Taylor-Wiles系の復習

山下　剛*

平成21年1月31日

目 次

*2008/7/30 版を少し改訂. EPSRC grant EP/E049109/1 の補助を受けています.

0 はじめに.

本稿は「$R = T$ の最近の発展についての勉強会」(2008 年 3 月 17〜21 日, 八ヶ岳) における講演「Review of Taylor-Wiles system」の報告書である. 4 章は Kisin による修正 Taylor-Wiles 系 (本報告集 [Y] 参照) により不要になり, 3 章は底変換と正定値四元数代数上の保型形式を用いることで容易に示すことができるもので置き換えることができるようになった (そういう理由で講演では 1 章, 2 章, 5 章を紹介し 3 章と 4 章は軽く触れるのとどめた) が, Kisin の修正 Taylor-Wiles 系の解説は [Y] に譲ることにして Kisin 以前の Taylor-Wiles 系を本稿では復習する. また, 5 章は Taylor-Wile 系の話題ではないが, 潜在的保型性 ([T2], [T3], [HSBT]) や Serre 予想の証明のテクニック ([Kh1], [KW1], [KW2], [KW3]) の原型にあたり, 講演において紹介したことと, 本報告集の他稿との関連から本稿に入れることにした. そういうわけで, 1 章と 2 章 (と 6 章) の次に [Y](と本報告集今井氏の記事) を読むのが速習コースと思われる. Diamond-藤原の改良を使っているぶん [DDT] より簡素化されてはいるものの, 3 章と 4 章が入ったことで記述が [DDT] に近いものとなってしまったのが少し残念である.

この勉強会は多くの方のご協力の上に初めて成り立ったものであることを筆者は痛感している. 報告集の原稿執筆を引き受けて下さった方々とすべての参加者に感謝する. また, 勉強会運営の資金援助をして下さった柏原正樹先生, 岡本久先生, 松本眞先生, 都築暢夫先生, 会場とペンションの手配と現地での準備のご協力をして下さった斎藤秀司先生, 報告集の編者になってくださった斎藤毅先生, 報告集作成の資金援助をしてくださる中村郁先生, 運営の準備に陰ながら多くのご協力とご助言をしてくださった玉川安騎男先生, 勉強会中の会場設営や買出しなどのお手伝いをして下さった中村健太郎君, 津嶋貴弘君, そして毎朝おいしい朝ごはんと楽しい懇親会を準備して下さったペンションのオーナーの柳平二四雄さんに深い感謝の意を表す.

また, 懇親会後に大変迷惑にもベッドで寝ゲロを吐いてしまった. ペンションのオーナーの柳平二四雄さん, 隣のベッドで臭い思いをなさった安田正大さん, ご自身の汚れていないベッドを提供して下さった中村健太郎君, 掃除をして下さった中村健太郎君と津嶋貴弘君にこの場を借りて深くお詫び申し上げる.

1 可換環論.

E を $\mathbb{Q}_p$ の有限次拡大, $\mathcal{O} = O_E$ をその付値環, λ を極大イデアル, $\mathbb{F}$ を剰余体とする. E の代数閉包 $\overline{E}$ を固定する. 次の可換環論的命題が Taylor-Wiles 系の鍵となる命題である (適用する時は, R は普遍変形環, T は局所化された Hecke 環, H は局所化された保型形式の空間で各々適当なものをとる).

命題 1.1 (Diamond-藤原の Taylor-Wiles 系) $R \twoheadrightarrow T$ を完備 Noether 局所 $\mathcal{O}$ 代数の全射とする. T は有限生成平坦 $\mathcal{O}$ 加群であるとする. H を 0 でない忠実 T 加群で $\mathcal{O}$ 上有限階数自由とする. ある自然数 r が存在して, 任意の自然数 n に対して以下の可換図式が存在すると仮定する.

$$\begin{tikzcd}
 & \mathcal{O}[[X_1, \ldots, X_r]] \arrow[d] & & \\
\mathcal{O}[[S_1, \ldots, S_r]] \arrow[r] & R_n \arrow[r, two heads] \arrow[d, two heads] & T_n \arrow[r, hook] \arrow[d, two heads] & \mathrm{End}(H_n) \arrow[d] \\
 & R \arrow[r, two heads] & T \arrow[r, hook] & \mathrm{End}(H).
\end{tikzcd} \tag{1}$$

ここで, $R_n \twoheadrightarrow T_n$ は完備 Noether 局所 $\mathcal{O}$ 代数の全射, T_n は有限生成平坦 $\mathcal{O}$ 加群, H_n は忠実 T_n 加群で $\mathcal{O}$ 上有限階数自由なもので以下を満たすもの.

1. $R_n/(S_1, \ldots, S_r) \xrightarrow{\sim} R,\ T_n/(S_1, \ldots, S_r) \xrightarrow{\sim} T,\ H_n/(S_1, \ldots, S_r) \xrightarrow{\sim} H,$

2. $\mathrm{Ann}_{\mathcal{O}[[S_1,\ldots,S_r]]}(H_n) \subset ((S_1+1)^{p^n} - 1, \ldots, (S_r+1)^{p^n} - 1),$

3. H_n は $\mathcal{O}[[S_1, \ldots, S_r]]/\mathrm{Ann}_{\mathcal{O}[[S_1,\ldots,S_r]]}(H_n)$ 上自由.

この時, 次が成立.

1. $R \xrightarrow{\sim} T,$

2. R, T は局所完全交叉 (locally complete intersection)$\mathcal{O}$ 代数,

3. H は T 上自由. □

注意 1.1.1 T_n は $R_n \to \mathrm{End}(H_n)$ の像で定義すればいいので定理の条件に出てこなくてもよい. また, 証明でも実際は T_n と証明中で定義する T_∞ は使わない (R_∞ が形式冪級数環と同型で, Auslander-Buchsbaum 公式から H_∞ が R_∞ 上自由であることが分かりさえすればよい. T_n, T_∞ を出さない議論については [Y] 参照).

本稿では, オリジナルの Taylor-Wiles 系がどのように改良されたのかを見る (6 章参照) ために便宜的に余分な議論 (T_n, T_∞ の導入と同型 $R_\infty \xrightarrow{\sim} T_\infty$) をする. □

注意 1.1.2 条件で, 以下の 3 点が重要である.

1. r は n に依存しない.

2. $\mathcal{O}[[X_1, \ldots, X_r]]$ と $\mathcal{O}[[S_1, \ldots, S_r]]$ の変数の数 r が一致している (少し緩めていうと $\mathcal{O}[[X_1, \ldots, X_{r'}]]$ の方の変数の数 r' が $\mathcal{O}[[S_1, \ldots, S_r]]$ の方の変数の数 r 以下で十分. ユニタリ群での $R = T$ 定理ではこの緩めたものを使用する ([CHT], [T4])).

3. 各 n に対して可換図式 (1) が存在することのみ仮定しており, n **についての整合性は仮定しない**. 特に, $R_{n+1} \to R_n$ などの射の存在は仮定しない. $\mathcal{O}[[X_1, \ldots, X_r]]$ についての条件も R_n の位相的生成元の個数が r 個以下であることを言っているだけである. $\square$

注意 1.1.3 ごく大雑把に言うと, $\mathcal{O}[[X_1, \ldots, X_r]] \twoheadrightarrow R_n$ の部分が "R が十分小さい" ことを言っており, 仮定の 2, 3 が "T と H が十分大きい" ことを言っている. $\square$

証明 $R, T, H, R_n, T_n, H_n, \mathcal{O}[[X_1, \ldots, X_r]], \mathcal{O}[[S_1, \ldots, S_r]]$ を $\otimes_{\mathcal{O}}\mathbb{F}$ したものに置き換えて証明すれば十分. $\mathfrak{a} := \ker\{R \twoheadrightarrow T\}$, $\mathfrak{a}_m := ((S_1+1)^{p^m}-1, \ldots, (S_r+1)^{p^m}-1) \subset \mathbb{F}[[S_1, \ldots, S_r]]$ とする. $m \leq n$ に対して,

$$R'_{n,m} := \mathrm{Im}\{R_n \to (R/\mathfrak{m}_R\mathfrak{a} \oplus T_n/\mathfrak{a}_m)\}$$

とおく ($\mathfrak{m}_R$ は R の極大イデアル). この時,

$$\#R'_{n,m} \leq \#(R/\mathfrak{m}_R\mathfrak{a})(\#\mathbb{F}[[S_1, \ldots, S_r]]/\mathfrak{a}_m)^{\dim_{\mathbb{F}} T} < \infty$$

に注意する. ここで, 可換図式

$$\begin{tikzcd}
 & \mathbb{F}[[X_1, \ldots, X_r]] \arrow[d] & & \\
\mathbb{F}[[S_1, \ldots, S_r]] \arrow[r] & R'_{n,m} \arrow[r, two heads] \arrow[d] & T_n/\mathfrak{a}_m \arrow[r, hook] \arrow[d] & \mathrm{End}(H_n/\mathfrak{a}_m) \arrow[d] \\
 & R/\mathfrak{m}_R\mathfrak{a} \arrow[r, two heads] & T \arrow[r, hook] & \mathrm{End}(H)
\end{tikzcd}$$

を $\mathcal{S}_{n,m}$ とおく ($m \leq n$). m を固定したとき, 上の注意からこういう可換図式の同型類は有限 ("同型類" をより正確に言うと, 可換図式

$$\begin{tikzcd}
 & \mathbb{F}[[X_1, \ldots, X_r]] \arrow[d] & & \\
\mathbb{F}[[S_1, \ldots, S_r]] \arrow[r] & A' \arrow[r, two heads] \arrow[d] & B' \arrow[r, hook] \arrow[d] & \mathrm{End}(M') \arrow[d] \\
 & A \arrow[r, two heads] & B \arrow[r, hook] & \mathrm{End}(M)
\end{tikzcd}$$

で

1. $A'/(S_1, \ldots, S_r) \xrightarrow{\sim} A,\ B'/(S_1, \ldots, S_r) \xrightarrow{\sim} B,\ M'/(S_1, \ldots, S_r) \xrightarrow{\sim} M,$

2. $\mathrm{Ann}_{\mathcal{O}[[S_1, \ldots, S_r]]}(M') \subset ((S_1+1)^{p^m}-1, \ldots, (S_r+1)^{p^m}-1),$

3. M' は $\mathbb{F}[[S_1,\dots,S_r]]/\mathrm{Ann}_{\mathbb{F}[[S_1,\dots,S_r]]}(M')$ 上自由

を満たすものと, その間の射として準同型射 $A'_1 \to A'_2$, $B'_1 \to B'_2$, $M'_1 \to M'_2$, $A_1 \to A_2$, $B_1 \to B_2$, $M_1 \to M_2$ の組で両者の可換図式と整合的なものを考え ($\mathbb{F}[[X_1,\dots,X_r]]$, $\mathbb{F}[[S_1,\dots,S_r]]$ 上では恒等射), 同型射として上の準同型射がすべて同型なものを考える).

従って, n の部分列 $n(m)$ を

- 無限個の n に対して $\mathcal{S}_{n(m),m} \cong \mathcal{S}_{n,m}$,
- $m>1$ の時, $\mathcal{S}_{n(m),m-1} \cong \mathcal{S}_{n(m-1),m-1}$

となるようにとれる (下図参照).

$$\begin{tikzcd}
\mathcal{S}_{n(m+1),m+1} \arrow[d] & (\cong \exists^\infty n\ \mathcal{S}_{n,m+1}) & & \\
\mathcal{S}_{n(m+1),m} \arrow[r, dash, "\cong"] & \mathcal{S}_{n(m),m} \arrow[d] & (\cong \exists^\infty n\ \mathcal{S}_{n,m}) & \\
 & \mathcal{S}_{n(m),m-1} \arrow[r, dash, "\cong"] & \mathcal{S}_{n(m-1),m-1} & (\cong \exists^\infty n\ \mathcal{S}_{n,m-1})
\end{tikzcd}$$

これで $\{\mathcal{S}_{n(m),m}\}_m$ は整合系になる (この議論を Taylor-Wiles 系の貼り合せの議論 (patching argument) という) ので,

$$R_\infty := \varprojlim_m R'_{n(m),m},\ \ T_\infty := \varprojlim_m T_{n(m)}/\mathfrak{a}_m,\ \ H_\infty := \varprojlim_m H_{n(m)}/\mathfrak{a}_m$$

と置くと, 可換図式

$$\begin{tikzcd}
 & \mathbb{F}[[X_1,\dots,X_r]] \arrow[d, two heads] & \\
\mathbb{F}[[S_1,\dots,S_r]] \arrow[r] \arrow[rrd, hook] & R_\infty \arrow[r, two heads] & T_\infty \arrow[d, hook] \\
 & & \mathrm{End}(H_\infty)
\end{tikzcd}$$

が得られる. ここで, $\cap_m \mathfrak{a}_{n(m)}{=}0$ と仮定 2, 3 より, 斜めの射が単射であることに注意. 従って, $\mathbb{F}[[S_1,\dots,S_r]] \to R_\infty$ も単射であり, R_∞ の Krull 次元は r 以上. もし全射 $\mathbb{F}[[X_1,\dots,X_r]] \twoheadrightarrow R_\infty$ の核が 0 でなければ, R_∞ の Krull 次元は r 未満になるので, この全射は同型 (ここで $\mathcal{O}[[X_1,\dots,X_r]]$ と $\mathcal{O}[[S_1,\dots,S_r]]$ の変数の数が一致することを使った). また, R_∞ の $\mathrm{End}(H_\infty)$ での像は $\mathbb{F}[[S_1,\dots,S_r]]$ を含むために Krull 次元は r 以上であり, もし全射 $R_\infty \twoheadrightarrow T_\infty$ の核が 0 でなければ, $R_\infty(\cong \mathbb{F}[[X_1,\dots,X_r]])$ の $\mathrm{End}(H_\infty)$ での像の Krull 次元は r 未満になるので, この全射も同型:

$$\mathbb{F}[[X_1,\dots,X_r]] \xrightarrow{\sim} R_\infty \xrightarrow{\sim} T_\infty \hookrightarrow \mathrm{End}(H_\infty).$$

ここで Auslander-Buchsbaum 公式

$$\mathrm{depth}_{\mathbb{F}[[X_1,\dots,X_r]]}H_\infty + \mathrm{proj.dim}_{\mathbb{F}[[X_1,\dots,X_r]]}H_\infty = \mathrm{depth}\ \mathbb{F}[[X_1,\dots,X_r]]$$

と $\mathrm{depth}_{\mathbb{F}[[X_1,\dots,X_r]]}H_\infty \geq r$, $\mathrm{depth}\,\mathbb{F}[[X_1,\dots,X_r]] = r$ をあわせると, H_∞ は $\mathbb{F}[[X_1,\dots,X_r]](\cong T_\infty)$ 上自由であることが分かる. あとは仮定 1 を使えば, R が $\mathbb{F}$ 上完全交叉代数であることと, 同型 $R \xrightarrow{\sim} T$ と, H が T 上自由であることが分かる. □

以下の章で, R, T, H, R_n, T_n, H_n を定義しつつこの命題の仮定が成り立つことを示していく. 2 章では R と R_n, 3 章では T, T_n と H, H_n を扱う. 前者は Galois 表現の普遍変形環でありその性質は Galois コホモロジーの計算によって示される. 後者は Hecke 環と Hecke 加群であり, その性質はモジュラー曲線のコホモロジーの計算によって示される.

2 普遍変形環.

この章では, [W1], [TW] で実際に Taylor-Wiles 系を適用する際の前章での "R が十分小さい" にあたる R の位相的生成元の個数の評価を 2.1, 2.2, 2.3 節で行い, 2.4 節で Taylor-Wiles 型の普遍変形環 R_Q の $\mathcal{O}[[S_1,\dots,S_r]]$ 代数構造を定義する.

R の位相的生成元の個数の評価のおおまかな方針は以下の通り (記号の意味は各節を参照).

1. 普遍変形環の接空間は随伴表現の Selmer 群と同型である (2.1 節)
$$\mathrm{Hom}(\mathfrak{m}_{R_\Sigma}/\mathfrak{m}_{R_\Sigma}^2, \mathbb{F}) \cong H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}),$$
2. Tate-Poitou 大域的双対性と大域的 Euler 指標公式により, Selmer 群の計算が双対 Selmer 群と簡単に計算できる局所項たちの和で書ける (2.2 節)
$$\dim H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) = \dim H^1_{\Sigma^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) + \sum_v (\dim L_{\Sigma,v} - \dim H^0(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})),$$
3. Cebotarev 密度定理と $\mathrm{PSL}_2(\mathbb{F})$ の部分群の分類を使い, うまく素数の有限集合 Q_n をとることで双対 Selmer 群を消す (2.3 節)
$$H^1_{Q_n^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) = 0.$$
4. 以上を組み合わせて,
$$\dim \mathfrak{m}_{R_{Q_n}}/\mathfrak{m}_{R_{Q_n}}^2 = \dim H^1_{Q_n}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) = \#Q_n$$
を得る. ここで, 完全系列
$$0 \to H^1_{Q_n^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \to H^1_{\emptyset^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \to \bigoplus_{v\in Q_n} H^1(\mathbb{F}_v, \mathrm{ad}^0\bar{\rho}(1)) \to 0$$

より,

$$\#Q_n = \dim H^1_{\emptyset^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1))$$

となり, これは n に依らない.

以下の 2 点が重要.

1. R_{Q_n} の位相的生成元の個数 $\#Q_n$ が n に依らない (注意 1.1.2 の 1 参照).
2. R_{Q_n} の位相的生成元の個数 $\#Q_n$ が Taylor-Wiles 系で "膨らませるパラメータ ($S_1, \dots, S_r$ のこと) の個数" と一致する (注意 1.1.2 の 2 と 2.4 章参照).

2.1 随伴表現の Selmer 群と普遍変形環の接空間.

G を位相的有限生成な副有限群, $\bar{\rho} : G \to \mathrm{GL}_d(\mathbb{F})$ を絶対既約な連続表現とする. $\mathrm{ad}\bar{\rho} := \mathrm{End}(\bar{\rho})$, $\mathrm{ad}^0\bar{\rho} := \mathrm{End}(\bar{\rho})^{\mathrm{tr}=0}$ とおく. これらには G が連続に作用する. $(\mathrm{ad}\bar{\rho})^\vee \cong \mathrm{ad}\bar{\rho}$ である ($(-)^\vee$ は Pontrjagin 双対). $\chi : G \to \mathcal{O}^\times$ を連続指標で $\chi \equiv \det\bar{\rho} \mod \lambda$ を満たすものとする.

D を副有限 $\mathcal{O}[G]$ 加群と連続準同型のなす圏の充満部分圏で, 部分と商と直積について閉じていて, かつ $\bar{\rho}$ を含むものとする. 次の変形関手を考える:

$$\Big(\text{完備 Noether 局所 } \mathcal{O} \text{ 代数 } A \text{ と同型射 } A/\mathfrak{m}_A \xrightarrow{\sim} \mathbb{F}\Big) \longrightarrow (\text{集合})$$

$$A \mapsto \mathrm{Def}^\chi_{\bar{\rho}}(A) := \left(\begin{array}{c} \text{圏 } D \text{ に入る連続表現 } \rho_A : G \to \mathrm{GL}_d(A) \text{ で,} \\ \rho_A \equiv \bar{\rho} \mod \mathfrak{m}_A,\ \det\rho_A = \chi \text{を満たすもの} \end{array} \right) \Big/ \sim .$$

ここで同値関係 $\sim$ は $\ker\{\mathrm{GL}_d(A) \to \mathrm{GL}_d(\mathbb{F})\}$ での共役. $\mathrm{Def}^\chi_{\bar{\rho}}(A)$ の元を $\bar{\rho}$ の $(\mathcal{O}, \chi, D)$ **型の変形**と呼ぶ.

定理 2.1 変形関手 $\mathrm{Def}^\chi_{\bar{\rho}}$ は表現可能. 即ち, ある $(\mathcal{O}, \chi, D)$ 型の変形

$$\rho_{R_D} : G \longrightarrow \mathrm{GL}_d(R_D)$$

が存在して, 任意の $(\mathcal{O}, \chi, D)$ 型の変形 $\rho_A : G \longrightarrow \mathrm{GL}_d(A)$ に対して, 準同型 $f : R_D \to A$ が一意的に存在して $f \circ \rho_{R_D} \sim \rho_A$ を満たす. □

証明は [DDT, 2.6], [S1] 参照. □

D の元 $\rho : G \to \mathrm{GL}_d(\mathcal{O}/\lambda^n)$ に対して同型 $\mathrm{Ext}^1_{\mathcal{O}/\lambda^n[G]}(\mathrm{ad}\rho, \mathrm{ad}\rho) \cong H^1(G, \mathrm{ad}\rho)$ での $\mathrm{Ext}^1_{D\cap(\mathcal{O}/\lambda^n[G]-\mathrm{Mod})}(\mathrm{ad}\rho, \mathrm{ad}\rho)$ の像を $H^1_D(G, \mathrm{ad}\rho)$ とおく. $H^1_D(G, \mathrm{ad}^0\rho) := H^1_D(G, \mathrm{ad}\rho) \cap H^1(G, \mathrm{ad}^0\rho)$ とおく.

補題 2.2 $\mathbb{F}$ ベクトル空間の標準的な同型

$$H^1_D(G, \mathrm{ad}^0\bar{\rho}) \cong \mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}_{R_D}/(\lambda, \mathfrak{m}^2_{R_D}), \mathbb{F})$$

が存在する. □

証明

$$H^1_D(G, \mathrm{ad}^0\bar{\rho}) \cong \mathrm{Def}^{\chi}_{\bar{\rho}}(\mathbb{F}[\varepsilon]/(\varepsilon^2)) \cong \mathrm{Hom}_{\mathcal{O}\text{-alg}}(R_D, \mathbb{F}[\varepsilon]/(\varepsilon^2)) \cong \mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}_{R_D}/(\lambda, \mathfrak{m}^2_{R_D}), \mathbb{F}).$$

ここで, 最初の同型は余輪体 $g \mapsto \phi(g)$ に対して, $g \mapsto (1+\phi(g)\varepsilon)\bar{\rho}(g)$ を対応させる射. ϕ が余輪体なのでこれは表現になり $((1+\phi(gh)\varepsilon)\bar{\rho}(gh) = (1+(\phi(g)+\bar{\rho}(g)\phi(h)\bar{\rho}(g)^{-1})\varepsilon)\bar{\rho}(g)\bar{\rho}(h) = (1+\phi(g)\varepsilon)(1+\bar{\rho}(g)\phi(h)\bar{\rho}(g)^{-1}\varepsilon)\bar{\rho}(g)\bar{\rho}(h) = (1+\phi(g)\varepsilon)\bar{\rho}(g)(1+\phi(h)\varepsilon)\bar{\rho}(h))$, 余境界が同値 $\sim$ に対応する $((1+(A-\bar{\rho}(g)A\bar{\rho}(g)^{-1})\varepsilon)\bar{\rho}(g) = (1+A\varepsilon)(1-\bar{\rho}(g)A\bar{\rho}(g)^{-1}\varepsilon)\bar{\rho}(g) = (1+A\varepsilon)\bar{\rho}(g)(1+A\varepsilon)^{-1})$ ことに注意. 2 つ目の同型は R_D の普遍性. 最後の同型は $\mathfrak{m}_{R_D}$ への制限から誘導されるもの. □

2.2 Selmer 群の計算.

M を連続離散 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 加群で $\#M$ が有限なものとする. $\mathcal{L} = \{L_v\}_v$ を $H^1(\mathbb{Q}_v, M)$ の部分空間 L_v の族で,

$$\{v \mid L_v \neq H^1(\mathbb{F}_v, M^{I_v})\}$$

が有限なものとする (I_v は v での惰性群). 局所条件 $\mathcal{L}$ に関する **Selmer 群**を

$$H^1_{\mathcal{L}}(\mathbb{Q}, M) := \ker\{H^1(\mathbb{Q}, M) \to \oplus_v H^1(\mathbb{Q}_v, M)/L_v\}$$

と定義する. $L_v^{\perp} \subset H^1(\mathbb{Q}_v, M^{\vee}(1))$ を局所 Tate 双対性での L_v の直交補空間とし, $\mathcal{L}^{\perp} := \{L_v^{\perp}\}_v$ とおく. **双対 Selmer 群**を

$$H^1_{\mathcal{L}^{\perp}}(\mathbb{Q}, M^{\vee}(1)) := \ker\{H^1(\mathbb{Q}, M^{\vee}(1)) \to \oplus_v H^1(\mathbb{Q}_v, M^{\vee}(1))/L_v^{\perp}\}$$

と定義する.

定理 2.3 ([DDT, Theorem 2.18]) $H^1_{\mathcal{L}}(\mathbb{Q}, M)$ は有限であり,

$$\frac{\#H^1_{\mathcal{L}}(\mathbb{Q}, M)}{\#H^1_{\mathcal{L}^{\perp}}(\mathbb{Q}, M^{\vee}(1))} = \frac{\#H^0(\mathbb{Q}, M)}{\#H^0(\mathbb{Q}, M^{\vee}(1))} \prod_{v \leq \infty} \frac{\#L_v}{\#H^0(\mathbb{Q}_v, M)}$$

が成立. □

注意 2.3.1 L_v は有限個を除いて $H^1(\mathbb{F}_v, M^{I_v})$ と一致し, 完全系列

$$0 \to H^0(\mathbb{Q}_v, M) \to M^{I_v} \to M^{I_v} \to H^1(\mathbb{F}_v, M^{I_v}) \to 0$$

より $\#H^1(\mathbb{F}_v, M^{I_v}) = \#H^0(\mathbb{Q}_v, M)$ なので, 上の積は実質有限積であることに注意. □

証明 $\mathbb{Q}$ の素点の有限集合 S を

$$S \supset \{\infty\} \cup \{v \mid v \mid \# M\} \cup \{v \mid M \text{ は } v \text{ で分岐 }\} \cup \{v \mid L_v \neq H^1(\mathbb{F}_v, M^{I_v})\}$$

となるようにとる. $\mathbb{Q}_S$ を $\mathbb{Q}$ の S の外最大不分岐拡大とし, $G_S := \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ とおく. $H^1(G_S, M)$ の有限性と完全系列

$$0 \to H^1_{\mathcal{L}}(\mathbb{Q}, M) \to H^1(G_S, M) \to \oplus_{v\in S} H^1(\mathbb{Q}_v, M)/L_v$$

より, $H^1_{\mathcal{L}}(\mathbb{Q}, M)$ は有限. Tate-Poitou 大域的双対性の完全系列

$$\begin{tikzcd}
0 \arrow[r] & H^0(G_S, M) \arrow[r] & (\oplus_{v\in S} H^0(\mathbb{Q}_v, M))/(1+c_0)M \arrow[r] & H^2(G_S, M^\vee(1))^\vee \arrow[d] \\
& H^1(G_S, M^\vee(1))^\vee & \oplus_{v\in S} H^1(G_S, M) \arrow[l] & H^1(G_S, M) \arrow[l]
\end{tikzcd}$$

(ここで, $(1+c_0)M$ は $H^0(\mathbb{Q}_\infty, M)$ に入っている (c_0 は複素共役)) と完全列

$$\oplus_{v\in S} L_v \to H^1(G_S, M^\vee(1))^\vee \to H^1_{\mathcal{L}^\perp}(\mathbb{Q}, M^\vee(1))^\vee \to 0$$

より, 完全系列

$$\begin{tikzcd}
& 0 \arrow[r] & H^0(G_S, M) \arrow[r] & (\oplus_{v\in S} H^0(\mathbb{Q}_v, M))/(1+c_0)M \arrow[d] \\
& \oplus_{v\in S} L_v \arrow[d] & H^1_{\mathcal{L}}(\mathbb{Q}, M) \arrow[l] & H^2(G_S, M^\vee(1))^\vee \arrow[l] \\
& H^1(G_S, M^\vee(1))^\vee \arrow[r] & H^1_{\mathcal{L}^\perp}(\mathbb{Q}, M^\vee(1))^\vee \arrow[r] & 0
\end{tikzcd}$$

がでる. これと大域的 Euler 指標公式

$$\chi(G_S, M^\vee(1)) = \frac{\# H^0(\mathbb{R}, M^\vee(1))}{\# M^\vee(1)} = \frac{1}{\#(1+c_0)M}$$

から定理が従う. □

$p > 2$ と仮定する. 埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{E}$ を固定する. $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ を絶対既約な連続表現とする. 以下では $\bar{\rho}$ の変形関手と $\mathrm{ad}^0\bar{\rho}$ の Selmer 群を考える.

$(\mathrm{ad}^0\bar{\rho})^\vee \cong \mathrm{ad}\bar{\rho}/\mathbb{F}\cdot 1$ であるが, $p > 2$ より, $\mathrm{ad}\bar{\rho}/\mathbb{F}\cdot 1 \cong \mathrm{ad}^0\bar{\rho}$ である ($p = 2$ の時は中心 $\mathbb{F}\cdot 1$ が $\mathrm{ad}^0\bar{\rho}$ に入り, $\mathrm{ad}^0\bar{\rho} \not\cong \mathrm{ad}\bar{\rho}/\mathbb{F}\cdot 1$ となるため, 以下で見る Galois コホモロジーの計算を修正しないといけない. 結論から言うと, その修正による寄与は $p = 2$ の時に存在する無限素点の項の寄与とキャンセルされることになる. [KW3] 参照.).

$\bar{\rho}$ に関して, 以下の仮定をおく:

1. $\bar{\rho}$ は**保型的**, すなわち, ある正規化された Hecke 固有形式 f が存在し, ほとんど全ての素数 ℓ に対して (固定した埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{E}$ に関して) 極大イデアルを法として $\mathrm{Tr}\bar{\rho}(\mathrm{Fr}_\ell) \equiv a_\ell(f)$ が成立する (Fr は算術的 Frobenius),

2. $\det \bar{\rho} = \bar{\varepsilon}$ ($\bar{\varepsilon}$ は法 p 円分指標),

3. $\bar{\rho}$ は全ての素点で**準安定**, 即ち,

$$\begin{cases} \bullet\ \ell \neq p \text{ の時, } \bar{\rho}|_{I_\ell} \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \\ \bullet\ \ell = p \text{ の時, } \bar{\rho}|_{D_p} \text{ は } \mathbb{Z}_p \text{ 上有限平坦群スキームからくる (平坦という) か,} \\ \quad \text{あるいは, } \bar{\rho}|_{D_p} \text{ に作用で安定な 1 次元部分空間 } W \text{ で,} \\ \quad W|_{I_p} \text{ は } \bar{\varepsilon} \text{ で作用し, } (\bar{\rho}/W)|_{I_p} \text{ は自明な表現になるものが存在すること (通常という)} \\ \quad (D_p \text{ は } p \text{ での分解群).} \end{cases}$$

(ここで, p では平坦または通常を準安定とよんでいる. 平坦かつ通常なこともある.)

例えば, E をすべての素点で準安定還元を持つ $\mathbb{Q}$ 上の楕円曲線とした時, $E[p]$ が $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の表現として既約であれば, $E[p]$ は保型性以外の仮定を満たす ($p=3$ であれば保型性も満たす (5 章参照).). p の外でもこのような条件を課す理由は注意 3.6.2 参照.

Taylor-Wiles 系はより一般の状況 (総実代数体の場合や, p や p の外での局所条件を緩めたものなど) でも適用可能だが, 本稿では簡単のためと [W1][TW] を復習する目的で以上のような条件をおく.

また, $L := \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ とおくと, 上の仮定から

$$\textbf{(L)}: \ \ \bar{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}/L)} \text{ は絶対既約} \tag{2}$$

である ([DDT, Lemma 3.24]) ことも分かる ($\bar{\rho}$ の保型性とレベル下げを使うことに注意). この条件 (L) は以下 Taylor-Wiles 系の構成でしばしば出てくる重要な条件である.

Σ を素数の有限集合とする. $\bar{\rho}$ の変形 $\rho_A : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A)$ が Σ **型の変形**とは, 以下を満たすときにいう:

- $\det \rho_A = \varepsilon$ (ε は p 進円分指標),
- $\rho_A|_{D_p}$ は準安定,
- もし $p \notin \Sigma$ で $\bar{\rho}|_{D_p}$ が平坦なら, $\rho_A|_{D_p}$ も平坦,
- もし $\ell \notin \Sigma \cup \{p\}$ で $\bar{\rho}$ が ℓ で不分岐なら, ρ_A も ℓ で不分岐,
- もし $\ell \notin \Sigma \cup \{p\}$ なら, $\rho_A|_{I_\ell} \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

大雑把に言うと, 局所条件として Σ の中ではどんな変形でも許し (p では準安定な変形のみ許し), Σ の外では $\bar{\rho}$ と同程度な分岐をもった変形のみを許している. 例えば, $\mathbb{Q}$ 上の楕円曲線 E が p で準安定還元をもち, $E[p]$ が $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の表現として既約ならば, E が悪い還元を持つ素数をすべて含むような Σ に対して T_pE は $E[p]$ の Σ 型の変形である.

$\bar{\rho}$ の Σ 型の変形 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}/\lambda^n)$ に対して, 以下の $H^1(\mathbb{Q}, \mathrm{ad}^0\rho)$ の局所条件 $\mathcal{L}_\Sigma$ を考える.

- もし $\ell \in \Sigma \setminus \{p\}$ なら, $L_{\Sigma,\ell} := H^1(\mathbb{Q}_\ell, \mathrm{ad}^0\rho)$
- もし $\ell \notin \Sigma \cup \{p\}$ なら, $L_{\Sigma,\ell} := H^1(\mathbb{F}_\ell, (\mathrm{ad}^0\rho)^{I_\ell})$
- もし $p \in \Sigma$ なら, $L_{\Sigma,p} := H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}^0\rho) := H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho) \cap H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}\rho)$
- もし $p \notin \Sigma$ なら, $L_{\Sigma,p} := H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}^0\rho) := H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho) \cap H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho)$

ここで,

$$H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}\rho) := \mathrm{Im}\{\mathrm{Ext}^1_{\mathrm{semistable}}(\rho, \rho) \to H^1(\mathbb{Q}_p, \mathrm{ad}\rho)\},$$

$$H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho) := \begin{cases} H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}\rho), & \rho \text{ が平坦でない時}, \\ \mathrm{Im}\{\mathrm{Ext}^1_{\mathrm{flat}}(\rho, \rho) \to H^1(\mathbb{Q}_p, \mathrm{ad}\rho)\}, & \rho \text{ が平坦の時}. \end{cases}$$

また, $p > 2$ のため $H^1(\mathbb{R}, \mathrm{ad}^0\rho) = 0$ となるので, $L_{\Sigma,\infty}$ は 0 とおく. これにより, Selmer 群 $H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho) := H^1_{\mathcal{L}_\Sigma}(\mathbb{Q}, \mathrm{ad}^0\rho)$ と双対 Selmer 群 $H^1_{\Sigma^\perp}(\mathbb{Q}, \mathrm{ad}^0\rho(1)) := H^1_{\mathcal{L}_\Sigma^\perp}(\mathbb{Q}, \mathrm{ad}^0\rho(1))$ が定まる. $\Sigma = \emptyset$ の時を**極小**という.

D_Σ を Σ 型の変形のなす圏とすると, $\bar{\rho}$ の変形として固定した素数の有限集合 $\Sigma \cup \{p\} \cup \{v \mid v$ で $\bar{\rho}$ は分岐 $\}$ の外で不分岐なもののみを考えているため, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の位相的有限生成な商に関する表現と考えられるので, 前節の結果から普遍変形環 $R_\Sigma := R_{D_\Sigma}$ が存在する ([DDT, Theorem 2.41], [S1] 参照). この時, Selmer 群 $H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho)$ は 2.1 節で定義した $H^1_{D_\Sigma}(\mathbb{Q}, \mathrm{ad}^0\rho)$ と一致することが以下のように分かる. p では定義は同じ. $\ell \in \Sigma \setminus \{p\}$ はともに条件なし. $\ell \notin \Sigma \cup \{p\}$ で $\bar{\rho}$ が ℓ で不分岐の時は ρ の変形 ρ_A に対して対応する $H^1(\mathbb{Q}, \mathrm{ad}^0\rho)$ の元が $H^1(I_\ell, \mathrm{ad}^0\rho)$ で 0 になることを言い換えると $\rho_A|_{I_\ell} \simeq \rho|_{I_\ell} \otimes_{\mathcal{O}} A$ となることから分かる. $\ell \notin \Sigma \cup \{p\}$ で $\bar{\rho}$ が ℓ で分岐する時は $H^1(I_\ell, \mathrm{ad}^0\rho) \xrightarrow{\sim} H^1(I_\ell, \mathrm{ad}^0\rho/(\mathrm{ad}^0\rho)^{I_\ell})$ なので, ρ の変形 ρ_A に対して対応する $H^1(\mathbb{Q}, \mathrm{ad}^0\rho)$ の元が $H^1(I_\ell, \mathrm{ad}^0\rho)$ で 0 になることを言い換えると, $\rho_A|_{I_\ell}$ の像が上三角冪単部分群に入るような表示をとった時 N を GL_2 の上三角冪零部分群として $\rho_A|_{I_\ell} \simeq \rho|_{I_\ell} \otimes_{\mathcal{O}} A \mod N$ となることから分かる.

以上のことと補題 2.2, 定理 2.3 から

$$H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) \cong \mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}_{R_\Sigma}/(\lambda, \mathfrak{m}^2_{R_\Sigma}), \mathbb{F})$$

と

$$\frac{\# H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\bar{\rho})}{\# H^1_{\Sigma^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1))} = \frac{\# H^0(\mathbb{Q}, \mathrm{ad}^0\bar{\rho})}{\# H^0(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1))} \prod_{v \in \Sigma \cup \{p,\infty\}} \frac{\# L_{\Sigma,v}}{\# H^0(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})}$$

が分かる. ここで上式の各項は以下のように計算される.

命題 2.4 *1.* $H^0(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) = 0$,

2. $H^0(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) = 0$,

3. $v = \infty$ の項: $\frac{\# L_{\Sigma,\infty}}{\# H^0(\mathbb{R}, \mathrm{ad}^0\bar{\rho})} = (\#\mathbb{F})^{-1}$,

4. $v \neq \infty, p$ の項: $\frac{\# L_{\Sigma,v}}{\# H^0(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})} = \# H^0(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho}(1))$. もし $v \equiv 1 \mod p$ かつ $\bar{\rho}(\mathrm{Fr}_v)$ の固有値が相異なれば, この値は $\#\mathbb{F}$,

5. $v = p$ の項: $p \notin \Sigma$ の時, $\frac{\# L_{\Sigma,p}}{\# H^0(\mathbb{Q}_p, \mathrm{ad}^0\bar{\rho})} = \#\mathbb{F}$. $\square$

$p \in \Sigma$ の時は命題 4.5 参照.

証明 1. $\bar{\rho}$ が既約なので従う.

2. $H^0(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \neq 0$ ならば $p = 3$ かつ $\bar{\rho}|_{\mathbb{Q}(\sqrt{-3})}$ が絶対既約ではない, ということが以下のようにして分かるため, 条件 (L) とあわせると従う (ここで条件 (L) は $p = 3$ の時のみ使う). $\mathrm{ad}^0\bar{\rho}(1) \cong \mathrm{Sym}^2\bar{\rho}$ なので, $H^0(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1))$ の元は Galois 不変な対称二次形式である. 0 でない元をとってくる. もしそれが非退化でないなら, 核は Galois 不変で $\bar{\rho}$ の既約性に矛盾するので, 非退化である. この時, $\bar{\rho}$ の像は (その二次形式に関する) 直交群に含まれる. $\det\bar{\rho} = \bar{\varepsilon}$ であるが, $p \neq 3$ の時は $\bar{\varepsilon}^2 \neq 1$ なので矛盾するし, $p = 3$ の時の時は $\bar{\rho}|_{\mathbb{Q}(\sqrt{-3})}$ は絶対既約にはなりえない.

3. $\bar{\rho}(c_0)$ の固有値は 1, -1 なので $\mathrm{ad}^0\bar{\rho}(c_0)$ の固有値は 1, -1, -1 であることから従う.

4. 局所的 Euler 指標公式より, $\frac{\# H^1(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})}{\# H^0(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})} = \# H^2(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho})$ であり, 局所 Tate 双対性より, これは $\# H^0(\mathbb{Q}_v, \mathrm{ad}^0\bar{\rho}(1))$ と一致する. $v \equiv 1 \mod p$ かつ $\bar{\rho}(\mathrm{Fr}_v)$ が相異なる固有値 α, β を持つ時は, $\mathrm{ad}^0\bar{\rho}(1)(\mathrm{Fr}_v)$ の固有値は $\mathbb{F}$ で $v \equiv 1$, $v\alpha/\beta \neq 1$, $v\beta/\alpha \neq 1$ であることより従う.

5. Fontaine-Laffaille 理論を用いる. 4 章で使う目的から以下の一般化した形で証明する.

命題 2.5 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}/\lambda^n)$ を Σ 型の変形とする. $p \notin \Sigma$ の時,

$$\frac{\# L_{\Sigma,p}}{\# H^0(\mathbb{Q}_p, \mathrm{ad}^0\rho)} = \#\mathcal{O}/\lambda^n. \ \square$$

証明 $\mathrm{MF}_{\mathcal{O}}$ を以下を満たす組 $(D, D^0, \phi_{-1}, \phi_0)$ と構造を保つ準同型 ($\mathcal{O}$ 加群の準同型で D^0 を保ち ϕ_{-1}, ϕ_0 と整合的なもの) のなす圏とする.

- D は $\mathcal{O}$ 加群で D^0 はその部分 $\mathcal{O}$ 加群,
- $\phi_{-1} : D \to D$, $\phi_0 : D^0 \to D$ は $\mathcal{O}$ 加群の準同型,
- $\# D$ は有限,

- $\phi_{-1}|_{D^0} = p\phi_0$, $\mathrm{Im}\phi_{-1} + \mathrm{Im}\phi_0 = D$.

Fontaine-Laffaille 理論より, この圏 $\mathrm{MF}_{\mathcal{O}}$ は位数有限な $\mathcal{O}[G_{\mathbb{Q}_p}]$ 加群で平坦なもののなす圏と圏同値. $D = (D, D^0, \phi_{-1}, \phi_0)$ を ρ に対応する Fontaine-Laffaille 加群とする. $H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho) \cong \mathrm{Ext}^1_{\mathrm{flat}, \mathcal{O}/\lambda^n[G_{\mathbb{Q}_p}]}(\rho, \rho) \cong \mathrm{Ext}^1_{\mathrm{MF}_{\mathcal{O}}}(D, D)$ であり, $\mathrm{RHom}(D, D)$ は以下の 2 重複体に付随した複体で計算される:

$$\begin{tikzcd}
\mathrm{Hom}_{\mathcal{O}}(D, D) \arrow[r, "|_{D^0}"] & \mathrm{Hom}_{\mathcal{O}}(D^0, D) \\
\mathrm{Hom}_F(D, D) \arrow[u, "\cdot\phi_{-1} - \phi_{-1}\cdot"] \arrow[r, "\cdot\phi_0 - \phi_0\cdot|_{D^0}"'] & \mathrm{Hom}_{\mathcal{O}}(D^0, D). \arrow[u, "p"']
\end{tikzcd}$$

ここで, 左下が次数 0 の項, $\mathrm{Hom}_{\mathcal{O}}$ は $\mathcal{O}$ 加群の準同型, Hom_F は $\mathcal{O}$ 加群の準同型で D^0 を D^0 にうつすもの, 左の縦の射は $a \mapsto a\phi_{-1} - \phi_{-1}a$ で, 下の横の射は $a \mapsto a\phi_0 - \phi_0 a|_{D^0}$. 左上, 右上, 左下, 右下の $\mathbb{F}$ 上の次元はそれぞれ 4, 2, 3, 2 であり, $H^0 = \mathrm{Hom}_{F,\phi}(D, D) \cong \mathrm{Hom}_{G_{\mathbb{Q}_p}}(\bar{\rho}, \bar{\rho}) \cong H^0(\mathbb{Q}_p, \mathrm{ad}\bar{\rho})$, $H^2 = 0$(上の横の射は全射) である. $H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho)$ は変形の言葉で言い換えると $H^1(\mathbb{Q}_p, \mathrm{ad}\rho)$ の中で det が動かないものであり, H^1_{f} (や H^1_{st}) の時, 動きえる det は不分岐な指標による捻りだけなので, $\#(H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho)/H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}^0\rho)) = \#\mathcal{O}/\lambda^n$ であることを使うと, $\frac{\#H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}^0\rho)}{\#H^0(\mathbb{Q}_p, \mathrm{ad}^0\rho)} = \frac{\#H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho)}{\#H^0(\mathbb{Q}_p, \mathrm{ad}\rho)} = (\#\mathcal{O}/\lambda^n)^{4+2-2-3} = \#\mathcal{O}/\lambda^n$. □

最後に残された双対 Selmer 群であるが, 次節で素数の有限集合 Σ としてうまくとった Q_n に対して

$$H^1_{Q_n^{\perp}}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) = 0$$

を示すことができる. また, Q_n の各素数 q は $q \equiv 1 \mod p$ かつ $\bar{\rho}(\mathrm{Fr}_q)$ の固有値は相異なるようにとれる. 以上のことから, 次節でうまく素数の有限集合 Q_n をとった時 ($p \notin Q_n$ にも注意),

$$\dim_{\mathbb{F}} H^1_{Q_n}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) = \#Q_n$$

であり,

$$H^1_{Q_n}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}) \cong \mathrm{Hom}_{\mathbb{F}}(\mathfrak{m}_{R_{Q_n}}/(\lambda, \mathfrak{m}^2_{R_{Q_n}}), \mathbb{F})$$

から R_{Q_n} が $\#Q_n$ 個の元で位相的に生成されることが分かる.

2.3 双対 Selmer 群の消滅.

本節では素数の有限集合 Σ をうまくとって双対 Selmer 群を消す. この時構成する変形を Taylor-Wiles 型の変形といい, 記号として Σ ではなく Q を使うことにする. Frobenius 準同型 Fr_q を算術的 Frobenius (つまり, $a \mapsto a^q$) とし, 局所類体論の同型を素元が Fr_q に対応するものとする. 定理 2.3 の証明中でもでてきた完全系列

$$0 \to H^1_{Q^{\perp}}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \to H^1_{\emptyset^{\perp}}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \to \bigoplus_{q \in Q} H^1(\mathbb{F}_q, \mathrm{ad}^0\bar{\rho}(1))$$

を考える. 以下の条件を満たす素数の有限集合 Q_n がとれることを本節で示す.

1. $q \in Q_n$ に対して, $q \equiv 1 \mod p^n$,
2. $q \in Q_n$ に対して, $\bar{\rho}$ は q で不分岐で $\bar{\rho}(\mathrm{Fr}_q)$ の固有値は相異なる,
3. $H^1_{\emptyset^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \xrightarrow{\sim} \bigoplus_{q\in Q} H^1(\mathbb{F}_q, \mathrm{ad}^0\bar{\rho}(1))$.

この時, 上の完全系列から $H^1_{Q_n^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) = 0$ が示される. さらに, 上の条件 1, 2 から $\dim_{\mathbb{F}} H^1(\mathbb{F}_q, \mathrm{ad}^0\bar{\rho}(1)) = 1$(命題 2.4 の 4 参照) なので,

$$\dim_{\mathbb{F}} H^1_{\emptyset^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) = \#Q_n$$

となり, $\#Q_n$ は n に依らないことが分かる.

さて, Cebotarev 密度定理より, 次を示せば十分 ($H^1_{\emptyset^\perp}$ の基底の各元に対して以下の定理のような $\sigma = \mathrm{Fr}_q$ をとると, 射 $H^1_{\emptyset^\perp} \to \oplus_{q\in Q} H^1(\mathbb{F}_q, \mathrm{ad}^0\bar{\rho}(1))$ が全射になることにも注意).

定理 2.6 0 でないコホモロジー類 $[\psi] \in H^1_{\emptyset^\perp}(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1))$ に対して, 以下を満たす $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ が存在する*:*

- $\sigma|_{\mathbb{Q}(\zeta_{p^n})} = 1$,
- $\bar{\rho}(\sigma)$ は相異なる固有値を持つ,
- $\psi(\sigma) \notin (\sigma - 1)\mathrm{ad}^0\bar{\rho}(1)$. □

証明 $F_n := \overline{\mathbb{Q}}^{\ker(\mathrm{ad}^0\bar{\rho})}(\zeta_{p^n}) \supset \mathbb{Q}(\zeta_{p^n})$ とおく.

ステップ 1: $H^1(F_n/\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) = 0$ を示す.
次の完全系列を考える:

$$0 \to H^1(F_0/\mathbb{Q}, (\mathrm{ad}^0\bar{\rho}(1))^{G_{F_0}}) \to H^1(F_n/\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \to H^1(F_n/F_0, \mathrm{ad}^0\bar{\rho}(1))^{G_{\mathbb{Q}}}.$$

$p \nmid [F_1 : F_0]$ と $G_{\mathbb{Q}}$ の $\mathrm{Gal}(F_n/F_1)$ への作用が自明であることから

$$H^1(F_n/F_0, \mathrm{ad}^0\bar{\rho}(1))^{G_{\mathbb{Q}}} \cong \mathrm{Hom}(\mathrm{Gal}(F_n/F_1), (\mathrm{ad}^0\bar{\rho}(1))^{G_{\mathbb{Q}}})$$

であり, 命題 2.4 の 2 よりこれは 0 になる (ここで条件 (L) は $p = 3$ の時のみ使う). 次に, $H^1(F_0/\mathbb{Q}, (\mathrm{ad}^0\bar{\rho}(1))^{G_{F_0}}) = 0$ を示す. $H^1(F_0/\mathbb{Q}, (\mathrm{ad}^0\bar{\rho}(1))^{G_{F_0}})$ は以下の時以外は 0 になるので, この 2 つを仮定する.

1. $p \mid [F_0 : \mathbb{Q}]$ かつ,
2. 全射 $\mathrm{Gal}(F_0/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ が存在する時.

$\mathrm{Gal}(F_0/\mathbb{Q}) \cong (\mathrm{Im}\bar{\rho})/\mathbb{F}\cdot 1$ に注意する．ここで $\mathrm{PSL}_2(\mathbb{F})$ の部分群の分類を使う．$p > 3$ の時, $\mathrm{PSL}_2(\mathbb{F})$ の部分群で位数が p で割れ, $\mathbb{Z}/(p-1)\mathbb{Z}$ に全射があるものを考えると, $\mathrm{Im}\bar{\rho}$ は Borel 部分群の共役に含まれるものしかないが，これは $\bar{\rho}$ の既約性に矛盾．$p = 3$ の時は $\bar{\rho}$ の既約性から $\mathrm{Im}\bar{\rho}$ は Borel 部分群の共役に含まれないし，全射 $\mathrm{Im}\bar{\rho} \twoheadrightarrow \mathbb{Z}/2\mathbb{Z}$ の存在から $\mathrm{Im}\bar{\rho}$ は A_5(5 次交代群) と同型ではないので, $\mathrm{Im}\bar{\rho} \cong \mathrm{PGL}_2(\mathbb{F}_{3^r})$ か $\mathrm{Im}\bar{\rho} \cong \mathrm{PSL}_2(\mathbb{F}_{3^r})$ となる．$S_4 \cong \mathrm{PGL}_2(\mathbb{F}_3)$, $A_4 \cong \mathrm{PSL}_2(\mathbb{F}_3)$ (この同型は $\mathrm{PGL}_2(\mathbb{F}_3)$ の $\mathbb{P}^1(\mathbb{F}_3)$ への一次分数変換を考えるとすぐに分かる) よりこの場合も上記の場合に入っていることに注意．$2 \nmid p = 3$ より $H^1(F_0/\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \cong H^1(F_0/\mathbb{Q}(\zeta_3), \mathrm{ad}^0\bar{\rho}(1)) \cong H^1(F_0/\mathbb{Q}(\zeta_3), \mathrm{ad}^0\bar{\rho})$ なので

$$H^1(\mathrm{SL}_2(\mathbb{F}_{3^r}), \mathrm{End}^0(\mathbb{F}_{3^r}^2)) = 0$$

を示せば十分．これは群のコホモロジーの計算としてよく知られている (一般に $\mathbb{F}_{3^r}$ だけでなく，$q \neq 5$, $2 \nmid q$ である $\mathbb{F}_q$ に対して知られている [DDT, Lemma 2.48]．方針としては, $U \subset B$ をそれぞれ $G = \mathrm{SL}_2(\mathbb{F}_q)$ の冪単部分群と Borel 部分群, p を q を割る素数とすると，$p \nmid [G:B], [B:U]$ より $H^1(G, \mathrm{End}^0(\mathbb{F}_q^2)) \hookrightarrow H^1(B, \mathrm{End}^0(\mathbb{F}_q^2))$ $H^i(B, \mathrm{End}^0(\mathbb{F}_q^2)) \cong H^i(U, \mathrm{End}^0(\mathbb{F}_q^2))^{B/U}$ $(i \geq 0)$ であり, $\#\mathbb{F} = 3$ では $\ker\{1+\sigma+\sigma^2\}/(1+\sigma)\mathrm{End}^0 = 0$, $\#\mathbb{F} > 5$ では End^0 に各部分商が 1 次元になるフィルトレイションを入れて長完全系列で計算すると $H^1(U, \mathrm{End}^0(\mathbb{F}_q^2))^B = 0$ が分かる.).

　ステップ 2: 残り.
ステップ 1 ($H^1(F_n/\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) = 0$) と完全系列

$$0 \to H^1(F_n/\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \to H^1(\mathbb{Q}, \mathrm{ad}^0\bar{\rho}(1)) \to H^1(F_n, \mathrm{ad}^0\bar{\rho}(1))^{G_\mathbb{Q}} (\cong \mathrm{Hom}_{G_\mathbb{Q}}(G_{F_n}, \mathrm{ad}^0\bar{\rho}(1)))$$

から $0 \neq \psi(G_{F_n}) \subset \mathrm{ad}^0\bar{\rho}(1)$ が従う．$\mathrm{ad}^0\bar{\rho}(1)$ は条件 (L) より既約 $\mathrm{Gal}(F_n/\mathbb{Q})$ 加群である (命題 2.4 の 2 の証明参照．ここで条件 (L) は $p = 3$ の時のみ使う) ので, $\psi(G_{F_n}) = \mathrm{ad}^0\bar{\rho}(1)$．まず条件 1, 2 を満たすような $\sigma_0 \in G_{\mathbb{Q}(\zeta_{p^n})}$ がとれることを示す．もし条件 2 を満たすような σ_0 がとれないとすると, $\bar{\rho}(G_{\mathbb{Q}(\zeta_{p^n})})$ はトーラスに含まれるか, $G_{\mathbb{Q}(\zeta_{p^n})}$ の作用で安定な 1 次元部分空間をもつ．前者の時は $\bar{\rho}$ は $\mathbb{Q}(\zeta_{p^n})$ に含まれる 2 次体の指標からの誘導表現であり, $\bar{\rho}|_L$ が可約になり矛盾 (ここで条件 (L) は $p \neq 3$ の時も使う)．後者の時はその 1 次元部分空間は $G_\mathbb{Q}$ の作用でも安定なので $\bar{\rho}$ の既約性に矛盾する．よって条件 1, 2 を満たす $\sigma_0 \in G_{\mathbb{Q}(\zeta_{p^n})}$ をとれる．この時, $(\sigma_0 - 1)\mathrm{ad}^0\bar{\rho}(1) \neq \mathrm{ad}^0\bar{\rho}(1) = \psi(G_{F_n})$ に注意する．ここで, $\tau \in G_{F_n}$ をうまくとることで

$$\psi(\tau\sigma_0) = \tau\psi(\sigma_0) + \psi(\tau) = \psi(\sigma_0) + \psi(\tau) \notin (\sigma_0 - 1)\mathrm{ad}^0\bar{\rho} = (\tau\sigma_0 - 1)\mathrm{ad}^0\bar{\rho}$$

となるようにとれることを示せば証明が終わる．もし $\psi(\sigma_0) \notin (\sigma_0 - 1)\mathrm{ad}^0\bar{\rho}$ ならば $\tau = 1$ とればよい．もし $\psi(\sigma_0) \in (\sigma_0 - 1)\mathrm{ad}^0\bar{\rho}$ ならば, $\psi(\tau) \notin (\sigma_0 - 1)\mathrm{ad}^0\bar{\rho}(1)$ となる $\tau \in G_{F_n}$ をとればよい (このステップ 2 の別証明については [T3, Lemma 2.5] 参照)．□

2.4 Taylor-Wiles 型普遍変形環の $\mathcal{O}[\Delta_Q]$ 代数構造.

$Q := Q_n$ とおく．$q \in Q$ に対して, Δ_q を $(\mathbb{Z}/q\mathbb{Z})^\times$ の最大 p 冪商とし, $\Delta_Q := \prod_{q\in Q}\Delta_q$ とおく．Δ'_Q を $\prod_{q\in Q}(\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow \Delta_Q$ の核とする．本節では R_Q の $\mathcal{O}[\Delta_Q] \cong \mathcal{O}[[S_q : q \in Q]]/((1+S_q)^{\#\Delta_q}-1 : q \in Q)$ 代数の構造を考える．ここで, パラメータ S_q たちの数が $\#Q$ であり, これが R_Q の位相的生成元の個数と一致することが重要である (1.1.2 の 2 参照).

合成

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) \cong (\mathbb{Z}/q\mathbb{Z})^\times \twoheadrightarrow \Delta_q$$

を χ_q とし, $\chi_Q := \prod_{q\in Q}\chi_q : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \Delta_Q$ とおく．各 $q \in Q$ に対して $\bar\rho(\mathrm{Fr}_q)$ の固有値 α_q を選んでおく.

補題 2.7 Q 型普遍変形 $\rho_{R_Q} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(R_Q)$ に対して, $\xi_q(\mathrm{Fr}_q) \equiv \alpha_q \mod \mathfrak{m}_{R_Q}$ となる指標 $\xi_q : D_q \to R_Q^\times$ で,

$$\rho_{R_Q}|_{D_q} \sim \begin{pmatrix} \xi_q & 0 \\ 0 & \varepsilon\xi_q^{-1} \end{pmatrix}$$

となるものが存在する.

証明 Fr_q の D_q への持ち上げも Fr_q と書くことにする．$\bar\rho(\mathrm{Fr}_q)$ は相異なる固有値 α_q, β_q をもつので, Hensel の補題から $\rho_{R_Q}(\mathrm{Fr}_q) = \begin{pmatrix} \tilde\alpha_q & 0 \\ 0 & \tilde\beta_q \end{pmatrix}$ と書ける．$\bar\rho$ は q で不分岐なため, $\rho_{R_Q}|_{I_q}$ の像は副 p 群 $1_2 + M_2(\mathfrak{m}_{R_Q})$ に入るので ρ_{R_Q} は q で馴分岐 (tamely ramified). 従って, 任意の $\sigma \in I_q$ に対して $\rho_{R_Q}(\mathrm{Fr}_q)\rho_{R_Q}(\sigma)\rho_{R_Q}(\mathrm{Fr}_q)^{-1} = \rho_{R_Q}(\sigma)^q$. ここから $\rho_{R_Q}(\sigma)$ が対角であることが分かる．□

上で ρ_{R_Q} が q で馴分岐であることを言ったのと同じ議論から, $\xi_q|_{I_q}$ は χ_q を経由する:

$$\begin{tikzcd} I_q \arrow[r, "\xi_q|_{I_q}"] \arrow[d, "\chi_q"'] & R_Q^\times \\ \Delta_q. \arrow[ur, dotted, "\xi'_q"'] & \end{tikzcd}$$

$\xi'_Q : \Delta_Q \to R_Q^\times$ を $\prod_{q\in Q}\xi'_q$ で定義する．R_Q の $\mathcal{O}[\Delta_Q]$ 代数構造を $(\xi'_Q)^{-2}$ から誘導されるもので定義する.

注意 2.7.1 このように R_Q の $\mathcal{O}[\Delta_Q]$ 代数構造を定義する理由は, ダイヤモンド作用素で与えられる充 Hecke 環での $\mathcal{O}[\Delta_Q]$ 代数構造と整合的にするためである (充 Hecke 環と被約 Hecke 環の “捻られた” 同型が間にはさまっていることにも注意). 次章参照. □

次の系は定理 1.1 の仮定 1 の R の部分である.

系 2.8 $\mathfrak{a}_Q$ を $\mathcal{O}[\Delta_Q]$ の付加 (augmentation) イデアルとすると, 標準射 $R_Q \to R_\emptyset$ は同型

$$R_Q/\mathfrak{a}_Q \xrightarrow{\sim} R_\emptyset$$

を誘導する. □

3 Hecke 環と Hecke 加群.

この章では, 3.1 節で充 Hecke 環を定義し, 保型形式に付随した Galois 表現について軽く復習する. 3.2 節で被約 Hecke 環を定義し, それが充 Hecke 環と同型であることを示す. 3.3 節で定理 1.1 での "T, H が十分大きい" にあたる H_n の $\mathcal{O}[\Delta_Q]$ 上の自由性を示す. 充 Hecke は H_n の $\mathcal{O}[\Delta_Q]$ 上の自由性を示すのに使われ, 被約 Hecke は Galois 表現の係数環として自然に現れる.

[W1], [TW] での Taylor-Wiles 系は T_n が $\mathcal{O}[\Delta_Q]$ 上自由であることを要求していたため, 法 p での q 展開原理と重複度 1 を使って H_n が自由 T_n 加群であることを示すことで T_n の $\mathcal{O}[\Delta_Q]$ 上の自由性を示していた. しかし, Diamond-藤原の改良 ([D1]) により, Taylor-Wiles 系は T_n の $\mathcal{O}[\Delta_Q]$ 上の自由性ではなく H_n の $\mathcal{O}[\Delta_Q]$ 上の自由性で機能する上, Taylor-Wiles 系の存在から H が T 上自由であることも導出できるようになった. このようにして, 法 p での q 展開原理と重複度 1 という幾何的議論がいらなくなり, 可換環論的議論で置き換わった (6 章も参照). 本稿では Diamond-藤原の方法で紹介する.

この章で示す事柄は, その後さらに改良されて簡単に示すことができる事柄で置き換えることが可能になった (注意 3.9.1 参照) が, 本稿ではもとの議論を紹介し, 改良版は本報告集 [Y] と加塩氏の記事参照.

3.1 充 Hecke 環.

自然数 N に対して,

$$\begin{aligned}
\Gamma_0(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N \right\} \\
&\supset \Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a \equiv d \equiv 1, c \equiv 0 \mod N \right\} \\
&\supset \Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; a \equiv d \equiv 1, b, c \equiv 0 \mod N \right\}
\end{aligned}$$

とする. また, $(\mathbb{Z}/N\mathbb{Z})^\times$ の部分群 H に対して

$$\Gamma_0(N) \supset \Gamma_H(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; c \equiv 0 \mod N, d \mod N \in H \right\} \supset \Gamma_1(N)$$

とする．$\Gamma_1(N) \subset \Gamma \subset \Gamma_0(N)$ をみたす部分群 Γ をとる．$S_2(\Gamma)$ を重さ 2 の Γ に関する尖点形式のなす空間とする．$S_2(\Gamma, \mathbb{Z})$ をその中で Fourier 係数が整数になものとする．よく知られているように, $S_2(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} \cong S_2(\Gamma)$ である ([DDT, Theorem 1.31])．また, $S_2(\Gamma, \mathbb{Z})$ は Hecke 作用素とダイヤモンド作用素で保たれる．$\mathbb{Z}$ 代数 A に対して, $S_2(\Gamma, A) := S_2(\Gamma, \mathbb{Z}) \otimes_{\mathbb{Z}} A$ とおき, $\mathbb{T}_A(\Gamma) \subset \mathrm{End}(S_2(\Gamma, A))$ をすべての Hecke 作用素 T_n ($(n, N) = 1$), U_ℓ ($\ell \mid N$) とダイヤモンド作用素 $\langle d \rangle$ ($(d, N) = 1$) で A 上生成される部分 A 代数とする ($(m, n) = 1$ に対して, $(m, N) = 1$, $(n, N) = 1$ の時 $T_{mn} = T_m T_n$, $(m, N) = 1$, $(n, N) > 1$ の時 $U_{mn} = T_m U_n$, $(m, N) > 1$, $(n, N) > 1$ の時 $U_{mn} = U_m U_n$ であり, 素数 ℓ と $k \geq 1$ に対して $\ell \nmid N$ の時 $T_{\ell^{k+1}} = T_\ell T_{\ell^k} - \ell \langle \ell \rangle T_{\ell^{k-1}}$, $\ell \mid N$ の時 $U_{\ell^k} = U_\ell^k$ を満たす．素数 ℓ に対して T_ℓ ($\ell \nmid N$) と U_ℓ ($\ell \mid N$) の $f = \sum_{n>0} a_n q^n$ への作用ははそれぞれ

$$T_\ell f = \frac{1}{\ell} \sum_{i=0}^{\ell-1} f\left(\frac{\tau+i}{\ell}\right) + \ell \langle \ell \rangle f(\ell\tau), \quad U_\ell f = \frac{1}{\ell} \sum_{i=0}^{\ell-1} f\left(\frac{\tau+i}{\ell}\right) = \sum_{\ell \mid n} a_n q^{n/\ell}$$

で与えられ, ダイヤモンド作用素 $\langle d \rangle$ ($(d, N) = 1$) は $ad - bc = 1$, $c \equiv 0 \mod N$ となる a, b, c をとってきて $(\langle d \rangle f)(\tau) = (c\tau + d)^{-2} f(\frac{a\tau+b}{c\tau+d})$ で与えられる．特に, $(n, N) = 1$ の時 $a_1(T_n f) = a_n(f)$, $(n, N) > 1$ の時 $a_1(U_n f) = a_n(f)$ である)．X_Γ, J_Γ をそれぞれ Γ についてのモジュラー曲線とその Jacobi 多様体とする．$\tau \mapsto \tau$, $\tau \mapsto \ell\tau$ が誘導する射 $X_{\Gamma \cap \Gamma_0(\ell)} \to X_\Gamma$ をおのおの α, β とおく, Hecke 作用素 T_ℓ あるいは U_ℓ は $S_2(\Gamma) \cong H^0(X_\Gamma, \Omega^1_{X_\Gamma})$ に対して $\alpha_* \beta^*$ で与えられるという幾何的起源をもつことから, $\mathbb{T}_A$ は自然に $H_1(X_\Gamma, \mathbb{Z}) \otimes A$ に作用する．A が $\mathbb{Z}_p$ 代数の時は p 進 Tate 加群 $T_p J_\Gamma \otimes A$ にも自然に作用する．$\mathbb{T}_{\mathcal{O}}(\Gamma)$ の極大イデアル $\mathfrak{m}$ に対してその局所化 $\mathbb{T}_{\mathfrak{m}} := \mathbb{T}_{\mathcal{O}}(\Gamma)_{\mathfrak{m}}$ を**充 Hecke 環**という．定義から $\mathbb{T}_{\mathfrak{m}}$ はすべての Hecke 作用素とダイヤモンド作用素を含む．また, $\mathbb{T}_{\mathfrak{m}}$ は一般に被約とは限らない．

ペアリング

$$\begin{aligned} \mathbb{T}_A \otimes S_2(\Gamma, A) &\to A, \\ T \otimes f &\mapsto a_1(Tf), \end{aligned} \tag{3}$$

が完全であり, このペアリングにより $\mathbb{T}_A \to A$ で環の準同型になっているものと $S_2(\Gamma, A)$ の正規化された ($a_1(f) = 1$ ということ) Hecke 固有形式とが対応していることが容易に分かる．これより, $\mathbb{T}_E$ の極大イデアルと $S_2(\Gamma, \overline{E})$ の正規化された Hecke 固有形式の $\mathrm{Gal}(\overline{E}/E)$ 共役類が 1 対 1 に対応し, $\mathbb{T}_{\mathcal{O}}(\Gamma)$ の極大イデアルと $S_2(\Gamma, \overline{\mathbb{F}})$ の正規化された Hecke 固有形式の $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ 共役類が 1 対 1 に対応することが分かる ([DDT, §4.1] 参照)．

また, 上のペアリングから $S_2(\Gamma, A)^\vee$ が $\mathbb{T}_A$ 上階数 1 の自由加群と分かり, そこから $H_1(X_\Gamma, \mathbb{Q})$ が $\mathbb{T}_{\mathbb{Q}}$ 上階数 1 の自由加群であること, $\mathbb{Q}_p \otimes T_p J_\Gamma$ が $\mathbb{T}_{\mathbb{Q}_p}$ 上階数 2 の自由加群であることも分かる ([DDT, Lemma 1.34, Lemma 1.37, Lemmar 1.39])．しかし, $(T_p J_\Gamma \otimes \mathcal{O})_{\mathfrak{m}}$ が $\mathbb{T}_{\mathfrak{m}}$ 上階数 2 の自由加群であることは一般には不成立 ([MR, §13]) であり, ある種の局所化に対しては成立するがそれは深い結果である ([M1] で最初に示された)．Diamond-藤原によって Taylor-Wiles 系が改良される前は, この $\mathbb{T}_{\mathfrak{m}}$ 上の自由性を法 p での q 展開原理と重複度 1 を使って示し, $\mathbb{T}_{\mathfrak{m}}$ 上の自由性を使って Taylor-Wiles 系を構成していたが, Diamond-藤原によ

る Taylor-Wiles 系の改良により, Taylor-Wiles 系を構成するのに $\mathbb{T}_{\mathfrak{m}}$ 上の自由性は不要になり, かつ, Taylor-Wiles 系からの可換環論的な帰結として $\mathbb{T}_{\mathfrak{m}}$ 上の自由性が導出されるようになった. 6 章も参照.

また, $\mathbb{T}_E$ が局所完全交叉 E 代数であることも

$$\mathbb{T}_E \cong \prod_f E[X_{f,\ell} : \ell]/(X_{f,\ell}^{v_\ell(N/N_f)-1}(X_{f,\ell}^2 - a_\ell(f)X_{f,\ell} + \ell\psi_f(\ell)) : \ell)$$

から分かる. ここで f は $S_2(\Gamma)$ の新形式を動き, ℓ は N/N_f を割る素数を動き, N_f, ψ_F はそれぞれ f のレベルと指標を表す (ℓ が N_f を割る時は $\psi_f(\ell) = 0$ とおく). しかし, $\mathbb{T}_{\mathfrak{m}}$ がある種の状況で局所完全交叉 $\mathcal{O}$ 代数であることは Taylor-Wiles 系を用いて示される深い事実である.

重さ 2 の保型形式に付随した Galois 表現について軽く復習する. 埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{E}$ を固定する. 係数体 E を (固定した埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{E}$ で) すべての $f \in S_2(\Gamma)$ の Fourier 係数が入るように十分大きくとっておく (f の有限位数の指標 ψ_f も E に値をとるとみる). $f \in S_2(\Gamma)$ を正規化された Hecke 固有新形式とする. $E_f := \mathbb{Q}(a_n(f) : n > 0)$ とおくと $\mathbb{T}_{\mathbb{Q}} \cong S_2(\Gamma, \mathbb{Q})^\vee$ と $\dim_{\mathbb{Q}} S_2(\Gamma, \mathbb{Q}) < \infty$ から分かるように $[E_f : \mathbb{Q}] < \infty$ である. $\lambda_f : \mathbb{T}_{\mathbb{Q}} \to E_f$ $(T \mapsto a_1(Tf))$ を f に対応する射とし, $\mathbb{T}_{\mathbb{Z}} \supset I_f := \ker(\lambda_f) \cap \mathbb{T}_{\mathbb{Z}}$ とおく. **f に付随した Abel 多様体** A_f を $A_f := J_\Gamma/I_f J_\Gamma$ で定義する. $[f]$ を f の Galois 共役なもののなす有限集合とした時, $A_f \otimes \mathbb{C}$ は $S_2(\Gamma)^\vee/H_1(X_\Gamma, \mathbb{Z})$ の $[f]$ 成分と同型なので, $\dim A_f = [E_f : \mathbb{Q}]$ であることも分かる. A_f の p 進 Tate 加群 T_pA_f には Galois 群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ が作用し, この作用 ρ_f を **f に付随した Galois 表現**という. $T_pJ_\Gamma \otimes \mathbb{Q}_p$ が $\mathbb{T}_{\mathbb{Q}_p}$ 上階数 2 の自由加群であることから $T_pA_f \otimes \mathbb{Q}_p$ は $E_f \otimes_{\mathbb{Q}} \mathbb{Q}_p$ 上階数 2 の自由加群であることが分かる.

命題 3.1 素数 ℓ に対して ρ_f の I_ℓ 不変商を $(\rho_f)_{I_\ell}$ とおく.

1. ρ_f は Np の外不分岐,
2. ρ_f は絶対既約,
3. ρ_f の導手は f のレベル N と一致,
4. $\ell \nmid Np$ に対して $\det(1 - \mathrm{Fr}_\ell : T_pA_f) = \mathrm{Norm}_{E_f/\mathbb{Q}}(\lambda_f(1 - a_\ell(f) + \ell\psi_f(\ell)))$,
5. $\ell \mid N$, $\ell^2 \nmid N$, $\ell \neq p$ を満たす素数 ℓ について, χ を $\chi(\mathrm{Fr}_\ell) = a_\ell(f)$ を満たす D_ℓ の不分岐指標とすると, $\ell \nmid \mathrm{cond}(\psi_f)$ の時と $\ell \mid \mathrm{cond}(\psi_f)$ の時で各々

$$\rho_f|_{D_\ell} \simeq \begin{pmatrix} \chi\varepsilon & * \\ 0 & \chi \end{pmatrix}, \quad \rho_f|_{D_\ell} \simeq \chi^{-1}\varepsilon\psi'_f \oplus \chi.$$

特に, どちらの場合に関しても $(\rho_f)_{I_\ell}(\mathrm{Fr}_\ell) = a_\ell(f)$.

6. $p>2$, $p\nmid N$ かつ ρ_f が p で通常である (これは $a_p(f)$ の p での付値が 0 と同値 ([DDT, Thoerem 3.1 (f)])) 時, $(\rho_f)_{I_p}(\mathrm{Fr}_p)$ は $X^2-a_p(f)X+p\psi_f(p)$ の根で付値が 0 である方 (これを**単元根**ということにする) と一致する,

7. $p>2$, $p\mid N$, $p^2\nmid N$ かつ $p\nmid \mathrm{cond}(\psi_f)$ の時, ρ_f は通常でかつ $(\rho_f)_{I_p}(\mathrm{Fr}_p)=a_p(f)$. □

証明 1. 構成から, A_f は N の外で良還元を持つことから分かる.

2. Galois 表現 T_pA_f がもし絶対可約であれば, f の Fourier 係数の増大度は Eisenstein 級数と同程度になるが, f が尖点形式であることからくる Fourier 係数の増大度の上からの評価と矛盾するため, T_pA_f は絶対既約と分かる (Ribet の議論 [R2]).

3. Carayol-斎藤の局所・大域整合性 ($\ell\neq p$ 部分は[Ca1], $\ell=p$ 部分は [S3], 本報告集三枝氏の記事参照) から分かる.

4. Eichler-志村関係式 $T_\ell=\mathrm{Fr}_\ell+\langle\ell\rangle\mathrm{Fr}_\ell^t$ から分かる.

5. Carayol の局所・大域整合性 ([Ca1]) から分かる. これは基本的に $J_1(N)$ の法 ℓ 還元の様子からでる ([Ca1] は $\mathbb{Q}$ でない総実代数体で主に書かれているが, そこに書かれているように放物コホモロジーを使って適宜修正すれば $\mathbb{Q}$ でも通用する).

6. p 可除群 $A_f[p^\infty]$ がエタール部分 $(A_f[p^\infty])^{\text{ét}}$ を乗法的部分 $(A_f[p^\infty])^\mu$ で拡大したものになっていることと $A_f[p^\infty]$ の Dieudonné 加群への Frobenius の跡が $\ell\nmid Np$ に対する $T_\ell A_f$ の Frobenius の跡と一致することから分かる ([W2, Theorem 2.2],[W3, Lemma 2.1.5] 参照).

7. 6. と同様. □

注意 3.1.1 Eichler-志村関係式は, 例えば $\Gamma=\Gamma_1(N)$ の時, $X_1(N)$ のモジュライ解釈を使うことで以下のように示される. $\ell\nmid N$ の時 $X_1(N)$ は良還元を持つ. $X_1(N)_{/\mathbb{F}_\ell}$ の点 (E,P) に対して, $(E_\infty,P_\infty):=\phi_{X_1(N)_{/\mathbb{F}_\ell}}(E,P)$ とすると E の Frobenius 準同型 ϕ_E は (E,P) から (E_∞,P_∞) への次数 ℓ の同種射 (isogeny) になる. $\phi_{X_1(N)_{/\mathbb{F}_\ell}}$ は $J_1(N)_{/\mathbb{F}_\ell}$ の自己準同型 Fr_ℓ を誘導するが, ここではその転置 Fr_ℓ^t が考えられる. $\mathrm{Fr}_\ell^t(E,P)=(E_1,P_1)+\cdots+(E_\ell,P_\ell)$ とすると, E_i の Frobenius 準同型 ϕ_{E_i} は (E_i,P_i) から (E,P) への次数 ℓ の同種射を与える. その双対同種射は (E,P) から $(E_i,\ell P_i)$ への射である. E が ℓ で通常の時, $(E_\infty,P_\infty),(E_1,\ell P_1),\ldots,(E_\ell,\ell P_\ell)$ は (E,P) から次数 ℓ の同種射をもつもの全体であるので,

$$T_\ell(E,P)=(E_\infty,P_\infty)+(E_1,\ell P_1)+\cdots+(E_\ell,\ell P_\ell)=(\mathrm{Fr}_\ell+\langle\ell\rangle\mathrm{Fr}_\ell^t)(E,P)$$

が分かる. 通常な点 (E,P) は $X_1(N)_{/\mathbb{F}_\ell}$ で稠密なので, $J_1(N)_{/\mathbb{F}_\ell}$ の自己準同型として $T_\ell=\mathrm{Fr}_\ell+\langle\ell\rangle\mathrm{Fr}_\ell^t$ が従う. □

$\mathbb{T}_E$ の極大イデアル $\mathfrak{p}$ に対して, p 進 Tate 加群 $T_pJ_\Gamma \otimes_{\mathbb{Z}_p} E$ は $\mathbb{T}_E$ 上階数 2 の自由加群なので法 $\mathfrak{p}$ 還元することで表現

$$\rho_{\mathbb{T}_E/\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_E/\mathfrak{p})$$

を得る. また, $\mathbb{T}_\mathcal{O}(\Gamma)$ の極大イデアル $\mathfrak{m}$ で $\mathfrak{m} \cap \mathbb{T}_E = \mathfrak{p}$ となる唯一のものをとると, $\rho_{\mathbb{T}_E/\mathfrak{p}}$ の法 p 還元の半単純化 $\bar{\rho}_{\mathbb{T}_E/\mathfrak{p}}$ は $\mathbb{T}_\mathcal{O}/\mathfrak{m} \cong \mathbb{T}_\mathfrak{m}/\mathfrak{m}$ に値をもつ:

$$\rho_{\mathbb{T}_\mathfrak{m}/\mathfrak{m}} := \bar{\rho}_{\mathbb{T}_E/\mathfrak{p}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_\mathfrak{m}/\mathfrak{m}).$$

$\ell \nmid Np$ を満たす素数 ℓ に対して $\rho_{\mathbb{T}_E/\mathfrak{p}}(\mathrm{Fr}_\ell)$, $\rho_{\mathbb{T}_\mathfrak{m}/\mathfrak{m}}(\mathrm{Fr}_\ell)$ の特性多項式はそれぞれ

$$X^2 - T_\ell X + \ell\langle \ell \rangle \mod \mathfrak{p},\ X^2 - T_\ell X + \ell\langle \ell \rangle \mod \mathfrak{m}$$

である. $\mathbb{T}_\mathcal{O}$ の極大イデアル $\mathfrak{m}$ について, $\ell \equiv 1 \mod N$ を満たす任意の素数 ℓ に対して $T_\ell \equiv \ell + 1 \mod \mathfrak{m}$ を満たすとき, $\mathfrak{m}$ を **Eisenstein イデアル**という. これは表現 $\rho_{\mathbb{T}_\mathfrak{m}/\mathfrak{m}}$ が絶対可約であることと同値であることが容易に分かる ([DDT, Lemma 4.12]).

3.2 被約 Hecke 環.

この章では以下 $p > 2$ とする. 被約 Hecke 環を定義する. $\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ を 2 章と同様な法 p 表現, $N(\bar{\rho})$ を $\bar{\rho}$ の p の外の Artin 導手とする. Σ を素数の有限集合とする. 以下を仮定する:

仮定 (Σ)

- $p \in \Sigma$ ならば, $\bar{\rho}$ が p で平坦かつ通常,
- $\ell \in \Sigma$, $\ell \neq p$ ならば, $\bar{\rho}$ は ℓ で不分岐.

p の外でも条件を課す理由は, 注意 3.6.2 参照. この時,

$$N_\Sigma := p^{\delta(\bar{\rho})} N(\bar{\rho}) \prod_{\ell \in \Sigma \setminus \{p\}} \ell^{\dim \bar{\rho}^{I_\ell}} = p^{\delta(\bar{\rho})} \prod_{\ell | N(\bar{\rho})} \ell \prod_{\ell \in \Sigma \setminus \{\ell\}} \ell^2$$

とおく. ここで, $\delta(\bar{\rho})$ は

$$\delta(\bar{\rho}) := \begin{cases} 0 & \bar{\rho} \text{ は } p \text{ で平坦かつ } p \notin \Sigma, \\ 1 & \text{その他.} \end{cases}$$

$\mathcal{N}_\Sigma$ を重さ 2 の新形式 f でレベルが N_Σ を割り, f に付随した Galois 表現 ρ_f の法 p 還元 $\bar{\rho}_f$ が $\bar{\rho}$ と同値になるもの全体とする (Γ_0 構造で考えているので, $\psi_f = 1$ である). $\bar{\rho}$ は保型的と仮定しているので, [D3, Theorem 1.1, Theorem 5.1, Lemma 2.1] より, $N_f \mid N(\bar{\rho})p^{\delta(\bar{\rho})}$ と

なる Hecke 固有形式 f が存在する．$N(\bar{\rho}) \mid N_f$ が容易に分かる ([DDT, Lemmar 2.7]) のと [G, §8], [E, §2.4] から $p^{\delta(\bar{\rho})} \mid N_f$ も分かるので $N_f = N(\bar{\rho})p^{\delta(\bar{\rho})}$．従って，**任意の Σ に対して $\mathcal{N}_\Sigma$ は空集合でない** ([DDT, Theorem 3.15])．$\tilde{\mathbb{T}}_\Sigma := \prod_{f\in\mathcal{N}_\Sigma} \mathcal{O}_f$ とおく．$\ell \nmid N_\Sigma$ を満たす素数 ℓ に対して $\tilde{\mathbb{T}}_\Sigma \ni T_\ell := (a_\ell(f))_f$ とおき，$\mathbb{T}_\Sigma$ を T_ℓ $(\ell \nmid N_\Sigma)$ で $\mathcal{O}$ 上生成される部分 $\mathcal{O}$ 代数とする．$\mathbb{T}_\Sigma$ を**被約 Hecke 環**という．$\mathbb{T}_\Sigma$ は完備 Noether 局所 $\mathcal{O}$ 代数で剰余体は $\mathbb{F}$ である．構成から $\mathbb{T}_\Sigma$ は被約で，有限生成自由 $\mathcal{O}$ 加群である．$\mathbb{T}_\Sigma$ はすべての Hecke 作用素を使って定義していないことに注意する．また，Γ_0 構造で考えているのでダイヤモンド作用素は自明であることにも注意.

補題 3.2 連続表現

$$\rho_{\mathbb{T}_\Sigma} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_\Sigma)$$

で $\ell \nmid N_\Sigma$ をみたす素数 ℓ に対して $\rho_{\mathbb{T}_\Sigma}$ は ℓ で不分岐で，$\mathrm{Tr}\rho_{\mathbb{T}_\Sigma}(\mathrm{Fr}_\ell) = T_\ell$ を満たすものが存在する．□

証明 表現 $\rho_{\tilde{\mathbb{T}}_\Sigma} := \prod_{f\in\mathcal{N}_\Sigma} \rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\tilde{\mathbb{T}}_\Sigma)$ で複素共役 c_0 が $\rho_{\tilde{\mathbb{T}}_\Sigma}(c_0) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ を満たすように基底をとる．勝手な $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ をとり $\rho_{\tilde{\mathbb{T}}_\Sigma}(g) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とする．$a,b,c,d \in \mathbb{T}_\Sigma$ を示せば残りの主張は ρ_f の性質から従う．Cebotarev 密度定理から $\mathrm{Tr}\rho_{\tilde{\mathbb{T}}_\Sigma}(g) = a+d$ と $\mathrm{Tr}\rho_{\tilde{\mathbb{T}}_\Sigma}(c_0 g) = a-d$ は $\mathbb{T}_\Sigma$ に値をもつ．よって，$a,d \in \mathbb{T}_\Sigma$．$\bar{\rho}$ は既約なので，$\bar{\rho}(\sigma) = \begin{pmatrix} * & b' \\ * & * \end{pmatrix}$，$b' \neq 0$ となる $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ と $\bar{\rho}(\tau) = \begin{pmatrix} * & * \\ c'' & * \end{pmatrix}$，$c'' \neq 0$ となる $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ が存在する．基底を定数倍して $\rho_{\tilde{\mathbb{T}}_\Sigma}(\sigma) = \begin{pmatrix} a' & 1 \\ c' & d' \end{pmatrix}$，$\rho_{\tilde{\mathbb{T}}_\Sigma}(\tau) = \begin{pmatrix} a'' & b'' \\ 1 & d'' \end{pmatrix}$ とできる．$\rho_{\tilde{\mathbb{T}}_\Sigma}(\sigma g) = \begin{pmatrix} aa'+c & * \\ * & * \end{pmatrix}$，$\rho_{\tilde{\mathbb{T}}_\Sigma}(\tau g) = \begin{pmatrix} * & * \\ * & b+dd'' \end{pmatrix}$ なので，$aa'+c, b+dd' \in \mathbb{T}_\Sigma$ であるが，$a,a',d,d' \in \mathbb{T}_\Sigma$ より $c,b \in \mathbb{T}_\Sigma$ が分かる．□

局所・大域整合性より，$\rho_{\mathbb{T}_\Sigma}$ は Σ 型の変形と分かる．従って，射 $R_\Sigma \to \mathbb{T}_\Sigma$ が存在する．定義から $\mathbb{T}_\Sigma$ は Hecke 作用素 T_ℓ $(\ell \nmid N_\Sigma)$ で生成されるので，上の補題よりこれは全射 $R_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$ と分かる．本章で $\Sigma = \emptyset$ の時に Taylor-Wiles 系を使ってこれが同型であることを示し，次章で一般の Σ に対して数値的判定法を用いて $\Sigma = \emptyset$ の場合に帰着させることでこれが同型であることを示す.

さて，充 Hecke 環と被約 Hecke 環が定義されたので，その間の同型に話をすすめる．各 $f \in \mathcal{N}_\Sigma$ に対して，$f_1 \in S_2(\Gamma_0(N_\Sigma), E_f)$ を以下の条件をみたす正規化された Hecke 固有形式とする:

- $\ell \nmid N_\Sigma/N_f$ ならば $a_\ell(f_1) = a_\ell(f)$,

- $\ell \mid N_\Sigma/N_f$, $\ell \neq p$ ならば $a_\ell(f_1) = 0$,
- $p \mid N_\Sigma/N_f$ ならば $a_p(f_1)$ は $X^2 - a_p(f)X + p$ の単元根と一致 ($p \mid N_\Sigma/N_f$ より f は p で平坦かつ通常であることに注意).

この時, f_1 の法 p 還元 $\overline{f_1}$ は f に依らないことも分かる ([DDT, Lemma 4.6]). $\overline{f_1}$ に対応する $\mathbb{T}_{\mathcal{O}}(\Gamma_0(N_\Sigma))$ の極大イデアルを $\mathfrak{m}_\Sigma$, その局所化を $\mathbb{T}_{\mathfrak{m}_\Sigma}$(充 Hecke 環) とする. 係数体 E をすべての $f \in \mathcal{N}_\Sigma$ に対する $X^2 - a_p(f)X + p$ の単元根を (固定した埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{E}$ で) 含むように十分大きくとる.

補題 3.3 $\ell \nmid N_\Sigma p$ を満たす素数 ℓ に対して T_ℓ を T_ℓ に送る $\mathcal{O}$ 代数の同型 $\mathbb{T}_\Sigma \xrightarrow{\sim} \mathbb{T}_{\mathfrak{m}_\Sigma}$ が存在する. □

証明 E 代数の同型射 $\kappa : \mathbb{T}_{\mathfrak{m}_\Sigma} \otimes E \xrightarrow{\sim} \prod_{f \in \mathcal{N}_\Sigma} E$ で

$$\kappa(T_\ell)_f = \begin{cases} a_\ell(f) & \ell \notin \Sigma \text{の時}, \\ 0 & \ell \in \Sigma \setminus \{p\} \text{ の時}, \\ X^2 - a_p(f)X + p \text{ の単元根} & \ell = p \in \Sigma \text{の時}, \end{cases}$$

であるものが容易に構成できる. $\mathbb{T}_\Sigma$ を $T_\ell = (a_\ell(f))_f$ ($\ell \nmid N_\Sigma p$) で生成される $\prod_{f \in \mathcal{N}_\Sigma} E$ の部分 $\mathcal{O}$ 代数とみれば, すべての $\ell \mid N(\bar\rho)p$ に対して $\kappa(T_\ell)$ が $\mathbb{T}_\Sigma$ に含まれることを言えば十分.

$N(\bar\rho)p^{\delta(\bar\rho)}$ を割る素数 ℓ に対して, $\ell \neq p$ の時は命題 3.1 の 5, $\ell = p$ の時は命題 3.1 の 7 より, $\mathbb{T}_\Sigma \ni (\rho_{\mathbb{T}_\Sigma})_{I_\ell}(\mathrm{Fr}_\ell) = (a_\ell(f))_f = \kappa(T_\ell)$. 最後に残された $\delta(\bar\rho) = 0$, $\ell = p$ の場合を示す (以下は Ribet による補題. [W1, p.491 の Lemma] 参照. Galois 表現を用いた別証明は [W1, p.508] 参照). T_p 以外のすべての Hecke 作用素で生成される $\mathbb{T}_{\mathfrak{m}_\Sigma}$ の部分 $\mathcal{O}$ 代数を $\mathbb{T}'_{\mathfrak{m}_\Sigma}$ とおく. $\mathbb{T}'_{\mathfrak{m}_\Sigma} \otimes_{\mathbb{Z}} \mathbb{F}_p \to \mathbb{T}_{\mathfrak{m}_\Sigma} \otimes_{\mathbb{Z}} \mathbb{F}_p$ が全射であることを示せば十分. 双対で考えて

$$\mathrm{Hom}(\mathbb{T}_{\mathfrak{m}_\Sigma} \otimes \mathbb{F}_p, \mathbb{F}_p) \to \mathrm{Hom}(\mathbb{T}'_{\mathfrak{m}_\Sigma} \otimes \mathbb{F}_p, \mathbb{F}_p)$$

が単射であることを示す. ペアリング (3) から $S_2(\Gamma_0(N_\Sigma), \mathbb{F}_p) \cong \mathrm{Hom}(\mathbb{T}_{\mathfrak{m}_\Sigma} \otimes \mathbb{F}_p, \mathbb{F}_p)$ である. $f \in S_2(\Gamma_0(N_\Sigma), \mathbb{F}_p)$ を上の射の核の元とすると, $p \nmid n$ を満たす自然数 n に対して $(n, N_\Sigma) = 1$ の時 $a_n(f) = a_1(T_n f) \equiv 0 \mod p$, $(n, N_\Sigma) > 1$ の時 $a_n(f) = a_1(U_n f) \equiv 0 \mod p$ なので, f は $q\frac{d}{dq}$ の核に入っている. f の重さは 2 なので $p > 2$ では $q\frac{d}{dq}$ は単射 ([Ka, Corollary(5)]) なので主張が従う (Hasse 不変量 A を重さ $p-1$ の法 p 保型形式とみて, 重さ k の法 p 保型形式上の $q\frac{d}{dq}$ の核は $A^r g^p$ と書ける. ここで a, b は $ap + r(p-1) = k$, $0 \leq r \leq p-1$, $r + k \equiv 0 \mod p$ を満たす自然数で g は重さ a の法 p 保型形式). □

次に, 2.3, 2.4 節であつかったような Taylor-Wiles 型変形に対応する Hecke 環について考える. 被約 Hecke 環 $\mathbb{T}_Q$ は Γ_0 構造で考えているのでダイヤモンド作用素は自明であるが, ダイヤモンド作用素が非自明である別の Γ に関する充 Hecke 環と “捻った形での” 同型をいう. R_Q の $\mathcal{O}[\Delta_Q]$ 構造を一見不自然に入れたようにみえるのはこのように “捻った形での”

同型を使うことで全射 $R_Q \twoheadrightarrow \mathbb{T}_Q$ を通じて入る $\mathbb{T}_Q$ の $\mathcal{O}[\Delta_Q]$ 構造が充 Hecke 環でみるとダイヤモンド作用素になっているようにしたいためである.

素数の有限集合 Q をとる. 任意の $q \in Q$ について, $q \equiv 1 \mod p$, $\bar{\rho}$ は q で不分岐, $\bar{\rho}(\mathrm{Fr}_q)$ の固有値は相異なると仮定する. Δ_Q, Δ'_Q を 2.4 節で定義したものとする.

$$\Gamma_Q := \Gamma_0(N_\emptyset) \cap \Gamma_{\Delta'_Q}(\prod_{q\in Q} q)$$

とおく. ここで, $\Gamma_{\Delta'_Q}(\prod_{q\in Q} q)$ は 3.1 節で定義した Γ_H で $H = \Delta'_Q$ としたもの.

各 $f \in \mathcal{N}_\emptyset$ と各 $q \in Q$ に対して, $X^2 - a_q(f)X + q = 0$ の根で 2.4 節で選んだ α_q と合同なものを $\tilde{\alpha}_q(f)$ とおく. 係数体 E をすべての $f \in \mathcal{N}_\emptyset$ とすべての $q \in Q$ に対して $\tilde{\alpha}_q(f)$ を (固定した埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{E}$ で) 含むように十分大きくとる. 各 $f \in \mathcal{N}_\emptyset$ に対して, $f_1 \in S_2(\Gamma_Q, E_f)$ を以下の条件をみたす正規化された Hecke 固有形式とする:

- $\ell \notin Q$ ならば $a_\ell(f_1) = a_\ell(f)$,
- $\ell \in Q$ ならば $a_\ell(f_1) = \tilde{\alpha}_q(f)$,

この時, f_1 の法 p 還元 $\overline{f_1}$ は f に依らないことも分かる. $\overline{f_1}$ に対応する $\mathbb{T}_\mathcal{O}(\Gamma_Q)$ の極大イデアルを $\mathfrak{m}_Q$, その局所化を $\mathbb{T}_{\mathfrak{m}_Q}$ (充 Hecke 環) とする. 今回の $\mathbb{T}_{\mathfrak{m}_Q}$ はレベル $\prod_{q\in Q} q$ に関して $\Gamma_{\Delta'_Q}$ 構造を使っているので, 非自明なダイヤモンド作用素が入っていることに注意.

$d \in (\mathbb{Z}/\prod_{q\in Q} q\mathbb{Z})^\times$ に対して, $\langle d\rangle - 1 \in \mathfrak{m}_Q$ であり, $(\mathbb{Z}/\prod_{q\in Q} q\mathbb{Z})^\times \twoheadrightarrow \Delta_Q$ の核 Δ'_Q は $p \nmid \#\Delta'_Q$ より $\langle d\rangle^{\#\Delta'_Q - 1} + \ldots + \langle d\rangle + 1 \notin \mathfrak{m}_Q$ なので, $d \in \Delta'_Q$ に対して $\langle d\rangle - 1 = (\langle d\rangle^{\#\Delta'_Q - 1} + \ldots + \langle d\rangle + 1)^{-1}(\langle d\rangle^{\#\Delta'_Q} - 1) = 0$. よって, $\mathbb{T}_{\mathfrak{m}_Q}$ には $d \mapsto \langle d\rangle$ により $\mathcal{O}[\Delta_Q]$ 代数構造がはいる. 一方, 被約 Hecke 環 $\mathbb{T}_Q$ には $\mathcal{O}[\Delta_Q] \to R_Q \twoheadrightarrow \mathbb{T}_Q$ により $\mathcal{O}[\Delta_Q]$ 代数構造をいれる. 素数 $\ell \notin Q$ に対して, $x_\ell \in \mathcal{O}[\Delta_Q]$ を $x_\ell^{-2} = \bar{p}$ を満たす唯一の元とする.

命題 3.4 $\ell \nmid N_Q p$ を満たす素数 ℓ に対して T_ℓ を $x_\ell T_\ell$ に送る $\mathcal{O}[\Delta_Q]$ 代数の同型 $\mathbb{T}_Q \xrightarrow{\sim} \mathbb{T}_{\mathfrak{m}_Q}$ が存在する. □

証明 $S_2(\Gamma_Q)$ の新形式 g に対してそのレベルを N_g, 指標を ψ_g, ψ_g の導手を Q_g とする. 重さ 2 の新形式 g で $\bar{\rho}_g \cong \bar{\rho}$ かつ $\Gamma_0(N_\emptyset) \cap \Gamma_{\Delta'_Q}(\prod_{q\in Q} q)$ に関して保型性をもち, 各 $\ell \mid N_g/N_\emptyset$ に対して $a_\ell(g) \equiv \alpha_\ell$ を満たすもの全体を $\mathcal{N}$ とおく. 命題 3.1 の 5. より $N_g = N_\emptyset Q_g$ と分かる. $\psi_g \equiv 1 \mod \mathfrak{m}_Q$ より ψ_g は馴分岐で位数は p 冪. ξ_g を $(\mathbb{Z}/Q_g\mathbb{Z})^\times$ の p 冪指標で ξ_g^{-2} が ψ_g に付随した原始指標とする. $g \otimes \xi_g := \sum_{n>0} \xi_g(n) a_n(g) q^n$ は指標が自明になるので, $g \otimes \xi_g \in \mathcal{N}_{Q_g} \subset \mathcal{N}_Q$ である ($\mathcal{N}$ の方は $\Gamma_0(N_\emptyset) \cap \Gamma_{\Delta'_Q}(\prod_{q\in Q} q)$ 構造で, $\mathcal{N}_Q$ の方は $\Gamma_0(N_\emptyset \prod_{q\in Q} q^2)$ 構造であることを思い出しておく).

ステップ 1: この時, $g \mapsto g \otimes \xi_g$ は全単射 $\mathcal{N} \xrightarrow{\sim} \mathcal{N}_Q$ を与える.
逆射を構成する. $f \in \mathcal{N}_Q$ と $q \in Q$ に対して, 2.4 節の補題から

$$\rho_f|_{D_q} \sim \begin{pmatrix} \xi_{f,q} & 0 \\ 0 & \varepsilon\xi_{f,q}^{-1} \end{pmatrix}$$

となる．ここで $\xi_{f,q}:D_q\to E^\times$ は $\overline{\xi_{f,q}}\equiv\alpha_q \mod \lambda$ となる指標．特に, Q_f を $\xi_{f,q}$ が分岐するような q の積とすると, $N_f=N_\emptyset Q_f^2$. 指標 $\xi_f:(\mathbb{Z}/Q_f\mathbb{Z})^\times\to E^\times$ を各 $q\mid Q_f$ に対して $I_q\to\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\twoheadrightarrow\mathrm{Gal}(\mathbb{Q}(\zeta_{Q_f})/\mathbb{Q})\xrightarrow{\xi_f}E^\times$ が $\xi_{f,q}|_{I_q}$ に一致する唯一のものとする．g_f を $f\otimes\xi_f^{-1}$ (アプリオリにはこのレベルは $\Gamma_0(N_\emptyset)\cap\Gamma_{\Delta'_Q}(Q_f^2)$) に付随した新形式とすると,

$$\rho_{g_f}|_{I_q}\sim\begin{pmatrix}1&0\\0&\xi_{f,q}^{-2}\end{pmatrix}=\begin{pmatrix}1&0\\0&\psi_f\end{pmatrix},$$

$N_{g_f}=N_\emptyset Q_f$ であり, 各 $q\mid Q_f$ に対して $(\xi_f|_{D_q}^{-1}\xi_{f,q})(\mathrm{Fr}_q)\equiv\overline{\xi_{f,q}}(\mathrm{Fr}_q)=\alpha_q$ を満たすので, $g_f\in\mathcal{N}$ が分かる．

ステップ 2: 残り．

E 代数の同型射 $\kappa:\mathbb{T}_{\mathfrak{m}_Q}\otimes E\xrightarrow{\sim}\prod_{g\in\mathcal{N}}E$ で

$$\kappa(T_\ell)_g=\begin{cases}a_\ell(g) & \ell\notin Q\text{ または }\ell\mid Q_g\text{の時},\\ X^2-a_\ell(g)X+\ell\text{の根で}\alpha\text{と合同なもの} & \ell\in Q\text{ かつ }\ell\nmid Q_g\text{の時},\end{cases}$$

$$\kappa(\langle d\rangle)=\psi_g(d),\quad d\in\Delta_Q\text{の時},$$

であるものが容易に構成できる．$\mathbb{T}_Q$ は $T_\ell=(a_\ell(f))_f$ $(\ell\nmid N_\Sigma p)$ で生成される $\prod_{f\in\mathcal{N}_Q}E$ の部分 $\mathcal{O}$ 代数であるが, $\mathcal{O}$ 代数の射 $\kappa':\mathbb{T}_Q\hookrightarrow\prod_{f\in\mathcal{N}}E$ を $\ell\nmid N_Q$ に対して T_ℓ を $(\xi_g(\ell)a_\ell(g))_g=\kappa(x_\ell T_\ell)$ に送るとする (ここで, 右辺には $\mathbb{T}_{\mathfrak{m}_Q}$ からくる $\mathcal{O}[\Delta_Q]$ 代数構造をいれる)．R_Q の $\mathcal{O}[\Delta_Q]$ 代数構造は $(\xi'_Q)^{-2}$ で入れたことを思い出す．$(\xi'_Q)^{-2}\in R_Q$ を R_Q の普遍性からくる射で ρ_f の表現空間まで送り, 全単射 $\mathcal{N}\cong\mathcal{N}_Q$ を通じて $\prod_{f\in\mathcal{N}}E$ でみると, $(\xi_f)^{-2}=\psi_f$ となり, これはダイヤモンド作用素と一致するので, 上の射のは $\mathcal{O}[\Delta_Q]$ 代数の射になる．

上の射の像 $\kappa'(\mathbb{T}_Q)$ は $\kappa(\mathbb{T}_{\mathfrak{m}_Q})$ に含まれる．よって, すべてのダイヤモンド作用素 $\langle d\rangle$ とすべての $\ell\mid N_Qp$ に対する $\kappa(T_\ell)$ が $\mathbb{T}_Q$ に含まれることを言えば十分.

ダイヤモンド作用素については κ' の像は Δ_Q の像を含んでおり, 従って $\kappa(\langle d\rangle)$ を含むことから分かる．$N(\bar\rho)p^{\delta(\bar\rho)}$ を割る素数 ℓ と $\delta(\bar\rho)=0$, $\ell=p$ の場合に対しては前回の $\mathbb{T}_\Sigma\cong\mathbb{T}_{\mathfrak{m}_\Sigma}$ と同様の議論で分かる．$q\in Q$ の場合は, $g\in\mathcal{N}$ に対して $(\xi_f|_{D_q}^{-1}\xi_{f,q})(\mathrm{Fr}_q)\equiv\alpha_q$ なので $\kappa'(\mathbb{T}_Q)\ni(\xi_f|_{D_q}^{-1}\xi_{f,q})(\mathrm{Fr}_q)=\kappa(T_q)$ が分かる．□

3.3 $\mathcal{O}[\Delta_Q]$ 自由性.

本節で H_n の $\mathcal{O}[\Delta_Q]$ 上の自由性を証明するが, その時に Γ_Q が上半平面に自由に作用していないと困るのでここで**補助的素数**を r を以下のようにとる:

- $r\nmid 6N_Qp$ (特に, $\bar\rho$ は r で不分岐),
- $r\neq 1 \mod p$,

- $(\mathrm{Tr}\bar{\rho}(\mathrm{Fr}_r))^2 \neq (1+r)^2$.

最後の条件は, $\bar{\rho}(\mathrm{Fr}_r)$ の固有値を α, β とすると, $\alpha/\beta \neq r^{\pm 1}$ と同値である．このような r をとれることは 2.2 節の条件 (L)($p \neq 3$ の時は $\bar{\rho}$ の絶対既約性で十分) を使うと [DDT, Lemma 4.11] から分かる (ここでも $\mathrm{PSL}_2(\mathbb{F})$ の部分群の分類が使われている事に注意).

$$\Gamma'_Q := \Gamma_Q \cap \Gamma_1(r^2)$$

とおく．Γ'_Q は $\Gamma_1(r)$ に含まれるので, 楕円点を含まず, 上半平面に自由に作用する ($\Gamma_1(r) \ni \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ を位数有限の元とすると, その特性多項式 $X^2-(a+d)X+1=0$ は 1 の累乗根に根をもつ．一方, $a \equiv d \equiv 1 \mod r$ から $a+d \equiv 2 \mod r$ であるので, $r>3$ より $a+d=0$ と分かる).

各 $f \in \mathcal{N}_\emptyset$ に対して, $f'_1 \in S_2(\Gamma'_Q, E_f)$ を以下の条件をみたす正規化された Hecke 固有形式とする:

- $\ell \notin Q \cup \{r\}$ ならば $a_\ell(f'_1) = a_\ell(f)$,
- $\ell \in Q$ ならば $a_\ell(f'_1) = \tilde{\alpha}_q(f)$,
- $a_r(f'_1) = 0$.

Γ'_Q のレベルは r^2 で割れるので, r についての旧形式の空間で Hecke 作用素 U_r の特性多項式は $X(X^2 - a_r(f)X + r\langle r\rangle)$ であるため, 最後の条件を満たすものがとれることに注意する．この時, f'_1 の法 p 還元 $\overline{f'_1}$ は f に依らないことも分かる．$\overline{f'_1}$ に対応する $\mathbb{T}_{\mathcal{O}}(\Gamma'_Q)$ の極大イデアルを $\mathfrak{m}'_Q$, その局所化を $\mathbb{T}_{\mathfrak{m}'_Q}$(充 Hecke 環) とする．

補助的素数が "邪魔をしない" ことを示すため (とその後の $\mathcal{O}[\Delta_Q]$ 不変商の考察のため) に, 次の補題を用意する．

補題 3.5 *ℓ を $\bar{\rho}$ が不分岐な素数とする．この時, $\bar{\rho}|_{D_\ell}$ の変形 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell) \to \mathrm{GL}_2(\mathcal{O})$ で分岐するものは以下の 3 通り:*

1. $\rho|_{I_\ell} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ で, $\bar{\rho}(\mathrm{Fr}_\ell)$ の固有値を α, β とすると $\alpha/\beta = \ell^{\pm 1}$,
2. ψ_1, ψ_2 を馴分岐指標で $\psi_1 \equiv \varepsilon$, $\psi_2 \equiv 1 \mod \lambda$ であるものとして $\rho^{\mathrm{s.s.}} \sim \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix}$ で, $\ell \equiv 1 \mod p$,
3. $\mathbb{Q}_{\ell^2}$ を $\mathbb{Q}_\ell$ の不分岐 2 次拡大, ψ を $D_{\mathbb{Q}_{\ell^2}}$ の馴分岐指標で $\psi \equiv 1 \mod \lambda$ であるものとして $\rho \cong \mathrm{Ind}_{\mathbb{Q}_\ell}^{\mathbb{Q}_{\ell^2}} \psi$ で, $\ell \equiv -1 \mod p$. $\square$

より一般に $\bar{\rho}$ と ρ で導手が変わるものの分類は [Ca2] 参照.

証明　I_ℓ の像は副 p 群 $1_2+M_2(\lambda)$ に入るので, $I_\ell \twoheadrightarrow I_\ell^{\mathrm{tame}} \twoheadrightarrow \mathbb{Z}_p(1)$ を経由する. $\mathbb{Z}_p(1)$ の像が無限であるときは場合 1. になり, この時 $\sigma \in \mathbb{Z}_p(1)$ に対して $\mathrm{Fr}_\ell \sigma \mathrm{Fr}_\ell^{-1} = \sigma^\ell$ から $\alpha/\beta = \ell^{\pm 1}$ が分かる. $\mathbb{Z}_p(1)$ の像が有限の時は, $\rho|_{I_\ell}$ は馴分岐指標の和になるが, $\mathbb{Z}_p(1)$ の位相的生成元の値をそれぞれ a, b とすると, 同じく $\mathrm{Fr}_\ell \sigma \mathrm{Fr}_\ell^{-1} = \sigma^\ell$ から $\{a, b\} = \{a^\ell, b^\ell\}$ である. $a = a^\ell$ の時は場合 2. であり, $I_\ell^{\mathrm{tame}} = \varprojlim_n \mathbb{F}_{\ell^n}^\times \twoheadrightarrow \mathbb{F}_\ell^\times$ を経由して作用するので $\ell \equiv 1 \mod p$ である. $a \neq a^\ell$ の時は場合 3. であり, $I_\ell^{\mathrm{tame}} = \varprojlim_n \mathbb{F}_{\ell^n}^\times \twoheadrightarrow \mathbb{F}_{\ell^2}^\times$ を経由して作用し, $\mathbb{F}_\ell^\times$ を経由しないので $\ell^2 \equiv 1 \mod p$, $\ell \not\equiv 1 \mod p$ より, $\ell \equiv -1 \mod p$. □

系 3.6 ℓ を $\bar{\rho}$ が不分岐な素数とする. $(\mathrm{Tr}\bar{\rho}(\mathrm{Fr}_\ell))^2 \neq (\ell+1)^2$ かつ $\ell \not\equiv 1 \mod p$ の時, ρ は ℓ で不分岐. □

証明　補題で 3. の場合も $(\mathrm{Tr}\bar{\rho}(\mathrm{Fr}_\ell))^2 \equiv (\ell+1)^2 \equiv 0 \mod p$ が成立することに注意すればよい. □

これにより, r についての旧形式と新形式が $\mathfrak{m}'_Q$ を法として合同関係式をもたないことが分かる. $\mathfrak{m}_Q$, $\mathfrak{m}'_Q$ はそれぞれ T_r, U_r について r に関する旧形式の空間を 1 次元切り取っているため, 同型

$$\mathbb{T}_{\mathfrak{m}_Q} \cong \mathbb{T}_{\mathfrak{m}'_Q},\ S_2(\Gamma_Q, \mathcal{O})_{\mathfrak{m}_Q} \cong S_2(\Gamma'_Q, \mathcal{O})_{\mathfrak{m}'_Q}$$

が分かる. $\mathbb{T}_{\mathfrak{m}'_Q}$ には前節と同様の議論で $\mathcal{O}[\Delta_Q]$ 代数構造が入るが, 上の同型はそれぞれ $\mathcal{O}[\Delta_Q]$ 代数構造, $\mathcal{O}[\Delta_Q]$ 加群構造と整合的な同型である.

注意 3.6.1 原論文 [TW] の間違いについて. [TW] では

1. 補助的素数 r をとる時に [DT, Lemma 3] を引用して上述の条件の上にさらに "$\bar{\rho}(\mathrm{Fr}_r)$ の固有値が相異なる" という条件をつけ,
2. レベルを $M' := r\prod_{q\in Q} q$ ととり,
3. "補助的素数が邪魔しない" ことについて r で分岐主系列表現と特殊表現がでてこないことをチェックしている ($r^2 \nmid M'$ よりこの場合はそれで十分).

しかし 1. について, これは [DT, Lemma 3] からは分からない. もし固有値が相異なるという条件を落とすと, 固有値が一致してしまう時には r に関する旧形式の空間を 1 次元切り取ってくることができない!

[DDT] ではこの間違いを

1. レベルを $M' := r^2\prod_{q\in Q} q$ とすることで $a_r(f'_1) = 0$ とでき, r に関する旧形式の空間を 1 次元切り取ることができる,
2. 分岐主系列表現と特殊表現以外の表現がレベルを r^2 まで上げると出てくるが, その時も "補助的素数が邪魔しない" ことを [Ca2] を引用することでチェックする

という形で修正してある (そのように明示的には書いていないので [TW] と [DDT] を注意深く読み比べないと分からない). □

注意 3.6.2 補題 3.5 の 3. は, 不分岐拡大をして指標で捻るとレベルが下がる. $\bar{\rho}$ が分岐するときにはさらに以下のようなことがおこる. $\ell \equiv -1 \mod p$ とし, $\overline{\chi}$ を $D_{\mathbb{Q}_{\ell^2}}$ の法 p 指標, χ をその持ち上げ, ψ を $D_{\mathbb{Q}_{\ell^2}}$ の馴分岐指標で $\psi \equiv 1$ であるものとすると, 法 p 指標として, 分岐する法 p 表現 $\mathrm{Ind}_{D_{\mathbb{Q}_\ell}}^{D_{\mathbb{Q}_{\ell^2}}} \chi$ の変形として $\mathrm{Ind}_{D_{\mathbb{Q}_\ell}}^{D_{\mathbb{Q}_{\ell^2}}} (\chi\psi)$ というのもが考えられるが, これはある指標 ψ に対して導手が下がり得る.

"ℓ で分岐が極小な変形" を定める時に, 不分岐拡大と指標による捻りに関しての安定性がないとこのような変形が生じてしまう. このような変形はレベルの上げ下げでは探知できないため困難が生じる ([W1, p.511 の 2 つ目の Remark] 参照). [W1] で, "(C) 型変形" として $H^1(\mathbb{Q}_\ell, \mathrm{ad}^0\bar{\rho}) = 0$ という仮定 (これで上のような変形を排除できる) を p の外で付けていた理由や [DDT] で $\bar{\rho}$ が p の外でも冪単という仮定を付けたり (2.2 節参照), 素数の有限集合 Σ に仮定 (Σ) を付けた (3.1 節参照) 理由はこのためである. [D2] では局所 Langlands 対応をもちいて "極小性" を定めることでこの困難を克服した. □

本題に戻る. $\Gamma'_{Q-} := \Gamma_0(\mathcal{N}_\emptyset \prod_{q\in Q} q) \cap \Gamma_1(r^2)$ (Q で $\Gamma_{\Delta'_Q}$ 構造から Γ_0 構造に変えたもの) とし, $\mathbb{T}_{\mathcal{O}}(\Gamma'_{Q-})$ の極大イデアル $\mathfrak{m}'_{Q-}$ を Γ'_Q と同様に定義する. Γ'_{Q-} は Q で Γ_0 構造を使っているので, $f \in S_2(\Gamma'_{Q-}, \mathcal{O})_{\mathfrak{m}'_{Q-}}$ に付随した Galois 表現 ρ_f に関して $q \in Q$ では補題 3.5 の場合 2. は起こらない. また, $q \in Q$ で $(\mathrm{Tr}\bar{\rho})^2 \neq (1+q)^2 \mod p$ なので $S_2(\Gamma'_{Q-}, \mathcal{O})_{\mathfrak{m}'_{Q-}}$ は $Q \cup \{r\}$ に関して新形式は現れてこない (つまり, $Q \cup \{r\}$ に関する新形式と旧形式は $\mathfrak{m}'_{Q-}$ を法として合同関係式をもたない). $Q \cup \{r\}$ に関して旧形式の空間を 1 次元切り取っているので, 同型

$$\mathbb{T}_{\mathfrak{m}'_{Q-}} \cong \mathbb{T}_\emptyset, \quad S_2(\Gamma'_{Q-}, \mathcal{O})_{\mathfrak{m}'_{Q-}} \cong S_2(\Gamma_\emptyset, \mathcal{O})_{\mathfrak{m}_\emptyset}$$

が分かる ("補助的素数は邪魔をしない" と同様の議論).

$X_Q := X_{\Gamma_Q}$, $X'_Q := X_{\Gamma'_Q}$ をそれぞれ Γ_Q, Γ'_Q に関するモジュラー曲線, $Y'_Q := Y_{\Gamma'_Q}$, $Y'_{Q-} := Y_{\Gamma'_{Q-}}$ をそれぞれ Γ'_Q, Γ'_{Q-} に関するモジュラー曲線で尖点を除いたものとする. そのコホモロジー $H^1(X_Q, \mathcal{O})$, $H^1(X'_Q, \mathcal{O})$, $H^1(Y'_Q, \mathcal{O})$, $H^1(Y'_{Q-}, \mathcal{O})$ にも対応する Hecke 環が自然に作用する ($\mathcal{O}$ は構造層ではなく, 係数体の付値環 $\mathcal{O} = O_E$ である). 上述のことから

$$H^1(X'_Q, \mathcal{O})_{\mathfrak{m}'_Q} \cong H^1(X_Q, \mathcal{O})_{\mathfrak{m}_Q}, \tag{4}$$

$$H^1(Y'_{Q-}, \mathcal{O})_{\mathfrak{m}'_{Q-}} \cong H^1(Y_\emptyset, \mathcal{O})_{\mathfrak{m}'_\emptyset} \tag{5}$$

が成立する. $\bar{\rho}$ は既約なので, $\mathfrak{m}'_Q$ は Eisenstein イデアルではない. 従って,

$$H^1(X'_Q, \mathcal{O})_{\mathfrak{m}'_Q} \cong H^1(Y'_Q, \mathcal{O})_{\mathfrak{m}'_Q} \tag{6}$$

が成立する. $(\cdot)^\pm$ を複素共役 c_0 がそれぞれ ± 1 で作用する部分空間として,

$$H_Q := H^1(X_Q, \mathcal{O})^-_{\mathfrak{m}_Q}$$

とおく.

命題 3.7 $H^1(Y'_Q, \mathcal{O})^-_{\mathfrak{m}'_Q}$ は自由 $\mathcal{O}[\Delta_Q]$ 加群で

$$\mathrm{rank}_{\mathcal{O}[\Delta_Q]} H^1(Y'_Q, \mathcal{O})^-_{\mathfrak{m}'_Q} = \mathrm{rank}_{\mathcal{O}} H^1(Y'_{Q-}, \mathcal{O})^-_{\mathfrak{m}'_{Q-}}. \ \square$$

証明 $H^1(Y'_Q, E)^{\Delta_Q} \cong H^1(Y'_{Q-}, E)$ なので, $H^1(Y'_Q, \mathcal{O})^-_{\mathfrak{m}'_Q}$ が自由 $\mathcal{O}[\Delta_Q]$ 加群であることを証明すれば十分. Γ'_Q, Γ'_{Q-} は上半平面に自由に作用するので, これらは各々Y'_Q, Y'_{Q-} の基本群と同型. 従って群コホモロジーを使って

$$H^1(Y'_Q, \mathcal{O}) \cong H^1(\Gamma'_Q, \mathcal{O}) \cong H^1(Y'_{Q-}, \mathcal{O}[\Delta_Q])$$

とあらわされる. ここで, 最後の同型は Shapiro の補題. Γ'_{Q-} は自由群なので 1 余輪体群 $Z^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q])$ は自由 $\mathcal{O}[\Delta_Q]$ 加群 (Γ'_{Q-} の生成元の行き先で 1 余輪体が決定されるから). 複素共役の作用に対応する元 $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ は $\mathcal{O}[\Delta_Q]$ に自明に作用するので, 1 余境界は $Z^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q])^+$ に含まれる. よって, $H^1(Y'_Q, \mathcal{O})^- \cong Z^1(\Gamma'_{Q-}, \mathcal{O}[\Delta_Q])^-$ は自由 $\mathcal{O}[\Delta_Q]$ 加群 (以上の議論を de Shalit の議論という). $\square$

系 3.8 H_Q は自由 $\mathcal{O}[\Delta_Q]$ 加群であり,

$$H_Q/\mathfrak{a}_Q \xrightarrow{\sim} H_\emptyset, \ \mathbb{T}_Q/\mathfrak{a}_Q \xrightarrow{\sim} \mathbb{T}_\emptyset. \ \square$$

証明 同型 (4) と同型 (6) から最初の主張が分かる. 同型 (5) から 2 番目の主張が分かる. 最後の主張は 2 番目の主張から分かる. $\square$

$R_Q/\mathfrak{a}_Q \xrightarrow{\sim} R_\emptyset$ は簡単であったが, $H_Q/\mathfrak{a}_Q \xrightarrow{\sim} H_\emptyset$ は新形式と旧形式の間に合同関係式がないことや群コホモロジーを使った議論などが必要であった非自明な主張であることに注意する.

以上の 2 章と 3 章の結果により, 定理 1.1 を $R := R_\emptyset$, $T := \mathbb{T}_\emptyset$, $H := H_\emptyset$, $R_n := R_{Q_n}$, $T_n := \mathbb{T}_{Q_n}$, $H_n := H_{Q_n}$ に対して適用すると, 次が示される.

定理 3.9 (極小の時の $R = T$ 定理) 全射 $R_\emptyset \twoheadrightarrow \mathbb{T}_\emptyset$ は同型であり, $R_\emptyset$, $\mathbb{T}_\emptyset$ は局所完全交叉 $\mathcal{O}$ 代数で, $H_\emptyset$ は自由 $\mathbb{T}_\emptyset$ 加群. $\square$

次章では $\Sigma \neq \emptyset$ の時を扱う.

注意 3.9.1 この章で示された Hecke 加群に関する事柄は, その後以下のようにして簡単に示される事柄に置き換えられた.

$\mathbb{Q}$ の総実拡大体 F で, 拡大次数が偶数で $\mathbb{Q}$ 上可解な Galois 群を持つものをとり, F 上の正定値 (positive definite) 四元数代数 (quaternion algebra)D 上の保型形式を考える. それに付随した Galois 表現は構成されている ([T1], 本報告集の山上氏の記事参照). F は $\mathbb{Q}$ 上可解にとってあるので, 保型性持ち上げの目的としては F 上で示せば十分. D が正定値であることから対応する志村多様体の次元は 0 次元になるので, この章で示す事柄に対応するものは (位数の勘定程度で) 簡単に示すことができる ([Y] 参照). $\square$

4　極小でない場合.

前章までで $R_\emptyset \xrightarrow{\sim} \mathbb{T}_\emptyset$ の証明が終わった．この章では一般の Σ に対して，$R_\Sigma \twoheadrightarrow R_\emptyset$ と $\mathbb{T}_\Sigma \twoheadrightarrow \mathbb{T}_\emptyset$ (Diamond-藤原の方法では $H_\Sigma \twoheadrightarrow H_\emptyset$) が各々“どのくらい大きくなるか” を計算し，$\Sigma = \emptyset$ の場合に帰着させて $R_\Sigma \xrightarrow{\sim} \mathbb{T}_\Sigma$ を証明する．4.1 節で $\Sigma = \emptyset$ に帰着させるのに必要な可換環論を述べ，4.2 節で R の方の増分を計算し，4.3 節で H の方の増分を計算して証明を終える．

2.2, 2.3 節で行った Selmer 群の計算から $\Sigma \neq \emptyset$ の時には，R_Σ の位相的生成元の個数が Taylor-Wiles 型変形のパラメータ ($\mathcal{O}[[S_1, \ldots, S_r]]$ の $S_1, \ldots, S_r$ のこと) の個数よりも大きくなるので，1 章の可換環論は使えないことに注意する．

4.1　可換環論.

本節では，$\Sigma = \emptyset$ の場合に帰着させるのに必要な Diamond-藤原による数値的判定法を述べる．そのために，まず Wiles の数値的判定法から始める．

A を完備 Noether 局所 $\mathcal{O}$ 代数で剰余体が $\mathbb{F}$ であるもの，$\pi_Q : A \twoheadrightarrow \mathcal{O}$ を $\mathcal{O}$ 代数の全射とする．組 (A, π_A) と局所 $\mathcal{O}$ 代数の準同型 $\phi : A \to B$ で $\pi_B\phi = \pi_A$ であるもののなす圏を $\mathcal{C}$ とする．$\mathcal{C}$ の対象 (A, π_A) に対して，$\wp_A := \ker \pi_A$ とおき，$\wp_A/\wp_A^2$ を (A, π_A) の**余接空間**，$\eta_A := \pi_A(\mathrm{Ann}_A \wp_A)$ を (A, π_A) の**合同イデアル**とよぶ．対応 $A \mapsto \wp_A/\wp_A^2$ は関手的だが，対応 $A \mapsto \eta_A$ は関手的でないことに注意 (全射については関手的)．Fitting イデアルの一般的な性質から

$$\mathrm{Fitt}_{\mathcal{O}}(\wp_A/\wp_A^2) = \pi_A(\mathrm{Fitt}_A(\wp_A)) \subset \pi_A(\mathrm{Ann}_A(\wp_A)) = \eta_A \tag{7}$$

なので

$$\#\wp_A/\wp_A^2 \geq \#\mathcal{O}/\eta_A \tag{8}$$

が分かる (有限生成 A 加群 M に対して，短完全系列 $0 \to N \to A^n \to M \to 0$ をとり，N の元のすべての n 組 $v_1, \ldots, v_n$ を走らせた時に $\det(v_1, \ldots, v_n) \in A$ で生成されるイデアルは短完全系列のとり方に依らず，それを **Fitting イデアル**という．定義から $\mathrm{Fitt}_A(M) \subset \mathrm{Ann}_A(M)$，$\pi_A(\mathrm{Fitt}_A(M)) = \mathrm{Fitt}_{\mathcal{O}}(M \otimes_A \mathcal{O})$ が分かる．有限 $\mathcal{O}$ 加群 M に対して $\#\mathrm{Fitt}_{\mathcal{O}}(M) = \#M$ も分かる)．以下では $U := \mathcal{O}[[X_1, \ldots, X_n]]$ やその商を $\mathcal{C}$ の対象とみる時は法 $(X_1, \ldots, X_n)$ 還元射を π_U とする．素元 $\varpi \in \mathcal{O}$ を選ぶ．$\mathcal{O}[[X, Y]]/(X(X-\varpi), Y(Y-\varpi), XY)$ は $\wp/\wp^2 \cong \mathcal{O}/\lambda \oplus \mathcal{O}/\lambda$，$\eta = \lambda$ なので不等号 (8) において等号は一般に成立しない．

補題 4.1　([DDT, Theorem 5.21],[DDT, Theorem 5.24]) $\phi : A \twoheadrightarrow B$ を $\mathcal{C}$ の全射とする．

1. B が局所完全交叉平坦 $\mathcal{O}$ 代数で，$\phi : \wp_A/\wp_A^2 \xrightarrow{\sim} \wp_B/\wp_B^2$，$\#\wp_B/\wp_B^2 < \infty$ なら，ϕ は同型，

2. A が局所完全交叉平坦 $\mathcal{O}$ 代数，B は $\mathcal{O}$ 上平坦で，$\eta_A = \eta_B$，$\eta_A \neq 0$ なら，ϕ は同型．□

注意 4.1.1 • 1. で $\#\wp_B/\wp_B^2 < \infty$ の条件を落とすと $\mathcal{O}[[X]]/(X^3) \twoheadrightarrow \mathcal{O}[[X]]/(X^2)$ という反例がある ($\wp_A/\wp_A^2 \cong \wp_B/\wp_B^2 \cong \mathcal{O}$, $\eta_A = \eta_B = (0)$).

- 1. で B が局所完全交叉 $\mathcal{O}$ 代数の条件を落とすと $\mathcal{O}[[X,Y]]/(X(X-\varpi), Y(Y-\varpi)) \twoheadrightarrow \mathcal{O}[[X,Y]]/(X(X-\varpi), Y(Y-\varpi), XY)$ という反例がある ($\wp_A/\wp_A^2 \cong \wp_B/\wp_B^2 \cong \mathcal{O}/\lambda \oplus \mathcal{O}/\lambda$, $\eta_A = \lambda^2$, $\eta_B = \lambda$).
- 2. で $\eta_A \neq 0$ の条件を落とすと $\mathcal{O}[[X,Y]] \twoheadrightarrow \mathcal{O}[[X]]$ という反例がある ($\wp_A/\wp_A^2 \cong \mathcal{O}^2$, $\wp_B/\wp_B^2 \cong \mathcal{O}$, $\eta_A = \eta_B = (0)$).
- 2. で B が $\mathcal{O}$ 上平坦の条件を落とすと $\mathcal{O}[[X]]/(X(X-\varpi^n)) \twoheadrightarrow \mathcal{O}[[X]]/(X^2, \varpi^n X)$ という反例がある ($\wp_A/\wp_A^2 \cong \wp_B/\wp_B^2 \cong \mathcal{O}/\lambda^n$, $\eta_A = \eta_B = \lambda^n$).
- 2. で A が局所完全交叉 $\mathcal{O}$ 代数の条件を落とすと, $\mathcal{O}[[X,Y]]/(X(X-\varpi), Y(Y-\varpi), XY) \twoheadrightarrow \mathcal{O}[[X]]/(X(X-\varpi))$ という反例がある ($\wp_A/\wp_A^2 \cong \mathcal{O}/\lambda \oplus \mathcal{O}/\lambda$, $\wp_B/\wp_B^2 \cong \mathcal{O}/\lambda$, $\eta_A = \eta_B = \lambda$). □

証明 1. $\nu_B : U := \mathcal{O}[[X_1, \ldots, X_n]] \twoheadrightarrow B$ を $\mathcal{C}$ の全射とすると, 仮定 $\phi : \wp_A/\wp_A^2 \xrightarrow{\sim} \wp_B/\wp_B^2$ から $\nu_A : U \twoheadrightarrow A$ に持ち上がる. $\ker \nu_A \subset \ker \nu_B$ なので, $\ker \nu_A \supset \ker \nu_B$ を示せば主張が従う. $g_1, \ldots, g_n \in \ker \nu_A$, $f_1, \ldots, f_n \in \ker \nu_B$ を $\wp_U/\wp_U^2$ での像が $\ker\{\wp_U/\wp_U^2 \twoheadrightarrow \wp_A/\wp_A^2\}$, $\ker\{\wp_U/\wp_U^2 \twoheadrightarrow \wp_B/\wp_B^2\}$ をそれぞれ生成するものとする. $\ker \nu_A \subset \ker \nu_B$ より, $(g_1, \ldots, g_n) = (f_1, \ldots, f_n)M$ となる行列 $M \in M_2(U)$ が存在する. これを法 $(X_1, \ldots, X_n)$ 還元すると $(\overline{g_1}, \ldots, \overline{g_n})$, $(\overline{f_1}, \ldots, \overline{f_n})$ は $\wp_U/\wp_U^2$ の階数 n の同じ部分 $\mathcal{O}$ 加群を生成し, それらは指数有限 (ここで $\#\wp_B/\wp_B < \infty$ を使った) なので $\det \overline{M}$ は $\mathcal{O}$ の単元. 従って, M は可逆となり $\ker \nu_A \supset \ker \nu_B$ が分かる.

2. $x \in \wp_A \cap \mathrm{Ann}_A \wp_A$, $a \in \eta_A$ とし, $a' \in \mathrm{Ann}_A \wp_A$ を $\pi(a') = a$ となるものとする. $ax = (a-a')x = 0$ が成り立つ (最初の等号は $x \in \wp_A$, $a' \in \mathrm{Ann}_A \wp_A$, 次の等号は $a - a' \in \wp_A$, $x \in \mathrm{Ann}_A \wp_A$ から分かる). $\eta_A \neq 0$ であり A は $\mathcal{O}$ 上平坦なので, $\wp_A \cap \mathrm{Ann}_A \wp_A = 0$. 同様に, B も $\mathcal{O}$ 上平坦なので, $\wp_B \cap \mathrm{Ann}_B \wp_B = 0$. 従って, $\pi_A : \mathrm{Ann}_A \wp_A \xrightarrow{\sim} \eta_A$, $\pi_B : \mathrm{Ann}_B \wp_B \xrightarrow{\sim} \eta_B$. 仮定 $\eta_A = \eta_B$ を使うと, $\phi(\mathrm{Ann}_A \wp_A) = \mathrm{Ann}_B \wp_B$. 特に, $\ker \phi \cap \mathrm{Ann}_A \wp_A = 0$ であるので $\ker \phi \oplus \mathrm{Ann}_A \wp_A \subset A$ を得る. この余核は $A/(\ker \phi \oplus \mathrm{Ann}_A \wp_A) \cong B/(\phi(\mathrm{Ann}_A \wp_A)) = B/(\mathrm{Ann}_B \wp_B) \hookrightarrow \mathrm{End}_{\mathcal{O}}(\wp_B)$ なので $\mathcal{O}$ 上平坦. よって $\ker \phi \oplus \mathrm{Ann}_A \wp_A \subset A$ は分裂単射. 局所完全交叉 $\mathcal{O}$ 代数は Gorenstein $\mathcal{O}$ 代数 (Koszul 分解を使うとすぐに分かる. 次の定理の証明中の 3.⇒2. 参照) なので, $\mathcal{O}$ 双対を $(-)^\vee := \mathrm{Hom}_{\mathcal{O}}(-, \mathcal{O})$ とすると全射 $A \twoheadrightarrow (\ker \phi)^\vee \oplus (\mathrm{Ann}_A \wp_A)^\vee$ を得る. $\otimes_A \mathbb{F}$ すると $1 = \dim_{\mathbb{F}} A \otimes_A \mathbb{F} = \dim_{\mathbb{F}} (\ker \phi)^\vee \otimes_A \mathbb{F} + \dim_{\mathbb{F}} (\mathrm{Ann}_A \wp_A)^\vee \otimes_A \mathbb{F}$ であり, $\eta_A \neq 0$ なので, $\dim_{\mathbb{F}} (\mathrm{Ann}_A \wp_A)^\vee \otimes_A \mathbb{F} \neq 0$. よって $(\ker \phi)^\vee \otimes_A \mathbb{F} = 0$. 中山の補題より, $\ker \phi = 0$. よって主張が従う. □

定理 4.2 (Wiles の数値的判定法) $R \twoheadrightarrow T$ を $\mathcal{C}$ の全射で, T は有限生成平坦 $\mathcal{O}$ 加群で, $\eta_T \neq 0$ とする. 次は同値.

1. $\#\wp_R/\wp_R^2 \leq \#\mathcal{O}/\eta_T$,

2. $\#\wp_R/\wp_R^2 = \#\mathcal{O}/\eta_T$,

3. $R \twoheadrightarrow T$ は同型で, R, T は局所完全交叉 $\mathcal{O}$ 代数. □

注意 4.2.1 Wiles の原論文では Gorenstein 性を仮定していた [W1, appendix] が, Lenstra がその仮定が不要であることを示した ([L]).

証明 2.⇒1. は式 (8) から自明.

3.⇒2. R は局所完全交叉 $\mathcal{O}$ 代数なので, Gorenstein $\mathcal{O}$ 代数. 従って, 同型 $\Psi : R^\vee := \mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O}) \cong R$ が存在し, $\mathrm{Ann}_R \wp_R = \Psi\pi_R^\vee(\mathcal{O}^\vee)$ から $\eta_R = \pi_R\Psi\pi_R^\vee(\mathcal{O}^\vee)$ であるが, Koszul 複体を用いた Ψ の具体的な計算から主張が従う. 3.⇒2. よりも 1.⇒3. の方が鍵であるが, 一応詳しく述べる.

$\alpha : \mathcal{O}[[\underline{X}]] := \mathcal{O}[[X_1, \ldots, X_n]] \twoheadrightarrow R$ を $\mathcal{C}$ の全射, $a_i := \alpha(X_i)$, $\ker\alpha = (f_1, \ldots, f_n)$ とおく. $\beta : R[[\underline{X}]] \twoheadrightarrow R$ を $\beta(X_i) = a_i$ で定める. $\ker\beta = (X_1 - a_1, \ldots, X_n - a_n)$ である. $\mathcal{O}[[\underline{X}]]$ を自然に $R[[\underline{X}]]$ の部分代数とみると, $f_i \in \ker\beta$ なので, $(f_1, \ldots, f_n) = (X_1 - a_1, \ldots, X_n - a_n)M$ となる行列 $M \in M_n(R[[\underline{X}]])$ が存在する. $D := \det M \in R[[\underline{X}]]$ とおく. $\mathrm{Kos}(\underline{f})$ を $(f_1, \ldots, f_n)$ に関する $\mathcal{O}[[\underline{X}]]$ 上の Koszul 複体とする (次数 k では $\oplus_{i_1 < \ldots < i_k}\mathcal{O}[[\underline{X}]]u_{i_1} \wedge \ldots \wedge u_{i_k}$ であり, 微分は $d(u_{i_1} \wedge \ldots \wedge u_{i_k}) = \sum_{t=1}^k (-1)^t f_t u_{i_1} \wedge \ldots \wedge u_{i_{t-1}} \wedge u_{i_{t+1}} \wedge \ldots \wedge u_{i_k}$ である複体). 同様に $\mathrm{Kos}(\underline{X} - \underline{a})$ を $(X_1 - a_1, \ldots, X_n - a_n)$ に関する $R[[\underline{X}]]$ 上の Koszul 複体とする. $(f_1, \ldots, f_n)$ と $(X_1 - a_1, \ldots, X_n - a_n)$ はそれぞれ $\mathcal{O}[[\underline{X}]]$, $R[[\underline{X}]]$ で正則列 (regular sequence) なので (前者は R が局所完全交叉性から出る), $\mathrm{Kos}(\underline{f})$, $\mathrm{Kos}(\underline{X} - \underline{a})$ は各々自由 $\mathcal{O}[[\underline{X}]]$ 加群, 自由 $R[[\underline{X}]]$ 加群による分解になっている (帰納法から簡単に分かる). 複体の射 $\Phi : \mathrm{Kos}(\underline{f}) \to \mathrm{Kos}(\underline{X} - \underline{a})$ を次数 0 では自然な埋め込み $\Phi_0 : \mathcal{O}[[\underline{X}]] \hookrightarrow R[[\underline{X}]]$, 次数 1 では $(\Phi_1(u_1), \ldots, \Phi_1(u_n)) = (v_1, \ldots, v_n)M$, 次数 2 以上ではその外積から誘導される射で定義する. Φ の次数 n での射は $\Phi_n(u_1 \wedge \ldots \wedge u_n) = D \cdot v_1 \wedge \ldots \wedge v_n$ で与えられる. Φ は複体のホモトピー同値射であり, 0 次コホモロジーに恒等射を誘導する. 複体の射 Φ に $\mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(-, \mathcal{O}[[\underline{X}]])$ を施して n 次のコホモロジーをとると

$$\begin{aligned}\Phi_n : &\mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(R[[\underline{X}]], \mathcal{O}[[\underline{X}]])/(X_1 - a_1, \ldots, X_n - a_n) \\ &\xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(\mathcal{O}[[\underline{X}]], \mathcal{O}[[\underline{X}]])/(f_1, \ldots, f_n) \cong R\end{aligned}$$

が分かる. 具体的には $f \mapsto \Phi_n(f) = \alpha(f(D))$ で与えられる.

$f \in \mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O})$ に対して $\tilde{f} \in \mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(R[[\underline{X}]], \mathcal{O}[[\underline{X}]])$ を f の自然な拡張とし, それと Φ_n との合成 $f \mapsto \alpha(\tilde{f}(D))$ を $\Psi(f)$ とおく. $\Psi : \mathrm{Hom}_{\mathcal{O}}(R, \mathcal{O}) \to R$ は R 線型である (非自明) ことが次のように分かる. $a \in R$ を勝手な元, $a' \in \mathcal{O}[[\underline{X}]]$ を $\alpha(a') = a$ なる元とすると, $\Psi(af) = \alpha(\tilde{f}(aD)) = \alpha(\tilde{f}((a - a')D)) + \alpha(\tilde{f}(a'D))$ である. $a - a' \in \ker\beta = (X_1 - a_1, \ldots, X_n - a_n)$ であり, $(f_1, \ldots, f_n) = (X_1 - a_1, \ldots, X_n - a_n)M$ に行列 $DM^{-1} \in M_n(R[[\underline{X}]])$ をかけると $(X_i - a_i)D$ が $f_1, \ldots, f_n$ の $R[[\underline{X}]]$ 上の線型結合で表されるので, $(a - a')D$ も

$f_1,\dots,f_n$ の $R[[\underline{X}]]$ 上の線型結合で表される. $\tilde{f}$ は $\mathcal{O}[[\underline{X}]]$ 線型であり, $f_i \in \ker\alpha$ なので, $\alpha(\tilde{f}((a-a')D)) = 0$. よって, $\Psi(af) = \alpha(a'\tilde{f}(D)) = a\Psi(f)$ なので Ψ は R 線型. $f_1,\dots,f_n \in \mathrm{Hom}_{\mathcal{O}}(R,\mathcal{O})$ が $\mathcal{O}$ 上の基底の時, $\tilde{f}_1,\dots,\tilde{f}_n$ は $\mathrm{Hom}_{\mathcal{O}[[\underline{X}]]}(R[[\underline{X}]],\mathcal{O}[[\underline{X}]])$ の $\mathcal{O}[[\underline{X}]]$ 上の基底であることから Ψ が全単射であることが分かる. よって $\Psi : R^\vee = \mathrm{Hom}_{\mathcal{O}}(R,\mathcal{O}) \xrightarrow{\sim} R$ が得られた (R が R 加群として $\mathrm{Hom}_{\mathcal{O}}(R,\mathcal{O})$ と同型であるこの性質を $\mathcal{O}$ 上 **Gorenstein** であるという).

一方, $\mathrm{Ann}_R\wp_R = \Psi\pi_R^\vee(\mathcal{O}^\vee)$ が容易に分かるので, $\eta_R = \pi_R\Psi\pi_R^\vee(\mathcal{O}^\vee) = \pi_R\alpha\tilde{\pi}(D) = (\det(\partial f_i/\partial X_j(0)))$ が分かる. 余接空間 $\wp_R/\wp_R^2$ について, $\#\wp_R/\wp_R^2 = \#(\det(\partial f_i/\partial X_j(0)))$ も容易に分かるので, $\#\wp_R/\wp_R^2 = \#\mathcal{O}/\eta_R$ が従う.

1.⇒3. まず,

$$\#\mathcal{O}/\eta_T \le \#\wp_T/\wp_T^2 \le \#\wp_R/\wp_R^2 \le \#\mathcal{O}/\eta_T < \infty$$

である (最初の不等式は式 (8), 次の不等式は $R \twoheadrightarrow T$ の全射性, 最後の不等式は仮定から分かる). よって, $\#\mathcal{O}/\eta_T = \#\wp_T/\wp_T^2$ $(*)$ と $\#\wp_T/\wp_T^2 = \#\wp_R/\wp_R^2$ $(**)$ が分かる.

$\mathcal{C}$ の全射 $\phi : \tilde{T} \twoheadrightarrow T$ で $\tilde{T}$ は局所完全交叉 $\mathcal{O}$ 代数で有限平坦 $\mathcal{O}$ 加群かつ $\phi : \wp_{\tilde{T}}/\wp_{\tilde{T}}^2 \xrightarrow{\sim} \wp_T/\wp_T^2$ であるものがとれる (全射 $U := \mathcal{O}[[X_1,\dots,X_n]] \twoheadrightarrow T$ をとり, $f_1,\dots,f_n \in \wp_U$ を $\wp_U/\wp_U^2$ での像が $\ker\{\wp_U/\wp_U^2 \twoheadrightarrow \wp_T/\wp_T^2\}$ を生成するものとし, $U/(f_1,\dots,f_n)$ が $\mathcal{O}$ 上有限生成になるように f_i を選ぶ. 例えば, m を $f_1,\dots,f_n$ の次数の最大値, $a_i := \phi(X_i)$, $a_i^2 = h_i(a_1,\dots,a_n)$ として f_i を $f_i + X_i^m h_i - X_i^{m+2}$ と置き換えれば $\mathcal{O}$ 上有限生成になる). ここで,

$$\#\mathcal{O}/\eta_T \le \#\mathcal{O}/\eta_{\tilde{T}} \le \#\wp_{\tilde{T}}/\wp_{\tilde{T}}^2 = \#\wp_T/\wp_T^2 = \#\mathcal{O}/\eta_T < \infty$$

が成立 (最初の不等式は $\tilde{T} \twoheadrightarrow T$ の全射性, 次の不等式は式 (8), 3 番目の等式は同型 $\wp_{\tilde{T}}/\wp_{\tilde{T}}^2 \xrightarrow{\sim} \wp_T/\wp_T^2$, 最後の等式は上の $(*)$ から分かる). よって, $\#\mathcal{O}/\eta_T = \#\mathcal{O}/\eta_{\tilde{T}}$ が分かる. $\tilde{T}$ が局所完全交叉 $\mathcal{O}$ 代数であることを使うと補題 4.1 の 2. から, $\tilde{T} \xrightarrow{\sim} T$ である. よって, T は局所完全交叉 $\mathcal{O}$ 代数. T が局所完全交叉 $\mathcal{O}$ 代数であることを使うと, $(**)$ と補題 4.1 の 1. から同型 $R \xrightarrow{\sim} T$ が従う. □

次に, Wiles の数値的判定法を用いて, Diamond-藤原の数値的判定法を示す (後者を使う理由は, 法 p での q 展開原理と重複度 1 の議論をしなくてすむようになるからである).

定理 4.3 (Diamond-藤原の数値的判定法) $R \twoheadrightarrow T$ を $\mathcal{C}$ の全射で $H \neq 0$ を忠実 T 加群で $\mathcal{O}$ 上有限生成平坦とする (よって T も有限生成平坦 $\mathcal{O}$ 加群). $\wp_R$ は H の台 (support) に入ると仮定する. $d := \mathrm{rank}_{\mathcal{O}} H[\wp_T]$, $\Omega_H := H/(H[\wp_T] + H[\mathrm{Ann}_T\wp_T])$ とおく. $\mathrm{length}_{\mathcal{O}}\Omega_H < \infty$ を仮定する. この時次は同値.

1. $\mathrm{rank}_{\mathcal{O}} H \le d \cdot \mathrm{rank}_{\mathcal{O}} T$ かつ $d \cdot \mathrm{length}_{\mathcal{O}} \wp_R/\wp_R^2 \le \mathrm{length}_{\mathcal{O}}\Omega_H$,
2. $\mathrm{rank}_{\mathcal{O}} H = d \cdot \mathrm{rank}_{\mathcal{O}} T$ かつ $(\mathcal{O}/\mathrm{Fitt}_{\mathcal{O}}(\wp_R/\wp_R^2))^d \cong \Omega_H$,
3. $R \twoheadrightarrow T$ は同型, R, T は局所完全交叉 $\mathcal{O}$ 代数で, H は階数 d の自由 T 加群. □

証明 2.⇒1. は自明.

3.⇒2. 定理 4.2 より, 包含関係 (7) は等式と分かるのでそれから従う.

1.⇒3. $I_T := \mathrm{Ann}_{\mathcal{O}}\wp_T$ とおく. $x \in \Omega_H$, $a \in \eta_T$, $a' \in I_T$ を $\pi_T(a') = a$ となるものとすると, $ax = (a-a')x = 0$ である (最初の等式は $a' \in I_T$ と $H/H[\wp] \twoheadrightarrow \Omega_H$ と $I_T H \subset H[\wp_T]$, 次の等式は $a - a' \in \wp_T$ と $H/H[I_T] \twoheadrightarrow \Omega_H$ と $\wp_T H \subset H[I_T]$ から分かる). 従って, $\eta_T \subset \mathrm{Ann}_{\mathcal{O}}\Omega_H$ が分かる. 包含関係 (7) とあわせると

$$\mathrm{Fitt}_{\mathcal{O}}(\wp_T/\wp_T^2) \subset \eta_H \subset \mathrm{Ann}_{\mathcal{O}}\Omega_H \tag{9}$$

である. ここで $H/H[I_T] \cong I_T H \subset H[\wp_T]$ より $H/H[I_T]$ は階数 d 以下の平坦 $\mathcal{O}$ 加群. $d' := \mathrm{rank}_{\mathcal{O}} H/H[I_T]$ とすると, Ω_H は $\mathcal{O}$ 加群として d' 個の元で生成されるので, 包含関係 (9) より

$$\mathrm{length}_{\mathcal{O}}\Omega_H \le d' \cdot \mathrm{length}_{\mathcal{O}}(\wp_T/\wp_T^2) \le d \cdot \mathrm{length}_{\mathcal{O}}(\wp_T/\wp_T^2)$$

が分かる. 仮定 $d \cdot \mathrm{length}_{\mathcal{O}}(\wp_T/\wp_T^2) \le \mathrm{length}_{\mathcal{O}}\Omega_H$ とあわせると包含関係 (9) はすべて等号であり, $d' = d$ であることが分かる. $\mathrm{Fitt}_{\mathcal{O}}(\wp_T/\wp_T^2) = \eta_H$ より定理 4.2 を使うと, $R \xrightarrow{\sim} T$ であり, R, T は局所完全交叉 $\mathcal{O}$ 代数と分かる.

H が自由 T 加群であることと $\mathrm{rank}_{\mathcal{O}} H = d \cdot \mathrm{rank}_{\mathcal{O}} T$ を示す. 短完全系列 $0 \to (H[\wp_T] + H[I_T])/H[I_T] \to H/H[I_T] \to \Omega_H \to 0$ と $\mathrm{length}_{\mathcal{O}}\Omega_H < \infty$, $\mathrm{rank}_{\mathcal{O}} H/H[I_T] = d$ より, $(H[\wp_T] + H[I_T])/H[I_T]$ は階数 d の平坦 $\mathcal{O}$ 加群と分かるが, $H[\wp_T] \twoheadrightarrow H[\wp_T]/(H[\wp_T] \cap H[I_T]) \cong (H[\wp_T] + H[I_T])/H[I_T]$ と $H[\wp_T]$ が階数 d の平坦 $\mathcal{O}$ 加群であることから $H[\wp_T] \cap H[I_T] = 0$ となる. よって, $\Omega_H = H/(H[\wp_T] \oplus H[I_T]) \cong (\mathcal{O}/\eta_T)^d$ が従う.

$\Omega'_H := H/(H[I_T] + I_T H)$ とおく. $I_T H \subset H[\wp_T]$ より $\Omega'_H \twoheadrightarrow \Omega_H$ であるが $H/H[I_T] \twoheadrightarrow \Omega'_H$ より Ω'_H は $\mathcal{O}$ 上 d 個の元で生成される. また, $\eta_T \Omega'_H = 0$ が以前と同じ議論で示される ($x \in \Omega'_H$, $a \in \eta$, $a' \in I_T$, $\pi_T(a') = a$ として, $a' \in I_T$ より $a'x = 0$ であり, $a - a' \in \wp_T$, $\wp_T H \subset H[I_T]$ より $(a-a')x = 0$ である). よって Ω'_H も Ω_H と同様に, $\mathcal{O}$ 上 d 個の元で生成されかつ η_T で消えるということから全射 $\Omega'_H \twoheadrightarrow \Omega_H$ は同型と分かる. よって, $I_T \subset H[\wp_T]$ は等号で $I_T H$ は $\mathcal{O}$ 上階数 d で, $H/I_T H (= H/H[\wp_T] \cong \wp_T H \subset H)$ は平坦 $\mathcal{O}$ 加群と分かる.

$\otimes_{\mathcal{O}}\mathbb{F}$ を $\overline{(-)}$ であらわすことにする. $\mathfrak{m}_T$ を T の極大イデアルとすると $\overline{T}$ は Gorenstein $\mathbb{F}$ 代数であることから $\overline{T}[\mathfrak{m}_T] = I_T\overline{T}$ は 1 次元 $\mathbb{F}$ ベクトル空間. $H/I_T H$ は平坦 $\mathcal{O}$ 加群なので $I_T\overline{H}$ は d 次元 $\mathbb{F}$ ベクトル空間. $x_1, \ldots, x_d \in \overline{H}$ を $I_T\overline{H} = \oplus I x_i$ となるようにとる. $\alpha : \overline{T}^{\oplus d} \to \overline{H}$, $((r_1, \ldots, r_d) \mapsto \sum r_i x_i)$ の核を V とすると, $V \cap I_T\overline{T}^{\oplus d} = 0$ より $V[\mathfrak{m}_T] = 0$ なので, $V = 0$ となり α は単射. $\mathrm{rank}_{\mathcal{O}} H \le d \cdot \mathrm{rank}_{\mathcal{O}} T$ なので, 次元を比べると α は同型かつ $\mathrm{rank}_{\mathcal{O}} H = d \cdot \mathrm{rank}_{\mathcal{O}} T$. よって H は階数 d の自由 T 加群. □

さて, この数値的判定法を用いるために, 次節で R の増分を, 次々節で H の増分を計算する.

4.2 Galois 側の増分.

本節では R の増分を計算する. この章では以下 $p > 2$ を仮定する.

$\rho : G \to \mathrm{GL}_d(\mathcal{O})$ を $\bar{\rho}$ の D 型 (2.1 節参照) の変形とし，$\theta : R_D \to \mathcal{O}$ を $\rho = \theta \circ \rho_{R_D}$, $\wp := \ker\theta$ とする．$H^1_D(G, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) := \varinjlim_n H^1_D(G, \mathrm{ad}^0\rho \otimes \lambda^{-n}/\mathcal{O})$ とおく (2.1 節では $\mathrm{ad}\bar{\rho}$ や $\mathrm{ad}^0\bar{\rho}$ 係数だけでなく $\mathrm{ad}\rho$ や $\mathrm{ad}^0\rho$ 係数に対しても H^1_D を定義していた) と，補題 2.2 と同様に以下が成立する．

補題 4.4 $\mathcal{O}$ 加群の標準的な同型

$$H^1_D(G, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) \cong \mathrm{Hom}_{\mathcal{O}}(\wp/\wp^2, E/\mathcal{O})$$

が存在する．□

$\bar{\rho}$ を 2.2 節の条件を満たす法 p 表現とする．Σ を 3.2 節の仮定 (Σ) を満たす素数の有限集合とする．$\bar{\rho}$ の Σ 型の変形 $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$ に対して，

$$H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) := \varinjlim_n H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho \otimes \lambda^{-n}/\mathcal{O})$$

で定義する．**有限性** $\# H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) < \infty$ **はまだ分からない**ことに注意．同様に，

$$H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho \otimes E/\mathcal{O}) := \varinjlim_n H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho \otimes \lambda^{-n}/\mathcal{O}),$$

$$H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) := H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) \cap H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}\rho \otimes E/\mathcal{O}),$$
$$H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}\rho \otimes E/\mathcal{O}) := \varinjlim_n H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}\rho \otimes \lambda^{-n}/\mathcal{O}),$$
$$H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) := H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho \otimes E/\mathcal{O}) \cap H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}\rho \otimes E/\mathcal{O})$$

と定義する (2.2 節では $\bar{\rho}$ だけでなく ρ に対しても H^1_Σ や H^1_{f} などを定義していた)．ρ が p で平坦でないか，あるいは通常でない時には定義から $H^1_{\mathrm{st}} = H^1_{\mathrm{f}}$ である．

定義 4.1 1. $\bar{\rho}$ が不分岐である素数 $\ell \notin \Sigma$, $\ell \neq p$ に対して

$$c_\ell := (\ell - 1)((\mathrm{Tr}\rho(\mathrm{Fr}_\ell))^2 - (\ell + 1)^2) \in \mathcal{O}$$

と定義する (ρ は Σ 型の変形なので ℓ で不分岐であることに注意)．

2. $\bar{\rho}$ が p で平坦かつ通常で, $p \notin \Sigma$ の時, $\rho|_{D_p} \sim \begin{pmatrix} \varepsilon\chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ として，

$$c_p := (\chi_2/\chi_1)(\mathrm{Fr}_p) - 1 \in \mathcal{O}$$

と定義する (ρ は Σ 型の変形なので p で平坦かつ通常であることに注意)．□

命題 4.5 次が成立．

1. $\bar\rho$が不分岐である素数$\ell \notin \Sigma$, $\ell \neq p$に対して,

$$\#H^1(\mathbb{Q}_\ell, \mathrm{ad}^0\rho \otimes_{\mathcal{O}} E/\mathcal{O})/H^1(\mathbb{F}_\ell, (\mathrm{ad}^0\rho \otimes_{\mathcal{O}} E/\mathcal{O})^{I_\ell}) = \#\mathcal{O}/(c_\ell),$$

2. $\bar\rho$がpで平坦かつ通常で, $p \notin \Sigma$の時,

$$\#H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}^0\rho \otimes_{\mathcal{O}} E/\mathcal{O})/H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}^0\rho \otimes_{\mathcal{O}} E/\mathcal{O}) \leq \#\mathcal{O}/(c_p).\square$$

証明 $\rho_n := \rho \otimes \lambda^{-n}/\mathcal{O}$とおく.

1.$\#H^1(\mathbb{Q}_\ell, \mathrm{ad}^0\rho_n)/H^1(\mathbb{F}_\ell, (\mathrm{ad}^0\rho_n)^{I_\ell}) = \#H^1(\mathbb{Q}_\ell, \mathrm{ad}^0\rho_n)/H^0(\mathbb{Q}_\ell, \mathrm{ad}^0\rho_n)$であり, 局所的Euler指標公式と局所Tate双対性を使うとこれは$\#H^0(\mathbb{Q}_\ell, \mathrm{ad}^0\rho_n(1)) = \#\mathcal{O}/(c_\ell, \lambda^n)$と一致することから主張が従う($\alpha$, βを$\rho(\mathrm{Fr}_\ell)$の固有値として, $(\ell-1)(\ell\alpha/\beta-1)(\ell\beta/\alpha-1) = (\ell-1)(\ell^2-(\alpha^2+\beta^2)+1) = (\ell-1)(\ell^2-a_\ell(f)+2\ell+1) = (\ell-1)(-a_\ell(f)+(\ell+1^2))$.

2.を示す. $\mathrm{Fil}^1 \subset \rho$を$\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$で安定な1次元の部分空間とし, $F \subset \mathrm{ad}^0\bar\rho$を$F := \{g \in \mathrm{ad}^0\bar\rho \mid g(\mathrm{Fil}^1) = 0\}$, Fは$\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$で安定な$\varepsilon\chi_1/\chi_2$で作用する1次元の部分空間である. $F_n := F \otimes \lambda^{-n}/\mathcal{O}$とする. $u : H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho_n) \to H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho_n/F_n)$を$\mathrm{ad}^0\rho \to \mathrm{ad}^0\rho/F$が誘導する射,

$$\delta : H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho_n) \to H^1(I_p, \mathrm{ad}^0\rho_n/F_n)$$

をuと制限射$H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho_n/F_n) \to H^1(I_p, \mathrm{ad}^0\rho_n/F_n)$の合成とする. 定義から

$$H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}^0\rho_n) = \ker\{\delta : H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho_n) \to H^1(I_p, \mathrm{ad}^0\rho_n/F_n)\}$$

である. $h^i(-) := \#H^i(\mathbb{Q}_p, -)$とおく. 下の図式(横の射は完全系列をなす)

$$\begin{tikzcd}
 & & H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho_n) \arrow[d, "u"] \arrow[dr, "\delta"] & \\
0 \arrow[r] & H^1(\mathbb{F}_p, (\mathrm{ad}^0\rho_n/F_n)^{I_p}) \arrow[r] & H^1(\mathbb{Q}_p, \mathrm{ad}^0\rho_n/F_n) \arrow[r] & H^1(I_p, \mathrm{ad}^0\rho_n/F_n)
\end{tikzcd}$$

から

$$\#\mathrm{Im}\delta \geq \frac{\#\mathrm{Im}u}{\#H^1(\mathbb{F}_p, (\mathrm{ad}^0\rho_n/F_n)^{I_p})} = \frac{\#\mathrm{Im}u}{h^0(\mathrm{ad}^0\rho_n/F_n)} \tag{10}$$

が分かる. 短完全系列$0 \to F \to \mathrm{ad}^0\rho \to \mathrm{ad}^0\rho/F \to 0$が誘導する長完全系列から

$$\#\mathrm{Im}u = \frac{h^1(\mathrm{ad}^0\rho_n/F_n)h^2(\mathrm{ad}^0\rho_n)}{h^2(F)h^2(\mathrm{ad}^0\rho_n/F_n)} \tag{11}$$

が分かる. 命題2.5から

$$\frac{\#H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}^0\rho_n)}{\#H^1_{\mathrm{f}}(\mathbb{Q}_p, \mathrm{ad}^0\rho_n)} = \frac{\#H^1_{\mathrm{st}}(\mathbb{Q}_p, \mathrm{ad}^0\rho_n)}{h^0(\mathrm{ad}^0\rho_n)\#\mathcal{O}/\lambda^n}$$

であり, 式 (10) と式 (11) から

$$\frac{\#H^1_{\mathrm{st}}(\mathbb{Q}_p,\mathrm{ad}^0\rho_n)}{h^0(\mathrm{ad}^0\rho_n)\#\mathcal{O}/\lambda^n}=\frac{h^1(\mathrm{ad}^0\rho_n)}{\#\mathrm{Im}\delta\cdot h^0(\mathrm{ad}^0\rho_n)\#\mathcal{O}/\lambda^n}\le\frac{h^1(\mathrm{ad}^0\rho_n)h^0(\mathrm{ad}^0\rho_n/F_n)}{\#\mathrm{Im}u\cdot h^0(\mathrm{ad}^0\rho_n)\#\mathcal{O}/\lambda^n}$$

$$=\frac{h^2(F_n)h^2(\mathrm{ad}^0\rho_n/F_n)h^1(\mathrm{ad}^0\rho_n)h^0(\mathrm{ad}^0\rho_n/F_n)}{h^1(\mathrm{ad}^0\rho_n/F_n)h^2(\mathrm{ad}^0\rho_n)h^0(\mathrm{ad}^0\rho_n)\#\mathcal{O}/\lambda^n}$$

である. 局所的 Euler 指標公式より, これは

$$\#(\mathcal{O}/\lambda^n)^{4-3-1}\cdot h^2(F_n)=h^0(F_n^\vee(1))=\#\mathcal{O}/(c_p,\lambda^n)$$

と等しい. □

$\bar\rho$ が不分岐で $\ell\notin\Sigma$, $\ell\neq p$ である素数 ℓ に対して

$$H^1_\ell:=H^1(\mathbb{Q}_\ell,\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O})/H^1(\mathbb{F}_\ell,\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O}),$$

$\bar\rho$ が p で平坦かつ通常で $p\notin\Sigma$ の時

$$H^1_p:=H^1_{\mathrm{st}}(\mathbb{Q}_p,\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O})/H^1_{\mathrm{f}}(\mathbb{Q}_p,\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O})$$

とおく.

系 4.6 $\Sigma'\supset\Sigma$ をともに条件 (Σ) を満たす素数の有限集合とすると,

$$\#H^1_{\Sigma'}(\mathbb{Q},\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O})/H^1_{\Sigma}(\mathbb{Q},\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O})\le\#\mathcal{O}/(\prod_{\ell\in\Sigma'\setminus\Sigma}c_\ell)$$

が成立. もし等号が成立するなら,

$$0\to H^1_{\Sigma}(\mathbb{Q},\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O})\to H^1_{\Sigma'}(\mathbb{Q},\mathrm{ad}^0\rho\otimes_{\mathcal{O}}E/\mathcal{O})\to\oplus_{\ell\in\Sigma'\setminus\Sigma}H^1_\ell\to 0$$

は完全系列. □

次節で $f\in\mathcal{N}_\Sigma$ に対する ρ_f で等号が常に成立することが分かる. 補題 4.4 から次が分かる.

系 4.7 $\Sigma'\supset\Sigma$ をともに条件 (Σ) を満たす素数の有限集合とする. $\wp_{\Sigma'}$, $\wp_\Sigma$ をそれぞれ $R_{\Sigma'}$, R_Σ の普遍性からくる射 $R_{\Sigma'}\to\mathcal{O}$, $R_\Sigma\to\mathcal{O}$ の核とすると,

$$\#(\wp_{\Sigma'}/\wp_{\Sigma'}^2)/(\wp_\Sigma/\wp_\Sigma^2)\le\#\mathcal{O}/(\prod_{\ell\in\Sigma'\setminus\Sigma}c_\ell)$$

が成立. □

4.3 保型側の増分.

本節では H の増分を計算する.

Σ を 3.2 節の仮定 (Σ) を満たす素数の有限集合とする. $f \in \mathcal{N}_\Sigma$ をとり ($\mathcal{N}_\Sigma$ の定義は 3.2 節参照), $\pi_f : \mathbb{T}_\Sigma \twoheadrightarrow \mathcal{O}$ を f に対応する射, $\wp_{\mathbb{T}_\Sigma}$ をその核, $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$ を f に付随した Galois 表現とする. $(\mathbb{T}_\Sigma, \pi_f)$ に対してその合同イデアルを η_Σ とおく. $\mathbb{T}_\Sigma$ **は被約なので** $\eta_\Sigma \neq 0$ **である**ことに注意.

$$H_\Sigma := H^1(X_0(N_\Sigma), \mathcal{O})_{\mathfrak{m}_\Sigma},\ \Omega_\Sigma := \Omega_{H_\Sigma}$$

とおく (3.3 節と違って今回 Hecke 加群 H_Σ は負部分 $(\cdot)^-$ をとらない). H_Σ は自由 $\mathcal{O}$ 加群であり, $H_\Sigma[\wp_{\mathbb{T}_\Sigma}]$ は階数 2 の自由 $\mathcal{O}$ 加群である. Hecke 加群 H_Σ にはカップ積により自然にペアリング $H_\Sigma \otimes H_\Sigma \to \mathcal{O}$ が定まる. w_Σ を Atkin-Lehner 対合 $(z \mapsto -\frac{1}{N_\Sigma z})$ が誘導する射とすると合成 $H_\Sigma \xrightarrow{w_\Sigma} H_\Sigma \xrightarrow{\sim} \mathrm{Hom}_{\mathcal{O}}(H_\Sigma, \mathcal{O})$ は $\mathbb{T}_\Sigma$ 加群の構造と整合的である. 今後はこの $\mathbb{T}_\Sigma$ 加群の構造と整合的な射でペアリング $\langle \cdot, \cdot \rangle_\Sigma$ を考えることにする.

余接空間 $\wp_\Sigma/\wp_\Sigma^2$ は Selmer 群を使って計算されたが, $\mathrm{length}_{\mathcal{O}} \Omega_\Sigma$ (あるいは合同イデアル η_Σ) は Hecke 加群の $\mathbb{T}_\Sigma$ 整合的ペアリングで計算される.

補題 4.8 $\{x, y\}$ を $H_\Sigma[\wp_{\mathbb{T}_\Sigma}]$ の $\mathcal{O}$ 上の基底, v_λ を $\mathcal{O}$ の付値とすると,

$$\mathrm{length}_{\mathcal{O}} \Omega_\Sigma = 2 v_\lambda(\langle x, y \rangle_\Sigma)$$

が成立. □

注意 4.8.1 H_Σ が $\mathbb{T}_\Sigma$ 上自由な時, $\Omega_\Sigma \cong (\mathcal{O}/\eta_\Sigma)^{\oplus 2}$ となることから

$$\eta_\Sigma^2 = (\langle x, y \rangle_\Sigma)$$

も分かる. Diamond-藤原の改良以前は法 p での q 展開原理と重複度 1 の議論を用いて H_Σ が $\mathbb{T}_\Sigma$ 上自由であることを前もって証明する必要があったが, 改良以降は数値的判定法 (定理 4.3) から可換環論的に H_Σ が $\mathbb{T}_\Sigma$ 上自由であることが導出できるようになった. □

証明 $H_\Sigma / H_\Sigma[\mathrm{Ann}_{\mathbb{T}_\Sigma} \wp_{\mathbb{T}_\Sigma}] \cong \mathrm{Hom}_{\mathcal{O}}(H_\Sigma[\wp_{\mathbb{T}_\Sigma}], \mathcal{O})$ より Ω_Σ はペアリング $\langle \cdot, \cdot \rangle_\Sigma$ から誘導される射 $H_\Sigma[\wp_{\mathbb{T}_\Sigma}] \hookrightarrow \mathrm{Hom}_{\mathcal{O}}(H_\Sigma[\wp_{\mathbb{T}_\Sigma}], \mathcal{O})$ の余核である. この余核は

$$\mathcal{O} \Big/ \left(\det \begin{pmatrix} \langle x, x \rangle_\Sigma & \langle x, y \rangle_\Sigma \\ \langle y, x \rangle_\Sigma & \langle y, y \rangle_\Sigma \end{pmatrix} \right)$$

と同型であるので, ペアリング $\langle \cdot, \cdot \rangle_\Sigma$ の歪対称性から主張が従う. □

素数 ℓ を $\ell \neq p$, $\ell \notin \Sigma$ かつ $\bar{\rho}$ は ℓ で不分岐な素数か, あるいは $\ell = p$, $p \notin \Sigma$ かつ $\bar{\rho}$ は p で平坦かつ通常とする. $\Sigma' := \Sigma \cup \{p\}$ も条件 (Σ) を満たす.

さて, $H_{\Sigma'}$ と H_Σ を比べる. $\ell \neq p$ の時と $\ell = p$ の時と別々に射 $H_{\Sigma'} \to H_\Sigma$ を以下で定義する.

$\ell \neq p$ **の場合.** 射 $\alpha', \beta', \gamma' : X_0(N_{\Sigma'}) \to X_0(N_\Sigma)$ をそれぞれ $\tau \mapsto \tau$, $\tau \mapsto \ell\tau$, $\tau \mapsto \ell^2\tau$ が誘導する射とする. $a : H^1(X_0(N_{\Sigma'}), \mathcal{O}) \to H^1(X_0(N_\Sigma), \mathcal{O})^{\oplus 3}$ を $x \mapsto (\alpha'_* x, \beta'_* x, \gamma'_* x)$ で定義する. $b : H_\Sigma^{\oplus 3} \twoheadrightarrow H_\Sigma$ を行列

$$\begin{pmatrix} 1 & -\ell^{-1}T_\ell & \ell^{-1} \end{pmatrix}$$

が定める射とする. $f \in \mathcal{N}_\Sigma$ に対して, f をコホモロジー類と考える時は $f(z)dz$ で考えることに注意すると

$$\begin{aligned}
&(\alpha'^{,*} - \ell^{-1}\beta'^{,*}T_\ell + \ell^{-1}\gamma'^{,*})f(z)dz \\
&= f(z)dz - \beta'^{,*}(\ell^{-1}\sum_{\ell|n} a_n(f)q^{n/\ell}dz + \ell\langle\ell\rangle f(\ell z)dz) + \ell^{-1}f(\ell^2 z)d(\ell^2 z) \\
&= f(z)dz - (\sum_{\ell|n} a_n(f)q^n + \ell f(\ell^2 z))dz + \ell f(\ell^2 z)dz = \sum_{\ell\nmid n} a_n(f)q^n dz
\end{aligned}$$

であり, これは $\mathfrak{m}_{\Sigma'}$ に対応する Hecke 固有形式である (3.2 節で $\mathfrak{m}_{\Sigma'}$ を定める時, $a_\ell(f_1) = 0$ であったこと事を思い出せ). 従って, 合成

$$H^1(X_0(N_{\Sigma'}), \mathcal{O}) \xrightarrow{a} H^1(X_0(N_\Sigma), \mathcal{O})^{\oplus 3} \twoheadrightarrow H_\Sigma^{\oplus 3} \overset{b}{\twoheadrightarrow} H_\Sigma$$

は $H_{\Sigma'}$ を経由する. $\mathbb{T}_{\Sigma'} \cong \mathbb{T}_\Sigma[X]/(X(X^2 - T_\ell X + \ell)) \twoheadrightarrow \mathbb{T}_\Sigma[X]/(X) \cong \mathbb{T}_\Sigma$ を使って H_Σ を $\mathbb{T}_{\Sigma'}$ 加群とみた時, この射 $\phi : H_{\Sigma'} \to H_\Sigma$ は $\mathbb{T}_{\Sigma'}$ 加群の射である (3.2 節で $\mathfrak{m}_{\Sigma'}$ を定める時, $a_\ell(f_1) = 0$ であったので $\mathbb{T}_\Sigma[X]/(X)$ を経由するのが正しい作用であることに注意).

$\ell = p$ **の場合.** 射 $\alpha, \beta : X_0(N_{\Sigma'}) \to X_0(N_\Sigma)$ をそれぞれ $\tau \mapsto \tau$, $\tau \mapsto \ell\tau$ が誘導する射とする. $a : H^1(X_0(N_{\Sigma'}), \mathcal{O}) \to H^1(X_0(N_\Sigma), \mathcal{O})^{\oplus 2}$ を $x \mapsto (\alpha_* x, \beta_* x)$ で定義する. $\alpha_p \in \mathbb{T}_\Sigma$ を $X^2 - T_p X + p = 0$ の単元根とする (すべての $f \in \mathcal{N}_\Sigma$ に対して $X^2 - a_p(f)X + p = 0$ の単元根 $\alpha_p(f)$ が E に入るように E を十分大きくとってあるので, $\alpha_p \in \mathbb{T}_\Sigma$ である). $b : H_\Sigma^{\oplus 2} \twoheadrightarrow H_\Sigma$ を行列

$$\begin{pmatrix} 1 & -\alpha_p^{-1} \end{pmatrix}$$

が定める射とする. $a_{p^n}(f) = a_p(f)a_{p^{n-1}}(f) - pa_{p^{n-2}}(f)$ と $a_p(f) = \alpha_p(f) + p\alpha_p(f)^{-1}$ から $a_{p^n}(f) - p\alpha_p(f)^{-1}a_{p^{n-1}}(f) = \alpha_p(f)a_{p^{n-1}}(f) - pa_{p^{n-2}}(f) = \alpha_p(f)(a_{p^{n-1}}(f) - p\alpha_p(f)^{-1}a_{p^{n-2}}(f)) = \cdots = \alpha_p(f)^n$ が分かるので

$$\begin{aligned}
&(\alpha^* - \alpha_p^{-1}\beta^*)f(z)dz = f(z)dz - p\alpha_p(f)^{-1}f(pz)dz \\
&= \sum_{p\nmid n} a_n(f)q^n dz + \sum_{n=pm, m>0} \alpha_p(f)^m q^{pm} dz
\end{aligned}$$

であり, これは $\mathfrak{m}_{\Sigma'}$ に対応する Hecke 固有形式である (3.2 節で $\mathfrak{m}_{\Sigma'}$ を定める時, $a_p(f_1) = \alpha_p(f)$ であったこと事を思い出せ). 従って, 合成

$$H^1(X_0(N_{\Sigma'}), \mathcal{O}) \xrightarrow{a} H^1(X_0(N_\Sigma), \mathcal{O})^{\oplus 2} \twoheadrightarrow H_\Sigma^{\oplus 2} \overset{b}{\twoheadrightarrow} H_\Sigma$$

は $H_{\Sigma'}$ を経由する．$\mathbb{T}_{\Sigma'} \cong \mathbb{T}_{\Sigma}[X]/(X(X^2 - T_pX + p)) \twoheadrightarrow \mathbb{T}_{\Sigma}[X]/(X - \alpha_p) \cong \mathbb{T}_{\Sigma}$ を使って H_{Σ} を $\mathbb{T}_{\Sigma'}$ 加群とみた時, この射 $\phi : H_{\Sigma'} \to H_{\Sigma}$ は $\mathbb{T}_{\Sigma'}$ 加群の射である (3.2 節で $\mathfrak{m}_{\Sigma'}$ を定める時, $a_p(f_1) = \alpha_p(f)$ であったので $\mathbb{T}_{\Sigma}[X]/(X - \alpha_p)$ を経由するのが正しい作用であることに注意).

さて, $\ell \neq p$ または $\ell = p$ の状況に戻る．$\Gamma_1(N) \cap \Gamma_0(M)$ に関するモジュラー曲線を $X_1(N, M)$ とおく．

命題 4.9 (伊原の補題と Wiles によるその一般化, [I], [R3, Theorem 4.1, Corollary 4.2], [W1, Lemma 2.5]) $\ell \nmid N$ とする．

1. $x \mapsto (\alpha_* x, \beta_* x)$ により定まる射

$$H_1(X_1(N, \ell), \mathbb{Z}) \to H_1(X_1(N), \mathbb{Z})^{\oplus 2}$$

は全射,

2. $N > 3$, $\ell \neq p$ として, $x \mapsto (\alpha_* x, \beta_* x)$ と $(y, z) \mapsto \beta_* y - \alpha_* x$ により定まる図式

$$H_1(Y_1(N\ell, \ell^2), \mathbb{Z}_p) \to H_1(Y_1(N\ell), \mathbb{Z}_p)^{\oplus 2} \to H_1(Y_1(N), \mathbb{Z}_p)$$

は完全．□

1. は $\mathbb{Z}$ 係数で 2. は $\mathbb{Z}_p$ 係数 ($p \neq \ell$) であることに注意．特に, $p = \ell$ では上の 2. に相当する "増分" の計算は同様にはできない．これは Galois 側で Galois コホモロジーの計算が $p = \ell$ の時は複雑になるのと対応している．

証明 1. $N \leq 3$ の時 $X_1(N)$ の種数は 0 なので $N > 3$ と仮定してよい．$N > 3$ より $\Gamma_1(N)$ は自由に上半平面に作用するので, $Y_1(N, \ell)$ と $Y_1(N)$ のホモロジーは群のホモロジーで表される．$X_1(N)$ のホモロジーは $\Gamma_1(N)$ のホモロジーを放物元からくる 1 境界で割った群になる．$\gamma_\ell := \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ として $\Gamma^0(\ell) := \gamma_\ell \Gamma_0(\ell) \gamma_\ell^{-1} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, b \equiv 0 \mod \ell \right\}$, $\Gamma_1(N)^{\gamma_\ell} := \gamma_\ell^{-1} \Gamma_1(N) \gamma_\ell$ とおく．$\beta : \tau \mapsto \ell\tau$ から誘導される射は, 群のホモロジーでは γ_ℓ での共役 $\Gamma_1(N) \cap \Gamma_0(\ell) = \gamma_\ell^{-1}(\Gamma_1(N) \cap \Gamma^0(\ell))\gamma_\ell$ が誘導する同型と $\gamma_\ell^{-1}(\Gamma_1(N) \cap \Gamma^0(\ell))\gamma_\ell$ から $\Gamma_1(N)^{\gamma_\ell}$ への埋め込みが誘導する射の合成になる．よって,

$$H_1(\Gamma_1(N) \cap \Gamma_0(\ell), \mathbb{Z}) \to H_1(\Gamma_1(N), \mathbb{Z})/P(\Gamma_1(N)) \oplus H_1(\Gamma_1(N)^{\gamma_\ell}, \mathbb{Z})/P(\Gamma_1(N)^{\gamma_\ell}) \qquad (12)$$

の全射性を示せば十分．ここで $P(G)$ は G の放物元からくる 1 境界のなす部分群．$\Gamma := \langle \Gamma_1(N), \Gamma_1(N)^{\gamma_\ell} \rangle \subset \mathrm{SL}_2(\mathbb{Q})$ とすると, [Se3, Ch. II, §1.4] より $\Gamma \cong \Gamma_1(N) *_{\Gamma_1(N) \cap \Gamma_0(\ell)} \Gamma_1(N)^{\gamma_\ell}$ (アマルガム和) となる (Γ は $\mathrm{SL}_2(\mathbb{Z}[1/\ell])$ での $\Gamma_1(N)$ の類似物)．よって,

$$H_1(\Gamma_1(N) \cap \Gamma_0(\ell), \mathbb{Z}) \to H_1(\Gamma_1(N), \mathbb{Z}) \oplus H_1(\Gamma_1(N)^{\gamma_\ell}, \mathbb{Z})$$

の余核は $H_1(\Gamma,\mathbb{Z})$ と同型 (Lyndon の完全系列).

$$\Delta := \langle[\Gamma,\Gamma], P'(\Gamma_1(N)), P'(\Gamma_1(N)^{\gamma_\ell})\rangle \subset \Gamma$$

とおく ($[,]$ は交換子群, $P'(\cdot)$ は放物元のなす部分群) と, 射 (12) の余核は Γ/Δ と同型になる. Γ は放物元で正規的に (normally) 生成されている ([Me], [Se4] 参照) ので, $P'(\Gamma) \subset \Delta$ を示せば十分. $\gamma \in \Gamma$ を放物元とすると, ある正の整数 n に対して $\gamma = 1 + \ell^{-n}A$ となる. ここで A は整数係数の行列で, $A^2 = 0$ を満たすもの. よって, $\gamma^{\ell^n} = 1 + A \in \Gamma_1(N)$ となる ([I, p.178]). これより γ^{ℓ^n} は $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ の整数冪と共役なので, γ は $\begin{pmatrix}1&b\\0&1\end{pmatrix}$ $(b \in \frac{1}{\ell}\mathbb{Z})$ と共役と分かる. 一方, $\begin{pmatrix}1&b\\0&1\end{pmatrix}$ の ℓ^2 冪は $\begin{pmatrix}1&b\\0&1\end{pmatrix}$ と $\left(\begin{pmatrix}\ell^{-1}&0\\0&\ell\end{pmatrix}\text{で}\right)$ 共役なので, γ は $\gamma^{\ell^{2n}}$ と共役. よって, $\gamma \equiv \gamma^{\ell^{2n}} \mod [\Gamma,\Gamma]$ と $\gamma^{\ell^{2n}} \in \Gamma_1(N) \cap P'(\Gamma) = P'(\Gamma_1(N))$ より $\gamma \in \Delta$ が従う.

2. を示す. $N > 3$ なので $\Gamma_1(N)$ は上半平面に自由に作用するので, $Y_1(N)$, $Y_1(N\ell)$, $Y_1(N\ell,\ell^2)$ のコホモロジーは群のコホモロジーで表される.

$$\Gamma^1(\ell) := \left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} \middle| a \equiv d \equiv 1, b \equiv 0 \mod \ell\right\},$$

$\Gamma^1(N\ell) := \Gamma_1(N) \cap \Gamma^1(\ell)$ とおく. $\beta : \tau \mapsto \ell\tau$ から誘導される射は, 群のコホモロジーでは γ_ℓ で共役をとった $\gamma_\ell\Gamma_1(N\ell)\gamma_\ell^{-1} = \Gamma^1(N\ell)$ や $\gamma_\ell(\Gamma_1(N\ell)\cap\Gamma_0(\ell^2))\gamma_\ell^{-1} = \Gamma_1(N\ell)\cap\Gamma(\ell)$ への制限射になる. よって, Pontrjagin 双対をとって

$$\begin{aligned} H^1(\Gamma_1(N),\mathbb{Q}_p/\mathbb{Z}_p) &\xrightarrow{\mathrm{res}_1\oplus-\mathrm{res}^1} H^1(\Gamma_1(N\ell),\mathbb{Q}_p/\mathbb{Z}_p)\oplus H^1(\Gamma^1(N\ell),\mathbb{Q}_p/\mathbb{Z}_p) \\ &\xrightarrow{\lambda_1\oplus\lambda^1} H^1(\Gamma_1(N\ell)\cap\Gamma(\ell),\mathbb{Q}_p/\mathbb{Z}_p) \end{aligned}$$

が完全であることを示せば十分.

$B_1 := \Gamma_1(N\ell)/\Gamma_1(N)\cap\Gamma(\ell) \cong \left\{\begin{pmatrix}1&*\\0&1\end{pmatrix}\in \mathrm{SL}_2(\mathbb{F}_\ell)\right\}$, $B^1 := \Gamma^1(N)/\Gamma_1(N)\cap\Gamma(\ell) \cong \left\{\begin{pmatrix}1&0\\ *&1\end{pmatrix}\in \mathrm{SL}_2(\mathbb{F}_\ell)\right\}$ とおく. $p \nmid \#B_1, \#B^1$ なので膨張・制限 (inflation-restriction) 完全系列から同型

$$\lambda_1 : H^1(\Gamma_1(N\ell),\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\sim} H^1(\Gamma_1(N\ell)\cap\Gamma(\ell),\mathbb{Q}_p/\mathbb{Z}_p)^{B_1},$$

$$\lambda^1 : H^1(\Gamma^1(N\ell),\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\sim} H^1(\Gamma_1(N\ell)\cap\Gamma(\ell),\mathbb{Q}_p/\mathbb{Z}_p)^{B^1},$$

$$H^1(\Gamma_1(N),\mathbb{Q}_p/\mathbb{Z}_p) \xrightarrow{\sim} H^1(\Gamma_1(N\ell)\cap\Gamma(\ell),\mathbb{Q}_p/\mathbb{Z}_p)^{\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})}$$

を得る ($\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ の p Sylow 部分群は巡回群なので, $H^2(\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}),\mathbb{Q}_p/\mathbb{Z}_p)$ を p Sylow 部分群に制限すると消えるので, $H^2(\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}),\mathbb{Q}_p/\mathbb{Z}_p) = 0$ が分かる. 上の最後の同型はこ

れから分かる). λ_1 と λ^1 の像はそれぞれ B_1 不変部分, B^1 不変部分に入っている. B_1 と B^1 は $\Gamma_1(N)/\Gamma_1(N)\cap\Gamma(\ell)\cong \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ を生成するので, $\lambda_1(x)=-\lambda^1(y)$ とすると $\lambda_1(x)$ は $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ 不変部分に入る. よって上の 3 つ目の同型より, $\lambda_1(x)$ は $H^1(\Gamma_1(N),\mathbb{Q}_p/\mathbb{Z}_p)$ の元 x' の制限になっている. よって, $x-\mathrm{res}_1(x')\in\ker\lambda_1=0$ より ($\ell\neq p$ を必要としたのは λ_1, λ^1 の単射性の部分), $y=-\mathrm{res}^1(x')$ となり主張が従う. □

系 4.10 $\ell\neq p$, $\ell=p$ どちらの時も $\phi: H_{\Sigma'}\to H_\Sigma$ は全射. □

証明 $\ell=p$ の時を示す. $H^1(X_1(N_\Sigma),\mathcal{O})\to H^1(X_0(N_\Sigma),\mathcal{O})$ の余核は Eisenstein なので, 非 Eisenstein イデアルで局所化すると全射になる. よって, 命題 4.9 の 1. から主張が従う.

$\ell\neq p$ の時を示す. $N_\Sigma\le 3$ の時 $X_0(N_\Sigma)$ の種数は 0 なので $N_\Sigma>3$ と仮定してよい. 命題 4.9 の 2. を非 Eisenstein イデアル $\mathfrak{m}$ で局所化すると

$$H^1(X_1(N_\Sigma\ell,\ell^2),\mathcal{O})_\mathfrak{m}\to H^1(X_1(N_\Sigma\ell),\mathcal{O})_\mathfrak{m}^{\oplus 2}\to H^1(X_1(N_\Sigma),\mathcal{O})_\mathfrak{m}$$

が完全だと分かる. 上に述べたことと同様に $H^1(X_1(N_\Sigma\ell,\ell^2),\mathcal{O})\to H^1(X_1(N_\Sigma,\ell^2),\mathcal{O})$ と $H^1(X_1(N_\Sigma\ell),\mathcal{O})\to H^1(X_1(N_\Sigma,\ell),\mathcal{O})$ の余核は Eisenstein なので, 非 Eisenstein イデアル $\mathfrak{m}$ で局所化するとともに全射となる. 従って,

$$H^1(X_1(N_\Sigma,\ell^2),\mathcal{O})_\mathfrak{m}\to H^1(X_1(N_\Sigma,\ell),\mathcal{O})_\mathfrak{m}^{\oplus 2}\to H^1(X_1(N_\Sigma),\mathcal{O})_\mathfrak{m}$$

は完全と分かる. 命題 4.9 の 1. を使うと, $x\mapsto(\alpha'_*x,\beta'_*x,\gamma'_*x)$ で定まる射 $H^1(X_1(N_\Sigma,\ell^2),\mathcal{O})_\mathfrak{m}\to H^1(X_1(N_\Sigma),\mathcal{O})_\mathfrak{m}^{\oplus 3}$ は全射と分かる. $\mathfrak{m}$ として $\mathfrak{m}_{\Sigma'}$ をとれば主張が従う ($X_1(N_\Sigma,\ell^2)$ などに対しては $\mathbb{T}_\mathcal{O}(\Gamma_1(N_\Sigma)\cap\Gamma_0(\ell^2))$ の極大イデアルで $\mathfrak{m}_{\Sigma'}$ の上にあるものをとる). □

$\phi^\vee: H_\Sigma\to H_{\Sigma'}$ を $\langle\cdot,\cdot\rangle_\Sigma$ と $\langle\cdot,\cdot\rangle_{\Sigma'}$ に関する ϕ の随伴として, $\phi\circ\phi^\vee$ を計算する.

$\ell\neq p$ **の場合.**

$$\phi\circ\phi^\vee: H_\Sigma \xrightarrow{\begin{pmatrix}1\\-\ell^{-1}T_\ell\\ \ell^{-1}\end{pmatrix}} H_\Sigma^{\oplus 3} \xrightarrow{w_{\Sigma'}\begin{pmatrix}\alpha'^{,*} & \beta'^{,*} & \gamma'^{,*}\end{pmatrix}w_\Sigma} H_{\Sigma'} \xrightarrow{\begin{pmatrix}\alpha'_*\\ \beta'_*\\ \gamma'_*\end{pmatrix}} H_\Sigma^{\oplus 3} \xrightarrow{\begin{pmatrix}1 & -\ell^{-1}T_\ell & \ell^{-1}\end{pmatrix}} H_\Sigma$$

であり, $\alpha' w_{\Sigma'}=w_\Sigma\gamma'$, $\beta' w_{\Sigma'}=w_\Sigma\beta'$ なので ($-1/N_{\Sigma'}z=-1/N_\Sigma(\ell^2 z)$, $-\ell/N_{\Sigma'}z=-1/N_\Sigma(\ell z)$ から分かる),

$$\begin{aligned}
&\begin{pmatrix}1 & -\ell^{-1}T_\ell & \ell^{-1}\end{pmatrix}\begin{pmatrix}\alpha'_*\\ \beta'_*\\ \gamma'_*\end{pmatrix} w_{\Sigma'}\begin{pmatrix}\alpha'^{,*} & \beta'^{,*} & \gamma'^{,*}\end{pmatrix} w_\Sigma \begin{pmatrix}1\\-\ell^{-1}T_\ell\\ \ell^{-1}\end{pmatrix}\\
&=\begin{pmatrix}1 & -\ell^{-1}T_\ell & \ell^{-1}\end{pmatrix}\begin{pmatrix}\alpha'_*\gamma'^{,*} & \alpha'_*\beta'^{,*} & \alpha'_*\alpha'^{,*}\\ \beta'_*\gamma'^{,*} & \beta'_*\beta'^{,*} & \beta'_*\alpha'^{,*}\\ \gamma'_*\gamma'^{,*} & \gamma'_*\beta'^{,*} & \gamma'_*\alpha'^{,*}\end{pmatrix}\begin{pmatrix}1\\-\ell^{-1}T_\ell\\ \ell^{-1}\end{pmatrix}
\end{aligned}$$

$$= \begin{pmatrix} 1 & -\ell^{-1}T_\ell & \ell^{-1} \end{pmatrix} \begin{pmatrix} T_\ell^2-(\ell+1) & \ell T_\ell & \ell(\ell+1) \\ \ell T_\ell & \ell(\ell+1) & \ell T_\ell \\ \ell(\ell+1) & \ell T_\ell & T_\ell^2-(\ell+1) \end{pmatrix} \begin{pmatrix} 1 \\ -\ell^{-1}T_\ell \\ \ell^{-1} \end{pmatrix}$$
$$= -\ell^{-2}(\ell-1)(T_\ell^2-(\ell+1)^2) \sim (\ell-1)(T_\ell^2-(\ell+1)^2)$$

となる．ここで, $\sim$ は $\mathcal{O}$ の単数倍を除いての一致を意味する．上式で $\alpha'_*\alpha'^{,*} = \beta'_*\beta'^{,*} = \gamma'_*\gamma'^{,*} = \ell(\ell+1)$ は $[\mathrm{SL}_2(\mathbb{Z}), \Gamma_0(\ell^2)] = \ell(\ell+1)$ から分かり，$\alpha'_*\beta'^{,*} = \beta'_*\gamma'^{,*} = \ell T_\ell$ は $[\Gamma_0(\ell), \Gamma_0(\ell^2)] = \ell$ と $T_\ell = \alpha_*\beta^*$ から分かり，$\beta'_*\alpha'^{,*} = \gamma'_*\beta'^{,*} = \ell T_\ell$ は T_ℓ の随伴 $T_\ell^\vee$ が $\langle\ell\rangle^{-1}T_\ell = T_\ell$ と一致することから分かり，$\alpha'_*\gamma'^{,*} = \gamma'_*\alpha'^{,*} = T_\ell^2-(\ell+1)$ は $\alpha'_*\gamma'^{,*} = \alpha_*\alpha_*\beta^*\beta^* = \alpha_*(T_\ell - \langle\ell\rangle\beta_*)\beta^* = \alpha_*T_\ell\beta^* - \langle\ell\rangle(\ell+1) = T_\ell^2-(\ell+1)$ から分かる．また, c_ℓ を $\rho = \rho_f$ に対して前節で定義した量とすると,

$$\pi_f((\ell-1)(T_\ell^2-(\ell+1)^2)) = c_\ell$$

である.

$\ell = p$ **の場合.**

$$\phi\circ\phi^\vee : H_\Sigma \xrightarrow{\begin{pmatrix} 1 \\ -\alpha_p^{-1} \end{pmatrix}} H_\Sigma^{\oplus 2} \xrightarrow{w_{\Sigma'}\begin{pmatrix} \alpha^*, & \beta^* \end{pmatrix} w_\Sigma} H_{\Sigma'} \xrightarrow{\begin{pmatrix} \alpha_* \\ \beta_* \end{pmatrix}} H_\Sigma^{\oplus 2} \xrightarrow{\begin{pmatrix} 1 & -\alpha_p^{-1} \end{pmatrix}} H_\Sigma$$

なので,

$$\begin{pmatrix} 1 & -\alpha_p^{-1} \end{pmatrix} \begin{pmatrix} \alpha_* \\ \beta_* \end{pmatrix} w_{\Sigma'} \begin{pmatrix} \alpha^*, & \beta^* \end{pmatrix} w_\Sigma \begin{pmatrix} 1 \\ -\alpha_p^{-1} \end{pmatrix}$$
$$= \begin{pmatrix} 1 & -\alpha_p^{-1} \end{pmatrix} \begin{pmatrix} \alpha_*\beta^* & \alpha_*\alpha^* \\ \beta_*\beta^* & \beta_*\alpha^* \end{pmatrix} \begin{pmatrix} 1 \\ -\alpha_p^{-1} \end{pmatrix} = \begin{pmatrix} 1 & -\alpha_p^{-1} \end{pmatrix} \begin{pmatrix} T_\ell & \ell+1 \\ \ell+1 & T_\ell \end{pmatrix} \begin{pmatrix} 1 \\ -\alpha_p^{-1} \end{pmatrix}$$
$$= \alpha_p(p\alpha_p^{-2}-1)(\alpha_p^{-2}-1) \sim \alpha_p^2 - 1$$

また, c_p を $\rho = \rho_f$ に対して前節で定義した量とすると

$$\pi_f(\alpha_p^2-1) = (\chi_2/\chi_1)(\mathrm{Fr}_p) - 1 = c_p$$

である. 系 4.10$\phi : H_{\Sigma'} \twoheadrightarrow H_\Sigma$ より $\mathcal{O}$ 双対をとって $\phi^\vee : H_\Sigma \hookrightarrow H_{\Sigma'}$ の余核は $\mathcal{O}$ 平坦と分かるので, $\phi^\vee$ は同型 $\phi^\vee : H_\Sigma[\wp_{\mathbb{T}_\Sigma}] \xrightarrow{\sim} H_{\Sigma'}[\wp_{\mathbb{T}_{\Sigma'}}]$ を誘導する．よって, $\{x, y\}$ を $H_\Sigma[\wp_{\mathbb{T}_\Sigma}]$ の基底とした時, $\{\phi^\vee(x), \phi^\vee(y)\}$ は $H_{\Sigma'}[\wp_{\mathbb{T}_{\Sigma'}}]$ の基底となる．従って, 補題 4.8 より $\ell \neq p$, $\ell = p$ どちらの場合でも

$$\mathrm{length}_\mathcal{O}\Omega_{\Sigma'} = 2\langle\phi^\vee(x), \phi^\vee(y)\rangle_{\Sigma'} = 2\langle\phi\circ\phi^\vee(x), y\rangle_\Sigma = 2\#\mathcal{O}/(c_\ell) + \mathrm{length}_\mathcal{O}\Omega_\Sigma$$

と分かる．一般に, $\Sigma' \supset \Sigma$ をともに条件 (Σ) を満たす素数の有限集合とすると.

$$\mathrm{length}_\mathcal{O}\Omega_{\Sigma'} = 2\#\mathcal{O}/(\prod_{\ell\in\Sigma'\setminus\Sigma} c_\ell) + \mathrm{length}_\mathcal{O}\Omega_\Sigma \tag{13}$$

が成立する.

定理 4.11 ($R=T$ 定理) 条件 (Σ) を満たす素数の有限集合 Σ に対して, 全射 $R_\Sigma \twoheadrightarrow \mathbb{T}_\Sigma$ は同型であり, R_Σ, $\mathbb{T}_\Sigma$ は局所完全交叉 $\mathcal{O}$ 代数で, H_Σ は自由 $\mathbb{T}_\Sigma$ 加群. □

証明 定理 3.9, 定理 4.3 より $2\cdot \mathrm{length}_{\mathcal{O}}\wp_\emptyset/\wp_\emptyset^2 = \mathrm{length}_{\mathcal{O}}\Omega_\emptyset$ (3.3 節では $H_\emptyset$ は負部分 $(\cdot)^-$ をとっていたが, 負部分が $\mathbb{T}_\emptyset$ 上自由ならカップ積より正部分も $\mathbb{T}_\emptyset$ 上自由と分かるので本節での $H_\emptyset$ も $\mathbb{T}$ 上自由であることに注意). 系 4.7 と式 (13) より,

$$2\cdot \mathrm{length}_{\mathcal{O}}\wp_\Sigma/\wp_\Sigma^2 - 2\cdot \mathrm{length}_{\mathcal{O}}\wp_\emptyset/\wp_\emptyset^2 \le 2\#\mathcal{O}/(\prod_{\ell\in\Sigma} c_\ell) = \mathrm{length}_{\mathcal{O}}\Omega_\Sigma - \mathrm{length}_{\mathcal{O}}\Omega_\emptyset$$

が成立. よって $2\cdot \mathrm{length}_{\mathcal{O}}\wp_\Sigma/\wp_\Sigma^2 \le \mathrm{length}_{\mathcal{O}}\Omega_\Sigma$ なので, 定理 4.3 より主張が従う. □

以上のことと注意 4.8.1 と系 4.6 より次も得られる.

系 4.12 *1.* 条件 (Σ) を満たす素数の有限集合 Σ に対して $\#H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho_f \otimes_{\mathcal{O}} E/\mathcal{O}) = \#\mathcal{O}/\eta_\Sigma < \infty$.

2. $\Sigma' \supset \Sigma$ をともに条件 (Σ) を満たす素数の有限集合とすると,

$$0 \to H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\rho_f \otimes_{\mathcal{O}} E/\mathcal{O}) \to H^1_{\Sigma'}(\mathbb{Q}, \mathrm{ad}^0\rho_f \otimes_{\mathcal{O}} E/\mathcal{O}) \to \oplus_{\ell\in\Sigma'\setminus\Sigma} H^1_\ell \to 0$$

は完全系列. □

次が本稿の主定理である.

系 4.13 (保型性持ち上げ定理) $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O})$ を有限個の素点を除いて不分岐な連続絶対既約表現とする. 次を仮定する:

1. $\det\rho = \varepsilon$,
2. ρ は p で準安定,
3. $\bar\rho$ は絶対既約で保型的,
4. $\ell \ne p$ に対して, $\bar\rho|_{I_\ell} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ ならば, $\rho|_{I_\ell} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

この時, ρ は保型的, すなわち, ある正規化された Hecke 固有形式 f が存在し, ほとんど全ての素数 ℓ に対して (固定した埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{E}$ について) $\mathrm{Tr}\bar\rho(\mathrm{Fr}_\ell) = a_\ell(f)$ が成立する. □

証明 ρ が分岐して $\bar\rho$ が不分岐である p 以外の素数の集合を Σ' とし, もし $\bar\rho$ が p 平坦かつ通常であれば $\Sigma := \Sigma' \cup \{p\}$, そうでなければ $\Sigma := \Sigma'$ とする. すると, ρ は $\bar\rho$ の Σ 型の変形なので, 射 $R_\Sigma \twoheadrightarrow \mathcal{O}$ が存在して $\rho_{R_\Sigma} \otimes_{R_\Sigma} \mathcal{O} \simeq \rho$ となる. ここで, $R_\Sigma \cong \mathbb{T}_\Sigma$ なので, 射 $\mathbb{T}_\Sigma \twoheadrightarrow \mathcal{O}$ を得る. この射の核に対応する Hecke 固有形式を f とすると, $\rho \simeq \rho_f$ となるので ρ は保型的. □

5 Wilesの$(3,5)$トリック.

この章では$E[3]$が$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$の表現として既約でない時に使われたWilesの$(3,5)$トリックを解説する.

$\mathrm{GL}_2(\mathbb{F}_3) \cong S_4$ (4次対称群) は$\mathrm{GL}_2(\mathbb{C})$に埋め込めるので, 法3表現$\bar{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_3)$に対して, $\mathrm{GL}_2(\mathbb{F}_3) \hookrightarrow \mathrm{GL}_2(\mathbb{C})$を合成してArtin表現が得られる. $\mathrm{GL}_2(\mathbb{F}_3)$**は可解なので**, Langlands-Tunnellの定理[La][Tu]を使うと$\det \bar{\rho}(c) = -1$である任意の連続法3表現は保型的であることが分かる. 特に, $\mathbb{Q}$上の楕円曲線Eに対してその法3表現$E[3]$も保型的. ここで, $E[3]$の保型性をTate加群T_3Eの表現に持ち上げることができれば, Eの保型性がしたがう. Eを準安定と仮定すると, 前章までの考察が使える状況になる.

もし$E[3]$が$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$の表現として既約であれば, 保型性持ち上げ定理 (系 4.13) から, T_3Eも保型的である. $E[3]$が既約でない時を考える. この時, Mazurの定理 ($X_0(15) = \{$尖点$\}$)[M1], [M2]から, $E[5]$は既約であることが分かる. しかし, $E[5]$は保型的であることはまだ分からない.

ここで, 次の条件を満たす$\mathbb{Q}$上の楕円曲線E'をみつけてくる:

1. $E'[3]$は既約,
2. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$の表現として, $E'[5] \cong E[5]$,
3. E'は準安定.

もしみつけることができれば, $E'[3]$は保型的$\Rightarrow$ T_3E'は保型的 (系 4.13) $\Rightarrow E'$は保型的$\Rightarrow T_5E'$は保型的$\Rightarrow E'[5] \cong E[5]$は保型的$\Rightarrow T_5E$は保型的 (系 4.13) $\Rightarrow E$は保型的となり, 欲しかったEの保型性が示される (下図参照).

$$
\begin{tikzcd}
 & T_3E' \arrow[dl] \arrow[r, leftrightarrow, dotted] & T_5E' \arrow[dr] & & & T_5E \arrow[dl] \\
E'[3] & & & E'[5] \arrow[r, dash, "\sim"] & E[5]. &
\end{tikzcd}
$$

このようなE'を以下でみつける. レベル構造を$(\mathbb{Z}/5\mathbb{Z})^2$との同型ではなく$E[5]$との同型で与えたものはレベル$\Gamma(5)$構造付きの楕円曲線のモジュライのコンパクト化$X(5)$の捻り$X(E[5])$を与える. $X(5)$は種数0であり, $X(E[5])$は有理点$(E, E[5])$をもつので, $X(E[5]) \cong \mathbb{P}^1_{\mathbb{Q}(\zeta_5)}$である. 特に, 有理点は無限個存在する. 同様に, レベル$\Gamma(5) \cap \Gamma_0(3)$構造付きの楕円曲線のモジュライのコンパクト化$X(\Gamma(5) \cap \Gamma_0(3))$の捻りとして, $(\mathbb{Z}/5\mathbb{Z})^2$を$E[5]$で置き換えた$X(E[5], \Gamma_0(3))$を考える ($\Gamma_0(3)$構造はそのまま). $X(5,3)$は種数$9 > 1$なので, Faltingsの定理[Fa]より, $X(E[5], \Gamma_0(3))$の有理点は有限個 (Wilesの原論文[W1]ではHilbertの既約性定理を使った議論をする). 従って, $X(E[5])$の有理点は有限個を除いて, $X(E[5], \Gamma_0(3))(\mathbb{Q}) \to X(E[5])(\mathbb{Q})$の像に入っていない. この像に入らない有理点に対応する楕円曲線E'は, $E'[5] \cong E[5]$かつ$E'[3]$は既約である. この有理点を5進的に

$(E, E[5], \mathbb{Z}/3\mathbb{Z} \subset E[3])$ に十分近いものをとると, E' は準安定なものをとれる (Weierstrass 定義方程式で考えよ). 以上により, 望みの E' をみつけることができた. 従って, 以下が示された.

定理 5.1 [W1] E を $\mathbb{Q}$ 上の準安定な楕円曲線とすると, E は保型的. □

注意 5.1.1 すべての $\mathbb{Q}$ 上の楕円曲線は保型的であることが知られている [BCDT] が, Taylor-Wiles 系と $(3,5)$ トリックの復習をするという本稿の目的から逸れるために詳しいことはここでは紹介しない. 6 章と本報告集の記事 [Y] を参照. □

注意 5.1.2 $(3,5)$ トリック中で,

1. $E[3]$ が可約なら $E[5]$ が既約であること,
2. $X(\Gamma(5) \cap \Gamma_0(3))$ の種数が 1 より大きいこと,
3. $\mathrm{GL}_2(\mathbb{F}_3)$ は可解であること,
4. $X(5)$ は種数 0 であること,

を使ったが, これに関して,

1. $E[3]$ が可約なら任意の素数 $q > 3$ に対して $E[q]$ は既約,
2. Riemann-Hurwitz 公式から, 相異なる素数 p, q に対して $X(\Gamma(q) \cap \Gamma_0(p))$ の種数は
$$\begin{cases} (p-3)/2 & q = 2, \\ 1 + q(q^2-1)(p+1)/24 - (q^2-1)/2 & q > 2 \end{cases}$$
であり, $(p, q) = (3, 2), (5, 2), (2, 3)$ の 3 通り以外は 1 より大きい,

ので最初の 2 つに関しては $(3,5)$ の組以外でも通用する組が無数に存在するが,

3. $\mathrm{GL}_2(\mathbb{F}_p)$ が可解になるような素数 p は $p = 2, 3$ のみ,
4. 素数 q に対して $X(q)$ の種数は $q > 2$ の時 $(q-3)(q-5)(q+2)/24$, $q = 2$ の時 0 であり, これが 0 になるのは $q = 2, 3, 5$ のみ,

なので奇素数では $(3,5)$ の組しかこのトリックを行うことができない. □

注意 5.1.3 この $(3,5)$ トリックに対して, 後に Hilbert-Blumenthal モジュラー多様体を使った変種 [T2], [T3] や Calabi-Yau 族を使った変種 [HSBT] が考えられ, 前者からは GL_2 での潜在的保型性, 後者からはユニタリ群での潜在的保型性が証明された. 特に, 後者は佐藤-Tate 予想を緩い条件のもとで解決する応用をもつ (本報告集の津嶋氏, 原氏の記事参照).

また, モジュライの有理点を使うわけではないが, Serre 予想の証明で ℓ 進表現の厳整合系 (strictly compatible system) を使ったテクニック ([KW1], [Kh1], [KW2], [KW3]) も $(3,5)$ トリックの変種ともみなせる (本報告集の萩原氏, 山内氏の記事参照). 以上の注意は 6 章も参照. $\square$

系 5.2 (Fermat-Wiles の定理) $n \geq 3$ の時

$$x^n + y^n = z^n,$$

$xyz \neq 0$ を満たす整数解は存在しない. $\square$

証明 $n = 4$ の時は既に証明されている (Fermat) ので, n は奇素数 p としてよい. $a^p + b^p = c^p$ を a, b, c が互いに素な非自明解とする. a, b, c が互いに素なので楕円曲線

$$E : y^2 = x(x - a^p)(x + b^p)$$

(**Frey 曲線**という) は準安定. 従って定理 5.1 から E は保型的. E の判別式は $16((a^p - 0)(b^p - 0)(a^p + b^p))^2 = 16(abc)^{2p}$ なので, 法 p 表現 $E[p]$ は $2, p$ の外不分岐かつ p で平坦 (判別式を割る素数 ℓ に対して, 判別式は ℓ^{2p} で割れるので, E の Néron モデルの ℓ での特殊ファイバーは Néron $2p$ 角形であることから分かる). よって Ribet のレベル下げ ([R1]) により, 法 p 表現 $E[p]$ は $S_2(\Gamma_0(2))$ の Hecke 固有形式 f に対する $\bar{\rho}_f$ と同型になるが, $S_2(\Gamma_0(2)) = 0$ より矛盾. $\square$

特殊値 $L(\mathrm{Sym}^2 E, 2)$ への応用

最後に, $\# H^1_\emptyset(\mathbb{Q}, \mathrm{ad}^0 \rho_{E,p} \otimes \mathbb{Q}_p/\mathbb{Z}_p)$ が 2 次対称積の L 関数の特殊値 $L(\mathrm{Sym}^2 E, 2)$ と関係することについて簡単に述べる ([DDT, §4.4] 参照). ごく大雑把に述べると以下のように関係する:

$$\begin{aligned}
&\# H^1_\emptyset(\mathbb{Q}, \mathrm{ad}^0 \rho_{E,p} \otimes \mathbb{Q}_p/\mathbb{Z}_p) = \# \wp_\emptyset / \wp_\emptyset^2 \overset{R=T}{\longleftrightarrow} \# \mathbb{Z}_p/\eta_\emptyset \longleftrightarrow \Omega_E^{-1} \langle f, \overline{w_\emptyset f} \rangle_{\mathrm{Petersson}} \\
&\overset{\text{志村公式}}{\longleftrightarrow} \text{Rankin-Selberg 畳み込み } \Omega_E^{-1} \mathrm{res}_{s=2} D(f, f, 2) \\
&\longleftrightarrow \Omega_E^{-1} L(\mathrm{Sym}^2 f, 2) = \Omega_E^{-1} L(\mathrm{Sym}^2 E, 2).
\end{aligned}$$

ここで, Ω_E は E の周期であり, f は保型的楕円曲線 E に対応する保型形式. これは古典的な類数公式やコホモロジー的 Lichtenbaum 予想の ad^0 に対する類似になっていて, より一般に "モチーフ" に対して L 関数の特殊値を周期とレギュレーター (と高さペアリング) と Galois コホモロジーで表す Bloch-加藤の玉河数予想が $\mathrm{Sym}^2 E$ に対して (部分的に) 成立することを言っている. 重さが 2 以上の保型形式の Sym^2 の玉河数予想については [DFG] 参照.

E を $\mathbb{Q}$ 上の準安定楕円曲線, f を対応する新形式とする. $N := N_E$ を E の導手, $\Delta_E = \prod_{\ell | N_E} \ell^{d_\ell}$ を極小判別式とする. N_E は f のレベル N_f と一致する (命題 3.1 の 3.). p を $E[p]$ が既約で, $p \nmid 2 \prod_{\ell | N_E} d_\ell$ を満たす素数とする. $\rho_{E,p}$ を E の p 進 Tate 加群 $T_p E$ への Galois 表現とし, $\mathcal{N}_\emptyset$ を $\rho_{E,p}$ の法 p 還元にたいして 3.2 節で定めた新形式の集合, $N_\emptyset$ を同じく 3.2 節

で定めたレベルとする. $N_\emptyset \mid N_f$ であるが, $p \nmid \prod_{\ell | N_E} d_\ell$ より $N_\emptyset = p^{\delta(\bar\rho)} N(\bar\rho)$ が N_f より真に小さくはならないので $N_\emptyset = N_f = N$ であり, $f \in \mathcal{N}_\emptyset$ となる.

素数 ℓ に対して $a_\ell(E) := 1 + \ell - \#\tilde{E}(\mathbb{F}_\ell)$ ($\tilde{E}$ は E の Néron モデル) とおき, α_ℓ, β_ℓ を, $\ell \nmid N_E$ の時は $X^2 - a_\ell(E)X + \ell = 0$ の根, $\ell \mid N_f$ の時は $X^2 - a_\ell(E)X = 0$ の根とする.

$$L_\ell(\mathrm{Sym}^2 E, s) := \frac{1}{(1-\alpha_\ell^2 \ell^{-s})(1-\alpha_\ell\beta_\ell\ell^{-s})(1-\beta_\ell^2\ell^{-s})}$$

として $L(\mathrm{Sym}^2 E, s) = \prod_\ell L_\ell(\mathrm{Sym}^2 E, s)$ を E **の** 2 **次対称積の** L **関数**という. $L(\mathrm{Sym}^2 f, s)$ も $a_\ell(E)$ を $a_\ell(f)$ で置き換えて同様に定義する. $L(\mathrm{Sym}^2 f, s) = L(\mathrm{Sym}^2 E, s)$ である.

$\wp$ を f に対応する射 $\mathbb{T}_\mathcal{O}(N)$ の核, $\{x, y\}$ を $H_\emptyset[\wp]$ の基底とする. 一方, $H_\emptyset[\wp] \otimes_\mathcal{O} \mathbb{C} (\subset H^1(X_0(N), \mathbb{C}))$ には基底 $\{2\pi\sqrt{-1}f(z)dz, 2\pi\sqrt{-1}f(\bar z)d\bar z\}$ がある ($dq/q = 2\pi\sqrt{-1}dz$ より $2\pi\sqrt{-1}$ をつける). $(2\pi\sqrt{-1}f(z)dz, 2\pi\sqrt{-1}f(\bar z)d\bar z) = (x, y)A$ となる行列 $A \in \mathrm{GL}_2(\mathbb{C})$ をとる.

$$\langle x, y\rangle_\emptyset \det A = -4\pi^2 \int_{X_0(N)} f(z) \wedge f(\bar z) dz \wedge d\bar z = 8\pi^2\sqrt{-1}\langle f, \overline{(w_\emptyset f)}\rangle \tag{14}$$

が分かる (2 つ目の $\langle\cdot,\cdot\rangle$ は Petersson 内積). 志村の公式 ([Sh, (2.5)], [H, (5.13)]) より,

$$\langle f, \overline{(w_\emptyset f)}\rangle = (48\pi)^{-1}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]\mathrm{res}_{s=2} D(f, w_\emptyset f, s) \tag{15}$$

となる. ここで, $D(g, h, s)$ は $\sum_n a_n(g)a_n(h)n^{-s}$ で定まる Dirichlet 級数. (ℓ での Euler 因子は $(1-\ell^{2-2s})(1-\alpha_\ell(g)\alpha_\ell(h)\ell^{-2s})^{-1}(1-\alpha_\ell(g)\beta_\ell(h)\ell^{-2s})^{-1}(1-\beta_\ell(g)\alpha_\ell(h)\ell^{-2s})^{-1}(1-\beta_\ell(g)\beta_\ell(h)\ell^{-2s})^{-1}$ である). f は新形式なので $D(f, w_\emptyset f, s) = \pm D(f, f, s)$ であり, Euler 積表示から

$$D(f, f, s) = \zeta_N(s-1)L(\mathrm{Sym}^2 f, s)/\zeta_N(2s-2)$$

が分かる (ここで $\zeta_N(s)$ は Riemann ゼータ関数から N を割る Euler 因子を除いたもの). よって,

$$\mathrm{res}_{s=2} D(f, w_\emptyset f, s) = \pm\frac{1}{\zeta(2)} L(\mathrm{Sym}^2 f, s) \prod_{\ell | N} \frac{1-\ell^{-1}}{1-\ell^{-2}} = \frac{6}{\pi^2}\frac{NL(\mathrm{Sym}^2 f, s)}{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]} \tag{16}$$

となる. 式 (14), 式 (15), 式 (16) をあわせると

$$L(\mathrm{Sym}^2 f, 2) = \pm N^{-1}\pi\sqrt{-1}\langle x, y\rangle_\emptyset \det A$$

が得られる. $\eta_\emptyset^2 = (\langle x, y\rangle_\emptyset)$ なので,

$$L(\mathrm{Sym}^2 f, s) \sim N^{-1}\pi\sqrt{-1}\#\mathbb{Z}_p/\eta_\emptyset \det A$$

である ([DDT, Theorem 4.20, Corollary 4.21] 参照). ここで $\sim$ は $\mathbb{Z}_p$ の単数倍を除いての一致を意味する. 定理 4.11, 注意 4.8.1 より,

$$L(\mathrm{Sym}^2 f, s) \sim N^{-1}\pi\sqrt{-1}\det A \# H^1_\emptyset(\mathbb{Q}, \mathrm{ad}^0\rho_{E,p} \otimes \mathbb{Q}_p/\mathbb{Z}_p)$$

が証明された. E は準安定であることと, $p>2$ と $E[p]$ が既約であることを使うと, $\det A$ は $\mathbb{Z}_p$ の単数倍を除いて E の周期

$$\Omega_E := \int_{E(\mathbb{C})} \omega_E \wedge \bar{\omega}_E$$

(ω_E は E の Néron 微分形式) と一致することも分かる (E の保型性からくる射 $\pi : X_0(N) \to E$ に対して $\pi^* : H^1(E, \mathbb{Z}_p) \to H^1(X_0(N), \mathbb{Z}_p)$ の余核は $\mathbb{Z}_p$ 平坦であることと, π の Manin 定数は p で割れないことから分かる [M2]). よって次が得られた.

定理 5.3 ([DDT, Theorem 3.53]) E を $\mathbb{Q}$ 上の準安定な楕円曲線, Ω_E をその周期, N_E を導手, $\Delta_E = \prod_{\ell | N_E} \ell^{d_\ell}$ を極小判別式とする. S を以下を満たす素数の積とする (Serre の定理あるいは Mazur の定理より以下を満たす素数は有限個).

- $E[p]$ は可約, または
- $p \mid 2\prod_{\ell | N_E} d_\ell$.

この時,

$$L(\mathrm{Sym}^2 E, 2) \sim \pi\sqrt{-1}\Omega_E N_E^{-1} \prod_{p \nmid S} \# H^1_\emptyset(\mathbb{Q}, \mathrm{ad}^0 \rho_{E,p} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)$$

が成立する. ここで $\sim$ は $\mathbb{Z}[1/S]^\times$ 倍を除いての一致を意味する. □

6 歴史的補足.

6.1 Taylor-Wiles 系の改良.

Taylor-Wiles 系の議論は以下 1-4 のように改良された.

1. 元来の [TW, Theorem 1] の議論では Taylor-Wiles 系を (R, R_n, H, H_n は考えないで) “T, T_n に対してのみ” 考えることで, T が局所完全交叉 $\mathcal{O}$ 代数であることを導出し, Wiles の数値的判定法 ([W1, appendix Proposition 1, Proposition 2]) と Galois コホモロジーの計算 ([W1, Theorem 3.1(i)]) を使うことで, 同型 $R \xrightarrow{\sim} T$ を証明した ([W1, Theorem 3.1(ii)]).

2. Faltings は $\mathcal{O}[\Delta_Q]$ 代数構造を T_n から R_n に持ち上げ, Taylor-Wiles 系を “R, R_n, T, T_n に対して” 考えることで, 同型 $R \xrightarrow{\sim} T$ と R, T が局所完全交叉 $\mathcal{O}$ 代数であることが (Wiles の数値的判定法を使わないで) 同時に出るように改良した ([TW, appendix]).

3. Diamond-藤原は, Taylor-Wiles 系を “R, R_n, H, H_n に対して” 考え, “R と $\mathrm{End}(H)$ で T を挟み込む” ことで, 同型 $R \xrightarrow{\sim} T$ と R, T が局所完全交叉 $\mathcal{O}$ 代数であることと H が

T 上自由であることが同時に出るように改良した ([D1, Theorem 2.1]). また, 数値的判定法も同様に R と T を比べるのではなく R と H を比べることで H が T 上自由であることが同時に出るように改良した.

上記 1, 2 では, 以下の時に H が T 上自由であること ([W1, Theorem 2.1 の Corollary 1]) とその系である Hecke 環の Gorenstein 性 ([W1, Theorem 2.1 の Corollary 2]) を先に証明する必要があった:

(a) 極小の場合, Taylor-Wiles 系を構成する時に de Shalit の議論を用いて Hecke 環が群環 $\mathcal{O}[\Delta_Q]$ 上自由であることを示す ([TW, Theorem 2]) 時.

(b) 極小でない場合, Hecke 環の増分を計算する ([W1, Proposition 2.4 の前, Propositon 2.6 の前, Propostion 2.7 の前, Propsition 2.10 の前, Proposition 2.12 の前, Propositon 2.13 の前]) 時.

(c) Wiles の数値的判定法 ([W1, appendix Proposition 2]) を使う時.

ここで, H が T 上自由であることは標数 p の q 展開原理による重複度 1 の議論を使うことで証明していた ([W1, Theorem 2.1]) が, 上記 (a)-(c) の項目に関して,

(a) 極小の場合, H が T 上自由であることを前もって証明しなくても, de Shalit の議論を用いないで Hecke 環が群環 $\mathcal{O}[\Delta_Q]$ 上自由であることを示し ([D1, Lemma 3.2]), Diamond-藤原の改良された Taylor-Wiles 系を使うことで同型 $R \xrightarrow{\sim} T$ と R, T が局所完全交叉 $\mathcal{O}$ 代数であることと H が T 上自由であることが証明できるようになった.

(b) 極小でない場合, 数値的判定法を R と T ではなく R と H を用いて定式化することで, H が T 上自由であることを前もって証明しなくても数値的判定法から $\Sigma = \emptyset$ に帰着させることができるようになった ([D1, Theorem 2.4]).

(c) Wiles の数値的判定法は Lenstra により Gorenstein 性を仮定しない命題に拡張された ([L]).

これらのことにより, **標数 p の q 展開原理による重複度 1 の議論を使う代数幾何的議論を使わなくても, $R = T$ と Hecke 加群の自由性が可換環論から導出できるようになった.**

4. Kisin は普遍変形環を局所普遍変形環 (局所体の法 p Galois 表現の普遍変形環 (の完備テンソル積)) 上で考えることによって, 以下の改善を得た (本報告集 [Y] と今井氏の記事参照).

   (a) p での暴分岐 (wildly ramified) な法 p Galois 表現を考える場合, (Skinner-Wiles の底変換議論をした後) 普遍変形環と Hecke 環はもはや局所完全交叉であることが望めないが, そのような場合でも修正 Taylor-Wiles 系により同型 $R^{\mathrm{red}} \xrightarrow{\sim} T$ が示せる ([K1, Theorem 3.4.11]),

(b) 極小でない場合でも, (帰納法を使わないで) 直接修正 Taylor-Wiles 系から同型 $R^{\mathrm{red}} \xrightarrow{\sim} T$ が示せる. これにより, **代数幾何的な伊原の補題を使わなくても可換環論から $R^{\mathrm{red}} \xrightarrow{\sim} T$ が導出できるようになった.**

上記の標数 p の q 展開原理による重複度 1 の議論や伊原の補題が要らなくなったことと関連して余談になるが, Fermat 予想の証明に関して他に証明が簡素化されたものに次の 2 点がある.

A. Ribet のレベル下げ ([R1]) は志村曲線の p 進一意化を用いた証明であったが, Skinner-Wiles の底変換の議論 ([SW3], 本報告集加塩氏の記事参照) により, より簡単で代数幾何を使わない議論に置き換えることができるようになった.

B. Khare-Wintenberger による ℓ 進表現の厳整合系のテクニック ([KW1], [Kh1]) と Schoof の結果 ([Sc]) により, Fermat 予想の証明において Langlands-Tunnell の定理 ([La], [Tu]) を用いて法 3 表現が保型的であることを示すことも不要になった ([Kh2], 本報告集萩原氏と山内氏の記事参照). けれども Langlands の底変換 [La] はそれ以外の部分で必要であるし, 非 Galois 3 次拡大の底変換も局所・大域整合性で使う[1] (本報告集三枝氏の記事参照). Khare-Wintenberger のテクニックは Taylor の潜在的保型性 ([T2][T3]) も用いるため, 証明が “簡素化” されたといえるかは意見が分かれるかもしれない (しかし $\mathrm{GL}_2(\mathbb{F}_3)$ が可解であるという “奇跡” は要らなくなった).

以上のことにより, 多くの代数幾何的議論が可換環論に置き換わった. 代数幾何的議論が必要であるものは以下ぐらいである.

A. Galois 表現の構成 ([Ca1], [T1], 本報告集の三枝氏, 山上氏の記事参照),

B. 局所・大域整合性 ([Ca1], [S3], [S4], 本報告集の三枝氏の記事参照).

6.2 $R = T$ にまつわる発展.

Taylor-Wiles 系そのものの改良以外の $R = T$ にまつわる発展には以下のものがある (志村・谷山予想, 剰余的可約な時の保型性持ち上げ, 潜在的保型性, ユニタリ群に対する $R = T$, 佐藤-Tate 予想, Serre 予想等).

1. [W1][TW]: 準安定還元をもつ $\mathbb{Q}$ 上の楕円曲線に対して志村・谷山予想を証明した.

2. [D2]: 3 と 5 で準安定還元をもつ $\mathbb{Q}$ 上の楕円曲線に対して志村・谷山予想を証明した. 証明の本質的な改善は, p の外で “極小変形” を局所 Langlands 対応を使って定式化したこと ([W1] で p の外の条件を完全に一般にできなかった事については [W1, p.511 の 2 つ目の Remark] を参照).

[1] 本原稿の以前の版では “非 Galois 3 次拡大の底変換は不要になった” と書かれてあった. 三枝氏の指摘に感謝する.

3. [CDT]: 導手が 27 で割れない (すなわち, 3 で馴分岐拡大に底変換すると準安定還元をもつ)$\mathbb{Q}$ 上の楕円曲線に対して志村・谷山予想を証明した. 分岐指数が $p-1$ 以下の拡大を許すと有限平坦群スキームから来るような変形に関する普遍変形環の計算を Conrad がしており, それを用いて考えている ℓ-型 (ℓ-type) が受け入れ可能 (acceptable) であることを示すのが証明の本質的な部分. また, ここで述べられている予想は p 進局所 Langlands 対応と深い関係のある Breuil-Mézard 予想の雛形でもある.

4. [BCDT]: 志村・谷山予想の残された場合 (3 での導手が 27, 81, 243 の時) を証明した. Breuil 加群の細かい計算をすることで考えている ℓ 型 (3 での導手が 243 の時は拡張 ℓ 型) が弱受け入れ可能 (weakly acceptable) であることを示すのが証明の本質的な部分.

   [CDT][BCDT] の証明からも, p 進の理論 (特に整 p 進 Hodge 理論) が $R=T$ 定理の発展を支えていることが分かる.

5. [SW1]: $\mathbb{Q}$ 上 Abel な総実代数体の Galois 表現で, 剰余的可約で概通常 (nearly ordinary) な変形についての $R=T$ 定理. 一般の総実代数体でも結果はあるが (拡大体たちの) イデアル類群に関する条件が必要.

   証明は技術的. 剰余的可約な時は R から T に射が存在しないので, 擬表現の普遍変形環を補助的に使う. 肥田理論的な R や T を使うため商が有限とは限らず, Taylor-Wiles 系の貼り合わせの議論も少し複雑になっている.

   可解な体拡大をすることで R の中で可約な変形に対応するものの余次元を上げ, そこから Cohen-Macaulay 局所環のある種の局所閉集合の連結性に関する Raynaud の定理を使う, というのがアイデア. 余次元が十分に上がることを示すのに円分 $\mathbb{Z}_\ell$ 拡大についてのイデアル類群の $p(\neq \ell)$ 階数の振る舞いに関する Washington の定理を使う. また, 最初にナイス (nice) 素イデアルを見つけてくるために, p 進 L 関数の特殊値の法 $\pi(|\, p)$ での消滅を使う (ここでも可解な体拡大をする). 本報告集の新井氏の記事参照.

6. [SW2], [F]: [SW2] は [SW1] のテクニックを剰余的既約な場合に使ったもの. 剰余的既約だと [SW1] であった細かい技術的な困難がほとんどなくなる. $\mathrm{Gal}(\overline{F}/F(\zeta_p))$ に制限して既約であることを仮定しなくてもよい. [F] も総実代数体についての $R=T$ 定理.

7. [K1], [K5]: p で潜在的 Barsotti-Tate な変形に対する保型性持ち上げ. 有限平坦群モデルのモジュライを整 p 進 Hodge 理論により半 (semi-) 線型代数的な対象で記述して調べることが証明の本質的な部分. 特に, そのモジュライの特殊ファイバーの連結性を示すことが証明の鍵. 志村・谷山予想のより簡易化された証明も与える ([BCDT] のような Breuil 加群の細かい計算が不要になった). 本報告集の [Y] 参照.

   [K5] は [K1] の $p=2$ 版. Breuil 加群の理論が使えない部分を Zink の displays, windows の理論で代用することで $p=2$ に拡張した.

8. [K3]: p で中間重さ (即ち, 重さが $2p-1$ 以下) のクリスタリンである変形に関する $R=T$ 定理. [K1] で有限平坦モデルのモジュライを考えていたのを Wach 加群のモジュライで置き換えて考える. そのモジュライを調べるのに, [BLZ] や [BB1] によるクリスタリン表現の法 p 還元の計算を使うのが本質的. [BLZ] と [BB1] の半分は Wach 加群の族を具体的に構成して法 p 還元を計算する. [BB1] の残り半分は p 進局所 Langlands と法 p Langlands の整合性 ([C2]) 及び保型側での法 p 還元の計算 ([B2]) を使って計算をする. 本報告集の中村氏の記事参照.

9. [K6]: p で潜在的準安定 (重さは任意) な変形というかなり一般的な状況 (小さい条件も付く) での $R=T$ 定理. p 進局所 Langlands と古典的局所 Langlands の整合性 (三角表現の場合は [C1], 一般の場合はまだ書かれていない) を使って Breuil-Mézard 予想 ([BM]) を多くの場合に証明し, それを $R=T$ に応用する. R 側の Hilbert-Samuel 重複度が保型側の言葉で書かれる (Breuil-Mézard 予想) ことから Hecke 加群が R 上忠実であることを示す. 本報告集の阿部氏, 安田氏の記事参照.

   [K1], [K5], [K3], [K6] からも, p 進の理論, 特に整 p 進 Hodge 理論と p 進局所 Langlands 対応が $R=T$ の発展を促進していることが分かる.

10. [T2], [T3]: [T2] は p で通常 (ordinary) な変形に関する潜在的保型性定理. [T3] は p でクリスタリンな変形に関する潜在的保型性定理. Moret-Baily の定理を用いて Hilbert-Blumenthal モジュラー多様体に有理点を構成しそれを用いて $(3,5)$ トリックの変種をする. 局所体上の有理点の構成は, [T2] では, 本田-Tate 理論で有限体上で有理点を作り, Serre-Tate 理論で局所体上に持ち上げる. [T3] では, 考えている局所体上では一致するような Hilbert-Blumenthal モジュラー多様体の捻りを考え, 虚数乗法論から (代数体上の) 有理点を構成し, もとの多様体に局所体上の有理点を構成する. 本報告集の津嶋氏, 原氏の記事参照.

11. [CHT], [T4]: ユニタリ群に対しての $R=T$ 定理. [CHT] では極小の時は予想を仮定せず証明した ([CHT, Theorem 3.1.1]) が, 極小でない時はユニタリ群に対する伊原の補題 ([CHT, Conjecture I]) を予想として仮定していた. しかし, 上記 Kisin による普遍変形環を局所普遍変形環上で考える議論を使うことで [T4] で**極小でない場合も伊原の補題を仮定しないで証明できるようになった** ([T4, Theorem 4.1]). 本報告集の千田氏, 安田氏の記事参照.

12. [HSBT]: 佐藤-Tate 予想を緩い条件のもとで証明した. 上記 [CHT], [T4] と Calabi-Yau 多様体の族を用いた $(3,5)$ トリックの変種とあわせることで証明した. 本報告集の津嶋氏, 原氏の記事参照.

13. [KW1], [Kh1], [KW2], [KW3]: Serre 予想を証明した. [T2], [T3] を用いて ℓ 進表現の厳整合系を構成するのが新しいアイデア. 帰納法の最初では [Sc] を使う. $p=2$ については [K5] を使う. 本報告集の萩原氏, 山内氏の記事参照.

参考文献

[BB1] Berger, L., Breuil, C., *Sur la réduction des représentations cristallines de dimension* 2 *en poid moyens.* unpublished note,

次の論文に含まれる. Berger, L., *Représentations modulaires de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et représentations galoisiennes de dimension 2.* to appear in Astérisque

[B2] Breuil, C. *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbb{Q}_p)$ *II.* J. Inst. Mat. Jussieu **2** (2003), 1–36

[BB2] Berger, L., Breuil, C. *Sur quelques représentations potentiellement cristallines de* $\mathrm{GL}_2(\mathbb{Q}_p)$. to appear in Astérisque

[BCDT] Breuil, C., Conrad, B., Diamond, F., Taylor, R. *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises.* J. Amer. Math. Soc. **14**(4) (2001), 843–939.

[BLZ] Berger, L., Li, H., Zhu, H. J. *Construction of some families of* 2*-dimensional crystalline representations.* Math. Ann. **329**(2) (2004), 365–377.

[BM] Breuil, C., Mézard, A. *Multiplicités modulaires et représentations de* $\mathrm{GL}_2(\mathbb{Z}_p)$ *et de* $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ *en* $\ell = p$. Duke Math. J. **115**(2) (2002), 205–310.

[C1] Colmez, P. *Série principale unitaire pour* $\mathrm{GL}_2(\mathbb{Q}_p)$ *et représentations triangulines de dimension* 2*.* preprint.

[C2] Colmez, P. *Une correspondance de Langlands locale p-adique pour les représentations semi-stable de dimension* 2. preprint.

[Ca1] Carayol, H. *Sur les représentations* ℓ*-adiques associées aux formes modulaires de Hilbert.* Ann. Sci. École Norm. Sup. (4) **19**(3) (1986), 409–468.

[Ca2] Carayol, H. *Sur les représentations galoisiennes modulo* ℓ *attachées aux formes modulaires.* Duke Math. J. **59** (1989), 785–801.

[CDT] Conrad, B., Diamond, F., Taylor, R. *Modularity of certain potentially Barsotti-Tate Galois representations.* J. Amer. Math. Soc. **12**(2) (1999), 521–567.

[CHT] Clozel, L., Harris, M., Taylor, R. *Automorphy for some* ℓ*-adic lifts of automorphic mod* ℓ *Galois representations.* preprint.

[D1] Diamond, F. *The Taylor-Wiles construction and multiplicity one.* Invent. Math. **128** (1997) no. 2, 379–391.

[D2] Diamond, F. *On deformation rings and Hecke rings.* Ann. of Math. **144** (1996), 137–166.

[D3] Diamond, F. *The refined conjecture of Serre.* Elliptic Curves, Modular Forms, and Fermat's last Theorem (Hong Kong 1993), Internat. Press, Cambridge, MA, 1995, 22–37.

[DDT] Darmon, H., Diamond, F., Taylor, R. *Fermat's last theorem.* Elliptic Curves, Modular Forms, and Fermat's last Theorem (Hong Kong 1993), Internat. Press, Cambridge, MA, 1995, 1–154.

[DFG] Diamond, F., Flach, M., Guo L. *Adjoint Motives Of Modular Forms And The Tamagawa Number Conjecture.* Ann. Sci. École Norm. Sup. (4) **37** (2004), no. 5, 663–727.

[DT] Diamond, F., Taylor, R. *Lifting modular mod ℓ representations.* Duke Math. J., **74** (1994), 253–269.

[E] Edixhoven, B. *The weight in Serre's conjectures on modular forms.* Invent. Math. **109** (1992), 563–594.

[F] Fujiwara, K. *Deformation rings and Hecke algebras for totally real fields.* preprint.

[Fa] Faltings, G. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), no. 3, 349–366.

[G] Gross, B. H. *A tameness criterion for Galois representations associated to modular forms* $\bmod p$. Duke Math. J. **61** (1990), 445–517.

[H] Hida, H. *Congruences of cusp forms and special values of their zeta functions.* Invent. Math. **63** (1981), 225–261.

[HSBT] Harris, M., Shepherd-Barron, N., Taylor, R. *A family of Calabi-Yau varieties and potential automorphy.* preprint.

[I] Ihara, Y. *On modular curves over finite fields.* Proc. Intern. Coll. on discrete subgroups of Lie groups and application to moduli, Bombay, 1973, 161–202.

[K1] Kisin, M. *Moduli of finite flat group schemes and modularity.* to appear in Ann. of Math.

[K2] Kisin, M. *Crystalline representations and F-crystals.* Algebraic geometry and number theory, Progr. Math. **253**, Volume in honor of Drinfeld's 50th birthday, Birkhäuser, Boston (2006), 459–496.

[K3] Kisin, M. *Modularity for some geometric Galois representations.* L-functions and Galois representations (Durham 2004), 438–470.

[K5] Kisin, M. *Modularity of 2-adic Barsotti-Tate representations.* Current Developments in Mathematics 2005, 191-230.

[K6] Kisin, M. *The Fontaine-Mazur conjecture for* GL_2. preprint.

[Ka] Katz, N. *A result on modular forms in characteristic* p. Modular Functions of One Variable V, Springer LNM **601** (1976), 53–61.

[Kh1] Khare, C. *Serre's modularity conjecture: the level one case.* Duke Math. J. **134** (2006), 534–567.

[Kh2] Khare, C. *Serre's modularity conjecture: a survey of the level one case.* to appear in Proceedings of the LMS Durham conference L-functions and Galois representations (2005), eds. D. Burns, K.Buzzard, J. Nekovar.

[KW1] Khare, C., Wintenberger, J.-P. *On Serre's conjecture for 2-dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. to appear in Annals of Math.

[KW2] Khare, C., Wintenberger, J.-P. *Serre's modularity conjecture (I).* preprint.

[KW3] Khare, C., Wintenberger, J.-P. *Serre's modularity conjecture (II).* preprint.

[L] Lenstra, H.W. *Complete intersections and Gorenstein rings.* Elliptic Curves, Modular Forms, and Fermat's last Theorem (Hong Kong 1993), Internat. Press, Cambridge, MA, 1995, 99–109

[La] Langlands, R. *Base Change for* $\mathrm{GL}_2(2)$. Ann. of Math. Studies, Princeton University Press **96**, 1980.

[M1] Mazur, B. *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. No.**47** (1977), 33–186.

[M2] Mazur, B. *Rational isogenies of prime degree.* Invent. Math. **44** (1978), no. 2, 129–162.

[Me] Mennicke, J. *On Ihara's modular group.* Invent. Math. **4** (1967), 202–228.

[MR] Mazur, B., Ribet, K. *Two-dimensional representations in the arithmetic of modular curves.* Astérisque **196-197** (1991), 215–255.

[R1] Ribet, K. *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Invent. Math. **100** (1990), 241–280.

[R2] Ribet, K. *The ℓ-adic representations attached to an eigenforms with Nebentypus: a survey.* Modular Functions of One Variable V. Springer LNM **601** (1977), 17–52.

[R3] Ribet, K. *Congruence relations between modular forms.* Proc. Int. Cong. of Math. **17** (1983), 503–514.

[S1] 斎藤毅. Fermat 予想 1. 岩波書店, 2000.

[S2] 斎藤毅. Fermat 予想 2. 岩波書店, 2008.

[S3] Saito, T. *Modular forms and and p-adic Hodge theory.* Invent. Math. **129**(3) (1997), 607–620.

[S4] Saito, T. *Hilbert modular forms and and p-adic Hodge theory.* preprint.

[Se3] Serre, J.-P. *Arbres, Amalgames,* SL_2. Astérisque **46**, Société Mathématique de France, Paris, 1977

[Se4] Serre, J.-P. *La problème des groupes des congruences pour* SL_2. Ann. Math. **92** (1970), 489–527.

[Sc] Schoof, R. *Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only.* Compositio Math. **141** (2005), 847–868.

[Sh] Shimura, G. *The special values of the zeta functions associated with cusp forms.* Comm. Pure Appl. Math. **29** (1976), 783–804.

[SW1] Skinner, C., Wiles, A. *Residually reducible representations and modular forms.* Inst. Hautes Études Sci. Publ. Math., **89** (2000), 5–126.

[SW2] Skinner, C., Wiles, A. *Nearly ordinary deformations of irreducible residual representations.* Ann. Fac. Sci. Toulouse Math. (6) **10**(1) (2001), 185–215.

[SW3] Skinner, C., Wiles, A. *Base change and a problem of Serre.* Duke Math. J. **107**(1) (2001), 15–25.

[T1] Taylor, R. *On Galois representations associated to Hilbert modular forms.* Invent. Math. **98**(2) (1989), 265–280.

[T2] Taylor, R. *Remarks on a conjecture of Fontaine and Mazur.* J. Inst. Math. Jussieu, **1**(1) (2002), 125–143.

[T3] Taylor, R. *On the meromorphic continuation of degree two L-functions.* Documenta Math. Extra Volume: John Coates' Sixtieth Birthday (2006), 729–779.

[T4] Taylor, R. *Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations II.* preprint.

[Tu] Tunnell, J. *Artin's conjecture for representations of octahedral type.* Bull. A.M.S. **5** (1981), 173–175.

[TW] Taylor, R., Wiles, A. *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141**(3) (1995), 553–572.

[W1] Wiles, A. *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141**(3) (1995), 443–551.

[W2] Wiles, A. *On p-adic representations for totally real fields.* Ann. of Math. **123**(3) (1986), 407–456.

[W3] Wiles, A. *On ordinary λ-adic representations associated to modular forms.* Inv. Math. **94** (1988), 529–573.

[Y] 山下剛. Kisin の修正 Taylor-Wiles 系. 本報告集.