

無限個の素数で分岐する既約な p 進表現の構成について

富山恭敬

目次

1	導入	1
2	1次元（アーベル）の場合の結果と可約の場合の例	4
3	普遍変形環	6
4	持ち上げ定理	10
5	定理2の証明	12

1 導入

本稿では, Khare と Ramakrishna の論文 [KRam]

“Finiteness of Selmer groups and deformation rings”

に従い, 無限個の素数で分岐する既約な p 進表現の構成について概説する.

$\mathbb{Q}$ を有理数体とし, $\overline{\mathbb{Q}}$ を $\mathbb{Q}$ の代数的閉包とする. $G_{\mathbb{Q}}$ を $\mathbb{Q}$ の絶対ガロア群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ とする. $p > 2$ を素数とし, $\mathbf{k}$ を標数 p の有限体とする. $W(\mathbf{k})$ を $\mathbf{k}$ の Witt 環とする. G_l を素数 l での分解群とし, I_l を素数 l での惰性群とする. 以下, 表現といえば連続表現を意味することにする.

一般に次のことが知られている.

事実. $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}(V)$ を p 進ガロア表現とする. ρ が代数幾何から来る (i.e. ある射影的かつ滑らかな代数多様体 X があって, ρ は $H_{\mathrm{\acute{e}t}}^i(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_p(r))$ のある部分商と同型になる) とき, ρ は有限個の素数の外不分岐である.

この事実の証明に関しては三枝氏の [Mi] の系 3.26 を見られたい。したがって、この事実から、無限個の素数で分岐するガロア表現は代数幾何から来ないことが分かる。代数幾何から来る表現は常に半単純な表現であると予想されており、また代数体の絶対ガロア群自体が難しい群なので像が無限なガロア表現を構成することは容易ではなく、幾何からエタールコホモロジーで作ること自体も難しいのである。そのような事情により無限個の素点で分岐する半単純ガロア表現の例は存在するかどうかも長らく知られていなかった。また、すべての 1 次元のガロア表現は有限個の素数の外不分岐であることが知られている。これに関しては次の節で紹介する。

そのような背景もあって、Ramakrishna は 2000 年の論文 [R2]

“Infinitely ramified representations”

の中で次の定理を証明した。

定理 1 ([R2], Theorem 1). E を 3 で良い還元を持つ $\mathbb{Q}$ 上の半安定楕円曲線とする。このとき、無限に多く (ディリクレ密度 1) の素数 $p \geq 5$ に対して、無限個の素数で分岐する全射なガロア表現 $G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}_p)$ で、その表現の法 p 還元は E の p 等分点上のガロア作用と一致するようなものが存在する。

このようなガロア表現を構成するために Ramakrishna はガロア表現の変形理論を用いた。

この論文 [R2] の結果は 2003 年の論文 [KRam] の中で上の楕円曲線に限らず、より一般の法 p ガロア表現に対して無限個の素数で分岐する既約な p 進ガロア表現を構成した。また、その構成法も整理され分かりやすいものになっている。したがって、本稿では論文 [KRam] にしたがって無限個の素数で分岐するガロア表現を構成する。

$\bar{\rho}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbf{k})$ を法 p 表現とする。以下を仮定する。

- $p > 5$,
- $\bar{\rho}$ は odd である,
- $\bar{\rho}$ と $\mathrm{Ad}^0 \bar{\rho}$ は絶対既約である,
- $p \nmid \#\mathrm{Im} \bar{\rho}$,
- $\bar{\rho}$ は p で ordinary である。(定義については 3 節を見られたい.)

この仮定の下で次の定理が成り立つ。

定理 2 ([KRam], Theorem 25). 無限個の素数で分岐しかつ p で ordinary な既約ガロア表現 $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(W(\mathbf{k}))$ が存在して $\rho \bmod p = \bar{\rho}$ を満たす。

本稿ではこの定理の証明を紹介する. 上の仮定について少しコメントしておく. $\bar{\rho}$ が保型形式に付随するガロア表現であれば odd であることが知られている. これに関しては千田氏の [Ch] 定理 2.4 を見られたい. また, $\text{Im}(\bar{\rho}) \supset \text{SL}_2(\mathbf{k})$ であれば絶対既約性と $p \nmid \#\text{Im}\bar{\rho}$ が成り立つことが知られている. これに関しては [R1] を見られたい. 虚数乗法を持たない保型形式 f が与えられたとき, 無限に多くの素数 p に対して, f に付随する法 p ガロア表現 $\bar{\rho}_{f,p}$ の像は $\text{SL}_2(\mathbf{k})$ を含むことも知られている. これに関しては [Ri1], [Ri2] を見られたい. $\bar{\rho}$ が p で ordinary な保型形式に付随する法 p 表現であれば, $\bar{\rho}$ も ordinary であることが知られている. これに関しては [E] の Theorem 2.5 などを見られたい.

注意 1. 簡単のため p で ordinary な表現に限っているが, 論文 [KRam] では even な表現に関する結果もある.

この定理の証明をごく簡単に紹介しておく. 上の仮定を満たすガロア表現 $\bar{\rho}$ が与えられているとき, その表現を $\rho_2: G_{\mathbb{Q}} \rightarrow \text{GL}_2(W(\mathbf{k})/p^2)$ に持ち上げる. このとき ρ_2 では $\bar{\rho}$ よりも多く分岐するように持ち上げる. またさらに ρ_3 では ρ_2 よりも多く分岐するように持ち上げる. このように持ち上げを帰納的に構成し, それらの極限を取るにより無限に分岐する ρ を構成することができる.

以下の節で上の定理を証明するための準備をする. 既約な p 進表現で, 無限個の素数で分岐するようなものを構成することはやさしくない. 一方で, 可約な p 進表現でそのようなものを構成することはそれほど難しくはない. さらに, 可約な場合は, 全ての素数で分岐するようなものを構成することができる. この構成法については次の節で述べる. しかし, 既約な場合は, このようなすべての素数で分岐する p 進表現は存在しないことが Khare と Rajan による 2001 年の論文 [KRaj] によって知られている.

定理 3 ([KRaj], Theorem 1). L を代数体とし, K を $\mathbb{Q}_p$ の有限次拡大とする. $\rho: G_L \rightarrow \text{GL}_n(K)$ を半単純表現とする. このとき, ρ で分岐する素数の集合 S_ρ はディリクレ密度 0 である.

より一般に Khare と Larsen と Ramakrishna の 2005 年の論文 [KLR] の中で次の結果が得られている.

定理 4 ([KLR], Theorem 2.5). F を大域体とし, V を F の標数と等しくない剰余標数 l を持つ付値環とする. さらに, V は標数 0 の商体を持つと仮定する. $\rho: G_F \rightarrow \text{GL}_n(K)$ を半単純表現とする. このとき, ρ で分岐する F の素点の集合はディリクレ密度 0 である.

以下の節では, まず可約の場合の無限に分岐する表現を構成し, その後, 定理の証明に使われる変形環を準備し, それに関する「持ち上げ定理」と

その証明を紹介し、最後の節で定理 2 の証明をする。この「持ち上げ定理」は無限個の素点で分岐する表現を構成する際の核心部分なので、できるだけ詳細に説明する。また、以下ではコホモロジー群といえば全て連続コホモロジー群のこととする。ガロアコホモロジーの詳しい性質や証明などは佐藤氏の [Sa] や [NSW]などを参照していただきたい。

謝辞

本稿は第 17 回整数論サマースクールにおける筆者の講演に基づいている。サマースクールを企画してくださった世話人の落合理氏、千田雅隆氏、山内卓也氏に感謝したい。また落合氏と山内氏は筆者の講演の準備段階や本稿を書く段階で多くの助言を下さった。ここに感謝の意を表したい。

2 1 次元（アーベル）の場合の結果と可約の場合の例

この節では、1 次元（アーベル）なガロア表現は有限個の素数の外不分岐であるという結果と、全ての素数で分岐するような可約ガロア表現の構成を述べる。

命題 1. $p > 2$ とする。 $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\mathbb{Q}_p)$ を p 進ガロア表現とする。もし ρ の像がアーベルであるならば、 ρ は有限個の素数の外不分岐である。したがって、1 次元 p 進ガロア表現は有限個の素数の外不分岐である。

証明. 基底をうまく取ると、 ρ の像を $\mathrm{GL}_n(\mathbb{Z}_p)$ の中にとることができるから $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\mathbb{Z}_p)$ としてよい。 $\mathbb{Q}^{\mathrm{ab}}$ を $\mathbb{Q}$ の最大アーベル拡大とし、 $G_{\mathbb{Q}}^{\mathrm{ab}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ をそのガロア群とする。このとき ρ は像がアーベルだから、 $G_{\mathbb{Q}}^{\mathrm{ab}}$ を経由する。また、 I を $\mathbb{Q}$ のイデール群とすると、類体論の相互律から相互写像 $i: I \rightarrow G_{\mathbb{Q}}^{\mathrm{ab}}$ を持つ。そこで合成写像 $\rho \circ i: I \rightarrow G_{\mathbb{Q}}^{\mathrm{ab}} \rightarrow \mathrm{GL}_n(\mathbb{Z}_p)$ を考える。 $\mathbb{Q}_l^{\times}$ の単数群を U_l と書くと、類体論から $i(U_l)$ は $\mathrm{Gal}(\mathbb{Q}_l^{\mathrm{ab}}/\mathbb{Q}_l)$ の惰性群と一致する、ここで $\mathbb{Q}_l^{\mathrm{ab}}$ は $\mathbb{Q}_l$ の最大アーベル拡大である。したがって、有限個を除いたほとんど全ての素数 l で $\rho \circ i(U_l) = 1$ がいえればよい。そこで $\pi: \mathrm{GL}_n(\mathbb{Z}_p) \rightarrow \mathrm{GL}_n(\mathbb{F}_p)$ を自然な射影とし、 $I' := \mathrm{Ker}(\pi \circ \rho \circ i)$ と置くと、 I' は I の開部分群だから、イデール位相の定義から有限個を除いたほとんど全ての素数 l に対して $U_l \subset I'$ となる。よって $I' \rightarrow \mathrm{GL}_n(\mathbb{Z}_p)$ が有限個を除いたほとんど全ての素数 l で $\rho \circ i(U_l) = 1$ が成り立つことを示せばよい。ここで I' の像は $\Gamma := \mathrm{Ker} \pi$ の中に入っていることに注意する。 Γ は副 p 群であり、単数群の構造定理から $U_l \simeq (\text{有限群}) \times \mathbb{Z}_l$ の形にかける。 p と異なる素数 l に対して、 $\mathbb{Z}_l$ は副 l 群であるから、 U_l の像は有限群になる。ところが $\Gamma \simeq \mathrm{M}_n(\mathbb{Z}_p)$ に注意すると、 Γ の有限部分群は 1 のみであるから、 U_l の像は 1 であることが分かり、証明が終わる。 $\square$

命題 2. 全ての素数で分岐する可約な 2 次元ガロア表現 $\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}_p)$ が存在する.

証明. 構成法を簡単に述べる. まず次の連続写像を考える:

$$\rho: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Z}_p); \sigma \mapsto \begin{pmatrix} \chi_p(\sigma) & u(\sigma) \\ 0 & 1 \end{pmatrix}$$

ここで χ_p は p 進円分指標であり, $u: G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p$ は連続写像である.

このとき, ρ が連続準同型をなすことと, $u: G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p(1)$ がコホモロジー群 $H^1(G_{\mathbb{Q}}, \mathbb{Z}_p(1))$ の元を定めることは同値である. この対応によって, ρ が素数 l で分岐することと u がコホモロジー群 $H^1(G_{\mathbb{Q}}, \mathbb{Z}_p(1))$ の中で分岐することは同値である. ただし, $H^1(G_{\mathbb{Q}}, \mathbb{Z}_p(1))$ の元が素数 l で分岐するというのは

$$\mathrm{Ker}(H^1(G_{\mathbb{Q}}, \mathbb{Z}_p(1)) \rightarrow H^1(I_l, \mathbb{Z}_p(1)))$$

の元ではないことをいう. そこで, 全ての素数で分岐する ρ を構成するためには, コホモロジー群 $H^1(G_{\mathbb{Q}}, \mathbb{Z}_p(1))$ の中で (p 以外の) 全ての素数 l で分岐する元 u を構成すればよい.

$l \neq p$ とする. まず, 同型

$$H^1(G_{\mathbb{Q}}, \mathbb{Z}_p(1)) \simeq \varprojlim_n \mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^{p^n}$$

を思い出す. 次に素数 l に対して同型

$$H^1(I_l, \mu_{p^n}) \simeq \mathrm{Hom}(I_l, \mu_{p^n}) \simeq \mathrm{Hom}(\mu_{p^n}, \mu_{p^n}) \simeq \mathbb{Z}/p^n \mathbb{Z}$$

が成り立つ. これらの同型による次の図式は可換である:

$$\begin{array}{ccc} H^1(G_{\mathbb{Q}}, \mathbb{Z}_p(1)) & \longrightarrow & H^1(I_l, \mathbb{Z}_p(1)) \\ \downarrow & & \downarrow \\ \varprojlim_n \mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^{p^n} & \longrightarrow & \varprojlim_n \mathbb{Z}/p^n \mathbb{Z} \end{array}$$

下側の写像は各成分 $\mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^{p^n} \ni a_n$ を $\mathbb{Z}/p^n \mathbb{Z} \ni v_l(a_n)$ に写す写像である. ここで, v_l は l 進付値である.

そこで下側の写像を使って元を構成する. p 以外の素数の全てを $l_1, l_2, l_3, \dots$ と並べる. このとき

$$\mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^{p^n} \ni u_n := l_n^{p^{n-1}} l_{n-1}^{p^{n-2}} \cdots l_1$$

とおき,

$$\varprojlim_n \mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^{p^n} \ni u := (u_1, \dots, u_n, \dots)$$

とおくと, この u に対応する ρ はすべての素数で分岐している. それは, l_j に対して, $\mathbb{Z}/p^j\mathbb{Z} \ni v_{l_j}(u_j) = p^{j-1} \neq 0$ となっている事から分かる.

□

3 普遍変形環

この節では無限個の素数で分岐する既約なガロア表現を構成する際に使われる条件付の変形環について述べる. 変形理論に関する詳細は今井氏の [Ima] や [Ma1], [Ma2] などを参照されたい. まず最初に, 普遍変形環と半変形環の復習をする. Π を副有限群とし, そのすべての開部分群の pro- p 完備化は位相的有限生成であるとする. 表現 $\bar{\rho}: \Pi \rightarrow \mathrm{GL}_2(\mathbf{k})$ を考える. $\mathrm{Ad} \bar{\rho}$ を $\mathbf{k}$ 係数の 2×2 行列の集合であって, Π が $\bar{\rho}$ を通して共役に作用するものとする. $\mathcal{C}$ を完備ネーター局所 $W(\mathbf{k})$ 代数で剰余体が $\mathbf{k}$ であるものからなる圏とする, ここで, 射は対象の間の局所射で剰余体 $\mathbf{k}$ の間の恒等射を引き起こすものとする. $\bar{\rho}$ の $R \in \mathcal{C}$ への**持ち上げ**とは, 表現 $\rho: \Pi \rightarrow \mathrm{GL}_2(R)$ で $\rho \bmod \mathfrak{m}_R = \bar{\rho}$ となるもののことである. ここで $\mathfrak{m}_R$ は R の極大イデアルである. また, $\bar{\rho}$ の R への**変形**とは, $\bar{\rho}$ の R への持ち上げ ρ の狭義同値類 $[\rho]$ のことである, ここで Π から $\mathrm{GL}_2(R)$ への二つの持ち上げ ρ_1 と ρ_2 が狭義同値であるとは, $\mathrm{GL}_2(R) \rightarrow \mathrm{GL}_2(\mathbf{k})$ の核のある元によって互いに共役であることである. 次の関手を考える:

$$\mathrm{Def}_{\Pi}: \mathcal{C} \rightarrow \mathbf{Sets}; R \mapsto \{[\rho] \mid [\rho] \text{ は } \bar{\rho} \text{ の } R \text{ への変形}\}.$$

このとき, 次の定理が成り立つ.

定理 5 ([Ma2], Section 20, Proposition 2). (a) 関手 Def_{Π} は**半変形環** $R^v \in \mathcal{C}$ と**半変形** $\rho^v: \Pi \rightarrow \mathrm{GL}_2(R^v)$ を持ち, 次の性質を満たす: 任意の $\bar{\rho}$ の $A \in \mathcal{C}$ への変形 $[\rho]$ が与えられたとき, 射 $u: R^v \rightarrow A$ が存在して $[\rho] = [u \circ \rho^v]$ を満たす.

(b) もし $\mathrm{Im}(\bar{\rho})$ の中心が $\mathrm{GL}_2(\mathbf{k})$ の中心になるならば, 関手 Def_{Π} は上のペア (R^v, ρ^v) によって表現可能である. このとき, R^v を**普遍変形環**と言い, ρ^v を**普遍変形**と言う.

(c) 接空間 $\mathfrak{t} := \mathrm{Def}_{\Pi}(\mathbf{k}[X]/(X^2))$ は $\mathbf{k}$ ベクトル空間の構造を持ち, ガロアコホモロジー $H^1(\Pi, \mathrm{Ad} \bar{\rho})$ と $\mathbf{k}$ ベクトル空間として同型である.

この定理に関しては [Ima] の定理 2.1 や命題 3.1 も見られたい. 次に条件付の変形環を考える. 以下の条件付の変形に関しては [Ima] の 5 節も見られたい. まず, 変形条件の定義をする.

定義 1. $\bar{\rho}$ に関する**変形条件** $\mathcal{D}$ とは, $\bar{\rho}$ の持ち上げの集まりで次の性質を満たすもののことである:

- (I) $\mathcal{D}$ は $\bar{\rho}$ を含んでいる.
- (II) $\mathcal{D}$ は狭義同値と射で閉じている.
- (III) 元 $A, B, C \in \mathcal{C}$ の圏 $\mathcal{C}$ 内におけるカルテシアン図式

$$\begin{array}{ccc} A \times_C B & \xrightarrow{\pi_B} & B \\ \pi_A \downarrow & & \downarrow \beta \\ A & \xrightarrow{\alpha} & C \end{array}$$

と, $\bar{\rho}$ の持ち上げ $\rho: \Pi \rightarrow \mathrm{GL}_2(A \times_C B)$ を与えたとき, もし $\pi_A \circ \rho, \pi_B \circ \rho$ が $\mathcal{D}$ に含まれるならば, ρ も $\mathcal{D}$ に含まれる. ここで, π_A, π_B はそれぞれ $A \times_C B$ から $A, A \times_C B$ から B への射影である.

- (IV) $\rho: \Pi \rightarrow \mathrm{GL}_2(R)$ を $\bar{\rho}$ の持ち上げとする. すべての n に対して, $\rho \bmod \mathfrak{m}_R^n: \Pi \rightarrow \mathrm{GL}_2(R/\mathfrak{m}_R^n)$ は $\mathcal{D}$ に含まれるならば, ρ も $\mathcal{D}$ に含まれる.

変形条件 $\mathcal{D}$ は Def_Π の部分関手とみなすことができる. そこで $\mathcal{D}$ を関手とみなして $\mathcal{D}$ の接空間を $\mathfrak{t}_{\mathcal{D}} := \mathcal{D}(\mathbf{k}[X]/(X^2))$ と定める. このとき $\mathfrak{t}_{\mathcal{D}}$ は $\mathfrak{t} = \mathrm{Def}_\Pi(\mathbf{k}[X]/(X^2)) \simeq H^1(\Pi, \mathrm{Ad} \bar{\rho})$ の部分ベクトル空間の構造を持つ. 次の定理が成り立つ.

定理 6 ([Ma2], Section 23, Proposition). $\bar{\rho}$ が変形条件 $\mathcal{D}$ を持つとき, **タイプ $\mathcal{D}$ の半変形環 $R^{\mathcal{D}}$ とタイプ $\mathcal{D}$ の半変形 $\rho^{\mathcal{D}}$ が存在して,**

$$R^{\mathcal{D}} \simeq W(\mathbf{k})[[T_1, \dots, T_r]]/\mathbf{J}$$

と書ける. ここで, $r = \dim_{\mathbf{k}} \mathfrak{t}_{\mathcal{D}}$ である. また, $R^{\mathcal{D}}$ は半変形環 R^v の商環になっている.

重要な変形条件の 1 つに fixed determinant を持つ変形というものがある. この条件について述べる. 準同型 $\delta: \Pi \rightarrow W(\mathbf{k})^\times$ を 1 つ固定する. すべての $R \in \mathcal{C}$ に対して, δ_R を合成 $\delta_R: \Pi \xrightarrow{\delta} W(\mathbf{k})^\times \rightarrow R^\times$ とする. このとき, $\bar{\rho}$ の R への変形 ρ はもし $\det \rho = \delta_R$ ならば **fixed determinant δ を持つ**という. このような変形は変形条件を満たす. また, この変形条件の接空間は $H^1(\Pi, \mathrm{Ad}^0 \bar{\rho})$ と同型である. ここで $\mathrm{Ad}^0 \bar{\rho}$ は $\mathrm{Ad} \bar{\rho}$ のトレース 0 の部分空間である. **以下では, 単に変形といえば fixed determinant を持つ変形を意味することにする.**

次に定理 2 の証明で使われる変形条件を考える. $\bar{\rho}: G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbf{k})$ を odd な絶対既約法 p 表現とする. $\bar{\rho}$ は p で ordinary であると仮定する. $\bar{\rho}$ が p で ordinary とは $\bar{\rho}(I_p)$ が

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

と共役であることをいう. S を p と無限素点と $\bar{\rho}$ で分岐する素数からなる集合とする. S' を S と素な素数の有限集合で, 各 $s' \in S'$ に対して, 次を満たすものとする:

- $s' \not\equiv \pm 1 \pmod{p}$,
- $\bar{\rho}(\text{Frob}_{s'})$ は twist を除いて

$$\begin{pmatrix} s' & 0 \\ 0 & 1 \end{pmatrix}$$

と共役である. ここで $\text{Frob}_{s'}$ は s' での arithmetic Frobenius である.

$\bar{\rho}$ に関して次の条件を満たす変形 ρ を考える:

1. fixed determinant を持つ.
2. $S \cup S'$ の外不分岐である.
3. 各 $s \in S$ に対して, 次の条件を満たす.
 - (a) $p \neq s$ であり $p \nmid \#\bar{\rho}(I_s)$ であるような s に対して, $\#\rho(I_s) = \#\bar{\rho}(I_s)$ を満たす.
 - (b) $p \neq s$ であり $p \mid \#\bar{\rho}(I_s)$ であるような s に対して, $\rho|_{G_s}$ は指標による twist を除いて

$$\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$$

と共役である.

- (c) $p = s$ に対して, ρ は p で ordinary である. ρ が p で ordinary とは $\rho|_{I_p}$ が

$$\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$$

と共役であることをいう.

4. $s' \in S'$ に対して, $\rho|_{G_s}$ は指標による twist を除いて

$$\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$$

と共役である.

この条件を $\mathcal{D}_{S \cup S'}$ と書くと、次が成り立つ。

命題 3 ([KRam], Lemma 2). 上の条件 $\mathcal{D}_{S \cup S'}$ は変形条件を成している。そこでこの普遍変形環と普遍変形をそれぞれ $R_{S \cup S'}^{S'-\text{new}}$ と $\rho_{S \cup S'}^{S'-\text{new}}$ と書く。

$s \in S$ (resp. $s \in S'$) に対して, $\bar{\rho}|_{G_s}: G_s \rightarrow \text{GL}_2(\mathbf{k})$ とすると, 上の条件 3 (resp. 4) は $\bar{\rho}|_{G_s}$ の変形条件 $\mathcal{D}_s$ を成していることが分かる。その半変形環を R_s と書く。

$\mathbb{Q}_{S \cup S'}$ を $S \cup S'$ の外不分岐な $\mathbb{Q}$ の最大代数拡大とし, $G_{S \cup S'} := \text{Gal}(\mathbb{Q}_{S \cup S'}/\mathbb{Q})$ とする。各 $s \in S \cup S'$ に対して, L_s を $\mathbf{t}_{\mathcal{D}_s}$ に対応する $H^1(G_s, \text{Ad}^0 \bar{\rho})$ の部分空間とする。このとき $\mathbf{t}_{\mathcal{D}_{S \cup S'}}$ に対応する $H^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho})$ の部分空間は

$$\text{Ker}(H^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho}) \rightarrow \bigoplus_{s \in S \cup S'} H^1(G_s, \text{Ad}^0 \bar{\rho})/L_s)$$

と一致する。この群を $H_{\{L_s\}}^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho})$ と書き, **セルマー群** と呼ぶ。局所テイト双対性より perfect pairing $\text{Ad}^0 \bar{\rho} \times \text{Ad}^0 \bar{\rho} \rightarrow \mathbf{k}; (A, B) \mapsto \text{Trace}(AB)$ は perfect pairing

$$H^1(G_s, \text{Ad}^0 \bar{\rho}) \times H^1(G_s, \text{Ad}^0 \bar{\rho}(1)) \rightarrow H^2(G_s, \mathbf{k}(1)) \cong \mathbf{k}$$

を導くが, このとき $L_s^\perp \subset H^1(G_s, \text{Ad}^0 \bar{\rho}(1))$ をこの pairing の下での L_s の annihilator とする。**双対セルマー群** $H_{\{L_s^\perp\}}^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho}(1))$ を

$$\text{Ker}(H^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho}(1)) \rightarrow \bigoplus_{s \in S \cup S'} H^1(G_s, \text{Ad}^0 \bar{\rho}(1))/L_s^\perp)$$

で定義する。

セルマー群と普遍変形環に関する Böckle の結果を紹介する。各 $s \in S \cup S'$ に対して, $\bar{\rho}|_{G_s}$ のタイプ $\mathcal{D}_s$ の半変形環 R_s は定理 6 によって

$$W(\mathbf{k})[[T_{s,1}, \dots, T_{s,n_s}]]/\mathbf{J}_s$$

と書け, $n_s = \dim_{\mathbf{k}} L_s$ である。また同様に $R_{S \cup S'}^{S'-\text{new}}$ も

$$W(\mathbf{k})[[T_1, \dots, T_n]]/\mathbf{J}$$

と書け, $n = \dim_{\mathbf{k}} H_{\{L_s\}}^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho})$ である。このとき, 次の定理が成り立つ。

定理 7 ([B], Theorem 4.2).

$$\text{gen}(\mathbf{J}) \leq \sum_{s \in S \cup S'} \text{gen}(\mathbf{J}_s) + \dim_{\mathbf{k}} H_{\{L_s^\perp\}}^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho}(1))$$

が成り立つ。ここでイデアル $\mathbf{I}$ に対して, $\text{gen}(\mathbf{I})$ は $\mathbf{I}$ の生成元の個数である。

また, 次の命題も成り立つ.

命題 4 ([T], Section 1, Example). 各 $s \in S \cup S'$ に対して, $\text{gen}(\mathbf{J}_s) = 0$ である.

したがって, もし $H_{\{L_s\}}^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho}) = 0$, $H_{\{L_s^\perp\}}^1(G_{S \cup S'}, \text{Ad}^0 \bar{\rho}(1)) = 0$ なら, $R_{S \cup S'}^{S' - \text{new}} \simeq W(\mathbf{k})$ となることに注意する.

4 持ち上げ定理

この節では $\bar{\rho}: G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbf{k})$ を導入の定理 2 の上で述べた仮定を満たす表現とする.

定義 2. S' を S と素な素数の有限集合とする. 各 $s' \in S'$ に対して, 次を満たすとする.

- $s' \not\equiv \pm 1 \pmod{p}$,
- $\bar{\rho}(\text{Frob}_{s'})$ は twist を除いて

$$\begin{pmatrix} s' & 0 \\ 0 & 1 \end{pmatrix}$$

と共役である.

さらに $R_{S \cup S'}^{S' - \text{new}} \simeq W(\mathbf{k})$ を満たすとき, S' は **auxiliary 集合**であるという.

定理 8 (持ち上げ定理, [R3], Theorem 1). 与えられた $\bar{\rho}$ に対して, auxiliary 集合は存在する.

この定理は Ramakrishna によって [R1], [R3] の中で証明された. また Taylor は [T] の中で Ramakrishna の証明を簡略化し, 一般化した. ここでは持ち上げ定理の証明の流れを Taylor による方法に沿って簡単に紹介する.

証明. まず Wiles の公式 ([Sa] の定理 4.5 を見よ) により

$$\dim_{\mathbf{k}} H_{\{L_s\}}^1(G_S, \text{Ad}^0 \bar{\rho}) = \dim_{\mathbf{k}} H_{\{L_s^\perp\}}^1(G_S, \text{Ad}^0 \bar{\rho}(1))$$

が成立する. 前の節の最後に述べたことから, もし次元が 0 であれば S' として空集合をとればよい. そこで次元は 0 ではないと仮定すると, 0 でない元 $\phi \in H_{\{L_s^\perp\}}^1(G_S, \text{Ad}^0 \bar{\rho}(1))$ が取れる. このとき, 次を満たす素数 $w \notin S$ が存在する:

1. $w \not\equiv \pm 1 \pmod{p}$,
2. $\bar{\rho}(\text{Frob}_w)$ は twist を除いて

$$\begin{pmatrix} w & 0 \\ 0 & 1 \end{pmatrix}$$

と共役である.

3. $H^1_{\{L_s^\perp\} \cup \{L_w^\perp\}}(G_{S \cup \{w\}}, \text{Ad}^0 \bar{\rho}(1))$ から $H^1_{\{L_s\}}(G_S, \text{Ad}^0 \bar{\rho}(1))$ への単射が存在する.
4. $\phi \notin H^1_{\{L_s^\perp\} \cup \{L_w^\perp\}}(G_{S \cup \{w\}}, \text{Ad}^0 \bar{\rho}(1))$
5. $\dim_{\mathbf{k}} H^1_{\{L_s^\perp\} \cup \{L_w^\perp\}}(G_{S \cup \{w\}}, \text{Ad}^0 \bar{\rho}(1)) = \dim_{\mathbf{k}} H^1_{\{L_s\} \cup \{L_w\}}(G_{S \cup \{w\}}, \text{Ad}^0 \bar{\rho})$

したがって, 2 と 3 から

$$\dim_{\mathbf{k}} H^1_{\{L_s^\perp\} \cup \{L_w^\perp\}}(G_{S \cup \{w\}}, \text{Ad}^0 \bar{\rho}(1)) < \dim_{\mathbf{k}} H^1_{\{L_s^\perp\}}(G_S, \text{Ad}^0 \bar{\rho}(1))$$

となることが分かる. またこのセルマー群に対しても上の 1 から 5 を満たすような素数をとることができる. これを繰り返すとセルマー群は有限群だからいつかは 0 次元になり証明が終わる. w の存在についての証明はテクニカルなので省略する. 興味のある方は [T] の Lemma 1.2 を見られたい. $\square$

定理 2 の証明に入る前に定義と補題を準備する.

定義 3. $\rho: G_{\mathbb{Q}} \rightarrow \text{GL}_2(W(\mathbf{k})/p^n)$ を $\bar{\rho}$ の持ち上げとする. このとき素数 s が次を満たすとする.

- $s \not\equiv \pm 1 \pmod{p}$,
- $\rho|_{G_s}$ は指標による twist を除いて

$$\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$$

と共役である.

このとき ρ は s で**スペシャル**であるという.

補題 ([KRam], Lemma 8). $n \geq 2$ に対し, $\rho_n: G_{\mathbb{Q}} \rightarrow \text{GL}_2(W(\mathbf{k})/p^n)$ を X の外不分岐な $\bar{\rho}$ の持ち上げとする. ここで X は S を含む素数の有限集合で $X \setminus S$ はスペシャルな素数からなるものとする.

$$0 \neq \psi \in H^1(G_X, \text{Ad}^0 \bar{\rho}),$$

$$0 \neq \phi \in H^1(G_X, \text{Ad}^0 \bar{\rho}(1))$$

とする. このとき, ある $w \notin X$ が存在して次を満たす:

1. $\rho_{n-1} := \rho_n \bmod p^{n-1}$ は w でスペシャルである, しかし ρ_n は w でスペシャルではない,
2. $\psi|_{G_w} \neq 0$,
3. $\phi|_{G_w} \neq 0$.

5 定理 2 の証明

$\bar{\rho}$ は持ち上げの定理によって auxiliary 集合をもつから, 1つ選んでそれを S'_0 と書く. このとき, 同型 $R_{S \cup S'_0}^{S'_0 - \text{new}} \simeq W(\mathbf{k})$ により普遍変形

$$\rho_{S \cup S'_0}^{S'_0 - \text{new}} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(W(\mathbf{k}))$$

をもつ. $\rho_{S \cup S'_0, n}^{S'_0 - \text{new}} := \rho_{S \cup S'_0}^{S'_0 - \text{new}} \bmod p^n$ とおく.

$n = 1$ とする. 補題を使うと素数 q_1 で以下を満たすものが取れる:

- q_1 は $\rho_{S \cup S'_0}^{S'_0 - \text{new}}$ で不分岐である,
- $\rho_{S \cup S'_0, n}^{S'_0 - \text{new}}$ は q_1 でスペシャルである,
- $\rho_{S \cup S'_0, n+1}^{S'_0 - \text{new}}$ は q_1 でスペシャルでない.

まず $S'_0 \cup \{q_1\}$ は auxiliary であると仮定する. このとき, 同型 $R_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}} \simeq W(\mathbf{k})$ により普遍変形

$$\rho_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(W(\mathbf{k}))$$

をもつ. この変形の条件より, $\rho_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}}|_{G_{q_1}}$ は指標による twist を除いて

$$\begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}$$

と共役である. ここで $\rho_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}}$ が q_1 で不分岐であると仮定すると, $\rho_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}}$ は $\rho_{S \cup S'_0}^{S'_0 - \text{new}}$ を経由する. Witt 環の射の一意性より

$$\rho_{S \cup S'_0}^{S'_0 - \text{new}} = \rho_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}}$$

となる. よって $\rho_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}}$ は q_1 でスペシャルではないが, これは矛盾する. したがって, q_1 は $\rho_{S \cup S'_0 \cup \{q_1\}}^{S'_0 \cup \{q_1\} - \text{new}}$ で分岐する.

次に $S'_0 \cup \{q_1\}$ は auxiliary ではないと仮定する. 補題を使うと素数 q_2 で以下を満たすものが取れる:

- $\rho_{S \cup S'_0 \cup \{q_1\}, n}^{S'_0 \cup \{q_1\} - \text{new}}$ は q_2 でスペシャルである,
- $\rho_{S \cup S'_0 \cup \{q_1\}, n+1}^{S'_0 \cup \{q_1\} - \text{new}}$ は q_2 でスペシャルではない,
- $S''_0 := S'_0 \cup \{q_1, q_2\}$ は auxiliary である.

S''_0 が auxiliary であることを示すには, 少しガロアコホモロジーの計算を必要とする. 簡単に方針を述べておくと, S'_0 が auxiliary であることと, $\dim_{\mathbf{k}} H^1(G_{q_1}, \text{Ad}^0 \bar{\rho})/L_{q_1} = 1$ から (Wiles の公式などを使って)

$$\dim_{\mathbf{k}} H^1_{\{L_v\}}(G_{S \cup S'_0 \cup \{q_1\}}, \text{Ad}^0 \bar{\rho}) = \dim_{\mathbf{k}} H^1_{\{L_v\}}(G_{S \cup S'_0 \cup \{q_1\}}, \text{Ad}^0 \bar{\rho}(1)) = 1$$

がわかる. また補題の 2 と 3 から, q_2 は持ち上げ定理の証明の中の条件 1 から 5 を満たすことが分かる. このことからセルマー群の次元が 1 つ落ちて auxiliary であることが分かる. 詳細は [T] の Lemma 1.2 を見られたい.

S''_0 は auxiliary であるから $S'_0 \cup \{q_1\}$ が auxiliary である場合と同様に, 同型 $R_{S \cup S''_0}^{S''_0 - \text{new}} \simeq W(\mathbf{k})$ により普遍変形

$$\rho_{S \cup S''_0}^{S''_0 - \text{new}} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(W(\mathbf{k}))$$

をもつ. このとき, $\rho_{S \cup S''_0}^{S''_0 - \text{new}}$ は q_1 と q_2 の両方ともで不分岐であると仮定すると $\rho_{S \cup S''_0}^{S''_0 - \text{new}}$ は $\rho_{S \cup S'_0}^{S'_0 - \text{new}}$ を経由するから

$$\rho_{S \cup S''_0}^{S''_0 - \text{new}} = \rho_{S \cup S'_0}^{S'_0 - \text{new}}$$

となる. しかしこれは q_1 と q_2 の取り方により, $\rho_{S \cup S''_0}^{S''_0 - \text{new}}$ の変形の条件に矛盾する. したがって, 少なくとも q_1 か q_2 のどちらか一方は必ず分岐する.

そこで, もし $S'_0 \cup \{q_1\}$ が auxiliary であるならば, $S'_1 := S'_0 \cup \{q_1\}$ とおく. また, もし $S'_0 \cup \{q_1\}$ が auxiliary でないならば, $S'_1 := S''_0$ とおく. このとき, S'_1 は次の条件を満たしている:

- S'_1 は auxiliary である,
- $\rho_{S \cup S'_0, n}^{S'_0 - \text{new}} = \rho_{S \cup S'_1, n}^{S'_1 - \text{new}}$ を満たす,
- $\rho_{S \cup S'_1}^{S'_1 - \text{new}}$ は $S'_1 \setminus S'_0$ の少なくとも 1 つの素数で分岐している.

$n \geq 2$ で同じ事を帰納的に繰り返すと, 列

$$\rho_{S \cup S'_0}^{S'_0 - \text{new}}, \rho_{S \cup S'_1}^{S'_1 - \text{new}}, \dots, \rho_{S \cup S'_k}^{S'_k - \text{new}}, \dots$$

ができる. すると $\rho_{S \cup S'_k}^{S'_k - \text{new}}$ は $S'_k \setminus S'_{k-1}$ の少なくとも 1 つの素数で分岐していて, $\rho_{S \cup S'_k, k+1}^{S'_k - \text{new}} = \rho_{S \cup S'_{k+1}, k+1}^{S'_{k+1} - \text{new}}$ を満たす. したがって,

$$\varprojlim_k \rho_{S \cup S'_k, k+1}^{S'_k - \text{new}} : G_{\mathbb{Q}} \rightarrow \varprojlim_k \text{GL}_2(W(\mathbf{k})/p^{k+1}) = \text{GL}_2(W(\mathbf{k}))$$

は無限個の素数で分岐する.

参考文献

- [B] G. Böckle Presentations of universal deformation rings, In: D. Burns, K. Buzzard and J. Nekovář (eds.), *L-Functions and Galois Representations*, Cambridge University Press (2007).
- [Ch] 千田 雅隆, ガロア表現の基礎 II, in this proceeding.
- [E] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), 563–594.
- [Ima] 今井 直毅, Galois 表現の変形理論入門, in this proceeding.
- [KLR] C. Khare, M. Larsen and R. Ramakrishna, *Transcendental l -adic Galois representations*, Math. Res. Letters **12** (2005), 685–700.
- [KRaj] C. Khare and C. S. Rajan, *The density of ramified primes in semisimple p -adic Galois representations*, Internat. Math. Res. Notices (2001), 601–607.
- [KRam] C. Khare and R. Ramakrishna, *Finiteness of Selmer groups and deformation rings*, Invent. Math. **154** (2003), 179–198.
- [M1] B. Mazur, *Deforming Galois representations*, in Galois groups over $\mathbb{Q}$, ed. Ihara et al., Springer, Berlin, 2000.
- [M2] B. Mazur, *An introduction to the deformation theory of Galois representations*, in “Modular forms and Fermat’s last theorem” (Boston, MA, 1995), 243–311, Springer, New York, 1997.
- [Mi] 三枝 洋一, エタールコホモロジーと l 進表現, in this proceeding.
- [NSW] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, **323**. Springer-Verlag, Berlin, 2000.

- [R1] R. Ramakrishna, *Lifting Galois representations*, Invent. Math. **138** (1999), 537–562.
- [R2] R. Ramakrishna, *Infinitely ramified representations*, Ann. of Math. **151** (2000), 793–815.
- [R3] R. Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, Ann. of Math. **156** (2002), 115–154.
- [Ri1] K. Ribet, *On l -adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275.
- [Ri2] K. Ribet, *On l -adic representations attached to modular forms II*, Glasgow Math. J. **27** (1985), 185–194.
- [Sa] 佐藤 周友, ガロアコホモロジー, in this proceeding.
- [T] R. Taylor, *On icosahedral Artin representations, II*, Amer. J. Math. **125** (2003), 549–566.