数理解析研究所講究録
第583巻 1986年 120-132

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の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 $p \equiv 1 \pmod 4$

$\left(\frac{}{p}\right)$: 平方剰余記号

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

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

ρ : $\mathbb{C} \to \mathbb{C}$ complex conjugation

$f(z)=\sum_{n=1}^{\infty}a_n q^n,\quad a_1=1,\quad q=e^{2\pi\sqrt{-1}z}$ を $S_2(p,(\frac{}{p}))$ 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、次のことが成りたつことはよく知られている。

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

さらに、$K_f=\mathbb{Q}(a_n \mid 1\leqq n\in\mathbb{Z})$ 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、$f^{\sigma}(z)=\sum a_n^{\sigma}q^n$ は又 $S_2(p,(\frac{}{p}))$ 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

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

$$p=29 \text{ の時} \qquad a_p = 3\pm2\sqrt{-5},$$

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

これらの場合、p は K_f で完全分解で、a_p, a_p^{ρ} 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。$\overline{\mathbb{Q}}$ を $\mathbb{Q}$ の代数的閉包とし、p の上にある $\overline{\mathbb{Q}}$ の素因子 $\tilde{\mathfrak{p}}$ を1つ固定しておく。

<u>実験 I</u>　p を動かした時に次の条件(※):

(※) $\begin{cases} \text{ある primitive な } f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_2(p, (\frac{}{p})),\ a_1 = 1 \\ \text{が存在して } a_p \equiv a_p^{\,p} \equiv 0 \pmod{\tilde{\mathfrak{p}}} \text{ が成りたつ} \end{cases}$

がみたされるような p はどのくらいあるか？

実験の結果は

<u>定理 1</u>　$p < 760$ の範囲で(※)が成りたつ p は 229, 257 の2つの場合に限る。

この時 $S_2(p, (\frac{}{p}))$ 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。

$S_2(p, (\frac{}{p}))$ に作用している Hecke 作用素 $T(\ell)$ 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 $\ell = 2, 3, 5$ といった小さい値に対する例のみで、我々の役にたたない。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。$\bmod p$ 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。

<u>補題 1</u>　次のことは同値である。

(1)　p が条件(※)をみたす。

(2) $S_{\frac{p+3}{2}}$ を $SL(2,\mathbb{Z})$ に関する 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 $H_p(X)$ $(\in \mathbb{Z}[X])$ について

$$H_p(X) \equiv X^c H(X) \pmod{p\mathbb{Z}[X]}$$

（$c>0$，$H(X)$ はある多項式）が成りたつ。

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，次の補題が役にたつ。

<u>補題 2</u>　p について条件(*)が成りたち，(*)の中の primitive な cusp form $f(z)=\sum a_n q^n$ について，ある n に対して $a_n \not\equiv a_n^p \pmod{\tilde{\mathfrak{p}}}$ と仮定する。

（このことは $\left(\frac{n}{p}\right)=-1$ となる n で $a_n \not\equiv 0 \pmod{\tilde{\mathfrak{p}}}$ が成立つ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 について $H_l(X) \pmod{p\mathbb{Z}[X]}$ は

$\left(\frac{l}{p}\right)=1$ ならば $(X-\alpha)^2$，$\left(\frac{l}{p}\right)=-1$ ならば $(X-\alpha)(X+\alpha)$

の形の因子を持っている．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 (*) 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たす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．

<u>定理 2</u>　　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にあらわれる 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 $f(z)=\sum_{n=1}^{\infty} a_n q^n$, $a_1=1$ について 他のフーリエ係数 a_n, $(n,p)=1$ は $\bmod \tilde{\mathfrak{p}}$ でどんな規則を持っているか?

(*)が成りたつ $f(z)$ 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

$f(z)=\sum_{n=1}^{\infty} a_n q^n$, $a_1=1$ が $S_2(p,(\frac{}{p}))$ 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たつ:

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

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

しかも 上の全ての型の合同式のどれをとっても, それが成りたつような 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(※)をみたす$f(z)$はその候補しか分ってい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をみたしている。このことからも定理2のp達が(※)をみたし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っている。

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

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

で $\det\rho$ が odd なのが存在し その Artin L 関数 $L(s,\rho)$ について

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

が成りたつことが示された. 逆に 上記のような ρ が与えられた時 $GL_2(\mathbb{C})$ から $PGL_2(\mathbb{C})$ への射影をつなげて

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

とすれば $\mathrm{Im}\,\tilde{\rho}$ 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 Weil・Langlands で ρ とそれの twist 達に関して Artin 予想が成りたてばよいことがいえていた. 最近 (1976年) Langlands と Tunnel によって (2) の case は Artin 予想が証明でき. 従って weight 1 の cusp form の存在もいえた.

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

志村先生の[7][8]の結論の1つのいいかえとして、$S_2(p,(\frac{}{p}))$ の primitive な元 $f(z)$ に対して、K_f/F_f で分岐している或る種の素イデアル $\tilde{\mathfrak{r}}$ に対して、dihedral 型の weight 1 の cusp form $h(z)$ が存在して合同式

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

が成りたつことがいえる。([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 型のみが自由に取り扱かえたのに、現在の我々は A_4 型 S_4 型の form まで取り扱かえるという利点がある。

2.2

以下では、$f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_2(p,(\frac{}{p}))$, $a_1 = 1$ を primitive な元で (※) をみたしているもののみを考える。

この時、補題 1 によって、$S_{\frac{p+3}{2}}$ の primitive な元 $g(z) = \sum_{n=1}^{\infty} b_n q^n$, $b_1 = 1$ で

$$a_n \equiv b_n \pmod{\tilde{\mathfrak{P}}} \qquad \forall n \geq 1$$

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って $\mathbb{Q}$ 上定義されたアーベル多様体 A_f が対応させられ、A_f の

等分点を調べることができる．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．我々はその両方を使うことによって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) $Gal(M/\mathbb{Q}) \simeq S_4$.

(2) M は p の外で不分岐

(3) $M \supset \mathbb{Q}(\sqrt{p})$

(4) L を A_4 に含まれる $(2,2)$ 型の正規部分群に対応する M の部分体とすると $L/\mathbb{Q}(\sqrt{p})$ は不分岐拡大．

(5) $\mathbb{Q}(\sqrt{p})$ の類数は 3 で割れる．

(6) l を p と異なる素数に対して l の $M/\mathbb{Q}$ でのフロベニウス元の位数は予想にいう a_l の合同式の型の順番に 2, 3, 1, 2, 4 である．

(5)が成りたつことから実験 I を p が条件 (C-3) をみたすものの中で捜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．

<u>命題</u> 定理3と同じ仮定で同じ記号を使うと，次のことが成りたつ．

(1) Kは$\mathbb{Q}$上4次拡大で 総虚

(2) Kはpの外で不分岐で 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でのイデアル分解は $\mathfrak{P}_1^2\mathfrak{P}_2$ 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 $p<1458$ のはんいで 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を出発点にとる．KからMをへることによって $\tilde{\rho}: G_{\mathbb{Q}} \longrightarrow S_4 \hookrightarrow PGL_2(\mathbb{C})$ がつくれ，$\tilde{\rho}$の $GL_2(\mathbb{C})$への持ち上げがpの外で不分岐なままとれる．従って 2.1 で説明したように ρに対応する weight 1 の cusp form $h(z)$の存在がいえる． Serre [6] の結果を

見れば $h(z)$ は $\Gamma_0(p^2)$ に関する cusp form であって $\Gamma_0(p)$ 上のものとならないことがわかる。$h(z)$ は mod p の Dirichlet 指標の twist の自由度があるが我々は次のことを予想している.

<u>予想 2</u>　K を今数にいう体とする. 記号をそこと同じとする. この時 primitive な weight 1 の cusp form $h(z)$ で level が p^2 のものが次の性質をみたすものが唯1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)　$S_2\left(p, \left(\frac{\ }{p}\right)\right)$ の primitive な元 $f(z)$ が存在し
合同式 :　$f(z) \equiv h(z) \pmod{\tilde{\wp}}$
が成りたつ。

我々が §1 の実験の中で見つけだした $f(z)$ は全て上の予想の中に現れるだろうと考えている. これらはまだ証明できていないが, 次のことはいえている.

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