}),$$

を定める. いま i_* が $eH^1(\Gamma, L_{k-2}(\mathbb{F}))$ と $eH^1(\Gamma,\mathbb{F})$ の間の同型を与えることを示す.

Γ-module の完全列

$$0 \to \mathrm{Ker}(i) \to L_{k-2}(F) \to \mathbb{F} \to 0$$

により cohomology の完全列

$$H^1(\Gamma,\mathrm{Ker}(i)) \to H^1(\Gamma, L_{k-2}(\mathbb{F})) \to H^1(\Gamma,\mathbb{F}) \to H^2(\Gamma,\mathrm{Ker}(i))$$

が得られる.

$$\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

とおくとき α^ι は $\mathrm{Ker}(i)$ を保つので $T(p)$ は自然に $H^q(\Gamma,\mathrm{Ker}(i))$ に作用する. 一方 $\mathrm{Ker}(i)$ は $X^{k-2-j}Y^j$ $(j>0)$ で生成されるので α^ι は $\mathrm{Ker}(i)$ に nilpotent に作用する. このことと $T(p)$ の定義により $T(p)$ は $H^q(\Gamma,\mathrm{Ker}(i))$ $(q>0)$ は nilpotent に作用することが分かる. ゆえに $e_k H^q(\Gamma,\mathrm{Ker}(i)) = 0$ $(q>0)$. よって $eH^1(\Gamma, L_{k-2}(\mathbb{F})) \cong H^1(\Gamma,\mathbb{F})$ となる. 最後に適当な $T(p)$ の冪を取ることで $eH^1(\Gamma,\mathbb{F})$ の元は restriction map $H^1(\Gamma,\mathbb{F}) \to H^1(\Gamma_1(Np),\mathbb{F})$ の image に含まれることがわかるので Hida の projector の定義より

$$\dim_{\mathbb{F}} eH^1(\Gamma, L_{k-2}(\mathbb{F})) \leq \dim_{\mathbb{F}} eH^1(\Gamma_1(Np),\mathbb{F}) = \dim_{\mathbb{F}_p} eH^1(\Gamma_1(Np),\mathbb{F}_p)$$

が得られる. □

2.5 Λ-adic form

O を $\mathbb{Q}_p$ の有限次拡大体の整数環とし, $\Lambda = \mathbb{Z}_p[[T]]$, $\Lambda_O = O[[T]]$ とおく. $\varphi_k : \Lambda_O \to O$ を T に $(1+p)^{k-1} - 1$ を代入する写像とする. $N \geq 1$ とし $p \nmid N$ と仮定する. また,

$$\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$$

を Dirichlet character とする.

定義 2.4 (Λ-adic form) 形式的冪級数

$$\mathcal{F} = \sum_{n=0}^{\infty} A_n q^n,\ A_n \in \Lambda_O$$

が有限個を除く全ての $k \in \mathbb{Z}_{>0}$ に対して

$$\varphi_k(\mathcal{F}) := \sum_{n=0}^{\infty} \varphi_k(A_n) q^n \in M_k(Np^{\max\{r,1\}}, \chi\omega^{1-k}, O)$$

を満たすとき $\mathcal{F}$ は level N, character χ の Λ-adic form という. さらに有限個を除く全ての $k \in \mathbb{Z}_{>0}$ に対して

$$\varphi_k(\mathcal{F}) := \sum_{n=0}^{\infty} \varphi_k(A_n) q^n \in S_k(Np^{\max\{r,1\}}, \chi\omega^{1-k}, O)$$

を満たすとき $\mathcal{F}$ は level N, character χ の Λ-adic cusp form という.

例 2.5 奇数 i に対して $\mathcal{E}^{(i)}$ は level 1, character ω^i の Λ-adic form.

2.6 Λ-adic form の variant

1. $k \geq 1$, ζ を 1 の p^s 乗根とする. このとき, (k, ζ) という pair に対し,

   $$\psi_\zeta : (\mathbb{Z}/p^{s+1}\mathbb{Z})^\times \to \mathbb{Z}_p^\times$$

   を order p^s で $\psi_\zeta(1+p) = \zeta$ となる character とするとき, $\varphi_{k,\zeta}$ を

   $$\varphi_{k,\zeta} : \Lambda \ni 1 + T \to \zeta(1+p)^{k-1} \in O[\zeta]$$

   によって定める. このとき, 有限個を除く全ての $k \geq 1$ と ζ に対して

   $$\psi_{k,\zeta}(\mathcal{F}) \in M_k(Np^{\max\{r,1\}}, \chi\psi_\zeta\omega^{1-k}, O[\zeta])$$

   を満たすようなものを考えるという variant がある.

2. R を Λ の integral extension となっているような local complete な domain とする. $k \geq 1$ に対し

   $$\mathcal{X}_k = \left\{\widetilde{\varphi_k} : R \to \overline{\mathbb{Q}_p},\ \text{finite};\ \widetilde{\varphi_k}|_\Lambda = \varphi_k\right\},$$

   または (k, ζ) という pair に対して,

   $$\mathcal{X}_{k,\zeta} = \left\{\widetilde{\varphi_{k,\zeta}} : R \to \overline{\mathbb{Q}_p},\ \text{finite};\ \widetilde{\varphi_{k,\zeta}}|_\Lambda = \varphi_{k,\zeta}\right\},$$

とおく. このとき

$$\mathcal{F} = \sum_{n=0}^{\infty} A_n q^n,\ A_n \in R$$

が有限個を除く全ての $k \geq 1$ に対して

$$\varphi(\mathcal{F}) \in M_k(Np^{\max\{r,1\}}, \chi\omega^{1-k}, \varphi(R)),\ \text{for any } \varphi \in \mathcal{X}_k$$

を満たすとき, $\mathcal{F}$ は level N, character χ の R-adic form という. 同様に

$$\mathcal{F} = \sum_{n=0}^{\infty} A_n q^n,\ A_n \in R$$

が有限個を除く全ての $k \geq 1$ に対して

$$\psi(\mathcal{F}) \in S_k(Np^{\max\{r,1\}}, \chi\omega^{1-k}, \varphi(R)),\ \text{for any } \varphi \in \mathcal{X}_k$$

を満たすとき, $\mathcal{F}$ は level N, character χ の R-adic cusp form という. いま level N, character χ の R-adic form のなす空間を $\mathcal{M}(N,\chi,R)$ と書き, level N, character χ の R-adic cusp form のなす空間を $\mathcal{S}(N,\chi,R)$ と書くことにする. さらに

$$\mathcal{M}^{\mathrm{ord}}(N,\chi,R) := \left\{ \mathcal{F} \in \mathcal{M}(N,\chi,R) \;\middle|\; \begin{array}{c} \varphi(\mathcal{F}) \in M_k^{\mathrm{ord}}(Np^{\max\{r,1\}}, \chi\omega^{1-k}, \varphi(R)) \\ (\forall \varphi \in \mathcal{X}_k) \text{が十分大きな } k \text{ に対して成り立つ} \end{array} \right\},$$

$$\mathcal{S}^{\mathrm{ord}}(N,\chi,R) := \left\{ \mathcal{F} \in \mathcal{S}(N,\chi,R) \;\middle|\; \begin{array}{c} \varphi(\mathcal{F}) \in S_k^{\mathrm{ord}}(Np^{\max\{r,1\}}, \chi\omega^{1-k}, \varphi(R)) \\ (\forall \varphi \in \mathcal{X}_k) \text{が十分大きな } k \text{ に対して成り立つ} \end{array} \right\}$$

とおく.

注 2.6 *1.* $\mathfrak{p}_\varphi = \ker\varphi$ とおくと $\mathfrak{p}_\varphi$ は R の prime ideal で $R = \Lambda_O$ のとき

$$\varphi(\mathcal{M}(N,\chi,R)) \cong \mathcal{M}(N,\chi,R)/\mathfrak{p}_{\varphi_k}$$

が成り立つ. ここで $\mathfrak{p}_{\varphi_k} = (1+T-(1+p)^{k-1})$ とおいた.

2. 任意の $\varphi \in \mathcal{X}_k$ に対して

$$M_k(Np^{\max\{r,1\}}, \chi\omega^{1-k}, \varphi(R)) \subseteq \varphi(\mathcal{M}(N,\chi,R))$$

が成り立つ. いま $f \in M_k(Np^{\max\{r,1\}}, \chi\omega^{1-k}, \varphi(R))$ に対して,

$$\mathcal{G} = f \cdot \mathcal{E}^{(-1)}((1+p)^{-k}(1+T)-1)$$

とおく. このとき

$$\varphi_k(\mathcal{G}) = \mathcal{G}((1+p)^{k-1}-1) = f \cdot \mathcal{E}^{(-1)}((1+p)^{-1}-1) = u \cdot f,\ u \in \mathbb{Z}_p^\times$$

となる. また $k' > k$ のときは

$$\varphi_{k'}(\mathcal{G}) = \mathcal{G}((1+p)^{k'-1}-1) = f \cdot \mathcal{E}^{(-1)}((1+p)^{k'-k-1}-1)$$

であり, $\mathcal{E}^{(-1)}((1+p)^{k'-k-1}-1) \in M_k(Np, \omega^{k'-k}, \mathbb{Z}_p)$ なので $\varphi_{k'}(\mathcal{G}) \in M_k(Np, \chi\omega^{1-k'}, \varphi(R))$ となる. このことから $\mathcal{M}(N,\chi,R)$ は有限生成 R-module にはならないことがわかる. しかし前に述べたことから M_k^{ord} は k が大きくなっても rank は有界であったから $\mathcal{M}^{\mathrm{ord}}(N,\chi,R)$ は有限生成 R-module となる.

2.7 $T(m)$, $S(m)$ の action

$\ell \neq p$, $\ell \nmid N$, $R \supset \Lambda = \mathbb{Z}_p[[T]]$ とし,

$$\mathcal{F} = \sum_{n=0}^{\infty} A_n q^n \in \mathcal{M}(N, \chi, R)$$

とする. このとき,

$$\mathcal{F}|T(\ell) = \sum_{n=0}^{\infty} A_{n\ell} q^n + \chi(\ell)(1+T)^{a_\ell} \sum_{n=0}^{\infty} A_n q^{n\ell},$$

$$\mathcal{F}|S(\ell) = \chi(\ell)\ell^{-1}(1+T)^{a_\ell}\mathcal{F},$$

$$\mathcal{F}|T(p) = \sum_{n=0}^{\infty} A_{np} q^n$$

と定める. ($\omega(\ell)(1+p)^{a_\ell} = \ell$ であった) このとき $\varphi(\mathcal{F})$ ($\varphi \in \mathcal{X}_k$) が modular form ならば

$$\varphi(\mathcal{F}|T(\ell)) = \varphi(\mathcal{F})|T(\ell)$$

が成り立つ. 一般に $T(m)$, $S(m)$ の作用は $\varphi(\mathcal{F})$ が modular form のとき $\varphi(\mathcal{F}|T(m)) = \varphi(\mathcal{F})|T(m)$, $\varphi(\mathcal{F}|S(m)) = \varphi(\mathcal{F})|S(m)$ を満たす.

2.8 Ordinary R-adic form

命題 2.7 *1.* $\mathcal{M}^{\mathrm{ord}}(N, \chi, R)$, $\mathcal{S}^{\mathrm{ord}}(N, \chi, R)$ は有限生成 torsion free R-module.

2. $\mathcal{M}^{\mathrm{ord}}(N, \chi, \Lambda_O)$, $\mathcal{S}^{\mathrm{ord}}(N, \chi, \Lambda_O)$ は finite rank の free Λ_O-module.

証明
簡単のため χ は tame character とする. $\{\mathcal{F}_1, \dots \mathcal{F}_r\} \subseteq M^{\mathrm{ord}}(N, \chi, R)$ を R-線型独立な集合とし $n_1, \dots, n_r$ を $\Delta = \det(A_{n_i}(\mathcal{F})_j))_{1 \leq i,j \leq r} \neq 0$ となるようにとる. このとき, ある k, $\varphi \in \mathcal{X}_k$ があって

$$\varphi(\mathcal{F}_j) \in M_k^{\mathrm{ord}}(Np, \chi\omega^{1-k}, \varphi(R)),\ \varphi(\Delta) \neq 0$$

となる. ゆえに $\varphi(\mathcal{F}_1), \dots, \varphi(\mathcal{F}_r)$ は $M_k^{\mathrm{ord}}(Np, \chi\omega^{1-k}, \varphi(R))$ の中で $\varphi(R)$-線型独立である. よって Proposition 2.3 より

$$r \leq \mathrm{rank}_{\varphi(R)} M_k^{\mathrm{ord}}(Np, \chi\omega^{1-k}, \varphi(R)) \leq (k \text{ に依らない定数})$$

となる. いま r を maximal にとり, F_R を R の fraction field とする. このとき $\{\mathcal{F}_1, \dots \mathcal{F}_r\}$ は $M^{\mathrm{ord}}(N, \chi, R) \otimes_R F_R$ の basis となる. よって, いま任意の $\mathcal{F} \in M^{\mathrm{ord}}(N, \chi, R)$ は

$$\mathcal{F} = c_1\mathcal{F}_1 + \cdots + c_r\mathcal{F}_r$$

と書けるので

$$\begin{pmatrix} A_{n_1}(\mathcal{F}) \\ \vdots \\ A_{n_r}(\mathcal{F}) \end{pmatrix} = (A_{n_i}(\mathcal{F}_j))_{1 \leq i,j \leq r} \begin{pmatrix} c_1 \\ \vdots \\ c_r \end{pmatrix}$$

となる. ゆえに $\Delta c_j \in R$ がわかる. よって $\Delta\mathcal{F} \in \sum_{i=1}^{r} R\mathcal{F}_i$. 以上より

$$\mathcal{M}^{\mathrm{ord}}(N,\chi,R) \overset{\times\Delta}{\cong} \Delta\mathcal{M}^{\mathrm{ord}}(N,\chi,R) \subseteq \sum_{i=1}^{r} R\mathcal{F}_i$$

なので $\mathcal{M}^{\mathrm{ord}}(N,\chi,R)$ は有限生成 R-module であることがわかる. $\mathcal{S}^{\mathrm{ord}}(N,\chi,R) \subseteq \mathcal{M}^{\mathrm{ord}}(N,\chi,R)$ なので $\mathcal{S}^{\mathrm{ord}}(N,\chi,R)$ も有限生成 R-module. これで最初の主張は証明された.

さて, $\mathcal{M}^{\mathrm{ord}}(N,\chi,\Lambda_O)$ は有限生成 Λ_O-module なので, ある k が存在して任意の $\mathcal{F} \in \mathcal{M}^{\mathrm{ord}}(N,\chi,\Lambda_O)$ と任意の $\varphi \in \mathcal{X}_k$ に対して

$$\varphi(\mathcal{F}) \in M_k^{\mathrm{ord}}(N,\chi,O)$$

である. また,

$$\mathcal{M}^{\mathrm{ord}}(N,\chi,\Lambda_O)/((1+T)-(1+p)^{k-1})\mathcal{M}^{\mathrm{ord}}(N,\chi,\Lambda_O) \cong \varphi(\mathcal{M}^{\mathrm{ord}}(N,\chi,\Lambda_O)) \subseteq M_k^{\mathrm{ord}}(N,\chi,O)$$

であった. いま $f_1,\dots,f_s$ を $\varphi(\mathcal{M}^{\mathrm{ord}}(N,\chi,\Lambda_O))$ の O-basis とし $\mathcal{F}_1,\dots,\mathcal{F}_s$ を $\varphi(\mathcal{F}_i)=f_i$ となるようにとる. このとき $\mathcal{M} := \bigoplus \Lambda_O\mathcal{F}_i \subseteq \mathcal{M}^{\mathrm{ord}} := \mathcal{M}^{\mathrm{ord}}(N,\chi,\Lambda_O)$ 及び $t=(1+T)-(1+p)^{k-1}$ とおくと以下の可換図式が成り立つ.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \mathcal{M} & \xrightarrow{i} & \mathcal{M}^{\mathrm{ord}} & \longrightarrow & \operatorname{coker} i & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \times t} & & \downarrow{\scriptstyle \times t} & & \downarrow{\scriptstyle \times t} & & \\
0 & \longrightarrow & \mathcal{M} & \xrightarrow{i} & \mathcal{M}^{\mathrm{ord}} & \longrightarrow & \operatorname{coker} i & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \mathcal{M}/t\mathcal{M} & \xrightarrow{\cong} & \mathcal{M}^{\mathrm{ord}}/t\mathcal{M}^{\mathrm{ord}} & \longrightarrow & \operatorname{coker} i/t\operatorname{coker} i & \longrightarrow & 0 \\
 & & & & & & \| & & \\
 & & & & & & 0 & &
\end{array}$$

中山の補題より $\operatorname{coker} i = 0$ であるから二つ目の主張も得られる. □

注 2.8 *1.* 実は一般に $\mathcal{M}^{\mathrm{ord}}(N,\chi,R)$ は free R-module であることが知られている.

2. $M_k^{\mathrm{ord}}(N,\chi\omega^{1-k},O) \neq 0$ ならば $\mathcal{M}^{\mathrm{ord}}(N,\chi,R) \neq 0$ となる.

3. $f \in M_k^{\mathrm{ord}}(N,\chi\omega^{1-k},O)$ ならば $\varphi_k(\mathcal{F}) = f$ となる $\mathcal{F} \in \mathcal{M}^{\mathrm{ord}}(N,\chi,R)$ が存在する.

2.9 Ordinary idempotent(or projector)

命題 2.9 ある R-linear map

$$e : \mathcal{M}(N,\chi,R) \to \mathcal{M}^{\mathrm{ord}}(N,\chi,R)$$

が存在して次を満たす.

1. $e^2 = e$.

2. e は $\mathcal{M}^{\mathrm{ord}}(N,\chi,R)$ 上は identity.

3. $\varphi(\mathcal{F}) \in M_k(N, \chi\omega^{1-k}, O)$ となる任意の $\varphi \in \mathcal{X}_k$ に対して $\varphi(e\mathcal{F}) = e(\varphi(\mathcal{F}))$ が成り立つ.

4. e は $T(m)$ と commute する. つまり $e(\mathcal{F}|T(m)) = (e(\varphi(\mathcal{F})))|T(m)$ が成り立つ.

証明の outline
$\mathcal{M} = \mathcal{M}(N, \chi, R)$ とおく.

$$\Phi : \mathcal{M} \to \prod_{k\geq 1} \prod_{\varphi \in \mathcal{X}_k} \varphi(R)[[q]]$$

を $\Phi(\mathcal{F}) = (\varphi(\mathcal{F}))_\varphi$ で定める. いま $n > 0$ に対して

$$X_n := \prod_{k<n} \prod_{\varphi\in\mathcal{X}_k} \varphi(R)[[q]] \times \prod_{k\geq n} \prod_{\varphi\in\mathcal{X}_k} M_k(N, \chi\omega^{1-k}, \varphi(R)),$$

$$\mathcal{M}_n := \Phi^{-1}(X_n) = \{\mathcal{F} \in \mathcal{M} \,|\, \varphi(\mathcal{F}) \in M_k(N, \chi\omega^{1-k}, \varphi(R)),\ \forall \varphi \in \mathcal{X}_k,\ k \geq n\}$$

とおく. このとき $\mathcal{M} = \cup_n \mathcal{M}_n$ が成り立つ. $m \geq n$ に対して

$$\mathcal{M}_{n,m} := \mathcal{M}_n / \Big(\bigcap_{n\leq k\leq m,\, \varphi\in\mathcal{X}_k} \mathrm{Ker}(\varphi) \Big) \hookrightarrow \prod_{n\leq k\leq m} M_k(N, \chi\omega^{1-k}, \varphi(R))$$

であり, $\mathcal{M}_n = \varprojlim \mathcal{M}_{n,m}$ なので上の埋め込みを使って議論を通常の moudular form の空間の場合に帰着できる.□

系 2.10 ある $k_0 \geq 1$ が存在して, 任意の $k \geq k_0$, 任意の $\varphi \in \mathcal{X}_k$ に対して

$$\varphi(\mathcal{M}^{\mathrm{ord}}(N, \chi, R)) = M_k^{\mathrm{ord}}(N, \chi\omega^{1-k}, \varphi(R))$$
$$\varphi(\mathcal{S}^{\mathrm{ord}}(N, \chi, R)) = S_k^{\mathrm{ord}}(N, \chi\omega^{1-k}, \varphi(R))$$

が成り立つ.

注 2.11 実は $k_0 = 2$ と取れることが知られている *(Wiles).*

2.10 Ordinary Hecke algebra over R

Classical な modular form の空間のときと同様に

$$\mathbb{H}^{\mathrm{ord}}(N, \chi, R) := \langle T(\ell), T(p), S(\ell) | \ell \nmid pN \rangle_R \subseteq \mathrm{End}(\mathcal{M}^{\mathrm{ord}}(N, \chi, R))$$
$$\mathbb{T}^{\mathrm{ord}}(N, \chi, R) := \langle T(\ell), T(p), S(\ell) | \ell \nmid pN \rangle_R \subseteq \mathrm{End}(\mathcal{S}^{\mathrm{ord}}(N, \chi, R))$$

とおく. このとき通常の modular form の空間の場合の結果を使って

$$\mathcal{S}^{\mathrm{ord}}(N, \chi, R) \times \mathbb{T}^{\mathrm{ord}}(N, \chi, R) \ni (\mathcal{F}, T) \mapsto A_1(\mathcal{F}|T) \in R$$

は perfect pairing となることがわかる.

2.11 R-adic eigenform

$\mathcal{F} \in \mathcal{M}(N, \chi, R)$ とする. 任意の $T(m)$ に対して $C_m \in R$ があって $\mathcal{F}|T(m) = C_m\mathcal{F}$ を満たすとき $\mathcal{F}$ を R-adic eigenform という. このとき任意の eigenform $f \in M_k(N, \chi\omega^{1-k}, R)$ に対して $\varphi(\mathcal{F}) = f$, $\varphi \in \mathcal{X}_k$ となるような R-adic eigenform $\mathcal{F}$ が存在するかどうかというのは自然な疑問である. これに対しては次が知られている.

定理 2.12 (Hida) k を 2 以上の整数とする.

1. 任意の eigenform $f \in M_k(N, \chi\omega^{1-k}, R)$ に対して, ある R-adic eigenform $\mathcal{F}$, $\varphi \in \mathcal{X}_k$, non-zero constant c が存在して $\varphi(\mathcal{F}) = c \cdot f$ となる.
2. $\mathbb{H}^{\mathrm{ord}}(N, \chi, R)$ が Gorenstein 環なら任意の eigenform $f \in M_k(N, \chi\omega^{1-k}, R)$ に対して, ある R-adic eigenform $\mathcal{F}$, $\varphi \in \mathcal{X}_k$ が存在して $\varphi(\mathcal{F}) = f$ となる. 同様に $\mathbb{T}^{\mathrm{ord}}(N, \chi, R)$ が Gorenstein 環なら任意の eigenform $f \in S_k(N, \chi\omega^{1-k}, R)$ に対して, ある R-adic eigenform $\mathcal{F}$, $\varphi \in \mathcal{X}_k$ が存在して $\varphi(\mathcal{F}) = f$ となる.

証明については Hida [1] を参照のこと.

3 R-modular form と Selmer group

3.1 Modular form に付随する Galois 表現

$f \in S_k(N, \chi, O)$ を eigenform とし, $f|T(m) = c_m f$, $c_m \in O$ とする. このとき $a_1(f) = 1$ ならば $c_m = a_m(f)$ である. いま O は p-進体 $K/\mathbb{Q}_p$ の整数環とする.

定理 3.1 (Eichler, Shimura, Deligne, Serre) 上の仮定の下で,

$$\rho_f : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K)$$

が存在して, 以下の条件を満たす.

1. ρ_f は continuous な表現.
2. $\ell \nmid Np$ となる任意の素数 ℓ で ρ_f は不分岐. つまり $\rho_f|_{I_\ell} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. ここで I_ℓ は ℓ での惰性群.
3. ρ_f は absolutely irreducible.
4. $\ell \nmid Np$ となる任意の素数 ℓ に対して $\mathrm{trace}\rho_f(\mathrm{Frob}_\ell) = c_\ell$.
5. $\ell \nmid Np$ となる任意の素数 ℓ に対して $\det \rho_f(\mathrm{Frob}_\ell) = \chi(\ell)\ell^{k-1}$.
6. $c \in G_{\mathbb{Q}}$ を複素共役とすれば $\rho_f(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.
7. $\rho_f|_{D_p}$ は de Rham 表現. もし $p \nmid N$ なら crystalline 表現となる. ここで D_p は p での分解群.
8. (Deligne, Mazur-Wiles) $f \in S_k^{\mathrm{ord}}(N, \chi, O)$, $p|N$ のとき

$$\rho_f|_{D_p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix},\ \psi_2|_{I_p} = 1,\ \psi_2(\mathrm{Frob}_p) = c_p$$

となる.

ρ_f の構成の idea
いま ψ_f を

$$\psi_f : \mathbb{T}_k(N,\chi,O) \ni T \mapsto f \text{ に対する } T \text{ の固有値} \in O$$

(特に $\psi_f(T(m)) = c_m$ である) と定義して, $\mathfrak{p}_f = \mathrm{Ker}\psi_f$ とおく. このとき

$$K^2 \cong H^1(\Gamma, L_{k-2}(K))[\mathfrak{p}_f] \cong H^1_{\text{ét}}(\overline{X}_\Gamma, \mathcal{L}_{k-2})[\mathfrak{p}_f]$$

への $G_{\mathbb{Q}}$ の action から ρ_f が構成できる. ただし, $\overline{X}_\Gamma$ は $\mathbb{Q}$ 上の modular curve X_Γ の $\overline{\mathbb{Q}}$ への base change をあらわし, $\mathcal{L}_{k-2}$ は GL_2 の表現 L_{k-2} から定まる p-adic sheaf.

3.2 Pseudo representation (疑表現)

A を環とする. 三つの写像の組 $\phi = (a, d, x)$,

$$a : G_{\mathbb{Q}} \to A,\ d : G_{\mathbb{Q}} \to A,\ x : G_{\mathbb{Q}} \times G_{\mathbb{Q}} \to A$$

が任意の $\alpha, \beta, \sigma, \tau \in G_{\mathbb{Q}}$ に対して

1. $a(\sigma\tau) = a(\sigma)a(\tau) + x(\sigma,\tau)$.
2. $d(\sigma\tau) = d(\sigma)d(\tau) + x(\tau,\sigma)$.
3. $x(\sigma,\tau)x(\alpha,\beta) = x(\sigma,\beta)x(\alpha,\tau)$.
4. $x(\sigma\tau,\alpha\beta) = a(\sigma)a(\beta)x(\tau,\alpha) + d(\tau)a(\beta)x(\sigma,\alpha) + a(\sigma)d(\alpha)x(\tau,\beta) + d(\tau)d(\alpha)x(\sigma,\beta)$.
5. $x(\sigma,\mathrm{id}) = x(\mathrm{id},\sigma) = 0$, $a(\mathrm{id}) = d(\mathrm{id}) = 1$.
6. $x(\sigma,c) = x(c,\sigma) = 0$, $a(c) = 1$, $d(c) = -1$(c は複素共役).

を満たすとき ϕ は $G_{\mathbb{Q}}$ から A への pseudo representation という.

$\rho_f(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix}$ と書いたとき $\phi_f = (a,d,x)$ を $a(\sigma) = a_\sigma$, $d(\sigma) = d_\sigma$, $x(\sigma,\tau) = b_\sigma c_\tau$ とおくと ϕ_f は pseudo representation になる. 逆に, pseudo representation から representation を作るということをこの後で考える.

3.3 Pseudo representation から representation の構成

$\phi = (a,d,x)$ を $G_{\mathbb{Q}}$ から環 A への pseudo representation とする. A は離散付値環とする. もし $x(\sigma,\tau) = 0$ なら a, d は character であり,

$$\rho_\phi(\sigma) = \begin{pmatrix} a(\sigma) & 0 \\ 0 & d(\sigma) \end{pmatrix}$$

という二次元の Galois 表現が構成できる.

次に $x(\sigma,\tau) \neq 0$ とする. いま (σ_0,τ_0) を $x(\sigma_0,\tau_0)$ の付値が最小になるように選ぶ. このとき ϕ から得られる表現を

$$\rho_\phi(\sigma) = \begin{pmatrix} a(\sigma) & x(\sigma,\tau_0) \\ \frac{x(\sigma_0,\sigma)}{x(\sigma_0,\tau_0)} & d(\sigma) \end{pmatrix}$$

と定義する. A が体のときは $x(\sigma_0,\tau_0) \neq 0$ となるように (σ_0,τ_0) を選ぶことにする.

注 3.2 ρ_f から ϕ_f, ϕ_f から ρ_{ϕ_f} と構成すると $\rho_f \cong \rho_{\phi_f}$ となる.

3.4 “Patching together” pseudo representation

R を compact な topological ring とする. $i = 1, 2, \ldots$ に対して R の互いに異なる素 ideal の無限集合 $\{\mathfrak{p}_i\}_{i=1}^{\infty}$ を選び, $\phi_i = (a_i, d_i, x_i)$ と $G_{\mathbb{Q}}$ から $R/\mathfrak{p}_i$ への pseudo representaion とする. いま次の二つを仮定する.

1. ある素数の有限集合 Σ があって任意の i に対し ϕ_i は Σ の外で不分岐, つまり任意の $\ell \notin \Sigma$ に対して
$$\begin{cases} a_i(\sigma) = d_i(\sigma) = 1 & \text{for } \forall \sigma \in I_\ell \\ x_i(\sigma, \tau) = x_i(\tau, \sigma) = 0 & \text{for } \forall \sigma, \tau \in I_\ell. \end{cases}$$
2. 任意の $\ell \notin \Sigma$ に対して $c_\ell \in R$ があって
$$a_i(\mathrm{Frob}_\ell) + d_i(\mathrm{Frob}_\ell) = c_\ell \mod \mathfrak{p}_i$$
を満たす.

命題 3.3 以上の仮定の下で
$$\phi \mod \mathfrak{p}_i = \phi_i, \forall i$$
を満たす $G_{\mathbb{Q}}$ から R への pseudo representation $\phi = (a, d, x)$ が存在する.

証明 G_Σ を Σ の外不分岐最大拡大体の Galois 群とする. $\sigma \in G_\Sigma$ に対して素数の列 $\{\ell_j\}$, $\{\ell'_j\}$ を
$$\mathrm{Frob}_{\ell_j} \to \sigma, \mathrm{Frob}_{\ell'_j} \to \sigma c \, (j \to \infty)$$
となるようにとる. ($\{\mathrm{Frob}_\ell\}_\ell$ は G_Σ の中で dense なのでとることができる) このとき
$$\begin{aligned} a(\sigma) &:= \lim_{j\to\infty} (c_{\ell_j} + c_{\ell'_j}) \\ d(\sigma) &:= \lim_{j\to\infty} (c_{\ell_j} - c_{\ell'_j}) \\ x(\sigma, \tau) &:= a(\sigma\tau) - a(\sigma)a(\tau) \end{aligned}$$
とおけばよい. □

3.5 R-adic form に付随する Galois 表現

$\mathcal{F} \in \mathcal{S}(N, \chi, R)$ を R-adic eigenform とし $\mathcal{F}|T(m) = C_m\mathcal{F}$, $C_m \in R$ とする. いま $k_1, k_2, \ldots$ 及び $\varphi_i \in \mathcal{X}_{k_i}$ に対し $f_i = \varphi_i(\mathcal{F})$ は cusp form になっているとする. $\mathfrak{p}_i = \mathrm{Ker}\varphi_i$ とおき ϕ_i を f_i に付随する $G_{\mathbb{Q}}$ から $\varphi_i(R)$ への pseudo representation とする. このとき前の section の Proposition 3.3 より $G_{\mathbb{Q}}$ から R への pseudo representation $\phi_{\mathcal{F}} = (a_{\mathcal{F}}, d_{\mathcal{F}}, x_{\mathcal{F}})$ が存在して次を満たす.

1. 任意の $\ell \nmid Np$ に対して $a_{\mathcal{F}}(\mathrm{Frob}_\ell) + d_{\mathcal{F}}(\mathrm{Frob}_\ell) = C_\ell$ が成り立つ.
2. $\varphi(\mathcal{F})$ が modular form となるような $\varphi \in \mathcal{X}_k$ について $\varphi \circ \phi_{\mathcal{F}} = \phi_{\varphi(\mathcal{F})}$ が成り立つ.

前にやったように $\phi_{\mathcal{F}}$ から Galois 表現 $\rho_{\mathcal{F}}$ が構成できる. このとき
$$\rho_{\mathcal{F}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(F_R)$$
(F_R は R の fraction field) は次を満たす.

1. $\rho_{\mathcal{F}}$ は irreducible.
2. 任意の $\ell \nmid Np$ に対して $\mathrm{trace}\rho_{\mathcal{F}}(\mathrm{Frob}_\ell) = C_\ell$ が成り立つ.
3. 任意の $\ell \nmid Np$ に対して $\det \rho_{\mathcal{F}}(\mathrm{Frob}_\ell) = \chi(\ell)(1+T)^{a_\ell}$ が成り立つ.
4. $c \in G_{\mathbb{Q}}$ を複素共役とすれば $\rho_{\mathcal{F}}(c) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

R を integral closed とする. $\mathfrak{p} \subset R$ を height 1 prime とすると $R_{\mathfrak{p}}$ は離散付値環となるので $\rho_{\mathcal{F}}$ は $\mathrm{GL}_2(R_{\mathfrak{p}})$ への表現として実現できる. いま $\mathcal{F} \in \mathcal{S}^{\mathrm{ord}}(N, \chi, R)$ を R-adic eigenform とすると, その specialization に対する Deligne, Mazur-Wiles の結果より

$$\rho_{\mathcal{F}}|_{D_p} \sim \begin{pmatrix} \Psi_1 & * \\ 0 & \Psi_2 \end{pmatrix} \in \mathrm{GL}_2(F_R),\ \Psi_2|_{I_p} = 1,\ \Psi_2(\mathrm{Frob}_p) = C_p$$

と書くことができる.

3.6 Hecke algebra への pseudo representation (Galois 表現の別の構成法)

$\mathbb{T}^{\mathrm{ord}}(N, \chi, R)$ は reduced とする. (例えば $N = 1$ または $\mathrm{cond}(\chi) = Np$ ならこれが成り立つ) このときは $\phi_{\mathcal{F}}$ を構成するのに $\mathbb{T}^{\mathrm{ord}}(N, \chi, R)$ への pseudo representation を使うことができる. つまり $\phi_{\mathbb{T}^{\mathrm{ord}}(N,\chi,R)} = (A, D, X)$ を $A(\mathrm{Frob}_\ell) + D(\mathrm{Frob}_\ell) = T(\ell)$, $(\forall \ell \nmid Np)$ となる $\phi_{\mathbb{T}^{\mathrm{ord}}(N,\chi,R)}$ と $\mathbb{T}^{\mathrm{ord}}(N, \chi, R) \ni T(\ell) \mapsto C_\ell \in R$ によって同様に $\phi_{\mathcal{F}}$ を構成することができる.

3.7 Ribet の定理

R-modular form とその Galois 表現からどのようにして Iwasawa Main Conjecture が得られるのかを後で説明する. この方法は Wiles による. その前に証明の idea のもととなった Ribet の結果とその証明を紹介する.

定理 3.4 (Ribet [2], Herbrand の定理の逆) $X_0 = \bigoplus_{i \in \mathbb{Z}/(p-1)\mathbb{Z}} X_0^{(i)}$ を $\mathbb{Q}(\mu_p)$ の ideal 類群の p-part とする. i は odd とし $i \not\equiv 1 \mod p-1$ とする. このとき $p|L(0, \omega^i)$ ならば $p|\#X_0^{(-i)}$.

証明 まず $p|L(0, \omega^i)$ ならば $p|L(-1, \omega^{i-1})$ なので p は Eisenstein series $E_2(\omega^{i-1})$ の constant term の分子を割る. このあと見るように $a_0(g) = 1$ となるような $g \in M_2(p, \omega^{i-1}, \mathbb{Z}_p)$ が weight 1 の Eisenstein series の積として構成できる. いま e を ordinary projector とするとき

$$h = \sum_{n=0}^{\infty} a_n(h) q^n := e\left(E_2(\omega^{i-1}) - \frac{1}{2} L^{(p)}(-1, \omega^{i-1}) g\right) \in M_2^{\mathrm{ord}}(p, \omega^{i-1}, \mathbb{Z}_p)$$

とおくと $a_0(h) = 0$ であるが, 実は $h \in S_2^{\mathrm{ord}}(p, \omega^{i-1}, \mathbb{Z}_p)$ であることが証明できる (あとでより一般的に証明する). $eE_2(\omega^{i-1}) = E_2(\omega^{i-1})$ であるから

$$h = E_2(\omega^{i-1}) - \frac{1}{2} L(-1, \omega^{i-1}) e(g)$$

である. $p|L(-1, \omega^{i-1})$ なので $a_n(h) \equiv a_n(E_2(\omega^{i-2})) \mod p$ であるから $a_p(h) \equiv a_p(E_2(\omega^{i-1})) = 1 \mod p$ が成り立つ. また $\ell \neq p$ に対して

$$a_\ell(h) \equiv a_\ell(E_2(\omega^{i-1})) = 1 + \omega^{i-1}(\ell)\ell \equiv 1 + \omega^i(\ell) \mod p$$

である. いま $\mathbb{T}=\mathbb{T}_k^{\mathrm{ord}}(p,\omega^{i-1},\mathbb{Z}_p)$ とおき,

$$\phi:\mathbb{T}\ni t\mapsto a_1(h|t)\mod p\in\mathbb{F}_p=\mathbb{Z}_p/p\mathbb{Z}_p$$

と定める. $\ell\neq p$ なら

$$\phi(T(\ell))=a_1(h|T(\ell))\equiv a_1(E_2(\omega^{i-1})|T(\ell))\equiv a_\ell(E_2(\omega^{i-1}))\equiv 1+\omega^i(\ell)\mod p$$

である. また $t,t'\in\mathbb{T}$ なら $a_1(E_2(\omega^{i-1})|tt')=a_1(E_2(\omega^{i-1})|t)a_1(E_2(\omega^{i-1})|t')$ が成り立っているので ϕ は $\mathbb{Z}_p$-algebra homomorphism になっている. さらに

$$\mathcal{M}:=\mathrm{Ker}(\phi)\supseteq\{T(\ell)-1-\omega^{i-1}(\ell)|\ell\neq p\}$$

とおけば $\mathcal{M}$ は $E_2(\omega^{i-1})$ を annihilate する. 一方 $\mathbb{T}$ は finite rank の free $\mathbb{Z}_p$-module である. $\mathfrak{p}\subseteq\mathcal{M}$ を $\mathbb{T}$ の minimal な prime として

$$\psi:\mathbb{T}\twoheadrightarrow\mathbb{T}/\mathfrak{p}\overset{\overline{\psi}}{\hookrightarrow}\overline{\mathbb{Q}}_p$$

をひとつ固定し, O を $\mathbb{T}/\mathfrak{p}$ の商体の整数環とする. このとき

$$S_2^{\mathrm{ord}}(p,\omega^{i-1},O)=\mathrm{Hom}_O(\mathbb{T}_2^{\mathrm{ord}}(p,\omega^{i-1},O),O)$$

であるから eigenform $f\in S_2^{\mathrm{ord}}(p,\omega^{i-1},O)$ があって $T(\ell)f=c_\ell f$ としたとき $c_\ell=\psi(T(\ell))$ を満たす. また π を O の uniformizer とすれば $c_\ell\equiv 1+\omega^i(\ell)\mod\pi$, $c_p\equiv 1\mod\pi$ である. 以上のことから, もし $p|L(0,\omega^i)$ ならば $c_n=a_n(f)\equiv a_n(E_2(\omega^{i-1}))\mod\pi$ となるような eigenform $f\in S_2^{\mathrm{ord}}(p,\omega^{i-1},O)$ が存在することがわかった. いま f の Galois 表現

$$\rho_f:G_{\mathbb{Q}}\to\mathrm{GL}_2(K)$$

を考える (K は O の商体). 簡単のため $\rho_f:G_{\mathbb{Q}}\to\mathrm{GL}_2(O)$ とする. このとき f は ordinary であるから

$$\rho_f|_{D_p}\sim\begin{pmatrix}\psi_1 & *\\ 0 & \psi_2\end{pmatrix},\ \psi_2|_{I_p}=1,\ \psi_2(\mathrm{Frob}_p)=c_p=a_p(f)$$

である. さらに Galois 表現の基本的な性質 Theorem 3.1 により $\ell\neq p$ ならば

$$\det\rho_f(\mathrm{Frob}_\ell)=\omega^{i-1}(\ell)\ell$$

である. ゆえに $\det\rho_f=\omega^{i-1}\varepsilon$ (ε は cyclotomic character). 以上から

$$\psi_1|_{I_p}=\det\rho_f|_{I_p}=\omega^i\varepsilon|_{I_p},\ \psi_1|_{I_p}\equiv\omega^i|_{I_p}\not\equiv 1\mod\pi\ (\forall i:\mathrm{odd})$$

なので, $\sigma_0\in I_p$ があって $\alpha:=\psi_1(\sigma_0)\not\equiv 1\mod\pi$, $\psi_2(\sigma_0)=1\in O^\times$ を満たす.

いま $\rho_f(\sigma_0)=\begin{pmatrix}1 & 0\\ 0 & \alpha\end{pmatrix}$ と仮定してよいので $\rho_f|_{D_p}=\begin{pmatrix}\psi_2 & 0\\ * & \psi_1\end{pmatrix}$ となる.

さて, いま $\sigma\in G_{\mathbb{Q}}$ に対して $\rho_f(\sigma)=\begin{pmatrix}a_\sigma & b_\sigma\\ c_\sigma & d_\sigma\end{pmatrix}$ と書くことにすると任意の $\ell\neq p$ に対し $\rho_f|_{I_\ell}=\mathrm{id}$ であることにより p を含めた任意の素数 ℓ, 任意の $\sigma\in I_\ell$ に対し $b_\sigma=0$ である. しかし ρ_f は irreducible なので $b_\tau\neq 0$ となる $\tau\in G_{\mathbb{Q}}$ が存在する. いま $\tau_0\in G_{\mathbb{Q}}$ を $n=\mathrm{ord}_\pi(b_{\tau_0})$ が最小になるようにとる.

$\rho=\rho_f$ を $\begin{pmatrix}1&0\\0&\pi^n\end{pmatrix}\rho_f\begin{pmatrix}1&0\\0&\pi^{-n}\end{pmatrix}$ と取り替えることで $n=0$, つまり $b_{\tau_0}\in O^\times$ と仮定してよい. ここで

$$\overline{\rho}=\rho \mod \pi : G_{\mathbb{Q}}\ni\sigma\mapsto\begin{pmatrix}\overline{a}_\sigma&\overline{b}_\sigma\\\overline{c}_\sigma&\overline{d}_\sigma\end{pmatrix}\in \mathrm{GL}_2(\mathbb{F})$$

と書くことにすると $\ell\neq p$ に対し

$$\mathrm{trace}\rho(\mathrm{Frob}_\ell)=a_\ell(f)\equiv 1+\omega^i(\ell) \mod \pi,$$

つまり $\overline{a}_\sigma+\overline{d}_\sigma=\mathrm{trace}\overline{\rho}=1+\omega^i$ なので

$$\overline{a}_\sigma=1 \text{ or } \omega^i(\sigma),\ \overline{d}_\sigma=1 \text{ or } \omega^i(\sigma)$$

であることがわかる. さらに $\overline{\rho}(\sigma_0)=\begin{pmatrix}1&0\\0&\overline{\alpha}\end{pmatrix}$ であったから結局 $\overline{a}_\sigma=1$, $\overline{d}_\sigma=\omega^i(\sigma)$ でなくてはならない. 特に, このとき $\overline{d}_{\sigma\tau}=\overline{d}_\sigma\overline{d}_\tau$ が成り立つので, 通常の行列の計算から得られる式

$$\overline{d}_{\sigma\tau}=\overline{d}_\sigma\overline{d}_\tau+\overline{b}_\sigma\overline{c}_\tau$$

と比較することで, 任意の σ, τ に対して

$$\overline{b}_\sigma\overline{c}_\tau\equiv 0 \mod \pi$$

となることが分かる. しかし $\overline{b}_{\tau_0}\not\equiv 0 \mod \pi$ であったから結局, 任意の σ に対して $\overline{c}_\sigma=0$ であることが分かる. 以上より

$$\overline{\rho}(\sigma_0)=\begin{pmatrix}1&\overline{b}_\sigma\\0&\omega^i(\sigma)\end{pmatrix}\in\mathrm{GL}_2(\mathbb{F}),\ \mathbb{F}=O/(\pi)$$

であることがわかった. いま $H^1(G_{\mathbb{Q}},\mathbb{F}(\omega^{-i}))$ の cocycle を

$$h:=(\sigma\mapsto\omega^{-i}(\sigma)\overline{b}_\sigma)$$

で定めれば任意の ℓ, 任意の $\sigma\in I_\ell$ に対し $b_\sigma=0$ であるから h は任意の ℓ で unramified であり, $\overline{b}_{\sigma_0}\neq 0$ なので $h\neq 0$ である. いま L を $\mathbb{Q}(\mu_p)$ の最大不分岐 abel 拡大とすると

$$\begin{aligned}H^1(G_{\mathbb{Q}},\mathbb{F}(\omega^{-i}))&=\mathrm{Hom}_\Delta(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)),\mathbb{F}(\omega^{-i}))\\&\supseteq\mathrm{Hom}_\Delta(\mathrm{Gal}(L/\mathbb{Q}(\mu_p)),\mathbb{F}(\omega^{-i}))\\&=\mathrm{Hom}_\Delta(X_0,\mathbb{F}(\omega^{-i}))\\&=\mathrm{Hom}_\Delta(X_0^{(-i)},\mathbb{F}(\omega^{-i}))\\&=\mathrm{Hom}(X_0^{(-i)},\mathbb{F})\end{aligned}$$

であり, h は任意の ℓ で unramified であることより $0\neq h\in\mathrm{Hom}_\Delta(\mathrm{Gal}(L/\mathbb{Q}(\mu_p)),\mathbb{F}(\omega^{-i}))=\mathrm{Hom}(X_0^{(-i)},\mathbb{F})$. ゆえに $X_0^{(-i)}\neq 0$, すなわち $p|\#X_0^{(-i)}$. □

いままでの証明の要点をまとめると以下のようになる.

1. L-value と Eisenstein series の constant term を関係付ける.
2. $p|L$-value を使って Eisenstein series $\equiv$ cusp form $\mod p$ を示す.
3. cusp form の Galois 表現から Selmer 群の non-trivial な元を構成する.

3.8 Ribet の方法の一般化

Step1
i を odd とし $L_p(s,\omega^i)$ を p-進 L-関数とすると任意の $n \geq 1$ に対して

$$L_p(1-n,\omega^{i+1}) = L^{(p)}(1-n,\omega^{i+1-n})$$

であり, ある $g_i \in \Lambda$ があって $g_i((1+p)^s-1) = L_p(s,\omega^{i+1})$ を満たすのであった. いま $A_0^{(i)} \in \Lambda = \mathbb{Z}_p[[T]]$ を

$$A_0^{(i)}((1+T)^{-1}-1) = \frac{1}{2}g_i(T)$$

により決めれば, $i \not\equiv -1 \mod p-1$ のとき

$$2 \cdot A_0^{(i)}((1+p)^{k-1}-1) = L^{(p)}(1-k,\omega^{i+1-k})$$

となる. このとき $A_0^{(i)}$ は $\mathcal{E}^{(i)}$ の constant term のなる.
Step2
i を odd とし

$$\mathbb{T}_i := \mathbb{T}^{\mathrm{ord}}(1,\omega^i,R),$$
$$\mathbb{H}_i := \mathbb{H}^{\mathrm{ord}}(1,\omega^i,R)$$

とおく. このとき $\mathbb{H}_i \twoheadrightarrow \mathbb{T}_i$ であった. いま Eisenstein ideal $I_i \subseteq \mathbb{H}_i$ を

$$\{T(\ell)-1-\omega^i(\ell)(1+T)^{a_\ell}, S(\ell)-\omega^i(\ell)\ell^{-1}(1+T)^{a_\ell}, T(p)-1 \mid \ell \neq p\}$$

で生成される ideal とする. このとき I_i は $\mathcal{E}^{(i)}$ を annihilate する. $\mathbb{T}_i$ は R 上 $\{T(\ell),S(\ell),T(p) \mid \ell \neq p\}$ で生成されるので $\mathbb{T}_i = \langle I_i, R\rangle$ であることから $R \to \mathbb{T}_i$ は $R \twoheadrightarrow \mathbb{T}_i/I_i\mathbb{T}_i$ を induce する. ゆえに $J_i = \mathrm{Ker}[R \to \mathbb{T}_i/I_i\mathbb{T}_i]$ とおけば $R/J_i \cong \mathbb{T}_i/I_i\mathbb{T}_i$ が得られる.

定理 3.5 任意の height 1 prime $\mathfrak{p} \subseteq R$ に対して

$$\mathrm{ord}_{\mathfrak{p}}(J_i) \geq \mathrm{ord}_{\mathfrak{p}}(A_0^{(i)}),$$

すなわち

$$\mathrm{length}_{R_{\mathfrak{p}}}(\mathbb{T}_{i,\mathfrak{p}}/I_i\mathbb{T}_{i,\mathfrak{p}}) \geq \mathrm{ord}_{\mathfrak{p}}(A_0^{(i)})$$

が成り立つ.

証明 Ferrero-Washington の定理より $A_0^{(i)} \in \Lambda$ に対し $A_0^{(i)} = p^{\mu_i}(T^n + \cdots + a_n) \times (\text{unit})$ と書くとき $\mu_i = 0$ となるので $p \nmid A_0^{(i)}$ である. ゆえに $p \in \mathfrak{p}$ のときは $\mathrm{ord}_{\mathfrak{p}}(A_0^{(i)}) = 0$ となるからこの場合は明らか.
よって以降は $p \notin \mathfrak{p}$ と仮定する. このとき

$$A_0^{(i)} = \prod_{j=1}^{n}(T-\alpha_j) \times (\text{unit power series})$$
$$A_0^{(i-2)} = \prod_{j=1}^{m}(T-\beta_j) \times (\text{unit power series})$$

とおく. いま r を十分大きくとって (実は $r = n+1$ で十分), 1 の p^r 乗根 ζ を

$$\{\zeta^{-1}(\beta_j+1)(p+1)-1 \mid j=1,\ldots,m\} \cap \{\alpha_j \mid j=1,\ldots,n\} = \emptyset$$

となるように選ぶ. このとき $A_0^{(i-2)}(\zeta(1+T)(1+p)^{-1}-1)$ と $A_0^{(i)}$ は共通の根を持たない.

$$\mathbb{T}^{\mathrm{ord}}(1,\omega^i,R)\otimes_R R' \twoheadrightarrow \mathbb{T}^{\mathrm{ord}}(1,\omega^i,R')$$

なので ζ, α_j, $\beta_j \in R$ の場合を考えれば十分. $\mathrm{ord}_{\mathfrak{p}}A_0^{(i)}=0$ ならば明らかなので $\mathfrak{p}\subseteq R$ は $\mathrm{ord}_{\mathfrak{p}}A_0^{(i)}>0$ を満たすと仮定する. このとき ζ の取り方により $\mathrm{ord}_{\mathfrak{p}}A_0^{(i-2)}(\zeta(1+T)(1+p)^{-1}-1)=0$ であることに注意する. いま

$$\mathcal{G}=\sum_{n=0}^{\infty}B_nq^n := \mathcal{E}^{(i-2)}(\zeta(1+T)(1+p)^{-1}-1)\mathcal{E}^{(1)}(\zeta-1),\ B_n\in R$$

とおくとき

$$B_0 = A_0^{(i-2)}(\zeta(1+T)(1+p)^{-1}-1)L^{(p)}(0,\omega^i\psi_{\zeta^{-1}})$$

であり, ζ の取り方と $p\notin\mathfrak{p}$ により $\mathrm{ord}_{\mathfrak{p}}(B_0)=0$ となる. さらに十分大きな k に対して

$$\begin{aligned}\varphi_k(\mathcal{G}) &= \mathcal{E}^{(i-2)}(\zeta(1+p)^{k-2}-1)\mathcal{E}^{(1)}(\zeta-1)\\ &= \mathcal{E}^{(i-2)}(\zeta(1+p)^{k-2}-1)E_1(\omega\psi_{\zeta^{-1}})\\ &= E_{k-1}(\omega^{i-2+1-(k-1)}\psi_\zeta)E_1(\omega\psi_{\zeta^{-1}})\\ &= E_{k-1}(\omega^{i-k}\psi_\zeta)E_1(\omega\psi_{\zeta^{-1}})\in M_k(p^{r+1},\omega^{i+1-k},\mathbb{Z}_p[\zeta])\end{aligned}$$

なので $\mathcal{G}\in\mathcal{M}(p^{r+1},\omega^i,R)$ である. いま,

$$\mathcal{F}=\sum_{n=1}^{\infty}C_nq^n := e(B_0\mathcal{E}^{(i)}-A_0^{(i)}\mathcal{G}),\ C_n\in R$$

とおく. $n=\mathrm{ord}_{\mathfrak{p}}A_0^{(i)}$ とおけば $e\mathcal{E}^{(i)}=\mathcal{E}^{(i)}$ なので

$$B_0A_m(\mathcal{E}^{(i)})\equiv C_m \mod \mathfrak{p}^n$$

である. さらに

$$\mathcal{F}\in\mathcal{S}^{\mathrm{ord}}(1,\omega^i,R)$$

が成り立つ. これは後回しにしておく. いま Ψ を

$$\Psi:\mathbb{T}_{i,\mathfrak{p}}\to R_{\mathfrak{p}}/\mathfrak{p}^nR_{\mathfrak{p}}$$

を $t\mapsto B_0^{-1}\cdot A_1(\mathcal{F}|t) \mod \mathfrak{p}^n = A_1(\mathcal{E}^{(i)}|t) \mod \mathfrak{p}^n$ によって定めるとこれは環の全射準同型. さらに $t=T(\ell)-1-\omega^i(\ell)(1+T)^{a_\ell}$ のとき $\mathcal{E}^{(i)}|t=0$ なので $\Psi(t)=A_1(\mathcal{E}^{(i)}|t)=0$. ゆえに $I_i\mathbb{T}_{i,\mathfrak{p}}\subseteq\mathrm{Ker}(\Psi)$. それ故,

$$R_{\mathfrak{p}}/(\mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(J_i)}) = R_{\mathfrak{p}}/J_iR_{\mathfrak{p}}\cong\mathbb{T}_{i,\mathfrak{p}}/I_i\mathbb{T}_{i,\mathfrak{p}}\twoheadrightarrow\mathbb{T}_{i,\mathfrak{p}}/\mathrm{Ker}(\Psi)\xrightarrow{\sim}R_{\mathfrak{p}}/(\mathfrak{p}^n)$$

であるから $\mathrm{ord}_{\mathfrak{p}}(J_i)\geq n=\mathrm{ord}_{\mathfrak{p}}(A_0^{(i)})$ となる. これで定理の主張が得られた. あとは

$$\mathcal{F}\in\mathcal{S}^{\mathrm{ord}}(1,\omega^i,R)$$

を証明すればよい.

いま k を十分大きく取れば任意の $\varphi\in\mathcal{X}_k$ に対して $\varphi(\mathcal{F})$ は modular form. 一般に f は Eisenstein series と cusp form の線型結合としてかけるので,

$$\begin{aligned}f &= \sum(\text{Eisenstein series})+(\text{cusp form})\\ &= \sum_{\chi,\psi}\sum_{d\mid\frac{p^{r+1}}{\mathrm{cond}\,\chi\cdot\mathrm{cond}\,\psi}}c_{\chi,\psi,d}E_k(\chi,\psi,dz)+(\text{cusp form})\end{aligned}$$

となる. ここで

$$E_k(\chi,\psi,z)=c_0(k,\chi,\psi)+\sum_{n=1}^{\infty}\left(\sum_{d|n}\chi(n/d)\psi(d)d^{k-1}\right)q^n\in M_k(N,\chi\psi)$$

であり χ と ψ は $\chi\psi=\omega^{i+1-k}$, $(\operatorname{cond}\chi\cdot\operatorname{cond}\psi)\mid p^{r+1}$ を満たすものを動く. $E_k(\chi,\psi)$ の L-関数は $L(\chi,s)L(\psi,s-k+1)$ になる. $\mathcal{F}$ の定義より $\mathcal{F}\in\mathcal{M}^{\mathrm{ord}}$ なので $f=ef=\sum\sum c_{\chi,\psi,d}eE_k(\chi,\psi,dz)+$ (cusp form) となっている. もし $\chi\neq 1$ ならば $a_p(E_k(\chi,\psi,z))=\chi(p)+p^{k-1}\psi(p)=p^{k-1}\psi(p)\equiv 0 \mod p$ なので $eE_k(\chi,\psi,z)=0$ がわかる.

$$T(p)E_k(\chi,\psi,p^{s+1}z)=E_k(\chi,\psi,p^sz)$$

なので結局 $eE_k(\chi,\psi,dz)=eE_k(\chi,\psi,z)=0$ であるから $\chi\neq 1$ となる項は現れない. いま $\chi\psi=\omega^{i+1-k}$ であったから $\psi=\omega^{i+1-k}$. よって

$$f=cE_k(1,\omega^{i+1-k},z)+(\text{cusp form})=cE_k(\omega^{i+1-k})+(\text{cusp form})$$

しかし

$$0=a_0(f)=c\cdot a_0(E_k(\omega^{i+1-k}))=c\cdot L^{(p)}(1-k,\omega^{i+1-k})$$

であり, $L^{(p)}(1-k,\omega^{i+1-k})\neq 0$ なので $c=0$. 以上から f は cusp form であり $\mathcal{F}\in\mathcal{S}^{\mathrm{ord}}(1,\omega^i,R)$ であることが分かった. □

4 Iwasawa Main Conjecture の証明

4.1 Iwasawa Main Conjecture revisited

$\mu_{p^n}:=\{\zeta\in\overline{\mathbb{Q}}\mid\zeta^{p^n}=1\}$ とし $K_\infty:=\mathbb{Q}(\mu_{p^\infty})=\bigcup_{n\geq 0}\mathbb{Q}(\mu_{p^n})$ とおく. このとき

$$\mathrm{Gal}(K_\infty/\mathbb{Q})\cong\mathbb{Z}_p^\times\cong(\mathbb{Z}/p\mathbb{Z})^\times\times(1+p\mathbb{Z}_p)\cong\Delta\times\Gamma,\ \Gamma\cong(1+\mathbb{Z}_p)\cong\mathbb{Z}_p$$

であり, Γ の topological generator を γ とするとき γ に $1+T$ を対応させることで同型 $\mathbb{Z}_p[[\Gamma]]\cong\Lambda:=\mathbb{Z}_p[[T]]$ が成り立つのであった. いま $\Lambda_0:=\mathbb{Z}_p[[X]]$ とおき $1+X$ に $(1+T)^{-1}$ を対応させる同型 $\mathbb{Z}_p[[X]]\cong\mathbb{Z}_p[[T]]$ を考える. i を odd とし,

$$\Phi_i:G_{\mathbb{Q}}\twoheadrightarrow\Delta\times\Gamma\to\Lambda_0^\times$$

を $\Delta\times\Gamma\ni(a,\gamma)\mapsto\omega(a)^i(1+X)^{-1}\in\Lambda_0^\times$ によって定める. また $\Lambda_0^\vee:=\mathrm{Hom}_{\mathrm{cont}}(\Lambda_0,\mathbb{Q}_p/\mathbb{Z}_p)$ を $f\in\Lambda_0^\vee$, $m\in\Lambda_0$ に対し $(mf)(\lambda)=f(m\lambda)$ と定めることにより Λ_0-module とみなす. $\Lambda_0^\vee$ には Φ_i を通して $G_{\mathbb{Q}}$ が作用している. このとき

$$\mathrm{Sel}(\omega^i):=H^1_{\mathrm{ur}}(G_{\mathbb{Q}},\Lambda_0^\vee)=\mathrm{Ker}\left[H^1(G_{\mathbb{Q}},\Lambda_0^\vee)\to\prod_{\ell:\text{ prime}}H^1(I_\ell,\Lambda_0^\vee)\right]$$

と定義する. さらに

$$S(\omega^i):=\mathrm{Sel}(\omega^i)^\vee:=\mathrm{Hom}_{\mathrm{cont}}(\mathrm{Sel}(\omega^i),\mathbb{Q}_p/\mathbb{Z}_p)$$

とおくと $S(\omega^i)$ は有限生成 Λ_0-module.

予想 4.1 (Iwasawa Main Conjecture) L_∞/K_∞ を maximal unramified abelian pro-p extension として $X_\infty = \bigoplus_{i=1}^{p-1} X_\infty^{(i)}$ とおき, $f_i(T)$ を $X_\infty^{(i)}$ の characteristic power series とすれば

$$f_i(T)\Lambda = A_0^{(-i)}((1+T)^{-1}-1)\Lambda$$

が成り立つ.

補題 4.2 Iwasawa Main Conjecture は $S(\omega^i)$ が torsion Λ_0-module で

$$\mathrm{char}_{\Lambda_0} S(\omega^i) = A_0^{(-i)}(X)$$

が成り立つことと同値.

証明 $X_\infty^{(i)}$ には $1+X$ が γ^{-1} として作用している. このとき,

$$\begin{aligned}
\mathrm{Sel}(\omega^i) &\xrightarrow{\sim} H^1_{\mathrm{ur}}(G_{K_\infty}, \Lambda_0^\vee)^{G_\mathbb{Q}} \qquad \text{(restriction map)} \\
&= \mathrm{Hom}_{G_\mathbb{Q}}(X_\infty, \Lambda_0^\vee) \\
&= \mathrm{Hom}_\Gamma(X_\infty^{(i)}, \Lambda_0^\vee) \\
&\overset{\sim}{=} \mathrm{Hom}_{\Lambda_0}(X_\infty^{(i)}, \Lambda_0^\vee) \qquad (\Lambda\text{-isomorphism}) \\
&\overset{\sim}{=} \mathrm{Hom}_{\mathbb{Z}_p}(X_\infty^{(i)}, \mathbb{Q}_p/\mathbb{Z}_p) \quad (\Lambda\text{-isomorphism})
\end{aligned}$$

であるから

$$\mathrm{char}_{\Lambda_0} S(\omega^i) = \mathrm{char}_{\Lambda_0} X_\infty^{(i)} = (f((1+X)^{-1}-1))$$

となる. ただし $f(T) = \mathrm{char}_\Lambda X_\infty^{(i)}$ とおいた. (同型 $\Lambda_0 \cong \Lambda$ は $(1+X) \mapsto (1+T)^{-1}$ で与えられていたことに注意する) Iwasawa Main Conjecture は $f((1+X)^s - 1) = L_p(\omega^{-i+1}, s)\,(i \not\equiv -1 \mod p-1)$ であったからこれは $f((1+X)^{-1}-1) = A_0^{(-i)}(X)$ と同値である. ゆえにこの補題が証明された. □

4.2 十分大きな R の場合への帰着

R を Λ_0 の商体の有限次拡大の中での Λ_0 の整閉包とする. このとき

$$R^\vee := \mathrm{Hom}_{\mathrm{cont}}(R, \mathbb{Q}_p/\mathbb{Z}_p) = R \otimes_{\Lambda_0} \Lambda_0^\vee$$

には $G_\mathbb{Q}$ が Φ_i を通して作用している. また, $\mathrm{Sel}(\omega^i, R) := H^1_{\mathrm{ur}}(G_\mathbb{Q}, R^\vee)$, $S(\omega^i, R) := \mathrm{Sel}(\omega^i, R)^\vee = \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Sel}(\omega^i, R), \mathbb{Q}_p/\mathbb{Z}_p)$ とおく.

補題 4.3 Iwasawa Main conjecture と $\mathrm{char}_R S(\omega^i, R) = A_0^{(-i)}(X)$ が成り立つことは同値.

命題 4.4 ある R が存在して, 任意の odd な i と任意の height 1 prime $\mathfrak{p} \subseteq R$ に対して

$$\mathrm{length}_{R_\mathfrak{p}} S(\omega^i, R)_\mathfrak{p} \geq \mathrm{ord}_\mathfrak{p}(A_0^{(-i)}(X))$$

ならば Iwasawa Main Conjecture が成り立つ.

証明 類数公式によって任意の height 1 prime $\mathfrak{p} \subseteq R$ に対して

$$\sum_{i:\mathrm{odd}} \mathrm{ord}_\mathfrak{p}(\mathrm{char}_\Lambda X_\infty^{(i)}) = \sum_{i:\mathrm{odd}} \mathrm{ord}_\mathfrak{p}(A_0^{(-i)}((1+T)^{-1}-1))$$

であるから

$$\sum_{i:\mathrm{odd}} \mathrm{length}_{R_\mathfrak{p}} S(\omega^i, R)_\mathfrak{p} = \sum_{i:\mathrm{odd}} \mathrm{ord}_\mathfrak{p}(\mathrm{char}_R S(\omega^i, R)) = \sum_{i:\mathrm{odd}} \mathrm{ord}_\mathfrak{p}(A_0^{(-i)}(X))$$

である. ゆえに

$$\mathrm{length}_{R_\mathfrak{p}} S(\omega^i, R)_\mathfrak{p} \geq \mathrm{ord}_\mathfrak{p}(A_0^{(-i)}(X))$$

ならば

$$\mathrm{length}_{R_\mathfrak{p}} S(\omega^i, R)_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(A_0^{(-i)}(X))$$

でなくてはならない. これが任意の height 1 prime $\mathfrak{p} \subseteq R$ に対して成り立てば $\mathrm{char}_R S(\omega^i, R) = A_0^{(-i)}(X)$ なので Lemma 4.3 により Iwasawa Main Conjecture が成り立つ. □

4.3 Hecke algebra と Galois 表現

i を odd とし $\mathbb{T} = \mathbb{T}^{\mathrm{ord}}(1, \omega^i, R)$ とおけば $\mathbb{T}$ は reduced ring であり R を十分大きくとれば任意の R-adic eigenform に対応する minimal prime $Q \subseteq \mathbb{T}$ に対し $R \cong \mathbb{T}/Q$ となる.

$\mathcal{F}$ を R-adic eigenform とすれば $T(\ell)\mathcal{F} = C_\ell \mathcal{F}$, $C_\ell \in R$ となるのであった. $Q \subseteq \mathbb{T}$ を $\mathcal{F}$ に対応する minimal prime とするとき $R \xrightarrow{\sim} \mathbb{T}/Q$ という同型の下で $C_\ell \mapsto T(\ell)$ という対応になる. Hecke 環と modular form の空間の duality により

$$\mathcal{S}^{\mathrm{ord}}(1, \omega^i, R) \xrightarrow{\sim} \mathrm{Hom}_R(\mathbb{T}, R)$$

となっているのであった. いま $\mathfrak{p} \subseteq R$ を height 1 prime とする. 前に見たように $I_i \subseteq \mathbb{T}$ を $\{T(\ell) - 1 - \omega^i(\ell)(1+T)^{a_\ell}, S(\ell) - \omega^i(\ell)\ell^{-1}(1+T)^{a_\ell}\}_{\ell \neq p}$ と $T(p) - 1$ で生成される ideal として $R/J_i \xrightarrow{\sim} \mathbb{T}/I_i$ を考えると $\mathrm{ord}_\mathfrak{p}(J_i) \geq \mathrm{ord}_\mathfrak{p}(A_0^{(i)})$ となるのであった. $\mathfrak{p} \subseteq J_i$ と仮定する. $Q_1, \ldots, Q_n$ を $\mathbb{T}_\mathfrak{p}$ の minimal prime とする. このとき

$$\mathbb{T}_\mathfrak{p} \hookrightarrow \prod_{i=1}^n \mathbb{T}_\mathfrak{p}/Q_i = \prod_{i=1}^n R_\mathfrak{p}$$

となっている. いま $\widetilde{\mathbb{T}} := \mathrm{Im}[\mathbb{T} \to \mathbb{T}_\mathfrak{p}]$ とおく.

各 Q_j に対して Galois 表現 $\rho_j : G_\mathbb{Q} \to V_j$ ここで V_j は $L(= R$ の fraction field$= R_\mathfrak{p}$ の fraction field) 上の二次元 vector space で ρ_j は $\mathbb{T}$ への pseudo representation から induce されるものとする. Q_j を考えることと $\mathcal{S}^{\mathrm{ord}}(1, \omega^i, R)$ の基底 $\mathcal{F}_j$ たちの Galois 表現 $\rho_{\mathcal{F}_j}$ を考えることは同じである. このとき

1. $\rho_j = \rho_{\mathcal{F}_j}$ は irreducible.
2. $\rho_j|_{D_p} \simeq \begin{pmatrix} \psi_1^{(j)} & * \\ 0 & \psi_2^{(j)} \end{pmatrix}$, $\psi_2^{(j)}|_{I_p} = 1$.
3. $\det \rho_j(\gamma) = 1 + X$, $(A_0^{(i)} \in \mathbb{Z}_p[[X]])$

となる. いま $1 + X \notin \mathfrak{p}$ と仮定する. このとき

$$\rho_j(\gamma) = \begin{pmatrix} 1 & 0 \\ 0 & 1+X \end{pmatrix},$$

$$\rho_j : G_\mathbb{Q} \to \mathrm{GL}_2(R_\mathfrak{p})$$

と仮定してよい. $x_j \in V_j$ を $\rho_j(\gamma)x_j = (1+X)x_j$ を満たすように選ぶ. (I_p は x_j に $\bigoplus_i \psi_i^{(j)}|_{I_p}$ として作用する) $V := \bigoplus_{j=1}^n V_j$, $x := \bigoplus_{j=1}^n x_j$ とおく. いま $\mathbb{T}_\mathfrak{p} \hookrightarrow \bigoplus_{j=1}^n R_\mathfrak{p}$ の V への作用は $G_\mathbb{Q}$ の作用と可換である. $\mathcal{R} := \mathbb{T}_\mathfrak{p}[G_\mathbb{Q}]$ の V への作用をまた ρ と書くことにする. $\mathcal{L} := \mathcal{R}x$ とおけばこれは finite free $R_\mathfrak{p}$-module である.

4.4 Iwasawa Main Conjecture の証明のための準備

いま

$$\rho_j : G_{\mathbb{Q}} \to \mathrm{Aut}_L(V_j)$$

に対して rank が 2 の $G_{\mathbb{Q}}$-stable free $R_{\mathfrak{p}}$-module M_j を

$$\rho_j : G_{\mathbb{Q}} \to \mathrm{GL}_2(R_{\mathfrak{p}}) \simeq \mathrm{Aut}(M_j)$$

を満たすようにとる. このとき $\mathrm{trace}\rho_j : G_{\mathbb{Q}} \to R$ は continuous, ρ_j は irreducible であり p 以外で不分岐. いま M_j の $R_{\mathfrak{p}}$-basis を

1. Γ の topological generator γ の I_p への lift $\widetilde{\gamma}$ に対し $\rho_j(\widetilde{\gamma}) = \begin{pmatrix} 1 & 0 \\ 0 & 1+X \end{pmatrix}$.

2. $\rho_j|_{D_p} = \begin{pmatrix} \psi_2^{(j)} & 0 \\ * & \psi_1^{(j)} \end{pmatrix}$, $\psi_2^{(j)}|_{I_p} = 1$, $\psi_1^{(j)}\psi_2^{(j)} = \Phi_i$.

となるようにとる. さらに $\rho_j(\gamma)x_j = (1+X)x_j$ となる $x_j \in M_j$ を固定しておく. $V = \bigoplus_{j=1}^n V_j$ とし $\rho = \bigoplus_{j=1}^n \rho_j : G_{\mathbb{Q}} \to \mathrm{Aut}_L(V)$ とおく. いま $\mathbb{T}_{\mathfrak{p}} \subseteq \bigoplus_{j=1}^n R_{\mathfrak{p}}$ を

$$\langle \mathrm{trace}\rho(\mathrm{Frob}_\ell) = \bigoplus_{j=1}^n \mathrm{trace}\rho_j(\mathrm{Frob}_\ell) \mid \ell \neq p \rangle$$

で生成される $R_{\mathfrak{p}}$-module, いま $\widetilde{\mathbb{T}} \subseteq \bigoplus_{j=1}^n R$ を

$$\langle \mathrm{trace}\rho(\mathrm{Frob}_\ell) = \bigoplus_{j=1}^n \mathrm{trace}\rho_j(\mathrm{Frob}_\ell) \mid \ell \neq p \rangle$$

で生成される R-module, $I \subseteq \mathbb{T}_{\mathfrak{p}}$ を

$$\langle \mathrm{trace}\rho(\mathrm{Frob}_\ell) - 1 - \Phi_i(\mathrm{Frob}_\ell) \mid \ell \neq p \rangle$$

で生成される ideal とする. 以降, 簡単のため $I = I_i$, $J = J_i$ と書くことにする. 以上の仮定の下で $R_{\mathfrak{p}}/J \simeq \mathbb{T}_{\mathfrak{p}}/I$ のとき Theorem 3.5 により

$$\mathrm{ord}_{\mathfrak{p}}(J) \geq \mathrm{ord}_{\mathfrak{p}}(A_0^{(i)})$$

が分かっているのであった. さらに $\mathcal{R} = \mathbb{T}_{\mathfrak{p}}[G_{\mathbb{Q}}]$ とおき,

$$\mathcal{L}' := \widetilde{\mathbb{T}}[G_{\mathbb{Q}}]x \subseteq \mathcal{L} = \mathcal{R}x \subseteq \bigoplus M_j \subseteq V$$

とかくとき $\mathcal{L}'_{\mathfrak{p}} = \mathcal{L}$ となる. いま $\varepsilon_1 := -\frac{1}{X}(\gamma - (1+X))$, $\varepsilon_2 := \frac{1}{X}(\gamma - 1) \in \mathcal{R}$ とおくと $\varepsilon_1 + \varepsilon_2 = 1$ であり, 任意の $\ell \in \mathcal{L}$ に対し $\varepsilon_i^2\ell = \varepsilon_i\ell$, $\varepsilon_1\varepsilon_2\ell = \varepsilon_2\varepsilon_1\ell = 0$ を満たすので ε_i は projector. よって $\mathcal{L}_1 = \varepsilon_1\mathcal{L}$, $\mathcal{L}_2 = \varepsilon_2\mathcal{L}$ とおくと $\mathcal{L} = \mathcal{L}_1 \oplus \mathcal{L}_2$ となる.

注 4.5 $\mathcal{L}_1$, $\mathcal{L}_2$ は $\mathbb{T}_{\mathfrak{p}}$-module であるが $G_{\mathbb{Q}}$-stable ではない.

補題 4.6 *1.* $\mathcal{L}_2 = \mathbb{T}_{\mathfrak{p}}x$ が成り立つ.

2. $\mathrm{Fitt}_{\mathbb{T}_{\mathfrak{p}}}(\mathcal{L}_1) = 0$ が成り立つ.

証明
$\rho(\varepsilon_2) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ なので $\varepsilon_2 x = x$. ゆえに $\mathbb{T}_\mathfrak{p} x \subseteq \varepsilon_2 \mathcal{L} = \mathcal{L}_2$. $r \in \mathcal{R}$ に対し

$$\rho(r) = \begin{pmatrix} a_r & b_r \\ c_r & d_r \end{pmatrix} \in M_2(R_\mathfrak{p})$$

とかくとき $\rho(\varepsilon_2 r) = \begin{pmatrix} 0 & 0 \\ c_r & d_r \end{pmatrix}$ となるので $\rho(\varepsilon_2 r)x = d_r x = \varepsilon_2 r x$. いま $d_r = \mathrm{trace}\rho(\varepsilon_2 r) \in \mathbb{T}_\mathfrak{p}$ なので $\varepsilon_2 r x \in \mathbb{T}_\mathfrak{p} x$. ゆえに $\mathcal{L}_2 = \varepsilon_2 \mathcal{R} x \in \mathbb{T}_\mathfrak{p}$. これで 1. が示された.

$\mathbb{T}_\mathfrak{p}$ は reduced なので $\mathrm{Ann}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_1) = 0$ なら $\mathrm{Fitt}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_1) = 0$ であるからこれを示す. $t \in \mathbb{T}_\mathfrak{p}$ は $t\mathcal{L}_1 = 0$ を満たすとすると任意の $r \in \mathcal{R}$ に対し $\rho_j(t\varepsilon_1 r)x = 0$ となる. いま $t \neq 0$ とすると, ある j があって, 任意の $r \in \mathcal{R}$ に対して $\rho_j(\varepsilon_1 r)x = 0$, つまり $b_r = 0$ であるから ρ_j は reducible となってしまうが, これは起こりえない. よって $t = 0$ であり $\mathrm{Ann}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_1) = 0$. □

いま $r \in \mathcal{R}$ に対し

$$\rho(r) = \begin{pmatrix} A_r & B_r \\ C_r & D_r \end{pmatrix}$$

と書くとき,

$$A_r \in \mathrm{Hom}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_1, \mathcal{L}_1)$$
$$B_r \in \mathrm{Hom}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_2, \mathcal{L}_1)$$
$$C_r \in \mathrm{Hom}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_1, \mathcal{L}_2)$$
$$D_r \in \mathrm{Hom}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_2, \mathcal{L}_2)$$

となっている. $\mathbb{T}_\mathfrak{p} \ni d \mapsto (x \mapsto dx) \in \mathrm{Hom}_{\mathbb{T}_\mathfrak{p}}(\mathcal{L}_2, \mathcal{L}_2)$ は Lemma 4.6 により同型になる.

補題 4.7 *1. $\sigma \in D_p$ に対して $B_\sigma = 0$.*

2. $\mathcal{L}_1$ は $\{B_r \mid r \in \mathcal{R}\}$ の生成する $\mathbb{T}_\mathfrak{p}$-module.

3. $\{C_r \mid r \in \mathcal{R}\} \subseteq I\mathcal{L}_2 = Ix$ が成り立つ.

4. $\mathcal{L}_1/I\mathcal{L}_1$ は $G_\mathbb{Q}$-stable. さらに $G_\mathbb{Q}$ は trivial に作用する.

5. $D_r \mod I = \Phi_i(r) \mod I \in R_\mathfrak{p}/J \simeq \mathbb{T}_\mathfrak{p}/I$ が成り立つ.

証明

1. これは ρ_j の基底の取り方から明らか.

2. $\mathcal{L}_1 \oplus \mathcal{L}_2 = \mathcal{L} \subseteq \{B_r x \mid r \in \mathcal{R}\} \oplus \{D_r x \mid r \in \mathcal{R}\}$ であり $\mathrm{Im}\, B \subseteq \mathcal{L}_1$, $\{D_r x \mid r \in \mathcal{R}\} = \mathcal{L}_2$ であることから従う.

3. $D_r = \mathrm{trace}\rho(\varepsilon_2 r) \mod I = \mathrm{trace}(1 \oplus \Phi_i)(\varepsilon_2 r) \mod I = \Phi_i(r) \mod I$ であるから任意の $r, r' \in \mathcal{R}$ に対して $D_{rr'} \equiv D_r D_{r'} \mod I$. 一方, 直接計算すれば $D_{rr'} = D_r D_{r'} + C_r B_{r'}$ なので $\{D_r x \mid \mathcal{R}\} = \mathcal{L}_2$ を使うと $\{C_r B_{r'} x \mid r, r' \in \mathcal{R}\} \subseteq I\mathcal{L}_2 = Ix$. ゆえに $\{C_r x \mid r \in \mathcal{R}\} \subseteq I\mathcal{L}_2$.

4. $A_\sigma \mod I$ が identity になることを示す.

$$\rho(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ c_\sigma & d_\sigma \end{pmatrix} \in \bigoplus_{i=1}^{n} \mathrm{GL}_2(R_\mathfrak{p})$$

とおけば A_σ は $\varepsilon_1 rx \in \mathcal{L}_1$ に $a_\sigma = \bigoplus_{i=1}^n a_\sigma^{(i)} \in \bigoplus_{i=1}^n R_\mathfrak{p}$ 倍で作用する. しかし

$$a_\sigma = \mathrm{trace}\rho(\varepsilon_1\sigma) \equiv \mathrm{trace}(1 \oplus \Phi_i)(\varepsilon_1\sigma) = 1 \mod I$$

であるから $\mathrm{mod}\, I$ では identity として作用する. ゆえに $\mathcal{L}_1/I\mathcal{L}_1$ 上に $G_\mathbb{Q}$ は trivial に作用する.

5. この Lemma の 4 より $A_\sigma \equiv 1 \mod I$ であり, I は $\{\mathrm{trace}\rho(\mathrm{Frob}_\ell) - 1 - \Phi_i(\mathrm{Frob}_\ell)\}$ で生成される ideal であったから $D_r \equiv \Phi_i(r) \mod I$. □

この Lemma 4.7 により

$$\rho(\sigma) \equiv \begin{pmatrix} 1 & B_\sigma \\ 0 & \Phi_i(\sigma) \end{pmatrix} \mod I$$

となる.

いま $\mathcal{L}' := \widetilde{\mathbb{T}}[G_\mathbb{Q}]x \subset \mathcal{L}$ に対して $\overline{\mathcal{L}}' := \mathrm{Im}[\mathcal{L}' \to \mathcal{L}/I\mathcal{L}]$, $\overline{\mathcal{L}}'_1 := \overline{\mathcal{L}}' \cap (\mathcal{L}_1/I\mathcal{L}_1)$ とおく. このとき $\overline{\mathcal{L}}'_\mathfrak{p} = \mathcal{L}/I\mathcal{L}$ であり $\overline{\mathcal{L}}'_{1,\mathfrak{p}} = \mathcal{L}_1/I\mathcal{L}_1$ となる.

補題 4.8 $\overline{\mathcal{L}}'$ は $G_\mathbb{Q}$ が Φ_i として作用するような非自明な $\widetilde{\mathbb{T}}[G_\mathbb{Q}]$-submodule を含まない.

証明

ρ が既約であるので B_σ は non-trivial であることと $1 \not\equiv \Phi_i \mod I$ であることから従う. □

定義 4.9 $G_\mathbb{Q} \to \overline{\mathcal{L}}'_1$ の cocycle を

$$c(\sigma) = \Phi_i^{-1}(\sigma)B_\sigma(x) \mod I \in \overline{\mathcal{L}}'_1$$

により定義する. また α を

$$\alpha : \mathrm{Hom}(\overline{\mathcal{L}}'_1, R^\vee) \ni \psi \mapsto [\sigma \mapsto \psi(c(\sigma))] \in H^1(G_\mathbb{Q}, R^\vee)$$

によって定める.

補題 4.10 *1.* $\mathrm{Im}(\alpha) \subseteq H^1_{\mathrm{ur}}(G_\mathbb{Q}, R^\vee)$.

2. α は injective.

証明

1. これは作り方から明らか.

2. はじめに $0 \neq \psi \in \mathrm{Hom}(\overline{\mathcal{L}}'_1, R^\vee)$ は常に単射であることに注意する. なぜならば, もし単射ではないと仮定すると $\overline{\mathcal{L}}'_1/\mathrm{Ker}\psi \neq 0$ であり,

$$0 \to \overline{\mathcal{L}}'_1/\mathrm{Ker}\psi \to \overline{\mathcal{L}}'/\mathrm{Ker}\psi \to \mathrm{Im}[\overline{\mathcal{L}}' \to \mathcal{L}_2/I\mathcal{L}_2] \to 0$$

という exact sequence が得られ, これは構成から $\mathbb{Q}(\mu_{p^\infty})$ 上 split することがわかる. いま $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ は abelian であり, 素数 ℓ を適当に選べば

$$\overline{\mathcal{L}}'/\mathrm{Ker}\psi = \mathrm{Ker}(\mathrm{Frob}_\ell - \Phi_i(\mathrm{Frob}_\ell)) \oplus \mathrm{Ker}(\mathrm{Frob}_\ell - 1)$$

と書くことができるが, これは $G_{\mathbb{Q}}$-module としての splitting $\mathrm{Im}[\overline{\mathcal{L}}' \to \mathcal{L}_2/I\mathcal{L}_2] \to \overline{\mathcal{L}}'/\mathrm{Ker}\psi$ を与える. これは非自明な $\widetilde{\mathbb{T}}[G_{\mathbb{Q}}]$-module の map であり, その image には $G_{\mathbb{Q}}$ が Φ_i を通して作用するので, これは Lemma 4.8 に矛盾. よって ψ は単射でなくてはならない. もし $0 \neq \psi \in \mathrm{Ker}(\alpha)$ があったとすると $c(\sigma)$ が non-trivial であることに矛盾することから Lemma の主張が従う. □

Iwasawa Main Conjecture の証明

$\mathrm{Im}\alpha \subseteq \mathrm{Sel}(\omega^i) = H^1_{\mathrm{ur}}(G_{\mathbb{Q}}, R^\vee)$ であるから

$$S(\omega^i) = \mathrm{Sel}(\omega^i)^\vee \twoheadrightarrow (\mathrm{Im}\alpha)^\vee \simeq \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Hom}_R(\overline{\mathcal{L}}'_1, R^\vee), \mathbb{Q}_p/\mathbb{Z}_p) \simeq (\overline{\mathcal{L}}'_1)^\vee$$

となる. よって,

$$\begin{aligned} \mathrm{length}_{R_{\mathfrak{p}}} S(\omega^{-i})_{\mathfrak{p}} &\geq \mathrm{length}_{R_{\mathfrak{p}}} (\overline{\mathcal{L}}'_1)_{\mathfrak{p}} \\ &= \mathrm{length}_{R_{\mathfrak{p}}} \mathcal{L}_1/I\mathcal{L}_1 \\ &= \mathrm{ord}_{\mathfrak{p}} \mathrm{Fitt}_{R_{\mathfrak{p}}}(\mathcal{L}_1/I\mathcal{L}_1) \end{aligned}$$

であり Lemma 4.6 の 2 により

$$\mathrm{Fitt}_{R_{\mathfrak{p}}}(\mathcal{L}_1/I\mathcal{L}_1) \mod J = \mathrm{Fitt}_{R_{\mathfrak{p}}/J}(\mathcal{L}_1/I\mathcal{L}_1) = \mathrm{Fitt}_{\mathbb{T}_{\mathfrak{p}}/I}(\mathcal{L}_1/I\mathcal{L}_1) = 0$$

ゆえに

$$\mathrm{ord}_{\mathfrak{p}} \mathrm{Fitt}_{R_{\mathfrak{p}}}(\mathcal{L}_1/I\mathcal{L}_1) \geq \mathrm{ord}_{\mathfrak{p}}(J) \geq \mathrm{ord}_{\mathfrak{p}} A_0^{(i)}.$$

よって Proposition 4.4 により Iwasawa Main conjecture が従う. □

5 Λ-adic form の geometric version

$\mathcal{F} \in \Lambda[[q]]$ を Λ-adic eigenform とする. 十分大きな k に対し $\varphi_k(\mathcal{F})$ は weight k の modular form となる. ここで $\varphi_k : \Lambda \to \mathbb{Z}_p$ は $T \to (1+p)^{k-1} - 1$ で与えられるのであった.

ここでは R 上の modular form の geometric な見方を与える.

E を R 上の elliptic curve とする. $\omega \in H^0(R, \Omega^1)$ を至る所で non-vanishing な invariant differential とする. このようなものは local には常に存在する.

定義 5.1 (Geometric modular form) R' を R-algebra とする.

$$F : \{(E, \omega)_{/R'} \mid E : \text{elliptic curve}/R,\ \omega : \text{differential}\} \to R'$$

が次の条件を満たすとき weight k の geometric modular form という.

1. 任意の $R'^\times$ に対して $F(E, \lambda\omega) = \lambda^{-k} F(E, \omega)$.
2. $F(E, \omega)$ は $(E, \omega)_{/R'}$ の同型類のみで決まる.
3. F は係数の拡大 $R \to R'$ と可換.

R 上の weight k の geometric modular form のなす環を $M_k(R)$ と書く.

例 5.2 E を $\mathbb{C}$ 上の elliptic curve とすれば $\tau \in \mathbb{H}$ があって $E \simeq \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ であり $\omega = dz$ とする. $F(\tau)$ を $\mathbb{H}$ 上正則な weight k の modular form とすれば

$$F((\mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}), dx)) := F(\tau)$$

は weight k の geometric modular form.

5.1 q-expansion

$(\mathrm{Tate}(q), \omega_{\mathrm{can}})$ を $\mathbb{Z}((q))$ 上の Tate curve とする. F を R 上の geometric modular form とするとき F の q-expansion を

$$F(q) := F((\mathrm{Tate}(q), \omega_{\mathrm{can}})) \in R[[q]]$$

と定める.

注 5.3 F が classical な modular form $F(\tau)$ から構成されるときは $F(q)$ は通常の q-expansion となる.

$$(\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}, dz) \overset{\exp}{\mapsto} (\mathbb{C}^\times/q^{\mathbb{Z}}, dq/q),\ q = \exp(2\pi i z).$$

注 5.4 $1/p \in R$ のとき $\Gamma_0(p^n)$, χ に対応する geometric modular form は先の条件に加えて level structure $\varphi : \mu_{p^n} \hookrightarrow E[p^n]$ も考えることにより

$$F : \{(E, \omega, \varphi)\} \to R$$

で任意の $\alpha \in \mathbb{Z}_p^\times$ に対して

$$F((E, \omega, \alpha\varphi)) = \chi(\alpha)F((E, \omega, \phi))$$

を満たすものとして同様に定義できる.

5.2 Katz の generalized p-adic modular form

p を素数とし R, R' を p-進完備で分離的な環とする. E を elliptic curve とし, $\psi : \widehat{E} \to \widehat{\mathbb{G}}_m$ を R' 上の形式群の同型とする.

定義 5.5 F が $(E, \psi)_{/R'}$ に対する R-valued な関数で, 拡大 $R' \to R''$ に対して可換で $F((E, \psi))$ は $(E, \psi)_{/R'}$ の同型類のみによって決まるとき F を generalized p-adic modular function と呼ぶ. $\mathbb{V}_R$ を R 上の generalized p-adic modular function のなす環とする.

注 5.6

1. $\mathrm{Tate}(q)$ と $\psi = \psi_{\mathrm{can}/\widehat{\mathbb{Z}_p((q))}}$ に対し

$$F(q) := F((\mathrm{Tate}(q), \psi_{/R((q))})) \in \widehat{R((q))}$$

とおく.

2. F を R 上の weight k の geometric modular form とすると

$$(E, \psi)_{/R'} \mapsto F((E, \psi^*(dt/t)))$$

と考えることで $\mathbb{V}_R$ の元と考えることが出来る. よって $M_k(R) \to \mathbb{V}_R$ が得られる.

3. $\mathbb{V}_R \overset{q-\exp}{\to} \widehat{R[[q]]}$ の cokernel は R 上 flat.

4. $F \in M_k(R)$ の q-expansion と F の $M_k(R) \to \mathbb{V}_R$ での image の q-expansion は等しい.

5. $\{f_i\}$ を $\mathbb{Z}_p$ 上の weight k の geometric modular form の finite set とし,

$$\sum_i f_i(q) = p^n h(q) \in \mathbb{Z}_p[[q]]$$

とおくと, ある $h \in \mathbb{V}_{\mathbb{Z}_p}$ が存在して h の q-expansion は $h(q)$ に一致する.

6. $h_i \in \mathbb{V}_{\mathbb{Z}_p}$ に対し $h_i(q)$ は $\widehat{\mathbb{Z}_p[[q]]}$ の中で $h(q)$ に収束するとき, $h(q)$ はある $h \in \mathbb{V}_{\mathbb{Z}_p}$ の q-expansion になる. *($\mathbb{V}_R$ は p-進完備であり分離的である)*

7. $M_k(\Gamma_0(p^n), \chi)_{/\mathbb{Q}_p[\chi]} \hookrightarrow \mathbb{V}_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p[\chi]$ であり q-expansion と commute する. いま
$$M_k(\Gamma_0(p^n), \chi; O) := M_k(\Gamma_0(p^n), \chi)_{/\mathbb{Q}_p[\chi]} \cap \mathbb{V}_{\mathbb{Z}_p} \otimes_{\mathbb{Z}_p} O[\chi]$$
と定義する.

いま specialization $\mathbb{V}_\Lambda \ni F \mapsto \varphi_k(F) \in \mathbb{V}_{\mathbb{Z}_p}$ のもとで character χ の Λ-adic modular form の条件
$$\varphi(F) \in M_k(p^n, \chi\omega^{1-k}, O)$$
を考えることにより Λ-adic modular form の空間は $\mathbb{V}_\Lambda$ の Λ-submodule となる.

5.3 Measure theoretic な Λ-adic form

R を p 進完備で分離的な環とする.
$$\mathrm{Meas}(\mathbb{Z}_p, R) := \mathrm{Hom}_{\mathbb{Z}_p}(C(\mathbb{Z}_p, \mathbb{Z}_p), R)$$
の元のことを $\mathbb{Z}_p$ 上の R-valued measure と呼ぶ. $\mu \in \mathrm{Meas}(\mathbb{Z}_p, R)$ は $b_n := \mu(\begin{pmatrix} x \\ n \end{pmatrix})$ の値で決まる. いま
$$\mathrm{Meas}(\mathbb{Z}_p, R) \ni \mu \mapsto f_\mu := \sum b_n T^n \in R[[T]]$$
は同型であり
$$\mu((1+p)^{sx}) = f_\mu((1+p)^s - 1)$$
となる. $\mu_F \in \mathrm{Meas}(\mathbb{Z}_p, R)$ が $\mu_F((1+p)^{(k-1)x}) \in M_k(p^n, \chi\omega^{1-k}, O)$ を満たしていると仮定する. $n \geq 0$ に対し $\ell_n : \mathbb{V}_{\mathbb{Z}_p} \to \mathbb{Z}_p$ を f に対し f の n 番目の Fourier 係数を対応させる map とする. このとき $\ell \circ \mu \in \mathrm{Meas}(\mathbb{Z}_p, \mathbb{Z}_p) \simeq \mathbb{Z}_p[[T]]$ である. いま $f_n := f_{\ell_n \circ \mu_F}$ とおくと
$$F = \sum_{n=0}^{\infty} f_n q^n$$
は Λ-adic modular form になる. ゆえに
$$\{\mu_F \in \mathrm{Meas}(\mathbb{Z}_p, \mathbb{V}_{\mathbb{Z}_p}) \mid \mu_F((1+p)^{(k-1)x}) \in M_k(p^n, \chi\omega^{1-k}, O)\} \subseteq \{\Lambda\text{-modular form}\}$$
が成り立つ. classical な modular form の極限が $\mathbb{V}_{\mathbb{Z}_p}$ の元になることを使えば "$\supseteq$" もわかる.

参考文献

[1] H. Hida, *Elementary theory of L-functions and Eisenstein series*, London Mathematical Society Student Texts, Cambridge University Press **26** (1993).

[2] K. Ribet, *A modular construction of unramified p-extensions of* $\mathbb{Q}(\mu_p)$, Invent. Math. **34** (1976), 151–162.

[3] A. Wiles, *On ordinary λ-adic representations associated to modular forms*, Invent. Math. **94** (1988), 529–573.

[4] A. Wiles, *The Iwasawa conjecture for totally real feilds*, Ann. of Math. **131** (1990), 493-540.