On congruence of Galois representations of number fields

小関 祥康* (京都大学)

概 要

(代数体の) 二つの ℓ 進 Galois 表現の法 ℓ 表現が同型であるときに, 元の Galois 表現がある分解群に制限したときに同型になるかという問題に関して分かったことを記す. 応用の一つとして, 保型形式の Fourier 係数が法 ℓ でとある形をすることはありえないという類の結果についても述べる. なお, 本稿の内容は九州大学の田口雄一郎先生との共同研究である (cf. [2]).

本稿は 2013 年に開催された「第 8 回福岡数論研究集会」に於ける筆者の講演を基に書かれたものである. 講演の機会を与えていただいたオーガナイザーの方々に厚く感謝御礼申し上げたい.

1 はじめに

小学校で学ぶ算数は特に, 日常生活に直接密接したものが多い. その内容の一つである割り算と余りについて勉強したことのない人は, 少なくともこの報告集を読んでいる方の中にはいないと思うし, 実際に日常生活を営んでいく中で割り算と余りを考えるという状況は, 特に珍しいことでもないと思う. 例えばなにかの飲み会の幹事等を務めることとなった場合, 支払うべき金額が書かれた紙とにらみあいながら「この金額を〇人で支払うとして, 一人〇〇円だとすると〇〇円余るから $\cdots$」といった具合に余りの考えを用いるように, さりげなく日常生活に紛れ込んで「余り」は現れてくる. そんな風に身近で簡単な余りの概念だが, これがなかなかバカにできない. 整数論においては特に重宝されて扱われているものなのである. 一例として, 余りを考えると苦もなく解けるような整数問題を挙げてみよう.

問題 1. x, y に関する方程式 $x^2 - 3y^2 = 2$ は整数解を持つか.

答えは「持たない」である. 解き方はいろいろあると思うが, この問を整数の余りに着目した解き方で解いてみよう. とはいっても特に難しい話ではなく, 方程式が解を持つと仮定したときに, 両辺を 3 で割った余りを考えれば矛盾が導かれることが分かる. 実際, 左辺は 3 で割った余りが 0 か 1 にしかならないからである. この解き方は, $x^2 - 3y^2 = 2$ の図形を xy 平面に描いて図形をじっと眺めるよりも, はるかに簡単であるように思う (そもそもその方法で解けるかどうか筆者は知らないが). さて, ここで用いた解法は「$x^2 - 3y^2 = 2$ に関するある余りを考えることで本来の $x^2 - 3y^2 = 2$ そのものの性質を知る」という考え方に基づいたものとなっているといえる. つまり「ものの余りの計算から割る前のものの性質を知る」という手順を行ったのだと言えるだろう. こういった考え方を延長したものが本稿の話となる.

さて, もう少し直接的に本題に関連したことを述べていこう. まずは中学生 $\cdots$ あるいは説明の仕方次第では小学生でも分かる (かもしれない) ような, 整数に関連した次の簡単な性質を考えてみる.

*本研究は科学研究費補助金 (No. 25·173) による支援を受けております.

性質 2. c を十分大きい整数とする．このとき, 次が成り立つ: c に比べて十分小さい正の整数 a, b が $a \equiv b \bmod c$ を満たすならば $a = b$ である．

上に出てくる「c に比べて十分小さい」に関しても, どの程度小さければ良いのかということに関する正確な結論を得ることは何も難しくない[1]．このような性質は, 整数を代数的整数に変換しても適当な解釈のもとで成り立っている．先ほどの言葉を使えば性質 2 は「ものの余りの計算から割る前のものの性質を知る」ということを体現しているといえる (簡単な事実に対して随分と大げさな言い回しではあるが)．今回の研究における主結果を一言で大雑把に言えば, こういった性質の Galois 表現類似を考えたということである．もう少し具体的な問題設定は次のようなものであり, それを念頭において研究を進めた結果が今回の主結果である．

問題 3. K を代数体, $E/\mathbb{Q}$ を (無限次も許した) 代数拡大, $\mathbb{P}$ を Galois 表現に関する何らかの性質とする．このとき, 次の性質を満たすような定数 C が存在するといえるか:

> **性質:** 任意の素数 $\ell > C$ と ℓ 上の E の素点 λ に対し, 次が成り立つ: $\mathbb{P}$ を満たす $\mathrm{Gal}(\overline{K}/K)$ の E_λ 進ガロア表現 V, V' に対し, $V \equiv_{\mathrm{ss}} V'$ ならば $V \simeq_{\mathrm{ss}} V'$. (ここで, $V \simeq_{\mathrm{ss}} V'$ (resp. $V \equiv_{\mathrm{ss}} V'$) とは, V, V' (resp. V, V' の剰余表現) の半単純化が同型であることを意味する.)

本研究を始めるきっかけとなった問題は, 「Rasmussen-Tamagawa 予想」と呼ばれる特別な性質を持つ代数体上のアーベル多様体の個数の有限性に関する予想である (cf. [3])．これは $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ の副 ℓ 基本群に付随する有理数体の絶対 Galois 群の外 Galois 表現の定義体に関連した「伊原問題」を背景として現れた予想である[2]．この予想はここ最近, 数名の研究者によっていろいろな結果が得られてきている．その結果の一つとして「至る所半安定還元を持つ」という条件の下で既に解決されているわけだが (cf. [4], 一般化: [1]), その際の証明において, 上記の性質 2 に関する事柄が大きな役割を果たしている．そこで, その手法を改良できれば条件無しの一般の場合における Rasmussen-Tamagawa 予想が解けるのではないか $\cdots$ という期待を持ったことが, 本研究を行ってみることになった簡単な流れとなっている．結論から先に述べると, 問題はそう単純な話ではなく, 今回の研究結果からは残念なことに Rasmussen-Tamagawa 予想に対して大きな進展を得ることはできなかった．その代わり, 代数体のエタールコホモロジーや保系形式の Fourier 係数についての合同等の整数論で重要ないくつかの対象に関する興味深い結果を得ることができた．Fourier 係数に関する方の結果は研究を始めた当時にはそのようなことが分かるとは私は全く思ってもいなかったので, 共同研究者の田口先生から「応用としてこういったことが分かるのではないか」という話を最初に聞いた際には驚いた記憶がある．

記号. 本稿では, 特に断らない限り次の記号を用いることとする:

- ℓ : 素数.
- 体 F とその素点 w に対して, F_w : F の v での完備化, k_w : F の w での剰余体.
- $\mathcal{O}_F$: 体 F の整数環 (定義される場合).
- 基礎体に関する記号

[1] 読者にお任せする．

[2] Rasmussen-Tamagawa 予想が解けたからといって伊原問題に何らかの直接的なアプローチが得られるわけではないように思う．

- K : 代数体 (:= $\mathbb{Q}$ の有限次拡大体),
- $u \mid \ell,\ v \nmid \ell$: K の素点,
- $G_K \supset G_u \supset I_u$: 順に K の絶対 Galois 群, u での分解群, 惰性群. $G_v,\ I_v$ も同様,
- Frob_v:v の代数的 Frobenius,
- q_v : v の剰余体の位数,
- $V_u,\ V_v$: V の $G_u,\ G_v$ への制限 ($V : G_K$ の表現),
- $e = e(K_u/\mathbb{Q}_\ell)$: u の絶対分岐指数.

- 係数体に関する記号
  - E : 代数体,
  - $\lambda \mid \ell$: E の素点.

2 主結果

本研究において得られた結果について述べていきたい. 主結果そのものは, できる限り一般的な条件下で証明している. 主張を理解するためにはいわゆる「Fontaine の p 進ホッジ理論」に対する知識を必要とするが, 本稿を読む上ではその知識がなくても, あまり気にせずその部分は「流して」いただいて構わない. また, p 進ホッジ理論をご存じの読者にとっては誤解を招く恐れがあるため一言述べておくと, 本研究では係数体の剰余標数 ℓ が p 進 Hodge 理論の "p" に当たるものとして扱われているという点に注意していただきたい.

主結果にはいくつか似たような変化系があるのだが, 詳しいことは原論文 [2] を参照していただくこととして, 今回は冒頭の性質 2 に直結した結果と, Fourier 係数の合同への応用に必要となるものの 2 つに焦点を絞って紹介したい.

まず, 正の整数 n を事前に固定しておく.

定義 4. G_K の n 次元 E_λ 進 Galois 表現 V に対して, 次の性質が全て成り立つとき, **V は性質 (I) を満たす**[3]と呼ぶこととする:

(SS_v) V は v で半安定;

(Int_v) V は v で E 整;

(PST_u) K_u の有限次拡大 $K'_{u'}$ が存在して, $e(K'_{u'}/\mathbb{Q}_\ell)|e$ かつ V は $K'_{u'}$ で (Fontaine の "p 進 Hodge 理論" の意味で) 半安定 (特に, Hodge-Tate 表現であることに注意);

(HT_u) V の u での Hodge-Tate 重みは, 全て区間 $[0, (\ell-1)/e^2]$ の中にある;

($G_{u,v}$) V は (G) 型.

最後の「(G) 型」は造語で, Hodge-Tate 重みと Weil 重みの和に関する性質であり, 定義は付録に述べてある. 簡単な例外もあるが, 幾何から標準的に構成されるものならばだいたい成り立つことが期待されるものといえる. 性質自体は 5 つもあるわけだが, これらの性質を満たす表現は簡単に見つけることができる. 以下に代表的な例を挙げよう.

[3] 性質 (I) などと言うからには当然性質 (II) もあるのだろうと期待するわけだが, 本稿においてその言葉が出てくることはない. 勿論原著 [2] の最新版には出てくるのだが, 今現在アーカイブにあげているプレプリントにはない. とはいえたいしたものでもなく, 単に, 性質 (I) の定義から (SS_v) を除いたものを性質 (II) と呼んでいる.

例 5. (1) 自明な 1 次元表現 $\mathbb{E}_\lambda$ の i 回 Tate 捻り $\mathbb{E}_\lambda(i)$ は $i \in [0, (\ell-1)/e^2]$ のとき, 性質 (I) を満たす.
(2) X を K 固有滑らかな多様体とし, V を r 次エタールコホモロジー $H^r_{\mathrm{et}}(X \otimes_K \overline{K}, \mathbb{Q}_\ell)$ の双対表現とする. もし X が次の両方を満たしているならば, V は性質 (I) を満たす (ここでは $E = \mathbb{Q}$):

- X は v で半安定還元をもつ;
- K の有限次拡大 K' と絶対分岐指数が e の約数であるような u 上の K' の素点 u' が存在して, X は u' で半安定還元を持つ.

(3) 特に, (2) の性質を満たす X がアーベル多様体 A の場合, その ℓ 進 Tate 加群 $V = V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ は性質 (I) を満たす (ここでは $E = \mathbb{Q}$).

上の例の (1) で述べたものが (G) 型であることは簡単にわかる. 一方で (2) (ついでに (3) も) が (G) 型になることは今となってはよく知られていることだが, 決して明らかなことではないということは注意しておきたい.
それでは, 主定理を述べよう. 以下では, b を正の実数とする.

定理 6. 次を満たすような定数 $C = C([E:\mathbb{Q}], n, b, e, q_v)$ が存在する:
ℓ を $\ell > C$ なる任意の素数, u を $u \nmid \ell$ なる E の任意の素点とする. V, V' を性質 (I) を満たす G_K の E_λ 進表現とし, V の Hodge-Tate 重みは全て区間 $[0, (\ell-1)/e^2]$ の中にあるものとする. このとき, $V_u \equiv_{\mathrm{ss}} V'_u \pmod{\lambda}$ かつ $V_v \equiv_{\mathrm{ss}} V'_v \pmod{\lambda}$ ならば, 実は $V_v \simeq_{\mathrm{ss}} V'_v$. (特に, $V \equiv_{\mathrm{ss}} V' \pmod{\lambda}$ ならば $V_v \simeq_{\mathrm{ss}} V'_v$.)
さらに, C としては次の値を取ることができる:

$$C := \max\{e^2 b + 1, \left(2\binom{n}{[n/2]} q_v^{nb}\right)^{[E:\mathbb{Q}]/f_\lambda}\}.$$

上の定理は mod λ による余りから元の表現の情報を得るというものだが, 次に mod ℓ による余りから得られる結果を述べることとする.

定理 7. 次を満たすような定数 $\tilde{C} = \tilde{C}(n, b, e, q_v)$ が存在する: ℓ を $\ell > \tilde{C}$ なる任意の素数, u を $u \nmid \ell$ なる E の任意の素点とする. V, V' を性質 (I) を満たす G_K の E_λ 進表現とし, V の Hodge-Tate 重みは全て区間 $[0, (\ell-1)/e^2]$ の中にあるものとする. このとき, $\det(T - \mathrm{Frob}_v | V_u) \equiv \det(T - \mathrm{Frob}_v | V'_u) \pmod{\ell \mathcal{O}_E}$ かつ $V_v \equiv_{\mathrm{ss}} V'_v \pmod{\lambda}$ ならば, 実は $V_v \simeq_{\mathrm{ss}} V'_v$.
さらに, $\tilde{C}$ としては次の値を取ることができる:

$$\tilde{C} := \max\{e^2 b + 1, 2\binom{n}{[n/2]} q_v^{nb}\}.$$

上の二つの定理の大きな違いは, 出てくる定数が前者は E のサイズ $\cdots$ 正確には $[E:\mathbb{Q}]$ に依っているものであるのに対し, 後者はそれには依っていないということである. この後者の性質は, 後に述べる Fourier 係数の合同に関する応用を示す際に大きな役割を果たすこととなる. というのも, その応用の際には E を (正規化された) カスプ形式の Hecke 体 (= Fourier 係数を全添加した体) として扱うわけだが, そのサイズを気にしないで良いと保証してくれるのが後者の定理だからである.

3　応用

ここでは, 前節で述べた結果を用いて得られる応用を 2 つほど述べる.

系 8. ℓ を素数, b, n, r を正の整数とし, $1 \leq r \leq b$ であるとする. X を r 次 Betti 数が n 以下であるような, $\mathbb{Q}$ 上固有で滑らかな多様体とし, ℓ の外で良い還元を持ち, ℓ で半安定還元を持つものとする. このとき, $\ell > \binom{n}{[n/2]} 2^{nb+1}$ ならば $V = H^r_{\text{ét}}(X_{\bar{K}_\lambda}, \mathbb{Q}_\ell)$ の剰余表現 $\bar{V}$ から得られる自然な準同型写像 $G_K \to GL(\bar{V})$ の像は Borel 部分群には含まれない.

系 9. k を 1 か偶数とし, $N \geq 1$ を square free な整数とする. このとき, $\ell > 4^k$ ならば, 正規化された固有カスプ形式 $f = \sum_{n=1}^{\infty} \in S_k(N, k)$ で, 以下の合同関係式を満たすものは存在しない:

ある整数 i, j が存在して, ほとんどすべての素数 $p \nmid \ell N$ に対して $a_p \equiv p^i + p^j \pmod{\ell}$.

$\ell > 4^k$ という縛りが N に依っていないというところが新しい部分である. f に付随する法 λ Galois 表現 $\rho_{f,\lambda} \colon G_{\mathbb{Q}} \to GL_2(k_\lambda)$ (但し, E は f の Hecke 体, λ は ℓ 上の E の素点, k_λ はその剰余体) の像が $SL_2(k_\lambda)$ を含まないとき, ℓ を (f に関する) 例外素数と呼ぶが, 上の合同関係式を満たす素数 ℓ は特殊な例外素数である. 例外素数は有限個しかないことが知られているが, それがどの程度の大きさのものかということはまだいろいろな数学者の手によって研究されている問題である.

A　付録

この付録では, 性質 (I) を述べる際に用いた様々な用語の解説をする. (ただし, p 進 Hodge 理論に関しては省略する.) 記号 $K, E, u, v, \ldots$ は 1 節の最後に述べたものと同様のものとする. 以下では, V を G_K の n 次元 E_λ 表現とする.

(SS$_v$) と (Int$_v$) について: V が $v \nmid \ell$ で**半安定**とは, I_v が V に冪単に作用することを言う. このとき, V の $E_\lambda[G_K]$ 加群としての半単純化 V^{ss} に I_v は自明に作用しているので, Frob_v が V^{ss} に作用する. 従って, 特性多項式 $P(T) = \det(T - \text{Frob}_v | V^{\text{ss}})$ が定義される. これは定義からは E_λ 係数の n 次多項式となるが, これが E 係数であるとき, V は **v で E 整**であるという.

$(G)_{u,v}$ について: まず, 「(G) 型」と述べてはいるが, 実際には u, v の選び方に依っているということを注意しておく. $V|_{G_u}$ が Hodge-Tate 表現だと仮定する. このとき, $V|_{G_u}$ を $n \cdot [E_\lambda : \mathbb{Q}_\ell]$ 次元の $\mathbb{Q}_\ell$ 表現とみなしたときの Hodge-Tate 重みのなす多重集合を $\text{HT}_u(V)$ とかく (定義より, $n \cdot [E_\lambda : \mathbb{Q}_\ell]$ 個の元からなる).

一方, W を v で半安定であるような $\mathbb{Q}_\ell$ 表現とする. $\det(T - \text{Frob}_v | W^{\text{ss}})$ の任意の根 α に対して $\alpha \in \overline{\mathbb{Q}}$ であり, かつある整数 w_α が存在して, 任意の埋め込み $\iota \colon \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ に対して $|\iota(\alpha)| = q_v^{w_\alpha}$ が成り立つとき, W は (v に関して) **(W) 型**であるといい, 各 w_α を W の (v での) **Weil 重み**であるという. Weil 重み全てからなる多重集合を $W_v(W)$ とかく. 今, n 次元 E_λ 表現である V を $n \cdot [E_\lambda : \mathbb{Q}_\ell]$ 次元の $\mathbb{Q}_\ell$ 表現とみなすことで, V が (W) 型であるという概念を定義することができる. このとき, $W_v(V)$ は $n \cdot [E_\lambda : \mathbb{Q}_\ell]$ 個の元からなる多重集合である.

定義 10. V が u で Hodge-Tate かつ v で (W) 型であると仮定する. このとき, V が (G) 型であるとは, 等式

$$\Sigma(HT_u(V)) = \Sigma(W_v(V))$$

が成り立つときを言う. (ここで, 有限集合 X に対して, $\Sigma(X) := \sum_{x \in X} x$ と定義する.)

幾何から自然に構成されるものは大体 (G) 型である．

例 11. (1) E_λ の i 回 Tate ひねり $E_\lambda(i)$ は (G) 型.
(2) X を K 上固有滑らかな代数多様体とする．$H^r_{\text{ét}}(X_{\bar{K}_\lambda}, \mathbb{Q}_\ell)$ は (任意の v, u に対して) (G) 型.
(3) 正規化された固有カスプ形式 f に付随する λ 進 Galois 表現 $\rho_{f,\lambda} \colon G_\mathbb{Q} \to GL_2(E_\lambda)$ は (G) 型 (ここで, E は f の Hecke 体).

幾何から構成されていても (G) 型ではない例もある．

例 12. K を虚 2 次体, E を K 上の楕円曲線で K 上 CM を持つものとする．ℓ を K で分解する素数とする．このとき, $V_\ell(E)$ は G_K 安定な 1 次元表現の直和に分解する．そこに現れる 1 次元表現たちは (G) 型ではない.

参考文献

[1] Y. Ozeki, Non-existence of certain Galois representations with a uniform tame inertia weight, Int. Math. Res. Notices **2011** (2011), 2377–2395.

[2] Y. Ozeki and Y. Taguchi, On congruence of Galois representations of number fields, preprint, arXiv:1306.0321.

[3] C. Rasmussen and A. Tamagawa, A finiteness conjecture on Abelian varieties with constrained prime power torsion, Mathematics Research Letters **15** (2008), 1223–1231.

[4] C. Rasmussen and A. Tamagawa, Arithmetic of abelian varieties with constrained torsion, preprint, arXiv:1302.1477.