

Fermat 予想

@unaoya

2018 年 3 月 3 日

1. Cornell-Silverman-Stevens
2. Darmon-Diamond-Taylor
3. conrad の seminar <http://math.stanford.edu/~conrad/modseminar/>
4. 藤原先生

1 Darmon の survey

特別な場合に簡略化した証明をする。

定理 1. 楕円曲線 E/\mathbb{Q} が 5 で good reduction で Galois 表現が $E_5 \cong X_0(17)_5$ とする。このとき E は保型的。

$X = X_0(17)$ について調べることで以下がわかる。

補題 1. $X_0(17)$ の mod 5 表現 $\bar{\rho}_0: G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_5)$ は以下をみたす。

1. $\det(\bar{\rho}_0)$ は円分指標 $\bar{\epsilon}: G_{\mathbb{Q}} \rightarrow \mathbb{F}_5^{\times}$
2. $\bar{\chi}_2$ を位数 4 の不分岐指標として

$$\bar{\rho}_0|_{D_5} \cong \begin{pmatrix} \bar{\chi}_1 & * \\ 0 & \bar{\chi}_2 \end{pmatrix}, \bar{\rho}_0|_{I_5} \cong \begin{pmatrix} \bar{\epsilon} & * \\ 0 & 1 \end{pmatrix}$$

3. 非自明指標 $\bar{\Psi}|_{I_{17}}$ により

$$\bar{\rho}_0|_{D_{17}} \cong \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}$$

4. $\bar{\rho}_0$ は全射

定義 1. A を完備ネーター局所 \mathbb{Z}_5 代数で剰余体が \mathbb{F}_5 なるものとする。 $\bar{\rho}_0$ の変形 $\rho: G_{\mathbb{Q}} \rightarrow GL_2(A)$ が許容的とは以下をみたすこと。

1. $\det \rho$ が円分指標 $\epsilon: G_{\mathbb{Q}} \rightarrow \mathbb{Z}_5^{\times} \subset A$
- 2.

$$\bar{\rho}_0|_{D_5} \cong \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}, \bar{\rho}_0|_{I_5} \cong \begin{pmatrix} \epsilon & * \\ 0 & 1 \end{pmatrix}$$

- 3.

$$\bar{\rho}_0|_{D_{17}} \cong \begin{pmatrix} \epsilon & \Psi \\ 0 & 1 \end{pmatrix}$$

命題 1. E/\mathbb{Q} が 5 等分点で保型的なら T_5E は admissible

このことから以下を証明すればよい

定理 2. 全ての許容的な $\bar{\rho}_0$ の変形は保型的

保型的な変形と許容的な変形間の全単射を構成するが、そのままでは無限集合になる。変形の係数環と分岐条件を決めて有限集合の比較をする。言い換えると $MD_\Sigma(A) \rightarrow AD_\Sigma(A)$ が各 A, Σ について全単射であることを示す。もし AD_Σ および MD_Σ が表現可能関手であればそれらを表現する間の同型を示せばよい。

定理 3 (Mazur). AD_Σ は有限生成局所 \mathbb{Z}_5 代数で剰余体が \mathbb{F}_5 である R_Σ により表現される

$T_5X \in AD_\Sigma(\mathbb{Z}_5)$ なのでこれに対応する射 $\pi_{R_\Sigma}: R_\Sigma \rightarrow \mathbb{Z}_5$ が存在する。

MD_Σ の表現可能性をあらかじめ示すことはできないが、その候補を定義する。 $N_\Sigma = 17 \prod_{p \in \Sigma} p^2$ とし、それに対応する Hecke 環を $T(\Sigma)$ とする。これは $\ell \nmid N_\Sigma$ なる T_ℓ と $q \in \Sigma \cup \{17\}$ なる U_q で生成される。 f を X に対応する正規固有形式とし $T(\Sigma)$ の eigenform を inductive に

$$f_\emptyset = f, f_{\Sigma \cup \{q\}} = f_\Sigma(\tau) - a_q f_\Sigma(q\tau) + q f_\Sigma(q^2\tau)$$

と定義する。さらにイデアル $m_\Sigma \subset T(\Sigma)$ を $5, T_\ell - a_\ell, U_q, U_{17} + 1$ で生成されるものとし、 T_Σ を $T(\Sigma)$ の m_Σ による完備化とする。これは有限平坦局所 \mathbb{Z}_5 代数で剰余体が \mathbb{F}_5 である。さらに \mathbb{Z}_5 代数の射 $T_\Sigma \rightarrow O$ に対して、 $\Gamma_0(N_\Sigma)$ の 5 進固有形式で f_Σ と mod 5 で合同なるものが対応する。特に f_σ に対応する $\pi_{T_\Sigma}: T_\Sigma \rightarrow \mathbb{Z}_5$ が存在する。

定理 4 (Eichler-Shimura, Carayol).

$T(\Sigma)$ と $X_0(N_\Sigma), J_0(N_\Sigma)$ の関係。

上の定理と R_Σ の普遍性から $\phi_\Sigma: R_\Sigma \rightarrow T_\Sigma$ が定義される。これは π と整合的。目標は以下を示すこと。

定理 5. ϕ_Σ は同型

全射性は比較的容易に示せる。

1.1 可換環論

C を有限生成完備局所 \mathbb{Z}_p 代数 A と全射 $\pi: A \rightarrow \mathbb{Z}_p$ の組 (A, π) のなす圏とする。 $\Phi_A = \ker \pi / (\ker \pi)^2, \eta_A = \pi(\text{Ann}_A \ker \pi)$ とする。

定理 6. $R, T \in C$ で T は有限生成ねじれ自由 \mathbb{Z}_p 加群であり、 $\phi: R \rightarrow T$ を全射とする。 $|\Phi_R| \leq |\mathbb{Z}_p/\eta_T| < \infty$ ならば ϕ は同型。

定理 7. $\phi: A \rightarrow B$ を C の全射で B は完全交差とする。 $\Phi_\phi: \Phi_A \rightarrow \Phi_B$ が同型で、これらが有限なら ϕ は同型。

証明. B は完全交差なので C の全射 $\nu_B: U = \mathbb{Z}_p[[X_1, \dots, X_n]] \rightarrow B$ で $\ker \nu_B = (f_1, \dots, f_n)$ なるものが取れる。 $b_i \in \ker \pi_B$ に対し Φ_ϕ が同型から $a_i \in \ker \pi_A$ で $\phi(a_i) = b_i$ なるものが取れる。これを使って $\nu_A: \mathbb{Z}_p[[X_1, \dots, X_n]] \rightarrow A$ を $X_i \mapsto a_i$ として定めると中山の補題より ν_A は全射。 a_i の定義から $\ker \nu_B \subset$

$\ker \nu_A$ である。逆が言えるか？ $\Phi_{\nu_A}: \Phi_U \rightarrow \Phi_A$ の kernel の生成元を持ち上げて $g_1, \dots, g_n \in \ker \nu_A$ とする。この時 $M \in M_n(U)$ であつて $(g_1, \dots, g_n) = (f_1, \dots, f_n)M$ なるものが f_i が $\ker \nu_B$ の生成元であることから取れる。この M が正則であることを言えばよい。 $(\bar{g}_1, \dots, \bar{g}_n) = (\bar{f}_1, \dots, \bar{f}_n)\bar{M}$ で $\Phi_A \cong \Phi_B$ であることから $\det \bar{M} \in \mathbb{Z}_p^\times$ となりよい。したがって $\nu_A \nu_B^{-1}: B \rightarrow U \rightarrow A$ が定義でき、これが ϕ の逆を与える。 \square

1.2 Φ_{R_Σ} と η_{T_Σ}

$X = X_0(17), T = \text{end}(T_5(X)) = \{\text{Trace}(f) = 0\}$ とする。これは rank3 の自由 \mathbb{Z}_p 加群で $G_{\mathbb{Q}}$ の共役作用を持つ。 $A = T \otimes \mathbb{Q}_p/\mathbb{Z}_p$ とする。これは $G_{\mathbb{Q}}$ 加群。

Σ を素数の集合で $\{5, 17\}$ を含まないとする。これに対し $J_r \subset H^1(\mathbb{Q}_r, A)$ を素数 r に対して以下で定める。

1. $r \notin \Sigma \cup \{5, 17\}$ のとき $J_r = \ker(H^1(\mathbb{Q}_r, A) \rightarrow H^1(I_r, A))$
2. $r \in \Sigma$ のとき $J_r = H^1(\mathbb{Q}_r, A)$
3. $J_{17} = \ker(H^1(\mathbb{Q}_{17}, A) \rightarrow H^1(\mathbb{Q}_{17}, A/A_{(17)}^\circ))$
4. $J_5 = \ker(H^1(\mathbb{Q}_5, A) \rightarrow H^1(I_5, A/A_{(5)}^\circ))$

さらに

$$S_\Sigma(\mathbb{Q}, A) = \ker(H^1(\mathbb{Q}, A) \rightarrow \prod_r H^1(\mathbb{Q}_r, A)/J_r)$$

とする。つまり $S_\Sigma(\mathbb{Q}, A) = \{s \in H^1(\mathbb{Q}, A) \mid s_r \in J_r\}$ とする。

R_Σ は普遍変形環なので $\rho^{\text{univ}}: G_{\mathbb{Q}} \rightarrow GL_2(R_\Sigma)$ が存在する。対応する普遍コホモロジー類を $u_\Sigma \in H^1(\mathbb{Q}, M_2(\Psi_{R_\Sigma}))$ とする。 $\det(u_\Sigma) = 1$ なので u_Σ の像は $T \otimes \Psi_{R_\Sigma}$ に入る。これを用いて $\phi_\Sigma: \text{Hom}(\Psi_{R_\Sigma}, \mathbb{Q}_5/\mathbb{Z}_5) \rightarrow H^1(\mathbb{Q}, A)$ が定義できる。

命題 2. ϕ_Σ は $S_\Sigma(\mathbb{Q}, A)$ への同型

定理 8.

$$|\mathbb{Z}_5/\eta_{T_\Sigma}| = \prod_{q \in \Sigma} (q-1)(a_q^2 - (q+1)^2)$$

Σ の大きさに関する帰納法で示す。

1. $\eta_\emptyset = \mathbb{Z}_5$ であること。
2. Σ' を一つ素数を追加したものとし $\eta_{T'/T} = (q-1)(T_q^2 - (a+1)^2)$ となること。

$\Lambda = T_5(J) \otimes_T T, \Lambda' = T_5(J') \otimes_{T'} T'$ であり、

1.3 判定法の条件をみたすこと

$\Sigma = \emptyset$ の場合に帰着できる。

$\Sigma = \emptyset$ の場合、右辺は 1 なので、 $S_\emptyset(\mathbb{Q}, A)$ が自明であることを示す。

命題 3. $|S_\emptyset(\mathbb{Q}, A_5^*)| = 1$

証明. まず $s \in S$ と good prime q について $s_q = 0$ を示す。次に $H^1(\mathbb{Q}, A_5^*) \rightarrow H^1(K, A_5^*)$ が単射であることを示す。これを用いて証明。

$\bar{s} \in \text{Hom}(G_K, A_5^*)$ とみて、 L/K を \bar{s} が $U = \text{Gal}(L/K)$ を経由する最大拡大とする。 $\bar{s}: U \rightarrow A_5^*$ が 0 であることを言えばよい。

$\tau \in \Gamma$ を適切に固定。 $h \in U$ を任意にとり、 $h\tau \in \Gamma$ が Frob_q なる素数 q を選ぶ。すると τ の取り方から q は good prime であり、 $s_q = 0$ となる。特に q の上にある K の素点 Q に対し $\bar{s}(\text{Frob}_Q) = 0$ となる。 τ の取り方から K_Q/\mathbb{Q}_q の剰余次数は 4 で、 $\text{Frob}_Q = (h\tau)^4 = h^+ \in U^+$ となる。 h は任意なので \bar{s} は U^+ を消す。一方、 U への $\tau \in G$ の作用は τ の定義から固有値 1 を持つ、つまり U^+ は非自明。 \bar{s} は G 同変なので $0 \neq U^+ \subset \ker \bar{s} \subset U$ は G 部分加群で、 U は既約 G 加群なので $\ker \bar{s} = U$ 、すなわち $\bar{s} = 0$ である。 \square

$X = X_0(17)$ の 5 等分点への $G_{\mathbb{Q}_5}, G_{\mathbb{Q}_{17}}$ 作用、つまり MLT で持ち上げたい $\text{mod } 5$ 表現 $\bar{\rho}_0$ の定義。 $p = 17$ では \mathbb{F}_5^2 に $\begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}$ で作用。 $\bar{\Psi}$ は分岐指標。これの End^0 に定まる表現を計算する。 End^0 の基底を $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ でとると、これらの移り先は

$$\begin{aligned} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} \bar{\epsilon} & -\bar{\Psi} \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -2\bar{\Psi} \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 0 & \bar{\epsilon} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & \bar{\epsilon} \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} \bar{\Psi} & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \bar{\Psi}\bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi}^2 \\ \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \end{pmatrix} \end{aligned}$$

となる。従って A_5 への $G_{\mathbb{Q}_{17}}$ 作用は、1 次元ずつの filtration $A_5^0 \subset A_5^1 \subset A_5$ があって、それぞれの gr に $\epsilon, 1, \epsilon^{-1}$ で作用する。

命題 4. $h_{17} = 1$

証明. A_5 への $G_{\mathbb{Q}_{17}}$ 作用は、1 次元ずつの filtration $A_5^0 \subset A_5^1 \subset A_5$ があって、それぞれの gr に $\chi, 1, \chi^{-1}$ で作用する。ここで χ は円分指標。

$0 \rightarrow A_5^0 \rightarrow A_5 \rightarrow A_5/A_5^0 \rightarrow 0$ から Galois コホモロジーの長完全列をかくと、

$$\begin{aligned} 0 \rightarrow H^0(\mathbb{Q}_{17}, A_5^0) \rightarrow H^0(\mathbb{Q}_{17}, A_5) \rightarrow H^0(\mathbb{Q}_{17}, A_5/A_5^0) \\ \rightarrow H^1(\mathbb{Q}_{17}, A_5^0) \rightarrow H^1(\mathbb{Q}_{17}, A_5) \rightarrow H^1(\mathbb{Q}_{17}, A_5/A_5^0) \\ \rightarrow H^2(\mathbb{Q}_{17}, A_5^0) \rightarrow H^2(\mathbb{Q}_{17}, A_5) \rightarrow H^2(\mathbb{Q}_{17}, A_5/A_5^0) \rightarrow 0 \end{aligned}$$

$h_{17} = |H^0(\mathbb{Q}_{17}, A_5^*)|/[H^1(\mathbb{Q}_{17}, A_5) : \ker H^1(\mathbb{Q}_{17}, A_5) \rightarrow H^1(\mathbb{Q}_{17}, A_5/A_5^0)]$ を求める。上の完全列から $0 \rightarrow H^1(\mathbb{Q}_{17}, A_5)/\ker \rightarrow H^1(\mathbb{Q}_{17}, A_5/A_5^0) \rightarrow H^2(\mathbb{Q}_{17}, A_5^0) \rightarrow H^2(\mathbb{Q}_{17}, A_5) \rightarrow H^2(\mathbb{Q}_{17}, A_5/A_5^0) \rightarrow 0$ が完全なので

$$[H^1(\mathbb{Q}_{17}, A_5) : \ker] = \frac{h^1(A_5/A_5^0)h^2(A_5)}{h^2(A_5^0)h^2(A_5/A_5^0)}$$

となる。

双対性から $h^2(V) = h^0(V^*)$ である？ □

$p = 5$ では \mathbb{F}_5^2 に $\begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}$ で作用。 $\bar{\Psi}$ は分岐指標。これの End^0 に定まる表現を計算する。 End^0 の基底を $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ でとると、これらの移り先は

$$\begin{aligned} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} \bar{\epsilon} & -\bar{\Psi} \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -2\bar{\Psi} \\ 0 & -1 \end{pmatrix} \\ \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 0 & \bar{\epsilon} \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & \bar{\epsilon} \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon} & \bar{\Psi} \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} \bar{\Psi} & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \bar{\Psi}\bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi}^2 \\ \bar{\epsilon}^{-1} & -\bar{\epsilon}^{-1}\bar{\Psi} \end{pmatrix} \end{aligned}$$

となる。従って A_5 への $G_{\mathbb{Q}_{17}}$ 作用は、1 次元ずつの filtration $A_5^0 \subset A_5^1 \subset A_5$ があって、それぞれの gr に $\epsilon, 1, \epsilon^{-1}$ で作用する。

命題 5. $h_5 \leq \frac{1}{25}$

証明. $\phi_1: H^1(\mathbb{Q}_5, A_5) \rightarrow H^1(\mathbb{Q}_5, A_5/A_5^0), \phi_2: H^1(\mathbb{Q}_5, A_5/A_5^0) \rightarrow H^1(I_5, A_5/A_5^0)$ とし、その合成を ϕ とする。 $|Im\phi| \geq 25$ を示したい。 $|Im\phi| \geq |Im\phi_1|/|\ker\phi_2|$ である。 $|Im\phi_1| = 125$ であることは上の補題と同様にして長完全列を書いて示せる。 $|\ker\phi_2| = 5$ は inflation-restriction 系列をかく。 □

$p = \infty$ の場合。

補題 2. $h_\infty = |H^0(\mathbb{R}, A_5^*)| = |(A_5^*)^{G_{\mathbb{R}}}| = 25$

証明. これは $\bar{\rho}_0$ が odd であることから複素共役の固有値が $-1, 1, 1$ である。従って固定部分が \mathbb{F}_5 上 2 次元。 □

命題 6. $|S_\emptyset(\mathbb{Q}, A_5)| = 1$

証明. セルマー群の双対性から (Tate-Poitou 完全列?)。

$$\frac{|S_\emptyset(\mathbb{Q}, A_5)|}{|S_\emptyset(\mathbb{Q}, A_5^*)|} = h_\infty h_5 h_{17} \leq 1$$

□

話の流れ。 $\Sigma = \emptyset$ の時には判定法の条件を満たすので、 $R_\Sigma = T_\Sigma$ が証明できる。一般の Σ はこれに帰着する。

2 Galois cohomology

etale cohomology との関係、とくに Tate-Poitou duality と Poincare duality の関係。

有限体の Brauer 群。 $G = \hat{\mathbb{Z}}$ の群コホモロジーの計算。 local fields では $H^q(G, A) = \text{colim } H^q(G/nG, A^{nG})$ で定義する。(これは $M \mapsto M^G$ の derived functor ではない?) A が有限もしくは可除の場合に $H^2 = 0$ を示す。(実際には 2 以上全て消える?)

(副有限) 群の (連続) コホモロジーをサイトの非可換コホモロジーとして解釈したい。群コホモロジーと分類空間のコホモロジー、etale cohomology と Galois cohomology の対応

2.1 巡回群の有限係数コホモロジー

位数 n の巡回群は lens 空間を分類空間にもつ。 \mathbb{Z} の resolution として

2.2 表現の変形と Selmer 群

$\bar{\rho}: G \rightarrow GL_d(\mathbb{F})$ とその変形 $\rho: G \rightarrow GL_d(O/\lambda^n)$ に対し、 $Ext_{O/\lambda^n[G]}^1(ad\rho, ad\rho)$ と $H^1(G, ad\rho)$ は同型となる。これの部分群 $Ext_{D \cap O/\lambda^n[G]}^1(ad\rho, ad\rho)$ に対応する部分群として $H_D^1(G, ad\rho) \subset H^1(G, ad\rho)$ を定義し、さらに $H_D^1(G, ad\rho) = H_D^1(G, ad\rho) \cap H^1(G, ad^0\rho)$ を定義する。この時

問題 1. $Def_{\bar{\rho}}^X(\mathbb{F}[\epsilon]/\epsilon^2)$ と $H_D^1(G, ad^0\rho)$ と $Hom_{\mathbb{F}}(m_{R_D}/(\lambda, m_{R_D}^2), \mathbb{F})$ と $Hom_{O\text{-alg}}(R_D, \mathbb{F}[\epsilon/\epsilon^2])$ は同型。

一般論として deformation と H^1 の関係を SGA や小平に沿って理解する。