日本数学会・企画特別講演　　2009 年 3 月 26 日 (木) 13:00–14:00

佐藤 - テイト予想の解決と展望
— 非可換類体論の進展 —

Solution of the Sato-Tate Conjecture and Beyond

— Recent Developments in Non-abelian Class Field theory —

伊藤 哲史[1]

Tetsushi Ito

京都大学大学院理学研究科数学教室

Department of Mathematics, Faculty of Science, Kyoto University

1. はじめに

2006 年春，ハーバード大学教授のリチャード・テイラー (Richard Taylor) は，クローゼル (Clozel)，ハリス (Harris)，シェパード＝バロン (Shepherd-Barron) との共同研究に基づき，**佐藤 - テイト予想** (Sato-Tate conjecture) が多くの場合に解決されたことを発表した[2]．テイラーらはワイルズ (Wiles) により突破口が開かれた谷山 - 志村予想の証明の方法[3]を階数の高いユニタリ群 $U(n)$ に一般化することで高次元のガロア表現の保型性予想を（弱い形で）証明し，その帰結として佐藤 - テイト予想を解決したのである．

この講演では，佐藤 - テイト予想がどういう予想で，それが現代の整数論の中でどのような位置を占めていて，そしてテイラーらがそれをどのように証明したのかを紹介する．大ざっぱに言えば，楕円曲線から定まる n 次元ガロア表現の（潜）保型性から対称積 L 関数の解析的性質が導かれ，それから佐藤 - テイト予想が導かれる．L 関数の解析的性質の研究は現代の整数論の中心的なテーマであり，佐藤 - テイト予想はまさにその中心に位置する予想であると言える[4]．また，関連する話題として，カーレ (Khare) とヴァンテンベルジェ

[1]e-mail : tetsushi@math.kyoto-u.ac.jp

[2]3 本の論文からなる ([1], [2], [3])．[1], [3] は 2008 年に出版された．[2] は Annals of Mathematics 誌 (ワイルズがフェルマーの最終定理の証明を発表した雑誌) への掲載が決まっている．

[3]テイラー - ワイルズ系，$R = T$ 定理，保型性の持ち上げ定理など — ダイアモンド (Diamond)，藤原一宏，スキナー (Skinner)，キシン (Kisin) らにより一般化されていた．

[4]世の中には成り立っているかどうか証明されるまで分からないような予想がごまんとある．フェルマーの最終定理は,『難問題であるほかには，事実として興味のあるでもないこのような問題』([11] 高木貞治，初等整数論講義 第 2 版，p.252) にすぎなかった．(リベット (Ribet) により谷山 - 志村予想の系として得られることが示されるまでは！)

(Wintenberger) により 2007 年頃に解決された**セール予想** (Serre conjecture) についても述べる.

佐藤 - テイト予想とセール予想は表面的には異なる予想だが，その背後には，ウェーバー (Weber)，ヒルベルト (Hilbert)，高木貞治，アルチン (Artin) らにより 20 世紀初頭に打ち立てられた**類体論**（アーベル拡大の相互法則）を一般化する**非可換類体論**と呼ばれる枠組みがある[5]．実際，これらの 2 つの予想の証明のアイデアは似通っている．技術的には，キシンによる「ガロア表現の枠付き変形」「$R^{\mathrm{red}} = T$ 定理」（$R = T$ 定理の変種）とテイラーによる「潜保型性」が重要な役割を果たす.

2. 佐藤 - テイト予想

佐藤 - テイト予想は楕円曲線の mod p 有理点の個数の分布に関する予想である．有理数体 $\mathbb{Q}$ 上の**楕円曲線**とは，射影空間 $\mathbb{P}^2$ の中で方程式

$$E : y^2 = x^3 + ax + b \qquad (a, b \in \mathbb{Z},\ 4a^3 + 27b^2 \neq 0)$$

で定義された曲線のことをいう．E の **j-不変量**が

$$j(E) = \frac{1728 \cdot 4a^3}{4a^3 + 27b^2}$$

で定義される．E 上には無限遠点を単位元としたアーベル群の構造が定まる．$\mathbb{C}$ 係数の有理式で定義された写像 $f\colon E \to E$ で無限遠点を無限遠点に写すもの全体を $\mathrm{End}_{\mathbb{C}}(E)$ とおく．$\mathrm{End}_{\mathbb{C}}(E) \neq \mathbb{Z}$ のとき E **は虚数乗法を持つ**という[6]．$4a^3 + 27b^2$ と互いに素な 5 以上の素数 p に対し，方程式 $y^2 \equiv x^3 + ax + b \pmod{p}$ は有限体 $\mathbb{F}_p$ 上の楕円曲線を定める．その $\mathbb{F}_p$-有理点の個数を $\#E(\mathbb{F}_p)$ とおく．具体的に書くと

$$\#E(\mathbb{F}_p) = \#\left\{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \;\middle|\; 0 \leqq x, y \leqq p-1,\ y^2 \equiv x^3 + ax + b \pmod{p} \right\} + 1$$

である[7]．**ハッセの定理**より不等式

$$\left| p + 1 - \#E(\mathbb{F}_p) \right| \leqq 2\sqrt{p}$$

が成り立つ（ハッセの定理については [14] も参照）．つまり，$\#E(\mathbb{F}_p)$ は $p+1$ とほぼ等しく，その誤差は高々 $2\sqrt{p}$ である．実数 θ_p を用いて

$$p + 1 - \#E(\mathbb{F}_p) = 2\sqrt{p}\cos\theta_p \qquad (0 \leqq \theta_p \leqq \pi)$$

とおく.

---

[5] **非可換相互法則**や**ラングランズ対応**とも呼ばれる.

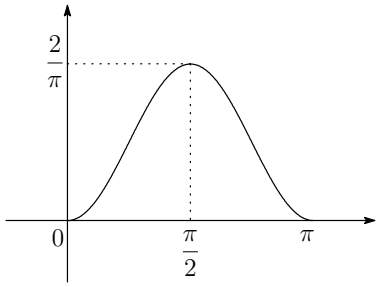
[6] E が虚数乗法を持つとき，$\mathrm{End}_{\mathbb{C}}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ は虚二次体になる．虚数乗法を持つ楕円曲線は虚二次体の類体の構成に応用がある (**クロネッカー (Kronecker) の青春の夢**).

[7] 最後に「+1」がついているのは，E の無限遠点も込めて有理点を数えていることに対応する.

予想 2.1 (**佐藤 - テイト予想**)**.** 楕円曲線 E が虚数乗法を持たないと仮定する．実数 α, β $(0 \leqq \alpha < \beta \leqq \pi)$ に対し，

$$\lim_{N\to\infty} \frac{(N \text{ 以下の素数 } p \text{ で，} \alpha \leqq \theta_p \leqq \beta \text{ をみたすものの個数})}{(N \text{ 以下の素数 } p \text{ の個数})} = \frac{2}{\pi}\int_{\alpha}^{\beta} \sin^2\theta\, d\theta$$

が成り立つ.



図． $y = \dfrac{2}{\pi}\sin^2\theta$ のグラフと銅鐸[8]

予想 2.1 は，難波完爾による数値実験の結果をもとに，1963 年春頃に佐藤幹夫により提出された (歴史については [12], [13] を参照)．その後，テイト (Tate) とセール (Serre) が理論的枠組みを整備し，今日では「佐藤 - テイト予想」と呼ばれるようになった.

定理 2.2 (クローゼル，ハリス，シェパード＝バロン，テイラー ([1], [2], [3]))**.** もし E の j-不変量 $j(E)$ が**整数でなければ**，佐藤 - テイト予想 (予想 2.1) は正しい.

ここでは $\mathbb{Q}$ 上の楕円曲線に対する定式化を説明したが，実際には，テイラーらは，より一般に総実代数体上の楕円曲線で j-不変量が代数的整数でないものに対して佐藤 - テイト予想を証明している.

3. セール予想

セール予想は 2 次元 mod ℓ ガロア表現に対する保型性予想である.

まずガロア表現について簡単に復習しよう．$\overline{\mathbb{Q}}$ を有理数体 $\mathbb{Q}$ の代数閉包とし，p 進体 $\mathbb{Q}_p$ の代数閉包 $\overline{\mathbb{Q}}_p$ と $\mathbb{C}$ との体同型 $\mathbb{C} \cong \overline{\mathbb{Q}}_p$ を固定する．$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ と考える．自然な全射 $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ による $(x \mapsto x^{p^{-1}}) \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ の逆像から元を 1 つ選び，Frob_p と書く (**幾何的フロベニウス元**という)．また，自然な埋め込み $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ による複素共役の像を c で表す．連続準同型

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$$

[8] この 2 つの形が似ていることは，加藤和也先生 (京大理) に指摘していただきました.

を n **次元 mod ℓ ガロア表現**という[9]．ρ を考えることと，有限次ガロア拡大 $K/\mathbb{Q}$ と埋め込み $\iota\colon \mathrm{Gal}(K/\mathbb{Q}) \hookrightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ の組 (K, ι) を考えることは同値なので，**ガロア表現は代数学・方程式論の世界の対象である**といえる．

次に保型形式について述べる．大ざっぱに言って，保型形式とは上半平面上の正則関数

$$f\colon \left\{ z \in \mathbb{C} \,\middle|\, \mathrm{Im}(z) > 0 \right\} \longrightarrow \mathbb{C}$$

であって，**保型性**と呼ばれる変換法則

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),\ c \equiv 0 \pmod{N} \text{ に対し，} \quad f\left(\frac{az+b}{cz+d}\right) = \varepsilon(d)(cz+d)^k f(z)$$

をみたすものである．$\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ を**指標**，k を**重さ**，N を**レベル**という[10]．保型形式はアデール群 $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ の表現論 (保型表現論) とも深く関係するから，**保型形式は解析学・表現論の世界の対象である**といえる．

定理 3.1 (**セール予想，カーレ - ヴァンテンベルジェの定理**([4], [5]))**.** $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ を 2 次元 mod ℓ ガロア表現とする．ρ は既約で,「**奇**」である ($\det\rho(c) = -1$ をみたす (c は複素共役)) と仮定する．このとき，保型形式

$$f = \sum_{n=1}^{\infty} a_n q^n, \qquad q = \exp(2\pi i z)$$

が存在して，ほとんどすべての素数 p に対し，

$$\mathrm{Tr}\,\rho(\mathrm{Frob}_p) \equiv a_p \pmod{p}$$

が成り立つ (ρ を**保型形式 f に伴う mod ℓ ガロア表現**という[11])．

実際には，より精密に，ガロア表現 ρ の分岐の様子から f の（mod p 保型形式としての）「重さ」や「レベル」を決定することができる[12]．ρ の ℓ における分岐の様子から「重さ」(**セールの重さ** (Serre weight)) が定まり，ℓ 以外の素数における分岐の様子 (**導手**) から f の「レベル」が定まる．

逆の方向，すなわち「正則保型形式に伴う (奇な) ℓ 進ガロア表現や mod ℓ ガロア表現の存在」は，アイヒラー (Eichler)，志村五郎，ドリーニュ(Deligne)，セールらの仕事により，すでに知られていた[13]．

---

[9] $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ には離散位相を入れて考える．

[10] 保型形式の空間には**ヘッケ作用素**と呼ばれる線形写像 T_p（p は素数）が作用する．本稿では，保型形式としては，尖点形式であってヘッケ作用素の同時固有関数となるものしか考えない．

[11]「**偶**」($\det\rho(c) = 1$) な mod ℓ ガロア表現 ρ には実解析的保型形式（**マースの波動形式**でラプラス作用素の固有値が $\lambda = 1/4$ となるもの）が伴うと予想されているが，これについてはほとんど何も分かっていない．

[12] f の $\mathbb{C}$ 上の保型形式としての「重さ」や「レベル」より，mod p 保型形式としての「重さ」や「レベル」の方が小さいこともある．

[13] **モジュラー曲線**の**エタールコホモロジー**を使ってガロア表現を構成する．マースの波動形式については，どちらの方向も知られていない．

セール予想は「ガロア表現」と「保型形式」という異なる 2 つの世界の対象を結びつける予想であり，理論的にはもちろん応用上も重要である．定理 3.1 に「保型性の持ち上げ定理」とファルティンクス (Faltings) の同種定理を組み合わせることで，谷山 - 志村予想の高次元版が得られる．($g = 1$ の場合が**谷山 - 志村予想**である．)

系 3.2 (GL(2) **型アーベル多様体の保型性**)**.** A を $\mathbb{Q}$ 上の g 次元アーベル多様体で，g 次拡大 $F/\mathbb{Q}$ と埋め込み $F \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ が存在すると仮定する．このとき，ある $N \geqq 1$ に対し，$\mathbb{Q}$ 係数の有理式で定義された定数でない写像 $\pi\colon X_1(N) \longrightarrow A$ が存在する ($X_1(N)$ はレベル N の**モジュラー曲線**).

系 3.3 (**2 次元アルチン予想**(**「奇」な場合**))**.** $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C})$ を既約表現とし，$\det \rho(c) = -1$ をみたすとする（c は複素共役）．ρ の L 関数を 2 次のオイラー積

$$L(s,\rho) := \prod_p \frac{1}{\det\left(1 - p^{-s}\rho(\mathrm{Frob}_p)\right)}$$

で定義する[14]．このとき，重さ 1 の保型形式 f で $L(s,\rho) = L(s,f)$ をみたすものが存在する．また，$L(s,\rho)$ は複素平面全体に正則関数として解析接続される．

セール予想 (定理 3.1) から系 3.3 が導かれることは次のようにして分かる．$\rho \pmod p$ に定理 3.1 を適用すると，$\rho \pmod p$ の保型性が分かる．これを無限個の p で行う．重さ 1，レベル N (N は ρ の導手) の保型形式の空間は有限次元だから，重さ 1 の保型形式 $f = \Sigma_n a_n q^n$ であって，合同式 $\mathrm{Tr}\,\rho(\mathrm{Frob}_p) \equiv a_p \pmod p$ が無限個の p で成り立つものの存在が分かる．これより，$\mathrm{Tr}\,\rho(\mathrm{Frob}_p) = a_p$ が得られる[15].

これ以外の応用として，一般に，$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ **の「奇」な 2 次元** ℓ **進表現の整合系の保型性**を示すことができる．**ガロアの逆問題**への応用もある．また，谷山 - 志村予想からフェルマーの最終定理が証明されたのと類似の議論で，**一般フェルマー型方程式** $x^p + y^q = z^r$ $(p^{-1} + q^{-1} + r^{-1} < 1)$ が「非自明な整数解を持たない」ことが，いくつかの場合に証明できる[16].

---

[14]本当は分岐する p に対する局所因子を正しく定義する必要があるが，ここでは省略する．

[15]この議論は (ワイルズの仕事よりも前から知られていた) 「セール予想 $\Rightarrow$ 谷山 - 志村予想」の証明と同様である.「重さ 1 の mod p 保型形式」は $\mathbb{C}$ 上の重さ 1 の保型形式に持ち上がるとは限らないから，少しだけ注意が必要である．有限個の「悪い p」を除いて議論すればよい (カーレ).

[16]田口雄一郎さん (九大数理) に教えていただきました．Darmon, H, *A fourteenth lecture on Fermat's Last Theorem*, Number theory, 103–115, CRM Proc. Lecture Notes 36, A.M.S., 2004 (`http://www.math.mcgill.ca/darmon/pub/Articles/Expository/09.Ribenboim/paper.pdf`) に紹介されています.

4. ゼータ関数と密度定理

素数の分布を研究するためには,「ゼータ関数」や「L 関数」と呼ばれる解析関数を考察する手法が強力である．ゼータ関数や L 関数の解析的性質から，素数に関する密度定理が導かれることを説明しよう．

ゼータ関数の中で最も基本的なものは**リーマン (Riemann) のゼータ関数**

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^2} + \frac{1}{6^s} + \cdots$$

である．上式の右辺は $\mathrm{Re}(s) > 1$ で絶対収束し，複素平面全体に有理型関数として解析接続され，$s = 1$ における一位の極を除いて正則である．$\zeta(s)$ は自然数に関する和（**ディリクレ (Dirichlet) 級数**）で定義されるが，素数に関する積 (**オイラー積**) の形に表すこともできる:

$$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}.$$

ゼータ関数 $\zeta(s)$ の解析的性質を研究することで，素数の分布に関する結果を導くことができる．例として,「$\zeta(1) = \infty$」を使って素数の逆数和が発散することを証明してみよう．$\mathrm{Re}(s) > 1$ において定義される解析関数

$$\log \zeta(s) = \sum_{p} -\log(1 - p^{-s}) = \sum_{p} \frac{1}{p^s} + \left(\sum_{p} \sum_{m=2}^{\infty} \frac{1}{m p^{ms}} \right)$$

を考える．$s \to 1$ で上式の右端の括弧の中は有界なので,

$$\lim_{s \to 1} \left(\sum_{p} \frac{1}{p^s} \right) = \lim_{s \to 1} \log \zeta(s) = \infty$$

となり，素数の逆数和が発散することが分かる．

さらに詳しく，素数の「密度」を評価するにはもう少し精密な解析的性質が必要となる．アダマール (Hadamard) とド・ラ・ヴァレ＝プーサン (de la Vallée Poussin) は，1896 年に「$\zeta(s)$ が $\mathrm{Re}(s) \geqq 1$ で零点を持たない」ことを示し，その応用として**素数定理**

$$\lim_{N \to \infty} \left((N \text{ 以下の素数 } p \text{ の個数}) \cdot \frac{\log N}{N} \right) = 1$$

を証明した．

次に 1837 年にディリクレによって証明された算術級数定理について述べよう．

定理 4.1 (**算術級数定理**)**.** $m \geqq 1$ を自然数とし a を m と互いに素な整数とすると，$p \equiv a \pmod{m}$ をみたす素数 p が無限個存在する．

ディリクレによる証明を思い出そう．準同型 $\chi\colon (\mathbb{Z}/m\mathbb{Z})^{\times} \longrightarrow \mathbb{C}^{\times}$ を (m を法とする) **ディリクレ指標**という．m と互いに素な整数 a を固定する．有限群の表現論（指標の直交性）か

ら，定数 $c_\chi \in \mathbb{C}$ をうまくとると，m と互いに素な整数 m に対し，

$$\sum_\chi c_\chi \chi(r) = \begin{cases} 1 & r \equiv a \pmod m \text{ のとき} \\ 0 & \text{そうでないとき} \end{cases}$$

が成り立つ[17]．自明指標 $\chi_{\mathrm{triv}} = 1$ に対し，$c_{\chi_{\mathrm{triv}}} = \dfrac{1}{\#(\mathbb{Z}/m\mathbb{Z})^\times} = \dfrac{1}{\varphi(m)}$ である．**ディリクレの L 関数**を

$$L(s,\chi) := \prod_p \frac{1}{1-\chi(p)p^{-s}}$$

で定めると[18]，

$$\begin{aligned} \sum_\chi c_\chi \log L(s,\chi) &= \sum_\chi c_\chi \left(\sum_p \frac{\chi(p)}{p^s} \right) + R_1(s) \\ &= \left(\sum_{p \equiv a \,(\mathrm{mod}\, m)} \frac{1}{p^s} \right) + R_2(s) \qquad \big(R_1(s), R_2(s) \text{ は } s \to 1 \text{ で有界}\big) \end{aligned}$$

と書ける．$\chi \neq \chi_{\mathrm{triv}}$ なら $L(s,\chi)$ は $s = 1$ で正則で $L(1,\chi) \neq 0$ が成り立つ[19]．左辺の和において $s \to 1$ で発散するのは $\chi = \chi_{\mathrm{triv}}$ の項だけである．(有限個の局所因子を除いて) $L(s,\chi_{\mathrm{triv}}) = \zeta(s)$ だから，$s \to 1$ の極限を考えて

$$\lim_{s\to 1} \left(\sum_{p \equiv a \,(\mathrm{mod}\, m)} \frac{1}{p^s} \right) = \lim_{s\to 1} \Big(c_{\chi_{\mathrm{triv}}} \log \zeta(s) \Big) = \lim_{s\to 1} \frac{-\log(s-1)}{\varphi(m)} = +\infty$$

となり，定理 4.1 が得られる．

ド・ラ・ヴァレ＝プーサンは，定理 4.1 を精密化して，密度バージョンの算術級数定理を証明した．

定理 4.2 (算術級数定理の密度バージョン).

$$\lim_{N\to\infty} \frac{(N \text{ 以下の素数 } p \text{ で } p \equiv a \pmod m \text{ をみたすものの個数})}{(N \text{ 以下の素数 } p \text{ の個数})} = \frac{1}{\varphi(m)}$$

証明のポイントは,「$\chi \neq \chi_{\mathrm{triv}}$ なら，$L(s,\chi)$ は $\mathrm{Re}(s) \geqq 1$ で正則で零点を持たない」ことを示すことである．

さて，佐藤 - テイト予想について，テイラーら以前に知られていたことを述べよう．E を虚数乗法を持たない楕円曲線とし，2 次方程式

$$T^2 - \big(p + 1 - \#E(\mathbb{F}_p)\big)T + p = 0$$

[17] もちろん当時は表現論は無かったから，ディリクレはこれを直接証明したのである．現代的に言えば，有限アーベル群 $(\mathbb{Z}/m\mathbb{Z})^\times$ 上の $a \pmod m$ に台を持つデルタ関数を「フーリエ変換」している．こういったところに，表現論が誕生する息吹を感じることができるのではないだろうか．

[18] 本当は m を割り切る有限個の p に対する局所因子を「正しく」定義する必要があるが，密度定理への応用上は有限個の素数を無視しても構わないので，ここでは省略する．

[19] これは類数公式とも関係した深い定理である．$\chi^2 = 1$ の場合が難しく，何通りもの証明が知られている ([8] を参照).

の解を $\{\alpha_p, \beta_p\}$ とおく．E の L **関数**を **2 次のオイラー積**[20]

$$L(s,E) := \prod_p \frac{1}{(1-\alpha_p p^{-s})(1-\beta_p p^{-s})} = \prod_p \frac{1}{1-\big(p+1-\#E(\mathbb{F}_p)\big)p^{-s}+p^{1-2s}}$$

で定める．また，$n \geqq 0$ に対して，**対称積** L **関数**を $(n+1)$ **次のオイラー積**

$$L(s,E,\mathrm{Sym}^n) := \prod_p \prod_{k=0}^{n} \frac{1}{1-\alpha_p^k \beta_p^{n-k} p^{-s}}$$

で定める[21]．ハッセの定理より $|\alpha_p| = |\beta_p| = \sqrt{p}$ が成り立つから，$L(s,E,\mathrm{Sym}^n)$ は $\mathrm{Re}(s) > 1+n/2$ で絶対収束することが分かる．

テイトとセールはタウバー型定理と $\mathrm{SU}(2)$ の表現論[22]を用いることで，対称積 L 関数の解析的性質から佐藤 - テイト予想が従うことを示した．

定理 4.3 (テイト，セール ([8]))**.** 全ての $n \geqq 1$ に対し，$L(s,E,\mathrm{Sym}^n)$ が $\mathrm{Re}(s) \geqq 1+n/2$ で正則で零点を持たなければ，佐藤 - テイト予想 (予想 2.1) は正しい．

5. 非可換類体論の視点から

対称積 L 関数 $L(s,E,\mathrm{Sym}^n)$ の解析的性質を定義から直接証明することは難しい．それは，オイラー積の各項を定める $\{\alpha_p, \beta_p\}$ が「素数 p ごとに定まっている」からである．そこで，$L(s,E,\mathrm{Sym}^n)$ を解析的性質が比較的よく分かる別の種類の L 関数と結びつけることを考える．その鍵となるのが**非可換類体論**と呼ばれる枠組みである．

類体論 ($\mathbb{Q}$ の場合は円分体論) から，$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の指標とイデール類群 $\mathbb{A}_{\mathbb{Q}}^{\times}/\mathbb{Q}^{\times}$ の指標（ヘッケ指標）の間の L 関数を保つ対応が得られる．その非可換化として

(5.1) “**予想**”：n 次元ガロア表現の L 関数は，$\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ の保型表現の L 関数と一致する．

という “予想” (**大域ラングランズ (Langlands) “予想”**) がある．この “予想” から佐藤 - テイト予想が**自然に導かれる**ことを説明しよう．

ポイントは，楕円曲線のテイト加群から 2 次元 ℓ 進ガロア表現

$$\rho_{E,\ell} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

が得られ，$\rho_{E,\ell}$ の L 関数を 2 次のオイラー積

$$L(s,\rho_{E,\ell}) := \prod_p \frac{1}{\det\big(1-p^{-s}\rho_{E,\ell}(\mathrm{Frob}_p)\big)}$$

[20] E の定義方程式が $y^2 = x^3+ax+b$ のとき，p は $4a^3+27b^2$ と互いに素な 5 以上の素数を動く．すべての p に対して L 関数の局所因子を「正しく」定義することもできるが，ここでは省略する．

[21] (有限個の局所因子を除いて) $L(s,E,\mathrm{Sym}^0) = \zeta(s)$，$L(s,E,\mathrm{Sym}^1) = L(s,E)$ である．

[22] $\mathrm{SU}(2)$ の全ての既約表現が自然表現の対称積で得られることがポイントである．全ての χ に対する $L(s,\chi)$ の解析的性質から算術級数定理が得られるのと同様に，全ての n に対する $L(s,E,\mathrm{Sym}^n)$ の解析的性質から佐藤 - テイト予想が導かれる．なお，関数「$\sin^2\theta$」は，$\mathrm{SU}(2)$ のハール測度を跡写像 $\mathrm{Tr}\colon \mathrm{SU}(2) \to [-2,2]$，$A \mapsto \mathrm{Tr}\,A$ で押し出したもの（のスケール変換）に対応する．

で定めると L 関数の等式[23] $L(s,\rho_{E,\ell}) = L(s,E)$ が成り立つことである．また，$\rho_{E,\ell}$ と対称積 $\mathrm{Sym}^n\colon \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell) \longrightarrow \mathrm{GL}_{n+1}(\overline{\mathbb{Q}}_\ell)$ を合成することで $(n+1)$ 次元ガロア表現

$$\mathrm{Sym}^n\rho_{E,\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho_{E,\ell}} \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell) \xrightarrow{\mathrm{Sym}^n} \mathrm{GL}_{n+1}(\overline{\mathbb{Q}}_\ell)$$

が得られ，L 関数の等式 $L(s,\mathrm{Sym}^n\rho_{E,\ell}) = L(s,E,\mathrm{Sym}^n)$ が成り立つ．すなわち，**楕円曲線の対称積 L 関数 $L(s,E,\mathrm{Sym}^n)$ は $(n+1)$ 次元 ℓ 進ガロア表現 $\mathrm{Sym}^n\rho_{E,\ell}$ の L 関数であること**が分かる．

大域ラングランズ “予想” により，$\mathrm{Sym}^n\rho_{E,\ell}$ は**保型的**であること，すなわち

$$L(s+n/2,\,\mathrm{Sym}^n\rho_{E,\ell}) = L(s,\Pi_{n+1})$$

をみたす $\mathrm{GL}_{n+1}(\mathbb{A}_\mathbb{Q})$ **の尖点的**[24]**な保型表現** Π_{n+1} が存在することが期待される．そして，保型表現の L 関数については $L(s,\Pi_{n+1})$ は $\mathrm{Re}(s) \geqq 1$ で正則で零点を持たないことが分かっているから，$L(s,E,\mathrm{Sym}^n)$ が $\mathrm{Re}(s) \geqq 1+n/2$ で正則で零点を持たないことが期待される．

(5.1) であえて “予想” と “　” で囲って書いたのは，この形ではまだ数学的な予想になっていないからである．ラングランズにより，代数多様体からエタールコホモロジーによって得られる ℓ 進ガロア表現は常に保型的であると予想されている．一方で，**フォンテーヌ - メイザー予想** (Fontaine-Mazur conjecture) によると，有限個の素数を除き不分岐で「ℓ **でド・ラーム**[25]」な $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の ℓ 進表現は，代数多様体からエタールコホモロジーによって得られると予想されている．この 2 つの予想を組み合わせて，$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の 2 次元 ℓ 進表現に関する保型性予想を，数学的な予想として定式化することができる．

予想 5.1 (**フォンテーヌ - メイザー + ラングランズ予想**)**.** ρ を $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の 2 次元 ℓ 進表現とし，有限個の素数を除き不分岐で「ℓ でド・ラーム」と仮定する．

(1) ρ が「**奇**」なら，整数 n と**正則保型形式** f が存在して，$L(s+n/2,\,f) = L(s,\rho)$ が成り立つ．
(2) ρ が「**偶**」なら，整数 n と**マースの波動形式** f（でラプラス作用素の固有値が $\lambda = 1/4$ となるもの）が存在して，$L(s+n/2,\,f) = L(s,\rho)$ が成り立つ．

もう少し正確に，上の予想に現れる整数 n や保型形式 f の重さを，ρ の「**ホッジ - テイトの重さ**」を用いて記述することもできる．

---

[23]本当は有限個の悪い素数で正しく局所因子を定める必要があるが，ここでは省略する．$p=\ell$ における局所因子の定義には p **進ホッジ理論** (フォンテーヌの D_{pst} 関手) が必要である．

[24]$\mathrm{Sym}^n\rho_{E,\ell}$ が $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の**既約表現**になることがセールにより示されているので（ここで E **が虚数乗法を持たない**という仮定を用いる），Π_{n+1} は**尖点的**であると期待される．

[25]「ℓ でド・ラーム」とは，$p=\ell$ における p 進ホッジ理論から来る**局所的な条件**であり，**ガロア表現の代数性**を記述していると考えられる．このことは，コルメツ (Colmez) の p **進局所ラングランズ対応**によって，明快に説明される．

予想 5.2 (GL_n **の大域ラングランズ予想**)**.** 有限個の素数を除き不分岐で「ℓ **でド・ラーム**」な $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の n 次元 (既約)ℓ 進表現 ρ と，$\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ の「**代数的**」な (尖点的) 保型表現 Π の間には，L 関数を保つ一対一の対応 (**大域ラングランズ対応**) がある．

数論幾何（特に p 進ホッジ理論）の進展により，非可換類体論の予想を，数学的な予想として定式化できるようになった．この定式化には**ラングランズ双対群**などの「仮想的な群」は必要ない．また,「1 つの ℓ」しか現れない．(古典的な定式化と異なり) ガロア表現の整合系を考察する必要がないことにも注意しておこう．

6. 証明の方針

佐藤 - テイト予想とセール予想の証明の方針を大ざっぱに説明しよう．詳細は原論文 [1], [2], [3], [4], [5] や解説記事 [9], [13] を参照していただきたい．証明の中では，ガロア表現の「整合系」と「保型性の持ち上げ定理」が効果的に用いられる．

ガロア表現の整合系は谷山豊によって考案された概念である．一般に，代数多様体のエタールコホモロジーから ℓ 進ガロア表現 ρ_ℓ が得られる．ℓ として様々な素数を取ることができ，それらを全てまとめたもの $\{\rho_\ell\}_\ell$ をガロア表現の**整合系** (Compatible System) という．整合系の中で L 関数は不変である[26]．整合系だけではあまり役に立たないが，次に述べる保型性の持ち上げ定理と組み合わせることで威力を発揮する．

ℓ 進ガロア表現 $\rho_\ell\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ が保型的なとき，それを $\bmod \ell$ して得られるガロア表現 $\rho_\ell \pmod{\ell}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ はもちろん保型的である．この逆

$$\rho_\ell \pmod{\ell} : \text{保型的} \quad \Rightarrow \quad \rho_\ell : \text{保型的}$$

が成り立つというタイプの定理を総称して**保型性の持ち上げ定理** (Modularity Lifting Theorem) という．テイラー - ワイルズ以降，様々なタイプの保型性の持ち上げ定理が得られている．キシンによる「ガロア表現の枠付き変形」を用いて示される保型性の持ち上げ定理は特に有用であり，佐藤 - テイト予想とセール予想の両方の証明の中で本質的な役割を果たす．

6.1. **佐藤 - テイト予想の証明の方針.** 前節でガロア表現 $\mathrm{Sym}^n\rho_{E,\ell}$ の保型性から佐藤 - テイト予想が自然に導かれることを説明した．しかし，テイラーらは $\mathrm{Sym}^n\rho_{E,\ell}$ の保型性を証明したの**ではない**．テイラーらが証明したのは $\mathrm{Sym}^n\rho_{E,\ell}$ の**潜保型性**— 総実代数体 $F/\mathbb{Q}$ と $\mathrm{GL}_{n+1}(\mathbb{A}_F)$ の保型表現 $\Pi_{F,n+1}$ が存在して，

$$L\big(s+n/2,\, (\mathrm{Sym}^n\rho_{E,\ell})|_{\mathrm{Gal}(\overline{F}/F)}\big) = L(s, \Pi_{F,n+1})$$

[26]任意の素数 ℓ, ℓ' に対し，ρ_ℓ, $\rho_{\ell'}$ の L 関数の局所因子が有限個の素数を除いて等しい．全ての素数における局所条件を課した**強整合系**の概念もあり，重要だが，本稿では説明しない．

をみたすこと — である[27]．**ブラウアー (Brauer) の誘導定理**とアーサー (Arthur) - クローゼルの基底変換定理を用いると，潜保型性から対称積 L 関数の解析的性質を導くことができ，佐藤 - テイト予想を証明することができる．

潜保型性の証明の概略は次の通りである．射影空間 $\mathbb{P}^{n+1}$ の中で，λ をパラメータとする n 次元**カラビ - ヤウ (Calabi-Yau) 多様体族**

$$C_\lambda : X_1^{n+2} + X_2^{n+2} + \cdots + X_{n+2}^{n+2} = (n+2)\lambda X_1 X_2 \cdots X_{n+2}$$

を考えよう[28]．$\lambda \in F$ のとき，C_λ の n 次エタールコホモロジー (の一部) をとることで，$\mathrm{Gal}(\overline{F}/F)$ の $(n+1)$ 次元ガロア表現の整合系

$$\left\{\tau_\ell \colon \mathrm{Gal}(\overline{F}/F) \longrightarrow \mathrm{GL}_{n+1}(\overline{\mathbb{Q}}_\ell)\right\}_\ell$$

が得られる．ここで総実代数体 F，パラメータ $\lambda \in F$，素数 $\ell' \neq \ell$ を**うまく**選ぶと[29]，$(n+1)$ 次巡回拡大 K/F と $\mathbb{A}_K^\times/K^\times$ の代数的ヘッケ指標に伴う 1 次元 ℓ' 進表現 ψ_K が存在して，

$$\begin{aligned}\tau_\ell &\equiv (\mathrm{Sym}^n \rho_{E,\ell})|_{\mathrm{Gal}(\overline{F}/F)} \pmod{\ell} \\ \tau_{\ell'} &\equiv \mathrm{Ind}_K^F \psi_K \pmod{\ell'}\end{aligned}$$

が成り立つ．つまり，**整合系 $\{\tau_\ell\}_\ell$ によって，ℓ 進ガロア表現 $(\mathrm{Sym}^n \rho_{E,\ell})|_{\mathrm{Gal}(\overline{F}/F)}$ と ℓ' 進ガロア表現 $\mathrm{Ind}_K^F \psi_K$ が「結ばれて」しまう**．アーサー - クローゼルの保型誘導定理により，誘導表現 $\mathrm{Ind}_K^F \psi_K$ は保型的なので，保型性の持ち上げ定理より，

$$\begin{aligned}\mathrm{Ind}_K^F \psi_K : \text{保型的} &\Rightarrow \tau_{\ell'} \pmod{\ell'} : \text{保型的} \\ &\Rightarrow \tau_{\ell'} : \text{保型的} \qquad \text{(保型性の持ち上げ定理)} \\ &\Rightarrow \tau_\ell : \text{保型的} \qquad (\{\tau_\ell\}_\ell \text{ が整合系をなすから}) \\ &\Rightarrow \tau_\ell \pmod{\ell} : \text{保型的} \\ &\Rightarrow (\mathrm{Sym}^n \rho_{E,\ell})|_{\mathrm{Gal}(\overline{F}/F)} \pmod{\ell} : \text{保型的} \\ &\Rightarrow (\mathrm{Sym}^n \rho_{E,\ell})|_{\mathrm{Gal}(\overline{F}/F)} : \text{保型的} \qquad \text{(保型性の持ち上げ定理)}\end{aligned}$$

となって，$\mathrm{Sym}^n \rho_{E,\ell}$ の潜保型性が導かれる[30]．

---

[27] 実際には，「n **が奇数**」などの様々な技術的条件が必要であるが，本稿では説明しない．

[28] $n = 1$ のときは楕円曲線族 $X^3 + Y^3 + Z^3 = 3\lambda XYZ$ である．$n = 2$ のときは $K3$ 曲面族である．実は，佐藤 - テイト予想の証明の中では，この族がカラビ - ヤウであること (標準因子が自明なこと) は**一切使わない**．十分豊富な ℓ 進ガロア表現 (の整合系) を生むモチーフの族であれば何でも構わないのである．

[29] うまいパラメータの存在には，カラビ - ヤウ多様体族の幾何的モノドロミーが大きいことと**モレ＝ベイイー (Moret-Bailly) の定理**を用いる．この部分が構成的でないため，現状では，$F/\mathbb{Q}$ のコントロールができない．

[30] 「保型性の持ち上げ定理」を適用するには様々な仮定が満たされている必要がある．それらが全て満たされるように，$F, \lambda, \ell', K, \psi_K$ を注意深く選ぶ必要がある．

6.2. **セール予想の証明の方針.** $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ を 2 次元 mod ℓ ガロア表現とする．証明の最初のステップは，ρ **を整合系に埋め込む**ことである．これは次のようにして示す．まず，佐藤 - テイト予想の証明と同様の方針で，ρ の潜保型性を示す[31]．総実代数体 $F/\mathbb{Q}$ と $\mathrm{GL}_2(\mathbb{A}_F)$ の保型表現 Π であって，$\rho|_{\mathrm{Gal}(\overline{F}/F)}$ が Π に伴う mod ℓ ガロア表現となるものをとる．すると，Π に伴う ℓ 進ガロア表現の整合系 $\{\rho_{\Pi,\ell}\}_\ell$ が存在するから，$\rho|_{\mathrm{Gal}(\overline{F}/F)}$ が整合系に埋め込まれることが分かる．ブラウアーの誘導定理を使ってもう少し議論すると，$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の ℓ 進表現の整合系 $\{\tau_\ell\}_\ell$ であって，$\rho \equiv \tau_\ell \pmod{\ell}$ をみたすものが構成できる．しかも，ガロア表現の変形環の構造を注意深く調べることで，τ_ℓ が適切な**局所条件**[32]をみたすように，整合系に埋め込むこともできる．

ここで，**もし仮に**，セール予想が ℓ より小さい素数で証明されていれば，佐藤 - テイト予想の証明と同様の論法が使える可能性がある．ℓ より小さい素数 $\ell' < \ell$ をとると，仮定より $\tau_{\ell'} \pmod{\ell'}$ は保型的だから，

$$\begin{aligned} \tau_{\ell'} \pmod{\ell'} : \text{保型的} &\Rightarrow \tau_{\ell'} : \text{保型的} \qquad (\text{保型性の持ち上げ定理}) \\ &\Rightarrow \tau_\ell : \text{保型的} \qquad (\{\tau_\ell\}_\ell \text{ が整合系をなすから}) \\ &\Rightarrow \tau_\ell \pmod{\ell} : \text{保型的} \end{aligned}$$

という方針が考えられる．しかし，現時点ではこのような単純な方法でセール予想を証明することは**できない**．その理由は，現在証明されている「保型性の持ち上げ定理」には様々な技術的仮定が必要であり，ℓ を簡単に小さくすることができないからである．また，帰納法の出発点として小さい ℓ（例えば $\ell = 2$ や 3）でセール予想を “直接証明” する必要があるが，それは難しいだろう．

この困難を克服するため，カーレ - ヴァンテンベルジェはかなり込み入った議論を行う．まず，整合系への埋め込みを**うまく**とって**余計な分岐を消していく**．

> **ℓ における分岐を減らす方法:** ρ が ℓ で沢山分岐している (セールの重さが大きい) としよう．このとき，ρ を整合系 $\{\tau_\ell\}_\ell$ に**うまく**埋め込み，素数 ℓ' ($\ell' \neq \ell$) を**うまく**選んで，$\tau_{\ell'} \pmod{\ell'}$ を考える．さらに，$\tau_{\ell'} \pmod{\ell'}$ を別の整合系 $\{\tau'_\ell\}_\ell$ に**うまく**埋め込んで，$\tau'_\ell \pmod{\ell}$ を考察する．「mod ℓ 表現 → mod ℓ' 表現 → mod ℓ 表現」と巧妙に移っていくことで，ℓ における分岐を減らす (セールの重さを小さくする) ことができる．

[31] 佐藤 - テイト予想よりも前に，テイラーはこの場合を研究していた．カラビ - ヤウ多様体族の代わりに**ヒルベルト - ブルメンタール (Hilbert-Blumenthal) のアーベル多様体族**が用いられる．テイラーによる「潜保型性」の論文 Taylor, R., *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu 1 (2002), no. 1, 125–143. と Taylor, R., *On the meromorphic continuation of degree two L-functions*, Doc. Math. 2006, Extra Vol., 729–779. はこの分野の「古典」と言ってよいだろう．

[32] カーレ - ヴァンテンベルジェの証明の中では,「**重さ 2 の整合系**」と「**ℓ でクリスタリンな整合系**」が巧妙に使い分けられている．

ℓ の外の分岐を減らす方法: ρ が素数 ℓ' ($\ell' \neq \ell$) で分岐していたとする．このとき，ρ を**うまく**整合系 $\{\tau_\ell\}_\ell$ に埋め込んだ後，$\tau_{\ell'}$ ($\mathrm{mod}\,\ell'$) を考える．「mod ℓ 表現 $\to$ mod ℓ' 表現」と移行することで，ℓ' における分岐が消えてしまう（ように見える）．これは，mod ℓ ガロア表現のレベルが，ℓ の外の分岐の様子にしかよらないことを巧妙に利用したテクニックである．

余計な分岐を消すことに成功したら，問題は，カーレが以前に証明した**レベル 1 の場合**[33]に帰着される．2 次元 mod ℓ ガロア表現 ρ が **ℓ の外で不分岐**であると仮定しよう．ここで**素数 ℓ に関する帰納法**を用いる．

「ρ を**うまく**整合系に埋め込み，素数 $\ell' \neq \ell$ を**うまく**選んで mod ℓ' をとる」

という操作を繰り返しながら，ℓ を小さくしていき，最終的に $\ell = 2, 3, 5$ の場合に帰着する．$\ell = 2, 3, 5$ のときは，既約な mod ℓ ガロア表現で ℓ の外で不分岐なものが存在しないから[34]，τ_ℓ ($\mathrm{mod}\,\ell$) は**可約**となり，スキナー - ワイルズの定理（剰余表現が可約な場合の保型性の持ち上げ定理[35]）が使えて，帰納法の出発点として機能するのである．

実際には，現在利用可能な「保型性の持ち上げ定理」には，様々な技術的仮定が必要である．整合系を使って素数 ℓ を次々と取り替えていく際，その仮定が全て満たされることを注意深く確かめておく必要があるため，カーレ - ヴァンテンベルジェの論文はかなり込み入ったものになってしまっている．詳しくは原論文 [4] を参照していただきたい．

7. 最近の進展

テイラーらの定理（定理 2.2）には「j-不変量 $j(E)$ が整数でない」という仮定がついていた．これは，ユニタリ型志村多様体を用いて GL_n の保型表現に伴うガロア表現を構成する際に跡公式の安定化の問題 (エンドスコピーの問題) を回避するための技術的な仮定である．最近のローモン (Laumon)，エンゴー (Ngo)，ヴァルジュプルジェ (Waldspurger) らによる「基本補題」の解決と，シン (Shin)，モレル (Morel) らの精力的な研究により，かなり弱い仮定の下でガロア表現が構成できるようになってきた．「j-不変量 $j(E)$ が整数でない」という仮定が外れる日も近いかもしれない．

総実代数体上のセール予想の研究も行われている．保型表現の「重さ」を mod ℓ ガロア表現を使って記述する際に，表現論的な困難が生じる (バザード (Buzzard), ダイアモンド, ジャービス (Jarvis)，ジー (Gee))．また，GL_n のセール予想の定式化の研究 (ヘルチッ

[33] Khare, C, *Serre's modularity conjecture: the level one case*, Duke Math. J. 134 (2006), no. 3, 557–589.

[34] $\ell = 2, 3$ のときはセール，テイトによる分岐の計算から分かる．$\ell = 5$ については，テイラーによる潜保型性を用いて，5 の外で良い還元を持ち 5 で半安定な $\mathbb{Q}$ 上のアーベル多様体は存在しないというブルメール (Brumer) とクラメール (Kramer)(およびスクーフ (Schoof)) の定理に帰着させる．

[35] 可約なガロア表現はアイゼンシュタイン級数に伴うから常に保型的である（類体論の帰結！）．

ヒ (Herzig)) や，GSp_4 に対する保型性の持ち上げ定理やセール予想の研究もある (ティルイン (Tilouine), ジェネスティ (Genestier))．

$\mathbb{Q}$ 上の GL_2 の場合も様々な進展がある．コルメツによる $\mathrm{GL}_2(\mathbb{Q}_p)$ の p 進局所ラングランズ対応を用いることで，従来よりもさらに弱い仮定の下で「保型性の持ち上げ定理」が得られるようになった (キシン)．コルメツの理論では，(φ,Γ)-加群を用いることで，ド・ラームとは限らない $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ の任意の p 進表現を「いっぺんに」扱うことができる．肥田理論 (p 進保型形式の理論) やセール予想を大域的な p 進ラングランズ対応や mod p ラングランズ対応として，保型表現の言葉で定式化する研究も進んでいる (エマートン (Emerton))．

8. おわりに

類体論の創始者である高木貞治の言葉を引用しよう．

> 『$\cdots$ 二次体と 1 の巾根との間に密接な関係のあることが感ぜられるであろう．有理整数に関する二次の問題が二次体の問題として取り扱われるときに透明なる解釈が可能で，それを説明することが本書後半部の目標であったが，それと同様に，二次体の整数論もさらに一段の高所から見おろすときに，初めてその全景をほしいままに展望することができるのである．その展望台は，すなわち 1 の巾根から生ずる数体 (Abel 体) の理論（現代的の「円理」!）である．われわれは明媚なる風景に魅惑せられて，いつか予定の目標を超えて，思わず深入りをしたが，このあたりでひとまず馬を返さねばなるまい.』
>
> ([11] 高木貞治，初等整数論講義 第 2 版，p.397)

類体論が確立されてから 80 年以上が経過して，私たちは，ようやく「非可換類体論」(ラングランズ対応) という新しい展望台に足を踏み入れることができるようになった．技術的な道具が発達したおかげで，従来は果てしなく難しいと思われていた佐藤 - テイト予想やセール予想にも手が届くようになった．しかし,『なぜ非可換類体論が成り立つのか?』という根本的な問いに対する答えは，いまだに得られていないと思う．私感だが，どうも，幾何的な部分に謎が隠されているような気がする (気のせいかもしれない)．ウィッテン (Witten) によると，ラングランズ対応は，幾何的にはヒッチン (Hitchin) のファイブレーションのミラー対称性として理解されるらしいが，私には何のことやらさっぱり分からない.「全景をほしいままに展望する」には，まだまだ時間がかかりそうである．

謝辞. 吉田輝義氏（ハーバード大・ケンブリッジ大），谷口隆氏（神戸大理）には原稿に目を通していただき，有益なコメントをいただきました．また，安田正大氏（京大数理研）には，セール予想の証明の細部を何時間にも渡って丁寧に解説していただき，本稿を執筆

する際の参考にさせていただきました.(紙数および著者の能力の問題から，セール予想の証明の細部については，ほとんど紹介することができなかったことをお詫びします.)

参考文献

[1] Clozel, L., Harris, M., Taylor, R., *Automorphy for some ℓ-adic lifts of automorphic mod ℓ representations*, Publ. Math. IHES 108 (2008), 1–181.
(`http://www.math.harvard.edu/~rtaylor/`)

[2] Harris, M., Shepherd-Barron, N., Taylor, R., *A family of Calabi-Yau varieties and potential automorphy*, to appear in Annals of Math.
(`http://www.math.harvard.edu/~rtaylor/`)

[3] Taylor, R., *Automorphy for some ℓ-adic lifts of automorphic mod ℓ representations. II*, Publ. Math. IHES 108 (2008), 183–239.
(`http://www.math.harvard.edu/~rtaylor/`)

[4] Khare, C., Wintenberger, J.-P., *Serre's modularity conjecture I,II*, preprint.
(`http://www.math.ucla.edu/~shekhar/papers/papers.html`
古いホームページ：`http://www.math.utah.edu/~shekhar/papers.html`)

[5] Kisin, M., *Modularity of 2-adic Barsotti-Tate representations*, preprint.
(`http://www.math.uchicago.edu/~kisin/preprints.html`)

[6] Serre, J.-P., *Abelian ℓ-adic representations and elliptic curves*, McGill University lecture notes, Benjamin, Inc., New York-Amsterdam 1968. (邦訳：J.-P. セール (鈴木治郎訳),『楕円曲線と ℓ 進アーベル表現』，ピアソン・エデュケーション, 1999 年．)

[7] リチャード・テイラー,『相互法則と密度定理』(日本語訳は [13] に収載．原文は `http://www.math.harvard.edu/~rtaylor/` から入手可能．)

[8] 加藤和也，斎藤毅，黒川信重,『数論 I — Fermat の夢と類体論』，岩波書店，2005 年.

[9] 加藤和也,『類体論と非可換類体論 I — フェルマーの最終定理・佐藤 - テイト予想解決への道』，岩波書店，2009 年.

[10] 斎藤毅,『フェルマー予想』，岩波書店，2009 年.

[11] 高木貞治,『初等整数論講義』 第 2 版，共立出版，1971 年.

[12] 『佐藤幹夫の数学』(木村達雄（編）)，日本評論社，2007 年.

[13] 数学のたのしみ，2008 最終号，フォーラム:現代数学のひろがり『佐藤 - テイト予想の解決と展望』，日本評論社，2008 年.

[14] 『この定理が美しい』，数学書房，2009 年 4 月刊行予定.

テイラーらによる佐藤 - テイト予想の証明は [1], [2], [3] に，カーレ - ヴァンテンベルジェによるセール予想の証明は [4] (および [5]) にまとめられている．楕円曲線の対称積 L 関数の解析的性質から佐藤 - テイト予想が導かれることは，セールによる ([6])．[7] にはテイラー自身による相互法則と密度定理についての非専門家向けの明快な解説があるので，ぜひ一読されたい．テイラー - ワイルズの仕事に関する日本語の文献は [10] がある．また，佐藤 - テイト予想の歴史や証明の解説については，[9], [12], [13] を参照していただきたい.