数理解析研究所講究録
1154巻 2000年 97-105

Mod p Galois 表現について (特に像が可解の場合)

北大理　田口雄一郎 (Yuichiro Taguchi)
都立大理　文賢淑 (Hyunsuk Moon)

次の問題を考える：

問題 F. 与えられた有限次代数体 K, 素数 p, 整数 $d \geq 1$, K の整 ideal N に対し、連続半単純表現

$$\rho : G_K \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$$

であって $N(\rho)|N$ なるものの同型類は有限個か？

(ここで G_K は K の絶対 Galois 群 $\mathrm{Gal}(\overline{K}/K)$, $\overline{\mathbb{F}}_p$ は p 元体 $\mathbb{F}_p$ の代数閉包、$N(\rho)$ は ρ の「p の外での Artin 導手」(下に説明) である。)

これに対し「像 $\mathrm{Im}(\rho)$ が可解なものに限れば有限個である」([14]) というのが本講演の主結果である。

以下 §1 ではこの様な問題を考えたくなる背景を、§2 ではこれまでに知られている結果を、§3 では主結果とその証明の概略を述べる。附録として多少関係しそうな仕事 ([4], [8], [1]) の超簡単な解説を付けた。

本論に入る前にここで Artin 導手 $N(\rho)$ の定義を述べてしまおう (cf. e.g. [18], §1.2)。V を有限次元 $\overline{\mathbb{F}}_p$-ベクトル空間とする。表現[1] $\rho : G_K \to \mathrm{GL}_{\overline{\mathbb{F}}_p}(V)$ が与えられたとき、

$$N(\rho) := \prod_{\mathfrak{q} \nmid p} \mathfrak{q}^{n_{\mathfrak{q}}(\rho)}$$

の形で定義する (ここに $\mathfrak{q}$ は p と素な K の素 ideal を走る) のだが、指数の $n_{\mathfrak{q}}(\rho)$ は次の様に定義する： ρ が経由する G_K の有限商 $\mathrm{Gal}(L/K)$ を取り、$G_{\mathfrak{q},i}$ をその $\mathfrak{q}$ (の上にある L の素 ideal) に関する第 i 分岐群とし、

$$n_{\mathfrak{q}}(\rho) := \sum_{i \geq 0} \frac{1}{(G_{\mathfrak{q},0} : G_{\mathfrak{q},i})} \dim_{\overline{\mathbb{F}}_p}(V/V^{G_{\mathfrak{q},i}})$$

(V^G は V の G-固定部分)。すると $n_{\mathfrak{q}}(\rho)$ は非負整数で、
「$n_{\mathfrak{q}}(\rho) > 0 \iff \rho$ は $\mathfrak{q}$ で分岐」である。

1. 背景. 発端は Serre の予想 ([16], [18]) である。

Serre 予想. 任意の 2 次元既約表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ であって odd (i.e. det(複素共役) $= -1$) なものに対しある $\overline{\mathbb{F}}_p$-係数の eigenform f of level $N(\rho)$, weight $k(\rho)$ が存在して $\rho \simeq \rho_f$ ($= f$ に伴う表現) となる。

[1] 以下「表現」と言ったら「連続表現」のこととする。

ここで $N(\rho)$ は上に定義したものだが、$k(\rho)$ は $\rho|_{(p\text{ での惰性群})}$ から決まるある整数 ≥ 1 で、

$$(*) \qquad k(\rho) \leq p^2 - 1$$

を満たす。

これは大変強い予想で、例えば次のことが従う：

(1) 上の様な $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ は標数 0 の表現 $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ に持上がる。

(2) 任意の $N \geq 1$ に対し、上の様な $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ であって $N(\rho)|N$ なるものの同型類は有限個しか存在しない。

ここで (2) の有限性には (*) が利いていることに注意されたい。

これらの問題はより一般の Galois 表現 $\rho : G_K \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ に対して考えられる。(2) を一般化したのが冒頭に掲げた問題である。(1) を一般化した問題は、Mazur が Galois 表現の変形理論 ([12]) を定式化したときから既に基本的な問題として存在していたわけだが、一応書いておけば：

問題 L. 表現 $\rho : G_K \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ が与えられたとき、ρ はいつ $\tilde{\rho} : G_K \to \mathrm{GL}_d(\overline{\mathbb{Q}}_p)$ に持上がるか？ 持上がるとしたら、どれくらいの持上げがあるか？ その普遍変形環は存在するか？ その構造は？ さらに $\tilde{\rho}$ は「よい」もの (e.g. Fontaine-Mazur の意味の "geometric" (cf. [6], [22])) に取れるか？

… などなど。

この方面での研究はたくさんなされているが、ここでは Ramakrishna ([15]) の結果「$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ は "多くの場合" (even でも) $\tilde{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(W(\mathbb{F}_q))$ に持上がり、しかも odd のときは geometric に持上がる」に言及するに止めておく。

これらの問題と他の予想との論理的関係を少し見てみよう。

(1) $d = 2$ のとき、問題 L の「$\tilde{\rho}$ は geometric に取れる」が正しければ

$$\text{Fontaine-Mazur の保型性予想} \implies \text{Serre 予想.}$$

(2) 問題 L の「$\tilde{\rho}$ は geometric に取れる」が正しく、かつ (*) に相当する適当な条件を仮定すれば

$$\text{Fontaine-Mazur の有限性予想} \implies \text{問題 F の有限性が成立.}$$

(3) (これは論理的な関係ではないが) 問題 F は「G_K の p 進表現たちの間には合同関係がたくさんあるか」という問題と関連している、と言えるだろう。

問題 F に関する注意をいくつか述べる。

(1) 「半単純」という仮定は必要 (例： 無限個の非同型な表現 $\rho : (\mathbb{Z}/p\mathbb{Z})^2 \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$, $\rho \sim \left(\begin{smallmatrix} 1 & * \\ & 1 \end{smallmatrix}\right)$, がある)。

(2) $\overline{\mathbb{F}}_p$ の代わりに有限体 $\mathbb{F}_q$ を使えば有限性は自明 (Hermite-Minkowski の定理 (S の外不分岐かつ次数 $\leq n$ なる拡大 L/K は有限個) による)。

(3) p の外では N で導手 $N(\rho)$ を押さえないと有限性は成り立たない (しかし p の上では導手を押さえなくてよい — 勝手におさまってしまうから (§3 の「証明の概略」を参照))。

(4) L/K が有限次拡大のとき、(L, p, d, N) に対する有限性は $(K, p, [L : K]d, N')$ (for some N') に対する有限性に帰する (誘導表現を使う)。

(5) K が $\mathbb{Q}$ 上有限次でないときは有限性は必ずしも成立しない。

2. 知られている結果. この節では問題 F に関して知られている結果を述べる。

(1) $d=1$: 類体論により Yes.

(2) $d=2$, $K=\mathbb{Q}$, $N=1$: この場合は Serre の予想との関係で研究されている。まず Tate ([23]) が 1973 年に、Serre 予想の原始的な形についての Serre からの手紙に対し、その返事として、$p=2$, $N=1$ のときには予想が正しいことを「odd かつ既約な ρ は存在しない」という形で証明した。これは $\mathrm{Ker}(\rho)$ に対応する体の判別式を、類体論により上から、Minkowski bound により下から、それぞれ評価して矛盾を導く、という方針である。Serre (『全集』第 III 巻 p. 710) はその直後、Minkowski bound の代わりに Odlyzko bound ([17]) を使えば $p=3$ でも成り立つことを注意した。Brueggeman ([5]) は同様の方法で $p=5$ でも、GRH (= Generalized Riemann Hypothesis) の下、予想が正しいことを示した。

有限性だけなら、その他、次の各場合に知られている ([13]):

$p=5$ で ρ は総実 (i.e. $\mathrm{Ker}(\rho)$ に対応する体が総実 i.e. ρ は無限素点でも不分岐);

$p=7,11,13$ で ρ は総実、かつ GRH を仮定。

(3) $d>2$, $K=\mathbb{Q}$, $N=1$: このとき $p=2,3$ で $d\leq 8$ のいくつかの場合に (2) と同様の方法で有限性が証明されている ([13]):

$$\begin{array}{lll} p=2 & d\leq 4 & \text{(総実)} \\ & d\leq 4 & \text{(GRH)} \\ & d\leq 8 & \text{(総実、GRH)} \\ p=3 & d\leq 4 & \text{(総実、GRH)} \end{array}$$

(4) 古典類似： Anderson-Blasius-Coleman-Zettler ([1]) は次を証明している (R. Greenberg も独立に証明したそうである)。これは問題 F の「古典類似」と見做せる。

定理. 与えられた $d\geq 1$ と N に対し、表現 $\rho: G_K \to \mathrm{GL}_d(\mathbb{C})$ であって $N(\rho)|N$ なるものの同型類は有限個しか存在しない。

(ここの導手 $N(\rho)$ は全ての素点を含む (普通の) Artin 導手である。) この定理だけなら $\mathrm{GL}_d(\mathbb{C})$ の有限部分群の構造についての Jordan の定理 (e.g. [21]) を介して Hermite-Minkowski の定理と類体論 (ideal 類群の有限性) とを組合わせることにより得られるが、[1] ではもう少し強いことが証明されている (附録 C 参照)。

(5) その他の示唆的な仕事：ここでは

(A) A. Ash による、群の cohomology 群の中の Hecke eigenclass と mod p 表現とを結びつける試み ([2], [3], [4]) と

(B) B. Gross による「代数的保型形式」から Galois 表現を構成しようというアプローチ ([8])

があることに注意しておく (附録 A, B 参照)。どちらの場合も Hecke 側の有限性が Galois 側の有限性を (少なくとも部分的に) 示唆するはずである。

3. 像が可解の場合.

定理. 与えられた K, p, d, N に対し、半単純表現 $\rho : G_K \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ であって $N(\rho)|N$ かつ像 $\mathrm{Im}(\rho)$ が可解であるものの同型類は有限個しか存在しない。

さらに、一般の場合の有限性は次の statement に帰着される：半単純表現 $\rho : G_K \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ であって $N(\rho)|N$ かつ像 $\mathrm{Im}(\rho)$ が標数 p の Lie 型有限単純群であるものの同型類は有限個しか存在しない。

註. これの函数体$_{/\text{有限体}}$ 版もある (但し定数体の拡大の無い (または bounded な) ρ だけに限る)。

(証明の概略)　鍵は Hermite-Minkowski の定理、類体論、Larsen-Pink の定理の三つである。まづ $\mathrm{Ker}(\rho)$ に対応して出て来る体拡大 L/K の可能性が有限であることを言えばよいことに注意しておく。Larsen-Pink の定理 ([11]) によれば、d のみに依存するある定数 J_d が存在して、任意の有限部分群 $G \subset \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ は正規部分群 G_i による filtration

$$G \supset G_1 \supset G_2 \supset G_3$$

を持ち

(0) $(G : G_1) \leq J_d$,

(1) $G_1/G_2 = \prod$(標数 p の Lie 型有限単純群),

(2) G_2/G_3 は位数が p と素な Abel 群,

(3) G_3 は p 群,

となる。これを $G = \mathrm{Im}(\rho) = \mathrm{Gal}(L/K)$ に適用する。$\mathrm{Im}(\rho)$ が可解ならば (1) の G_1/G_2 の部分が存在しないことに注意されたい。(0) ～ (3) の各段階について、対応する体拡大の可能性が有限であることを言えばよいのだが、
(0) については Hermite-Minkowski の定理により、
(2) については類体論により、
(3) については、$G_3 \subset \{$ 対角成分が 1 の上三角行列 $\}$ だから G_3 は長さ $\leq \lceil \log_2 d \rceil$ の filtration であって各 gr が elementary p 群となるものが入り ([13], §3 の冒頭)、elementary p 拡大については p での導手が上から評価でき ([13], 補題 2.1 の証明)、従って再び類体論により有限性が従う。

最後に関連する問題を少し述べよう。大域体 K と、K の素点の有限集合 S とを固定する。このとき S の外不分岐な有限次 Galois 拡大 L/K であって $\mathrm{Gal}(L/K)$ が単純群 (resp. Lie 型有限単純群)(resp. 固定された標数の Lie 型有限単純群) であるものは有限個か？ K が函数体$_{/\text{有限体}}$ のときは Frey-Kani-Völklein ([7]) が (ある条件を満たす K に対し) 無限個の不分岐 Galois 拡大 L_i/K であって $\mathrm{Gal}(L_i/K) \simeq \mathrm{PSL}(d, \mathbb{F}_{p_i})$ なるものを構成している。この例では Lie 型有限単純群の標数 p_i が動いてしまうが、標数を固定して、例えば $\mathrm{Gal}(L_i/K) \simeq \mathrm{PSL}(d, \mathbb{F}_{p^{n_i}})$ なる無限個の不分岐 Galois 拡大 L_i/K の例は作れるだろうか？

ちなみに「$\mathrm{Gal}(S$ の外不分岐最大拡大$/K)$ は (位相的に) 有限生成か？」という問題 ([20]) があり、この群が有限個の Frobenius 共役類 で生成されることは知られている ([10])。$\mathrm{Gal}(L_i/K)$ が皆同型な S の外不分岐 Galois 拡大 L_i/K が無限個あれば上の群は無限生成だが、$\mathrm{Gal}(L_i/K)$ たちがほとんど全て互いに非同型な有限単純群ならば $\prod_i \mathrm{Gal}(L_i/K)$ は有限生成である。

附録 A. Ash-Sinnott の予想. 次の形の正方行列を「Γ_0型」と呼ぶことにする：

$$\begin{pmatrix} * & * & \cdots & * \\ 0 & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & * & \cdots & * \end{pmatrix}$$

p を素数とし、N を p と素な自然数とする。記号を次の様に定める：

$\Gamma_0(N) = \{\gamma \in \mathrm{SL}_d(\mathbb{Z});\ \gamma(\mathrm{mod}\ N)$ は Γ_0型 $\}$

$S_N = \{\gamma \in \mathrm{M}_d(\mathbb{Z});\ \det\gamma > 0,\ (\det\gamma, N) = 1$ かつ $\gamma(\mathrm{mod}\ N)$ は Γ_0型 $\}$

$\mathcal{H}(N) = \overline{\mathbb{F}}_p[\Gamma_0(N)\backslash S_N/\Gamma_0(N)]$

$D(\ell,k) =$ 対角行列 $(1,\cdots,1,\ell,\cdots,\ell)$ (1 が k個、ℓ が $(d-k)$ 個)

$T(\ell,k) = D(\ell,k)$ の類 $= \Gamma_0(N)D(\ell,k)\Gamma_0(N) \in \mathcal{H}(N)$

すると S_N は半群であり $\mathcal{H}(N)$ は可換環になる。$\mathcal{H}(N)$ は $T(\ell,k)$ $(0 \le k \le d,\ \ell$: 素数 $\nmid N)$ たちで生成される。

H を $\mathcal{H}(pN)$-加群とする。$\beta \in H$ は eigen 即ち全ての $0 \le k \le d$ と 素数 $\ell \nmid N$ に対し

$$T(\ell,k)\beta = a(\ell,k)\beta \qquad \text{for some } a(\ell,k) \in \overline{\mathbb{F}}_p$$

であるとする。このとき、表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ が β に付随するとは、ρ は pN の外不分岐かつ

$$\sum_{k=0}^{d}(-1)^k \ell^{k(k-1)/2} a(\ell,k)X^k = \det(1-\rho(\mathrm{Frob}_\ell)X) \qquad \text{for all } \ell \nmid pN$$

なること、と定義する。

V を $\overline{\mathbb{F}}_p[\mathrm{GL}_d(\mathbb{Z}/N\mathbb{Z})]$-加群であって $\overline{\mathbb{F}}_p$上有限次元であるものとする (reduction mod N によりこれを$\overline{\mathbb{F}}_p[S_N]$-加群とも思う)。Cohomology 群 $H^*(\Gamma_0(N),V)$ は $\mathcal{H}(pN)$-加群になる (以下で cohomology の次元 * は特定しない)。

予想 ([2][2]). 任意の $\mathcal{H}(pN)$-eigenclass $\beta \in H^*(\Gamma_0(N),V)$ に対し、これに付随する表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ が存在するであろう。

これに対し [4] では「逆向き」の予想を述べている。まず弱い形として：

予想 ([4], 弱形). 任意の半単純表現 $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ であって pN の外不分岐かつ

$$\rho(\text{複素共役}) \text{ の固有値} = \pm(1,-1,1,-1,\cdots)$$

であるものに対し

N': 自然数で $\{N'$ の素因子 $\} \subset \{pN$ の素因子 $\}$ なるもの

V: $\overline{\mathbb{F}}_p[S_{pN'}(\mathrm{mod}\ pN')]$-加群

$\beta \in H^*(\Gamma_0(N'),V)$: $\mathcal{H}(pN')$-eigenclass

が存在して ρ は β に付随する表現となる。

---

[2] この論文にはこれより少し強い形で述べられている。

さらに V が (Serre の所謂) niveau 1 の場合には level N' や "weight" V として何が取れるべきかについても予想がある。それを次に述べる。まず N' は簡単で、ρ の Artin 導手である；$N' = N(\rho)$.

また、$\varepsilon(\rho)$ を Serre 予想の場合と同様に定義する。即ち $\det\rho = \varepsilon\omega^{k-1}$ (ω は円分指標 mod p) と書いたときの $\varepsilon : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^{\times}$ (これは p で不分岐、$(\mathbb{Z}/N(\rho)\mathbb{Z})^{\times}$ を経由する)。

V の選び方はやや複雑だが、次にこれを述べよう。整数列 $(b_1, \cdots, b_d)$ が (p に関し) good とは $0 \le b_1 - b_2 \le p-1, \cdots, 0 \le b_{d-1} - b_d \le p-1, 0 \le b_d \le p-2$ であること。各 good d-tuple $(b_1, \cdots, b_d)$ に対し、既約 $\mathrm{GL}_d(\mathbb{F}_p)$-加群 $F(b_1, \cdots, b_d)$ なるものが存在する。これは $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$ の双対 Weyl 加群であって最高 weight が $(b_1, \cdots, b_d)$ であるものの unique な単純部分加群 (の $\mathrm{GL}_d(\mathbb{F}_p)$ への制限) である。$\overline{\mathbb{F}}_p$上の既約 $\mathrm{GL}_d(\mathbb{F}_p)$-加群たちはこれらで "parametrize" される。ちなみに $g = b_1 + pb_2 + \cdots + p^{d-1}b_d$ とおくと $F(b_1, \cdots, b_d)$ は $\mathrm{GL}_d(\mathbb{F}_p)$-加群として $\mathrm{Sym}^g(\overline{\mathbb{F}}_p^{\oplus d})$ に埋め込まれる。

整数列 $(a_1, \cdots, a_d)$ に対し、$(a_1, \cdots, a_d)'$ により $(a_1, \cdots, a_d)$ と mod $(p-1)$ で合同な good d-tuple を表す (必ずしも unique ではない)。

一般に指標 $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \overline{\mathbb{F}}_p^{\times}$ を $S_{pN} \to (\mathbb{Z}/N\mathbb{Z})^{\times}$; $\left(\begin{smallmatrix} a & * \\ * & \end{smallmatrix}\right) \mapsto a(\mathrm{mod}N)$ で引戻して $\varepsilon : S_{pN} \to \overline{\mathbb{F}}_p^{\times}$ とも思うことにする。$\overline{\mathbb{F}}_p(\varepsilon) := (\overline{\mathbb{F}}_p$ with S_{pN}-action via $\varepsilon)$ とおく。$\mathrm{GL}_d(\mathbb{F}_p)$-加群 V に対し

$$V(\varepsilon) \ := \ V \otimes_{\overline{\mathbb{F}}_p} \overline{\mathbb{F}}_p(\varepsilon).$$

とおく。これは S_{pN}-加群である (左には mod p で、右には mod N で作用する)。

ρ が可約で $\rho = \sigma_1 \oplus \cdots \oplus \sigma_m$ のとき、$\dim\sigma_i = d_i$ とすると、$\mathrm{Im}(\rho)$ は GL_d の $(d_1, \cdots, d_m)$ 型 Levi 部分群 L に含まれると仮定してよい。

ρ が strict parity condition を満たす とは、ρ(複素共役) が $L(\overline{\mathbb{F}}_p)$ の中で ±対角行列 $(1, -1, 1, -1, \cdots)$ と共役であること、と定義する。

予想 ([4], 強形). $p \ge 3$ とする。$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ を半単純表現、L を上の様な Levi 部分群とし、ρ は strict parity condition を満たすと仮定する。さらに$\rho|_p$ での惰性群 は niveau 1 即ち $L(\overline{\mathbb{F}}_p)$ の中で

$$\begin{pmatrix} \omega^{a_1} & * & * \\ & \ddots & * \\ & & \omega^{a_d} \end{pmatrix} \qquad \text{for some } a_i \in \mathbb{Z}$$

の形の表現と同値であると仮定する ($\omega : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ は円分指標 mod p). このとき上の予想 (弱形) に於ける N', V として

$$N' \ = \ N(\rho),$$

$$V \ = \ F(a_1 - (d-1), a_2 - (d-2), \cdots, a_d)'(\varepsilon(\rho))$$

と取れる。(Good d-tuple $(*, \cdots, *)'$ の取り方に曖昧さがあるときは「都合のよい方」を取る。)

附録 B. Gross の予想. Serre は Collège de France での講義 (1987/88) 及び Tate への手紙 [19] で次を示した：

定理. D を $\mathbb{Q}$ 上の四元数環で $\{p,\infty\}$ で分岐するものとし、$D_{\mathbb{A}}^{\times}$ をその乗法群 ($\mathbb{Q}$ 上の代数群) の adèle 化とする。このとき、Katz の mod p modular eigenform から来る Hecke 固有値列 $(a_\ell)_{\ell\neq p}$ $(a_\ell \in \overline{\mathbb{F}}_p)$ と、局所定数函数 $f : D_{\mathbb{Q}}^{\times}\backslash D_{\mathbb{A}}^{\times} \to \overline{\mathbb{F}}_p$ から来る Hecke 固有値列 $(a_\ell)_{\ell\neq p}$ とは 1 対 1 に対応する。(前者の保型形式は全ての weight と tame level を考えている。)

これの証明を見ると §1 で出て来た条件 (*) $k(\rho) \leq p^2-1$ も自然に解釈できる。

今のところ後者つまり $D_{\mathbb{A}}^{\times}$ 上の保型形式から Galois 表現を直接構成することはなされていない様だが、Gross ([8]) は (1) $D_{\mathbb{A}}^{\times}$ 上の保型形式の「無限素点での解析が出て来ない」という状況を一般化し、(2) その場合の eigenform から Galois 表現が構成できるはずだ、という予想を立てている。これを簡単に記しておく。

G を $\mathbb{Q}$ 上の連結代数群で、次の同値な条件を満たすものとする：

(1) 全ての数論的部分群 $\Gamma \subset G(\mathbb{Q})$ は有限；

(2) $G(\mathbb{Q})$ は $G(\widehat{\mathbb{Q}})$ の離散的部分群 (ここに $\widehat{\mathbb{Q}} = \widehat{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Q}$ とおいた)；

(3) $G(\mathbb{Q})$ は $G(\widehat{\mathbb{Q}})$ の離散的部分群であり、かつ商 $G(\mathbb{Q})\backslash G(\widehat{\mathbb{Q}})$ は compact.

$\mathbb{A}$ を $\mathbb{Q}$ の adèle 環とする。G の $\mathbb{Q}$ 上の既約表現 V と、$G(\widehat{\mathbb{Q}})$ の開 compact 部分群 K に対し

$$\begin{aligned} M(V) &= \{f : G(\mathbb{A}) \to V;\ f \text{ は局所定数 かつ } f(\gamma g) = \gamma f(g) \text{ for } \gamma \in G(\mathbb{Q})\}, \\ M(V,K) &= \{f : G(\mathbb{A})/(G(\mathbb{R})_+ \times K) \to V;\ f(\gamma g) = \gamma f(g) \text{ for } \gamma \in G(\mathbb{Q})\}, \end{aligned}$$

とおく (ここに $G(\mathbb{R})_+$ は $G(\mathbb{R})$ の連結成分)。$M(V,K)$ には自然な Hecke 環の作用があり、$M(V)$ は $M(V,K)$ たちの順極限になる。ちなみに $G(\mathbb{Q})\backslash G(\mathbb{A})/(G(\mathbb{R})_+ \times K)$ は有限集合である。

代数群 G の root datum の「最小分解体」を k とする (これは $\mathbb{Q}$ の有限次 Galois 拡大)。$\widehat{G}$ を G の双対群として、G の L-群 ${}^LG$ を

$$\begin{aligned} {}^LG &:= \widehat{G} \rtimes \mathrm{Gal}(k/\mathbb{Q}) \\ &(\text{群演算は } (g,\sigma)\cdot(g',\sigma') = (g\sigma(g'),\sigma\sigma')) \end{aligned}$$

と定義する (これを $\mathbb{Z}$ 上の群 scheme と見る)。

「${}^LG$ の半単純共役類を分類する代数多様体$_{/\mathbb{Q}}$」$\mathrm{Cl}({}^LG)$ が考えられるが、これはさらに$\sigma \in \mathrm{Gal}(k/\mathbb{Q})$ ごとに分けられる；

$$\mathrm{Cl}({}^LG) = \coprod_{\sigma\in\mathrm{Gal}(k/\mathbb{Q})} \mathrm{Cl}_\sigma.$$

Eigenform があると各素数 ℓ に対して Hecke 固有値 a_ℓ がある様に、$M(V,K)$ の単純 Hecke 部分加群 N があると k の (ほとんど全ての) 素点 λ ごとに「局所径数」$h_\lambda(N) \in \mathrm{Cl}({}^LG)(E)$ が定義できる (ここに $E = (\mathrm{End}_{\mathrm{Hecke}}(N)$ の中心) — これは CM 体になる)。

予想 ([8]). V, N について適当な仮定[3] をおく。このとき、各素数 p に対し表現

$$\rho :\ G_{\mathbb{Q}} \to {}^LG(E \otimes_{\mathbb{Q}} \mathbb{Q}_p)$$

[3] 詳細は略させていただきます。

であって次を満たすものが存在する：

(1) ρ(複素共役) $\equiv h_\infty(N)$ in $\mathrm{Cl}_\tau(E\otimes_{\mathbb{Q}}\mathbb{Q}_p)$
(ここに $\tau=$(複素共役) $\in \mathrm{Gal}(k/\mathbb{Q})$);

(2) $\ell\neq p$ かつ ℓ は k で不分岐かつ ℓ は「level を割らない」とき、ρ は ℓ で不分岐。さらに $G_{\mathbb{Q}}\to\mathrm{Gal}(k/\mathbb{Q})$ に於いて $s_\lambda\mapsto \mathrm{Frob}_\lambda$ とすると $\rho(s_\lambda)$ は ${}^LG(E\otimes_{\mathbb{Q}}\mathbb{Q}_p)$ の半単純元であり、$\rho(s_\lambda)\equiv h_\lambda(N)$ in $\mathrm{Cl}_{\mathrm{Frob}_\lambda}(E\otimes_{\mathbb{Q}}\mathbb{Q}_p)$.

さらに、上で除外した素点での分解群に ρ を制限したときの様子についても予想がある。

附録 C. Anderson-Blasius-Coleman-Zettler の定理. $W_{\mathbb{Q}}$ (resp. $W_{\mathbb{R}}$) により $\mathbb{Q}$ (resp. $\mathbb{R}$) の Weil 群を表す。$W_{\mathbb{Q}}$ の表現 $\rho: W_{\mathbb{Q}}\to \mathrm{GL}_d(\mathbb{C})$ の infinity type とはρ の $W_{\mathbb{R}}$ への制限の同型類 $[\rho|_{W_{\mathbb{R}}}]$ のことである。

定理 ([1]). 与えられた d, N 及び infinity type $[\rho_\infty]$ に対し、表現 $\rho: W_{\mathbb{Q}}\to\mathrm{GL}_d(\mathbb{C})$ であって $N(\rho)|N$ かつ ρ の infinity type $=[\rho_\infty]$ なるものの同型類は有限個しか存在しない。

これの証明のポイントは次の「Jordan の定理の Lie 群版」を示すことである：

定理. K を連結 compact Lie 群とする。このときある定数 J が存在して次が成り立つ：K の閉部分群 G は potentially abelian ならば指数 $\leq J$ なる正規 abelian 部分群を持つ。(ここで G が potentially abelian とは、単位元の連結成分 G° が abelian かつ指数 $(G:G^\circ)$ が有限であること。)

彼らの動機は、保型表現側には Harish-Chandra の有限性定理 ([9], 定理 1) なるものがあるのでその Galois 対応物を考えた、ということらしい。($\mathbb{C}$ 上でなく) $\overline{\mathbb{Q}}_p$上での Galois 対応物は Fontaine-Mazur の有限性予想だと言えるだろう。

References

1. G. Anderson, D. Blasius, R. Coleman and G. Zettler, *On representations of the Weil group with bounded conductor*, Forum Math. **6** (1994), 537-545.
2. A. Ash, *Galois representations attached to mod p cohomology of* $\mathrm{GL}(n,\mathbb{Z})$, Duke Math. J. **65** (1992), 235–255.
3. A. Ash, *Monomial Galois representations and Hecke eigenclasses in the mod p cohomology of* $\mathrm{GL}((p-1),\mathbb{Z})$, Math. Ann. (1999), 263–280.
4. A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of* $\mathrm{GL}(n,\mathbb{Z})$, to appear in Duke Math. J.
5. S. Brueggeman, *The nonexistence of certain Galois extensions unramified outside 5*, J. Number Theory **75** (1999), 47–52.
6. J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, Proc. Conf. on elliptic curves and modular forms, Hong Kong, 1993, International Press, 1995, pp. 41–78 (第 2 版では pp. 190–227).
7. G. Frey, E. Kani and H. Völklein, *Curves with infinite K-rational geometric fundamental group*, Aspects of Galois Theory (H. Völklein, P. Müller, D. Habater and J.G. Thompson, eds.), vol. 256, London Math. Soc. Lect. Note Ser., pp. 85–118.
8. B. Gross, *Algebraic modular forms*, Israel J. Math. **113** (1999), 61–93.

9. Harish-Chandra, *Automorphic forms on semisimple Lie groups*, Lect. Notes in Math., vol. 62, Springer-Verlag, 1968.
10. Y. Ihara, *How many primes decompose completely in an infinite unramified Galois extension of a global field?*, J. Math. Soc. Japan **35** (1983), 693–709.
11. M.J. Larsen and R. Pink, *Finite subgroups of algebraic groups*, preprint (1998).
12. B. Mazur, *Deforming Galois representations*, Galois groups over $\mathbb{Q}$ (Y. Ihara, K. Ribet and J.-P. Serre, eds.), Springer-Verlag, 1989.
13. H. Moon, *Finiteness results on certain mod p Galois representations*, to appear in J. Number Theory.
14. H. Moon and Y. Taguchi, *Mod p Galois representations of solvable image*, to appear in Proc. A.M.S.
15. R. Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, preprint (1999).
16. J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo ℓ*, Journées arith. Bordeaux, Astérisque **24-25** (1975), 109–117.
17. J.-P. Serre, *Minorations de discriminants*, Œuvres Vol. III, Springer-Verlag, 1986, pp. 240–243.
18. J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), 179–230.
19. J.-P. Serre, *Two letters on quaternions and modular forms (mod p)*, Israel J. Math. **95** (1996), 281–299.
20. I. Shafarevich, *Algebraic number fields*, Proc. Int. Congr. Math., Stockholm 1962, (also in: 『Shafarevich 全集』 pp. 283–294).
21. D.A. Suprunenko, *Matrix Groups*, A.M.S., Providence, 1976.
22. 田口雄一郎, *Fontaine-Mazur* 予想の紹介,『代数的整数論とその周辺』(1998), 数理解析研究所講究録, vol. 1097, 1999, pp. 37–49.
23. J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside 2*, Contemp. Math. **174** (1994), 153–156.

moon@math.sci.hokudai.ac.jp
taguchi@math.sci.hokudai.ac.jp