重さ 1 の保型形式と数論

(第 18 回 津田塾大学 数学史シンポジウム)

平松 豊一 (法政大学)　斎藤 正顕 (法政大学)

2007 年 10 月 28 日

＜目次＞

§1. Gauss (1777 ～ 1855) : 算術幾何平均

$$a \geqq b > 0,$$

$$a_0 = a, \quad b_0 = b,$$

$$a_{n+1} = \frac{a_n + b_n}{2}, \quad b_{n+1} = \sqrt{a_n b_n} \quad (n = 0, 1, 2, \cdots)$$

によって, 2 つの数列

$$\{a_n\}, \quad \{b_n\}$$

を定義する. そのとき,

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = M(a,b)$$

を a と b の算術幾何平均という.

ここで, $a, b \in \mathbb{C}^\times$, $a \neq \pm b$ として, $M(a,b)$ を拡張する. $M(a,b)$ の値を求める過程で, Gauss は次の重さ 1 の保型形式を発見した.

$$q = e^{\pi i \tau}, \quad \mathrm{Im}\,\tau > 0,$$

$$p(\tau) = 1 + 2\sum_{n=1}^{\infty} q^{n^2} \quad (= \theta_3(\tau))$$

$$q(\tau) = 1 + 2\sum_{n=1}^{\infty} (-1)^n q^{n^2} \quad (= \theta_4(\tau))$$

とするとき, $\{p(\tau)\}^2$, $\{q(\tau)\}^2$ は重さ 1 の保型形式である：

$$\Gamma(2)_0 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2) \,:\, a \equiv d \equiv 1 \pmod 4 \right\},$$

$$\Gamma(2)_4 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)_0 \,:\, c \equiv 0 \pmod 4 \right\}$$

とおくとき,

$$p(\gamma(\tau))^2 = (c\tau + d)p(\tau)^2, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)_0,$$

$$q(\gamma(\tau))^2 = (c\tau + d)q(\tau)^2, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)_4.$$

Gauss は, $\{p(\tau)\}^2$, $\{q(\tau)\}^2$ のフーリエ係数も計算している (ガウス全集 X_1).

§2. H.J.S. Smith (1826 ～ 1883) : Report on the theory of numbers, I～VI

$$\eta(\tau) = q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n) \text{ : Dedekind のエータ関数 } (q = e^{2\pi i \tau})$$

のとき,

$$\eta(8\tau)\eta(16\tau) = \sum_{n=1}^{\infty} a(n) q^n$$

が $\Gamma_0(128)$ に関する重さ 1 の cusp form であることを示し, $a(n)$ を決定した：VI (1894), 289-358 (§128)

p : を素数とする.

(1) $p \equiv 1 \pmod 8$ のとき,

$$a(p^v) = \varepsilon^v (-1)^{\frac{p^v - 1}{8}} (v + 1),$$

$$\varepsilon \equiv 2^{\frac{p-1}{4}} \pmod p \quad (\varepsilon = \pm 1);$$

(2) $p \equiv 3 \pmod 8$ のとき,

$$a(p^{2v}) = (-1)^v;$$

(3) $p \equiv 5, 7 \pmod 8$ のとき,

$$a(p^{2v}) = 1.$$

§3. E. Hecke (1887 ～ 1947), H. Petersson (1902 ～ 1984)

Hecke は

Zur Theorie der elliptischen Modulfunctionen, Math. Ann., Bd. **97**, 1926, S.210-242.

で 2 次体に関するテータ関数を導入した. すなわち, 虚 2 次体の類指標の L-関数または実 2 次体の類

指標の L-関数で Γ-因子が $\Gamma(\frac{s}{2})\Gamma(\frac{s+1}{2})$ タイプのものを夫々 Dirichlet 級数にもつ保型形式が重さ 1 の cusp form になることを示した：

F : 判別式 D の実 2 次体

$\mathfrak{O}_F$: F の全整数環

Q : 自然数

$\mathfrak{U}_0$: $\varepsilon \equiv 1 \bmod Q\sqrt{D}$ をみたす $\mathfrak{O}_F$ の総正単数群

$\mathfrak{a}$: $\mathfrak{O}_F$ の整イデアル, $|N(\mathfrak{a})| = A$

とするとき,

$$\vartheta_\kappa(\tau;\, \rho,\, \mathfrak{a},\, Q\sqrt{D}) = \sum_{\substack{\mu\in\mathfrak{O}_F \\ \mu\equiv\rho \bmod \mathfrak{a}Q\sqrt{D} \\ \mu\in\mathfrak{O}_F/\mathfrak{U}_0,\, N(\mu)\kappa>0}} (\operatorname{sgn}\mu)\, q^{N(\mu)/AQD},$$

ここで, $\kappa = \pm 1$, $\rho \in \mathfrak{a}$ とする. このとき, $\vartheta_\pm$ は, level QD のある種の合同部分群に関する重さ 1 の cusp form である. ただし, $\vartheta_\kappa \not\equiv 0$ とする.

$\vartheta_\kappa \not\equiv 0$ となる条件は?

Hecke は次元公式にも言及している：

Ob damit das volle System von elliptischen Modulformen (-1)-ter Dimension gewonnen ist, ist für beliebige Stufenzahl noch immer eine offene Frage, $\cdots$

While it is relatively easy to construct modular forms of weight $k > 1$, and Riemann-Roch theorem tells us exactly how many of them there are at each level, it is not so easy to exhibit forms of weight 1, and the Riemann-Roch formula fails to predict how may of them there are at a given level.
(J. Tate : The general reciprocity law, Proc. Symp. in Pure Math., Vol. **28**, 1976)

Petersson :

Zur analytischen Theorie der Grenzkreisgruppen I ～ V (1938 ～ 1939)

Über Eisensteinsche Reihen und automorphe Formen von der Dimension -1, Comment. Math. Helv. **31** (1956), 318-343

N : 自然数

$$K_N = K = \sqrt{N}^{-1}\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$$

$\Phi_0 = \Gamma_0(N) \cup K\Gamma_0(N)$ $\cdots$ Fricke 群

v : $\Gamma_0(N)$ 上の odd 指標

とする. $v(K^2) = v(-I) = -1$ 故, $v(K) = \pm i$ として $\Phi_0(N)$ 上の指標に延長する：

$$v^\pm(K) = \pm i \quad (\text{複号同順})$$

このとき,

$$S_1(\Gamma_0(N), v) = S_1(\Phi_0(N), v^+) \oplus S_1(\Phi_0(N), v^-)$$

となる. ここで, $v = \left(\frac{*}{N}\right)$, N : odd とする. このとき,

$$v(-I) = \left(\frac{-1}{N}\right) = -1 \text{ より } N \equiv 3 \pmod 4$$
$$\mu_1^{\pm} = \dim S_1(\Phi_0(N), v^{\pm})$$

とおく. $N = p$: 素数のとき,

$$\mu_1^- - \mu_1^+ = \frac{1}{2}(h-1), \quad h = h(\mathbb{Q}(\sqrt{-p}))$$

が成立する. 次の結果は Serre :

$$\mu_1^- = \frac{1}{2}(h-1) + s + 2a,$$
$$\mu_1^+ = s + 2a,$$

ここで, s, a : ある種の条件をみたす体の個数を表す :

P. Deligne et J.-P. Serre :

Formes modulaires de poids 1, Ann. scient. Éc. Norm. Sup., 4° séries, t.**7** (1974), 507-530

J.-P. Serre :

Modular forms of weight one and Galois representations, in Proc. Symp. on Algebraic Number Fields, Academic Press, 1977, 193-268

Selberg の trace formula による次元公式については,

T. Hiramatsu : A formula for the dimension of spaces of cusp forms of weight 1, Adv. Studies in Pure Math., **15** (1989), 287-300

他に, Duke :

$$\dim S_1\left(\Gamma_0(p), \left(\frac{*}{p}\right)\right) \ll p^{\frac{11}{12}} \log^4 p$$

§4. Serre and Deligne : ガロア表現, Buhler, Frey, Taylor : Icosahedral 表現

与えられた有限次 Galois 拡大 K に対し,

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$$

なる Galois 表現 ρ で, $\mathrm{Gal}(\overline{\mathbb{Q}}/K) = \ker\rho$ となるものがある. このとき, 忠実表現

$$\rho : \mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$$

を得る. $n = 2$ とする. c を複素共役とし, 行列 $\rho(c)$ が固有値 ± 1 をもつとき ρ を odd という. このとき次の 2 つの定理が成立する.

定理 A (Weil-Langlands) ρ が既約で, conductor N とし, 次の条件 $(*)$ をみたすとする：

$(*)$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の任意の 1 次元表現 λ との twists $\rho\otimes\lambda$ に関する Artin L-関数 $L(s,\rho\otimes\lambda)$ が正則である.

そして, $L(s,\rho)=\sum_{n=1}^{\infty}a(n)n^{-s}$, $f(z)=\sum_{n=1}^{\infty}a(n)q^n$ とするとき, $f(z)$ は $\Gamma_0(N)$ に関する character $\det(\rho)$ で重さ 1 の newform である.

定理 B (Deligne-Serre) f を $\Gamma_0(N)$ に関する character ε で重さ 1 の newform とする. そのとき, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の既約で odd な 2 次元 Galois 表現 ρ で conductor N, $\varepsilon=\det\rho$ なるものがあって, $L_f(s)=L(s,\rho)$ が成立する.

定理 A + 定理 B より,

$$\left\{\begin{array}{l}\Gamma_0(N) \text{ に関する character } \varepsilon\\ \text{で重さ 1 の newforms}\end{array}\right\}\underset{1\text{ 対 }1}{\longleftrightarrow}\left\{\begin{array}{l}\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \text{ の既約 2 次元 Galois 表現で,}\\ \text{conductor } N, \text{ odd character } \varepsilon \text{ の同型類}\end{array}\right\}$$

が mod Artin 予想で成立する. このとき,

$$\tilde{\rho}:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\longrightarrow \mathrm{PGL}_n(\mathbb{C})$$

の像は有限群で

$$\tilde{\rho}\left(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\right)=\begin{cases}D_k\\ A_4\\ S_4\\ A_5\end{cases}$$

である (Klein).

Remark F を数体とし, K を F 上の有限次ガロア拡大とする. $G=\mathrm{Gal}(K/F)$ とおく.

$$\sigma: G\longrightarrow \mathrm{GL}_n(\mathbb{C})$$

を G の n 次元表現とする. 通常連続性を仮定する. F の各 place v に対し, σ_v を v での G の分解群への σ の制限とする. σ に関する Artin の L-関数は

$$L(s,\sigma)=\prod_v L(s,\sigma_v),$$

ここで, v が K で不分岐なら, C_v を v 上の Frobenius element として

$$L(s,\sigma_v)=\left[\det\left(I-\sigma(C_v)N_v^{-s}\right)\right]^{-1}$$

Artin 予想 σ が既約で non-trivial なら, $L(s,\sigma)$ は s の正則関数として解析接続される.

次に, F_v を v での F の完備化とし, A_F : F の adele 環,

$$\begin{aligned}G_A&=\mathrm{GL}_n(A_F)\\ &=\prod_v \mathrm{GL}_n(F_v) \quad \text{(制限直積)}\end{aligned}$$

とする. また, G_A 上の既約ユニタリー表現 π が, GL_n 上の保型形式 (cuspidal 保型形式) の空間での right translation operators として realize されるとき, π を GL_n の保型表現 (cuspidal 表現) という. このとき π に対し局所表現の族 $\{\pi_v\}$ が一意に決まり

(1) π_v は v で既約,

(2) π_v は almost every v で不分岐,

(3) $\pi = \bigotimes_v \pi_v$

が成立する.

Langlands の相互法則予想 各ガロア表現 σ に対し, $\mathrm{GL}_n(A_F)$ 上の保型表現 $\pi(\sigma)$ があって,

$$L(s, \sigma) = L(s, \pi(\sigma))$$

が成立する. また, σ が既約かつ non-trivial なら, $\pi(\sigma)$ は cuspidál である.

特に, $n = 2$, $F = \mathbb{Q}$ のとき, 定理 A より

$$\text{Artin 予想} \Longleftrightarrow \text{Langlands 予想}$$

が成立し, 定理 B より重さ 1 の保型形式がすべてこのように得られることがわかる. そして,

$$\begin{aligned} \tilde{\rho}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) &= D_k && \text{(Hecke)} \\ &= A_4,\ S_4 && \text{(Langlands, Tunnel)} \\ &= A_5 && \text{(Buhler : level 800, Frey ; Taylor ; Kisin ; Khare)} \end{aligned}$$

($n = 1$: **類体論**)

§5. Icosahedral Galois 表現と Serre 予想

1) C. Khare : Remarks on mod p forms of weight one, International Math. Research Notices, 1997, No. 3

2) B. Edixhoven : Overview of Khare's proof, Preprint, 2005

3) M. Kisin : Modularity of 2-dimensional Galois representations, Current Developments in Mathematics 2005

4) C. Khare : Modularity of Galois representations and motives with good reduction properties, J. Ramanujan Math. Soc. **22**, No.1 (2007), 75-100

Serre 予想 (定理 A の有限版 ! (J.-P. Serre : Duke Math. J., **54** (1) (1987), 179-230))

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F})$$

を連続, 絶対既約な 2 次元 odd mod p 表現 ($\mathrm{ch}(\mathbb{F}) = p$) とする. $\overline{\rho}$ を Serre type という. $\overline{\rho}$ の conductor を $N(\overline{\rho})$, $k(\overline{\rho})$ を $\overline{\rho}$ の重さとするとき, $\overline{\rho}$ は重さ $k(\overline{\rho})$, level $N(\overline{\rho})$ の newform から arise する.
証明は, Khare-Wintenberger I, II.

◎ Serre 予想が成立すれば, Artin 予想は成立する.
証明は, 1) の Proposition 1, 3) の Corollary (0.4).