

実2次体上の A_4 拡大と Hecke 作用素

名大 理 小池 正夫 (Masao Koike)

名大 理 谷川 好男 (Yoshio Tanigawa)

1変数の保型形式に関する Hecke 作用素の固有値についてのある数値実験と、その結果から推測できる weight 1 の保型形式についての予想について述べる。この結果は、志村先生が [7], [8] で研究された、実 Neben 型, weight 2 の cusp form の フーリエ係数と 実2次体上のあるアーベル拡大の相互法則の間、関係の類似にもなっている。

§.1 実験

記号を次のように定める。

p : 素数 $p \equiv 1 \pmod{4}$

$(\frac{\cdot}{p})$: 平方剰余記号

$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \mid c \equiv 0 \pmod{p} \right\}$

$S_2(p, (\frac{\cdot}{p}))$: $\Gamma_0(p)$ に関する type $(2, (\frac{\cdot}{p}))$ の cusp form 全体

$\rho: \mathbb{C} \rightarrow \mathbb{C}$ complex conjugation

$f(z) = \sum_{n=1}^{\infty} a_n z^n$, $a_1 = 1$, $g = e^{2\pi\sqrt{-1}z} \in S_2(p, (\overline{p}))$ の元で
primitive i.e. 全ての Hecke 作用素の同時固有関数とする。

この時 次のことが成り立つことはよく知られている。

$$\begin{cases} a_n^p = \left(\frac{n}{p}\right) a_n & \text{if } (n, p) = 1 \\ a_p \cdot a_p^p = p \end{cases}$$

さらに $K_f = \mathbb{Q}(a_n \mid 1 \leq n \in \mathbb{Z})$ は $\mathbb{Q}$ 上の総虚な有限次
拡大体で、その最大実部分体を F_f とかくと、 $[K_f : F_f] = 2$ 。
 F_f は総実である。 σ を勝手な $K_f \hookrightarrow \mathbb{C}$ なるうめこみとした
時 $f^\sigma(z) = \sum a_n^\sigma z^n$ は又 $S_2(p, (\overline{p}))$ の primitive
な元となる。

我々が注目するのは、level が p の cusp form の p 番目
の Hecke 作用素 $T(p)$ の p を動かした時のふるまいである。

$T(p)$ の固有値とは primitive な上記の $f(z)$ の p 番目の
フーリエ係数 a_p で a_p はその全ての共役 a_p^σ について

$a_p^\sigma \cdot a_p^{\sigma p} = p$ が成り立ち、Gauss 和と同じ性質をもっている。
しかし Gauss 和は Stickelberger の定理によつて、 p
の上のどんな素因子 f も Gauss 和を割るのに、 a_p は一般
にそうではない。例えば Hecke 全集に出ている 2 つの例：

$$p = 29 \text{ の時} \quad a_p = 3 \pm 2\sqrt{-5},$$

$$p = 37 \text{ の時} \quad a_p = 1 + 6\sqrt{-1}.$$

これらの場合、 p は K_f で完全分解で、 a_p, a_p^p はそれぞれ

相異なる素イデアルの生成元となる。そこで我々は次のような数値実験をやってみた。 $\overline{\mathbb{Q}} \in \mathbb{Q}$ の代数的閉包とし、 p の上にあり $\overline{\mathbb{Q}}$ の素因子 $\tilde{p}$ を 1 つ固定しておく。

実験 I p を動かした時に 次の条件 (*):

(*) $\left\{ \begin{array}{l} \text{ある primitive な } f(z) = \sum_{n=1}^{\infty} a_n z^n \in S_2(p, (\overline{p})), a_1 = 1 \\ \text{が存在して } a_p \equiv a_p^p \equiv 0 \pmod{\tilde{p}} \text{ が成り立つ} \end{array} \right.$
 がみたまれるような p はどのくらいあるか?

実験の結果は

定理 1 $p < 760$ の範囲で (*) が成り立つ

p は 229, 257 の 2 つの場合に限る。

この時 $S_2(p, (\overline{p}))$ の次元は各々 18, 20 である。

実験 I をどのように実行するか簡単にのべる。

$S_2(p, (\overline{p}))$ に作用している Hecke 作用素 $T(l)$ の固有値の計算例は [7], [8] に見られるが p が大きいところでは $l = 2, 3, 5$ といった小さい値にばかり例のみで我々の役にたかない。我々は $T(p)$ の固有値を直接計算して実験を進めたのではない。 $\text{mod } p$ の保型形式の理論を使って証明できる。次の補題が役に立つ。

補題 1 次のことは同値である。

(1) p が条件 (*) をみたす。

- (2) $S_{\frac{p+3}{2}}$ は $SL(2, \mathbb{Z})$ に属する weight が $\frac{p+3}{2}$ の cusp form の空間として, $T(p)$ をそこに作用する degree p の Hecke 作用素とした時, $T(p)$ の固有多項式 $H_p(X) (\in \mathbb{Z}[X])$ によって
- $$H_p(X) \equiv X^c H(X) \pmod{p\mathbb{Z}[X]}$$
- ($c > 0$, $H(X)$ はある多項式) が成り立つ。

我々が実験をしたのは 補題 1 の (2) の検証であった。それから 定理 1 が得られた。しかし p をさらに大きくすれば weight $\frac{p+3}{2}$ が大きくなり, $S_{\frac{p+3}{2}}$ の次元が大きくなり, (2) を検証することも容易ではなくなる。その時は, 次の補題が役に立つ。

- 補題 2 p によって 条件 (*) が成り立ち, (*) の中の primitive な cusp form $f(z) = \sum a_n q^n$ によってある n に対して $a_n \not\equiv a_n^p \pmod{\tilde{p}}$ と仮定する。
- (このことは $(\frac{n}{p}) = -1$ となる n で $a_n \not\equiv 0 \pmod{\tilde{p}}$ が成立するようなものがあればよいから容易にわかる)
- この時, $S_{\frac{p+3}{2}}$ に作用している degree l の Hecke 作用素 $T(l)$ の固有多項式を $H_l(X)$ とかくと, p と異なる素数 l によって $H_l(X) \pmod{p\mathbb{Z}[X]}$ は
- $$\left(\frac{l}{p}\right) = 1 \text{ ならば } (X-\alpha)^2, \quad \left(\frac{l}{p}\right) = -1 \text{ ならば } (X-\alpha)(X+\alpha)$$

の形の因子を持つ、である。ただし $\alpha \in \mathbb{F}_p$ とは限らぬ。

補題 2 が成りたっているかどうかを見るだけならば $T(2)$, $T(3)$, ... で充分なわけでも (*) を p がみたさないことはいえる。

それでも p が大きくなれば ひとつの計算が大変なので全ての p についてみることは能率が悪い。又ある予測が得られたので p について次の条件をみるものについてだけ実験を進めた:

条件(C-3): 実 2 次体 $\mathbb{Q}(\sqrt{p})$ の類数が 3 で割れる。

定理 2 p が素数で 条件(C-3) をみたしていて

$p < 2090$ とする。この時、次の p :

229, 257, 761, 1129, 1229, 1489, 2089

以外の p は (*) をみたさない。

定理 2 で (*) をみたさない p は 733, 1373, 1901 の

3 つで、定理 2 にあらわれない p について ある程度たくさん
の l について 補題 2 が成りたつことを確かめた。

これらで 実験 1 については、数学的に無意味でない現象がとらえられたと思う。

次に

実験 II

p が (＊) をみたしているとする. (＊) が成立する primitive な $f(z) = \sum_{n=1}^{\infty} a_n g^n$, $a_1 = 1$ について 他の フーリエ係数

a_n , $(n, p) = 1$ は $\text{mod } \tilde{p}$ でどんな規則をもち定まっているか?

(＊) が成り立つ $f(z)$ に何かを期待するのは虫がよい. ともいえるが. 我々は運のよいことに次の予想を数値実験から得ることができた。

予想 1

$f(z) = \sum_{n=1}^{\infty} a_n g^n$, $a_1 = 1$ が $S_2(p, (\frac{p}{p}))$ の primitive な元で

(＊) をみたしているとする. この時 p と異なる素数 l について 以下の合同式のどれかが成り立つ:

$$a_l^2 \equiv \begin{cases} 0 \\ l \\ 4l \end{cases} \pmod{\tilde{p}} \quad \text{if } \left(\frac{l}{p}\right) = 1,$$

$$a_l^2 \equiv \begin{cases} 0 \\ -2l \end{cases} \pmod{\tilde{p}} \quad \text{if } \left(\frac{l}{p}\right) = -1.$$

しかも 上の全ての型の合同式のどれをとっても, それか成り立つような l は 無数に存在する。

定理 2 の p 達のうち 229, 257 以外の p については

(*) とみえる $f(z)$ はその候補しか分らないわけだがその候補のフーリエ係数達も予想の合同式とみている。このことから、定理 2 の p 達が (*) とみえている可能性は充分高いと思える。

§2. 実験から予想の背景へ

我々は §1 での数値実験からある種のよい性質をもつ保型形式の系列の存在をさぐりあてることができたといえると思うが、ここではそれをより確実なものとするために、予想を weight 1 の保型形式との関連で見直す。そこには $\mathbb{Q}$ 上ガロア群が S_4 と同型になる拡大で p の外側で不分岐なものが自然にでてくる。その体は実 2 次体 $\mathbb{Q}(\sqrt{p})$ を含み、それ上 A_4 拡大 (i.e. ガロア群が A_4 と同型) となる。これが志村先生の場合に $\mathbb{Q}(\sqrt{p})$ 上のアーベル拡大と対応するものになる。

2.1 cusp forms of weight 1

ここで weight 1 の保型形式について復習しておく。

Deligne - Serre によつて primitive な weight 1 の cusp form $h(z) = \sum_{n=1}^{\infty} c_n z^n$, $c_1 = 1$ に対して $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ の既約な 2 次元表現 ρ

$$\rho : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{C})$$

で $\det \rho$ が odd なものが存在し、その Artin L 関数 $L(s, \rho)$

について

$$(4) \quad L(s, \rho) = \sum_{n=1}^{\infty} c_n n^{-s}$$

が成り立つことが示された。逆に上記のような ρ が与えら

れた時、 $GL_2(\mathbb{C})$ から $PGL_2(\mathbb{C})$ への射影をとって

$$\tilde{\rho} : G_{\mathbb{Q}} \longrightarrow PGL_2(\mathbb{C})$$

とすれば $\text{Im } \tilde{\rho}$ は有限群で次の形のものに限られる。

(1) dihedral group

(2) A_4, S_4

(3) A_5

ρ に対して weight 1 の cusp form $h(z)$ で (4) をみたすものが存在するかどうかという問題は (1) の case は Hecke によって証明され、(2) (3) については Weil-Langlands と ρ とその twist 達に關して Artin 予想が成りたてばよいことがいえられた。最近 (1976 年) Langlands と Tunnell によって (2) の case は Artin 予想が証明でき、従って weight 1 の cusp form の存在も示された。

primitive な weight 1 の cusp form に対して対応する $G_{\mathbb{Q}}$ の表現 $\tilde{\rho}$ の像によつて $h(z)$ が dihedral 型 とか S_4 型 とかと呼ぶことにする。

志村先生の [7][8] の結論の 1) の ... かえとして.

$S_2(p, (\bar{p}))$ の primitive な元 $f(z)$ に対して K_f/F_f は分裂してあるある種の素イデアル $\mathfrak{p}$ に対して dihedral 型 の weight 1 の cusp form $h(z)$ が存在して 合同式

$$f(z) \equiv h(z) \pmod{\mathfrak{p}}$$

が成り立つことがいえる ([3] 参照)

[7][8] の時点では Langlands 等の仕事はまだなくて weight 1 の cusp form の存在等については dihedral 型のみが自由に取っ換かえたのに 現在の我々は A_4 型 S_4 型の form まで取っ換かえるという利点がある。

2.2

以下では $f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_2(p, (\bar{p}))$, $a_1 = 1$ 且 primitive な元で (木) とみたいていもののみを考える。

この時 補題 1 によて $S_{\frac{k+1}{2}}$ の primitive な元

$$g(z) = \sum_{n=1}^{\infty} b_n q^n, \quad b_1 = 1$$

$$a_n \equiv b_n \pmod{\mathfrak{p}} \quad \forall n \geq 1$$

を満たすものが存在する。(補題 1 の証明の中で $g(z)$ の存在が示される。)

$f(z)$ に対しては weight 2 だから志村理論によて

① 上定義されたアーベル多様体 A_f が存在せよ。 A_f の

等分点を調べる：とができる。一方、 $g(z)$ に対しては Serre, Swinnerton-Dyer, Ribet 等による p -進表現の像の研究が使える。我々はその両方を用いる：とにより、次の定理を証明できる。

定理 3. 上記の $f(z)$ に対して予想が正しいとする。

この時、次の性質をみたす $\mathbb{Q}$ 上のガロア拡大 M が存在する。

- (1) $\text{Gal}(M/\mathbb{Q}) \simeq S_4$.
- (2) M は p の外で不分裂。
- (3) $M \supset \mathbb{Q}(\sqrt{p})$
- (4) $L \in A_4$ に含まれる $(2, 2)$ 型の正規部分群に対応する M の部分体を L とし、 $L/\mathbb{Q}(\sqrt{p})$ は不分裂拡大。
- (5) $\mathbb{Q}(\sqrt{p})$ の次数は 3 で割れる。
- (6) $\ell \neq p$ と異なる素数に対して ℓ の $M/\mathbb{Q}$ の

フロベニウス元の位数は 予想により q_ℓ の合同式、型の順番に $2, 3, 1, 2, 4$ である。

(5) が成り立つことから 実験 I を p が条件 (C-3) をみたすものの中で探す理由が少しは正当化される。

更に この時 S_4 の部分群で S_3 と同型なものに対応する M の部分体の 1 つを K とする。 K は $\mathbb{Q}$ 上 非-ガロア拡大で 相異なる 4 個の共役体がある。

命題 定理 3 と同じ仮定で同じ記号を使うと、次のことが成り立つ。

- (1) K は $\mathbb{Q}$ 上 4 次拡大で 総虚
- (2) K は p の外で 不分裂で 判別式は p である。
- (3) K の 真の部分体は $\mathbb{Q}$ しかない。
- (4) p の K での アイテール分解は $p_1^2 p_2$ である。
- (5) K の $\mathbb{Q}$ 上の ガロア 閉包が M で M は $\mathbb{Q}$ 上の ガロア 群が S_4 と同型である。

上記の命題にいう性質を持つ 4 次拡大 K については Godwin [2] の仕事があり それによれば $p < 1458$ のほかに K が存在する p は 以下：

$$229, 257, 761, 1129, 1229$$

の 5 つしかない。

Godwin の結果と 定理 2 とは完全に整合している。

そこで 命題にいう K を出発点にする。 K から M へ行くことにより $\tilde{\rho}: G_{\mathbb{Q}} \longrightarrow S_4 \hookrightarrow \mathrm{PGL}_2(\mathbb{C})$ がつくれ。 $\tilde{\rho}$ が $\mathrm{GL}_2(\mathbb{C})$ への持ち上げが p の外で 不分裂なまゝとれる。 後、2.1 で説明したように ρ に対応する weight 1 の cusp form $h(z)$ の存在がわかる。 Serre [6] の結果と

見れば $h(z)$ は $\Gamma_0(p^2)$ に属する cusp form であって $\Gamma_0(p)$ 上のものとならないうことがわかる。 $h(z)$ は mod p の Dirichlet 指標の twist の自由度があるが、我々此次のことは予想している。

予想 2 K を命題にいう体とする。記号をさして同じとする。この時 primitive な weight 1 の cusp form $h(z)$ の level が p^2 のものに対する性質をみえすものが唯一つある:

(1) $h(z)$ に対応する $G_{\mathbb{Q}}$ の表現 $\tilde{\rho}$ の kernel

に対応する体は M である。

(2) $S_2(p, \frac{1}{p})$ の primitive な元 $f(z)$ が存在して

$$\text{合同式: } f(z) \equiv h(z) \pmod{\tilde{\rho}}$$

が成り立つ。

我々が §1 の実験の中に見つけたいた $f(z)$ は全て上の予想の中に現れるように考えている。このことはまだ証明できていないが、此次のことはいえていく。

定理 4. $p = 229, 257$ に対して 予想 1, 2 は正しい。

詳しい証明は [5] を参照してください。

References

- [1] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*,
Ann. Sci. E.N.S., 7 (1974), 507-530.
- [2] H. J. Godwin, *On totally complex quartic fields with
small discriminants*, Proc. Cambridge Phil. Soc., 53
(1957), 1-4.
- [3] M. Koike, *Congruences between cusp forms and
linear representations of the Galois group*, Nagoya
Math. J., 64 (1976), 63-85.
- [4] M. Koike, *A note on modular forms mod p* , Nagoya
Math. J., 89 (1983), 89-107.
- [5] M. Koike and Y. Tanigawa, *A_4 -extensions over real
quadratic fields and Hecke operators*, preprint.
- [6] J.-P. Serre, *Modular forms of weight one and Galois
representations*, Algebraic Number fields edited by
A. Fröhlich, 193-268, London, Academic press 1977.
- [7] G. Shimura, *Introduction to the arithmetic theory of
automorphic functions*, Iwanami Shoten 1971.
- [8] G. Shimura, *Class fields over real quadratic fields
and Hecke operators*, Ann. of Math., 95 (1972), 130-190