

# モジュラー形式とヘッケ体に 関する前田予想

東京都立大学大学院理学研究科数理科学専攻

21843423 堀岡 大暉

2023 年 1 月 10 日

# 目次

第 1 章	はじめに	2
第 2 章	モジュラー形式	4
2.1	モジュラー形式 . . . . .	4
2.2	レベル 1 のモジュラー形式 . . . . .	6
2.3	ヘッケ作用素 . . . . .	6
2.4	判別式 . . . . .	8
第 3 章	ヘッケ体に関する前田予想	10
第 4 章	ヘッケ体の判別式に関する予想	13
4.1	ヘッケ体の判別式に関する予想 . . . . .	13
4.2	素数 2 の分岐に関する考察 . . . . .	14
	謝辞	16
	付録	17
	参考文献	21

# 第 1 章

## はじめに

1979 年に土井公二によって、カスプ形式がいくつかの重さに対して、non-splitting(定義 3.1 を参照) でないことを望み、カスプ形式の次元が 12 以下の 2 番目のヘッケ作用素の固有多項式を計算した。しかし、すべて non-splitting であることが土井公二と前田芳孝の計算によってわかった [2]。そして、任意の重さのカスプ形式が non-splitting であることを予想した。この予想はヘッケ体に関する前田予想と呼ばれている。

ヘッケ体に関する前田予想とは以下の予想のことをいう。

**予想 1.1.** 任意の  $k \in \mathbb{Z}$  に対し、 $S_k$  は non-splitting である。

さらに、 $d := \dim(S_k)$  としたとき、 $\text{Gal}(f_k)$  は  $d$  次対称群  $\text{Sym}(d)$  と同型。

これに関連して、前田芳孝によって提唱されたヘッケ体の判別式に関する予想も存在する。ヘッケ体の判別式に関する予想とは以下の予想のことをいう。

**予想 1.2.** 奇素数  $p$  が  $\mathbb{Q}(f_k)$  (定義 2.16 を参照) で分岐するとき、以下の 2 つが成り立つ。

- (1)  $p \mid d(k + p \pm 1)$ . (弱予想, 定義 2.18 を参照)
- (2)  $p$  は  $\mathbb{Q}(f_{k+p \pm 1})$  でも分岐する. (強予想, 定義 2.20 を参照)

そこで、本論文では  $p = 2$  の場合について考察を行い、ヘッケ体の判別式に関する予想を提唱した。

**予想 1.3.** 2 は  $\mathbb{Q}(f_k)$  で分岐するとする。この時、以下が成り立つ。

- (i)  $k \equiv 2 \pmod{4}$  のとき、2 は  $\mathbb{Q}(f_{k+6})$  でも分岐する。
- (ii)  $k \equiv 2 \pmod{4}$  のとき、2 は  $\mathbb{Q}(f_{2k+5 \pm 3})$  でも分岐する。
- (iii)  $k \equiv 0 \pmod{4}$  のとき、2 は  $\mathbb{Q}(f_{k-6})$  でも分岐する。
- (iv)  $k \equiv 0 \pmod{4}$  のとき、2 は  $\mathbb{Q}(f_{2k-7 \pm 3})$  でも分岐する。

本論文の構成について述べる。

第 2 章では、モジュラー形式をはじめとした、ヘッケ体に関する前田予想や、ヘッケ体の判別式に関する予想を考察するうえで必要となる定義や定理を述べる。

第 3 章では、ヘッケ体に関する前田予想について、歴史を追って説明する.

第 4 章では、ヘッケ体の判別式に関する予想についての先行結果や難しさを説明する. その上で、2 の分岐について数式処理ソフト Magma [1] を用いて実際に計算し、考察する.

## 第 2 章

# モジュラー形式

### 2.1 モジュラー形式

**定義 2.1.** 行列式が 1 であり, 成分が整数である 2 次正方行列を**特殊線形群**といい, その集合を  $\mathrm{SL}_2(\mathbb{Z})$  とかく.

**例 2.2.**  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  と  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  は,  $\mathrm{SL}_2(\mathbb{Z})$  の元である.

**命題 2.3.**  $\mathrm{SL}_2(\mathbb{Z})$  は,  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  と  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  で生成される.

**証明.**  $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  とし,  $S, T$  で生成される部分群を  $\langle S, T \rangle$  とかく. このとき,  $\mathrm{SL}_2(\mathbb{Z}) \supset \langle S, T \rangle$  は明らか. そこで,  $\mathrm{SL}_2(\mathbb{Z}) \subset \langle S, T \rangle$  を示す.

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$  とする.

$a = 0$  のとき,  $-bc = 1$  より,  $(b, c) = (1, -1), (-1, 1)$ . したがって,  $A = \begin{pmatrix} 0 & -1 \\ 1 & d \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & d \end{pmatrix}$  となり, これらはそれぞれ,  $ST^{-d}, S^3T^d$  となり,  $A \in \langle S, T \rangle$  が成り立つ.

$c = 0$  のとき,  $ad = 1$  より,  $(a, d) = (1, 1), (-1, -1)$ . したがって,  $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & b \\ 0 & -1 \end{pmatrix}$  となり, これらはそれぞれ,  $T^b, S^2T^{-b}$  となり,  $A \in \langle S, T \rangle$  が成り立つ.

また,  $ac \neq 0$  のとき,  $ad - bc = 1$  より,  $\mathrm{GCD}(a, c) = 1$  となる. ここで, ユークリッドの互除法により,  $a = nc + r, |r| < |c|$  を満たす整数  $n, r$  が存在する. よって,  $ST^{-n}A = \begin{pmatrix} -c & -d \\ r & b - nd \end{pmatrix}$ . ここで,  $c, r$  に対して, ユークリッドの互除法により,  $-c = mr + s, |s| < |r|$  を満たす整数  $m, s$  が存在する. よって,  $ST^{-m}(ST^{-n}A) = \begin{pmatrix} r & b - nd \\ s & -d - m(b - nd) \end{pmatrix}$ . 同様の操作を行い,  $A$  に  $S, T, S^{-1}, T^{-1}$

を左から有限回かけることで,  $\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} (x, y \in \mathbb{Z})$  となる. ここで,  $|A|=|S|=|T|=1$  より,  $\begin{pmatrix} 1 & x \\ 0 & y \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$  をえる. これは, 先に示した  $c = 0$  の場合であるので,  $A \in \langle S, T \rangle$  が成り立つ.  $\square$

自然数  $N$  に対し, 集合  $\Gamma_0(N)$  を

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}$$

と定義する. この集合  $\Gamma_0(N)$  を**合同部分群**という.

また, 集合  $\mathbb{H}$  を

$$\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$$

と定義する. この集合  $\mathbb{H}$  を**上半平面**という.

**定義 2.4.**  $z \in \mathbb{H}$ ,  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$  に対して,  $\gamma(z) = \frac{az+b}{cz+d}$  と定義する. これを, **一次分数変換**という.

**例 2.5.**  $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$  と  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  の一次分数変換を考えると, それぞれ

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (z) = -\frac{1}{z},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} (z) = z + 1$$

となる.

**定義 2.6.** 複素関数  $f : \mathbb{H} \rightarrow \mathbb{C}$  が, 以下の条件をみたすとき, 重さ  $k$ , レベル  $N$  の**モジュラー形式**であるという.

(i)  $f$  は  $\mathbb{H}$  上正則関数である.

(ii)  $z \in \mathbb{H}$ ,  $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$  に対して,

$$f(\gamma(z)) = (cz+d)^k f(z)$$

が成り立つ.

(iii) カスプにおいて正則である.

また, モジュラー形式のなす  $\mathbb{C}$  ベクトル空間を  $M_k(N)$  とかく. 特に, レベル 1 のとき  $M_k$  と略記する.

ここで, モジュラー形式である  $f$  に対し, 例 2.5 と, 定義 2.6 の (ii) より,  $f\left(\frac{1 \cdot z + 1}{0 \cdot z + 1}\right) = (0 \cdot z + 1)^k f(z)$  を満たす.

以上より,  $f(z+1) = f(z)$  が成り立つので, モジュラー形式である  $f$  は周期関数である. よって, フーリエ変換ができるので,  $q = e^{2\pi iz}$  を用いて,

$$f(q) = \sum_{n=0}^{\infty} a_n q^n$$

とかける. これを,  $q$ -展開という.

**定理 2.7.** モジュラー形式  $f(q) = \sum_{n=0}^{\infty} a_n q^n$  ( $q = e^{2\pi iz}$ ) は  $z \in \mathbb{H}$  で収束する.

**定義 2.8.** 重さ  $k$ , レベル  $N$  のモジュラー形式で,  $q$ -展開された  $f_k = \sum_{n=0}^{\infty} a_n q^n$  に対して,  $a_0 = 0$  をみたすとき,  $f_k$  は重さ  $k$ , レベル  $N$  のカスプ形式であるという. また, カスプ形式のなす  $\mathbb{C}$  ベクトル空間を  $S_k(N)$  とかく. 特に, レベル 1 のとき  $S_k$  と略記する.

定義より,  $M_k(N) \supset S_k(N)$  である.

## 2.2 レベル 1 のモジュラー形式

本節では, レベル 1 のモジュラー形式について考える.

**定理 2.9.**  $M_k$  に対して, 以下が成り立つ.

$$\dim(M_k) = \begin{cases} 0 & (k \text{ が奇数, または負の場合}) \\ [k/12] & (k \equiv 2 \pmod{12}). \\ [k/12] + 1 & (k \not\equiv 2 \pmod{12}). \end{cases}$$

ここで,  $[x]$  は  $x$  以下の最大の整数を意味する.

**例 2.10.** 重さ 12, レベル 1 のモジュラー形式の次元は 2 である. 実際に, 数式処理ソフト Magma [1] を用いて基底を計算し, それらを  $g, h$  とすると,

$$\begin{aligned} g &= 1 + 196560q^2 + 16773120q^3 + 398034000q^4 + 4629381120q^5 + 34417656000q^6 \\ &\quad + 187489935360q^7 + 814879774800q^8 + 2975551488000q^9 + 9486551299680q^{10} \\ &\quad + 27052945920000q^{11} + O(q^{12}), \\ h &= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 - 16744q^7 + 84480q^8 \\ &\quad - 113643q^9 - 115920q^{10} + 534612q^{11} + O(q^{12}) \end{aligned}$$

となる.

## 2.3 ヘッケ作用素

自然数  $n$  に対して, 集合  $X_n$  を以下の様に定義する:

$$X_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{Mat}_2(\mathbb{Z}) \mid a \geq 1, ad = n, 0 \leq b < d \right\}.$$

また,  $k$  を整数,  $n$  を自然数とする. モジュラー形式  $f$  と行列  $\gamma \in X_n$  に対して,

$$(f^{[\gamma]^k})(z) = |\gamma|^{k-1} (cz + d)^{-k} f(\gamma(z))$$

と定める.

**定義 2.11.**  $k$  を整数,  $n$  を自然数とする. 複素関数  $f: \mathbb{H} \rightarrow \mathbb{C}$  に対して,

$$T_n(f) = \sum_{\gamma \in X_n} (f^{[\gamma]^k})(z)$$

を  $n$  番目のヘッケ作用素という.

**定理 2.12.**  $q$ -展開されたモジュラー形式  $f = \sum_{n=0}^{\infty} a_n q^n$  に対して,

$$T_n(f) = \sum_{m \in \mathbb{Z}} \left( \sum_{\substack{d \geq 1 \\ d | \gcd(m, n)}} d^{k-1} a_{mn/d^2} \right) q^m.$$

特に,  $n = p$  が素数の場合,

$$T_p(f) = \sum_{m \in \mathbb{Z}} (a_{mp} + p^{k-1} a_{m/p}) q^m.$$

ただし,  $m/p \notin \mathbb{Z}$  のとき,  $a_{m/p} := 0$  とする.

定理 2.12 を証明するために, 以下の補題を用いる.

**補題 2.13.**  $0$  以上の整数  $b, m$  と自然数  $d$  に対して,

$$\sum_{0 \leq b < d} e^{2\pi i b m / d} = \begin{cases} 0 & (d \nmid m) \\ d & (d \mid m) \end{cases}$$

定理 2.12 の証明. モジュラー形式を  $f = \sum_{m=0}^{\infty} a_m q^m$  とする. 定義 2.11 と集合  $X_n$  の定義から,

$$(2.3.1) \quad T_n(f) = \sum_{\substack{ad=n \\ a \geq 1 \\ 0 \leq b < d}} n^{k-1} d^{-k} f\left(\frac{az+b}{d}\right)$$

をえる. ここで, 補題 2.13 を用いると, 式 2.3.1 は,

$$T_n(f) = \sum_{\substack{ad=n \\ a \geq 1 \\ 0 \leq b < d}} n^{k-1} d^{-k+1} a_m q^{am/d}$$

となり,  $m/d = s$  とすると,

$$T_n(f) = \sum_{\substack{ad=n \\ a \geq 1 \\ 0 \leq b < d}} \left(\frac{n}{d}\right)^{k-1} a_{ds} q^{as}$$

となる. よって,  $q$  のべき乗ごとに書けば, 定理は得られる. □



**例 2.14.** 重さ 12, レベル 1 のモジュラー形式を考える. 例 2.10 の  $g, h$  に対して, 2 番目のヘッケ作用素を求める. 定理 2.12 を用いて,

$$\begin{aligned} T_2(g) &= (a_0 + 2^{11}a_0) + (a_2 + 2^{11}a_{\frac{1}{2}})q + (a_6 + 2^{11}a_{\frac{3}{2}})q^2 + \cdots \\ &= 2049 + 196560q + 34417656000q^2 + \cdots, \\ T_2(h) &= (a_0 + 2^{11}a_0) + (a_2 + 2^{11}a_{\frac{1}{2}})q + (a_6 + 2^{11}a_{\frac{3}{2}})q^2 + \cdots \\ &= 0 - 24q - 6048q^2 + \cdots \end{aligned}$$

をえる. また,

$$T_2(g) = 2049g + 196560h, \quad T_2(h) = 0g + (-24)h$$

となるので,

$$T_2 = \begin{pmatrix} 2049 & 196560 \\ 0 & -24 \end{pmatrix}$$

と表す.

**定義 2.15.** 重さ  $k$ , レベル 1 のカスプ形式  $f_k = \sum_{n=1}^{\infty} a_n q^n$  (ただし  $a_1 = 1$ ) と,  $n$  番目のヘッケ作用素  $T_n$  に対して,  $T_n(f_k) = a_n f_k$  を満たす  $f_k$  を, 重さ  $k$  の正規化されたヘッケ固有形式という.

**定義 2.16.** 重さ  $k$  の正規化されたヘッケ固有形式  $f_k = \sum_{n=1}^{\infty} a_n q^n$  に対して,

$$\mathbb{Q}(f_k) := \mathbb{Q}(a_1, a_2, \dots)$$

をヘッケ体という.

**命題 2.17.** 重さ  $k$  の正規化されたヘッケ固有形式を  $f_k$  とする. この時, ヘッケ体  $\mathbb{Q}(f_k)$  は有限次拡大である.

## 2.4 判別式

**定義 2.18.**  $f(x) \in \mathbb{Z}[x]$  に対して,  $n = \deg f(x)$  とし,  $x^i$  ( $i \in \{1, 2, \dots, n\}$ ) の係数を  $a_i$  とする.  $f(x)$  の根を  $\alpha_1, \alpha_2, \dots, \alpha_n$  (重複を含む) とする. このとき,

$$d = a_n^{2n-2} \prod_{i,j(i < j)} (\alpha_i - \alpha_j)^2$$

を  $f(x)$  の判別式という.

以降, ヘッケ体  $\mathbb{Q}(f_k)$  の判別式を  $d(k)$  とかく.

**定義 2.19.** 代数体  $K$  に対して, 次元を  $n$  とし, 基底を  $\{\omega_1, \omega_2, \dots, \omega_n\}$  とする. さらに,  $i \in \{1, 2, \dots, n\}$  に対して,  $\omega_i$  の共役数を  $\omega_i^{(1)}, \omega_i^{(2)}, \dots, \omega_i^{(n)}$  とする. この

とき,

$$D(\omega_1, \omega_2, \dots, \omega_n)^2 = \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \cdots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \cdots & \omega_n^{(n)} \end{vmatrix}^2$$

を  $K$  の判別式という.

以降, 整数環  $\mathcal{O}_{\mathbb{Q}(f_k)}$  の判別式を  $D(k)$  とかく.

**定義 2.20.** 素数  $p$  が  $\mathbb{Q}(f_k)$  で分岐するとは,  $p|D(k)$  をみたすときをいう.

**命題 2.21.** 判別式  $d(k)$  と  $D(k)$  に対して, ある整数  $c$  が存在して,  $d(k) = c^2 D(k)$  が成り立つ.

**例 2.22.** 重さ  $k$  が 28, レベル  $N$  が 1 のとき,

$$\begin{aligned} d(28) &= 849559104 \\ &= 2^6 \cdot 3^6 \cdot 131 \cdot 139 \\ D(28) &= 18209 \\ &= 131 \cdot 139 \end{aligned}$$

となり, 131, 139 は  $\mathbb{Q}(f_{28})$  で分岐する. また,  $d(28) = (2^3 \cdot 3^3)^2 D(28)$  が成り立つ.

## 第 3 章

# ヘッケ体に関する前田予想

この章ではヘッケ体に関する前田予想を紹介し、先行結果を紹介する。また、この章では、重さ  $k$ 、レベル 1 のカスプ形式を考える。

正規化されたヘッケ固有形式  $f_k = \sum_{n=1}^{\infty} a_n q^n$  と  $\mathbb{C}$  上の任意の自己同型  $\sigma$  に対し、 $f_k^\sigma := \sum_{n=1}^{\infty} a_n^\sigma q^n$  とする。

また、ヘッケ体  $\mathbb{Q}(f_k)$  のガロア閉包のガロア群を  $\text{Gal}(f_k)$  とかく。

**定義 3.1.**  $S_k$  が **non-splitting** であるとは、任意の  $\sigma \in \text{Gal}(f_k)$  に対し、 $f_k^\sigma$  が  $S_k$  を張るときにいう。

**予想 3.2 (ヘッケ体に関する前田予想).** 任意の  $k \in \mathbb{Z}$  に対し、 $S_k$  は non-splitting である。

さらに、 $d := \dim(S_k)$  としたとき、 $\text{Gal}(f_k)$  は  $d$  次対称群  $\text{Sym}(d)$  と同型。

予想 3.2 が正しいとすると、以下の定理が成り立つ。

**定理 3.3.**  $S_k$  に対して、以下が成り立つ。

$$\dim(S_k) = \begin{cases} 0 & (k \text{ が奇数, または負の場合}) \\ [k/12] - 1 & (k \equiv 2 \pmod{12}). \\ [k/12] & (k \not\equiv 2 \pmod{12}). \end{cases}$$

ここで、 $[x]$  は  $x$  以下の最大の整数を意味する。

つまり、任意の 2 以上の整数  $d$  に対して、 $d$  次のヘッケ体が 6 つ得られる。

Lee-Hung によって 1995 年に以下が成り立つことが示されている [6].

**定理 3.4.**  $k \leq 62$ ,  $k \neq 60$  のとき、予想 3.2 は成り立つ。

つまり、 $\dim(S_k) \leq 4$  のとき、予想 3.2 は成り立つことを意味している。

次に、Buzzard によって 1996 年に以下が成り立つことが示されている [7].

**定理 3.5.** 素数  $p$  ( $2 \leq p \leq 19$ ) に対して、 $k = 12p$  のとき、予想 3.2 は成り立つ。

つまり、 $\dim(S_k) \leq 7$  または  $\dim(S_k)$  が 12 以下の素数であるとき、予想 3.2 は成

り立つことを意味している.

また, 定理 3.5 は以下の補題 3.6 を用いて確認されている.

**補題 3.6.** 素数  $p$  とモニックで既約な整数係数多項式を  $P$  ( $\deg P = p$ ) とする. さらに, 素数  $q$  に対して,  $\bar{P} = P \pmod{q} = \prod_{i=0}^r h_i \in \mathbb{F}_q[x]$  ( $h_i$  は相異なる  $\mathbb{F}_q$  上 既約な多項式) とする. この時, 以下の条件を満たすならば,  $\text{Gal}(f_k)$  は  $p$  次対称群  $\text{Sym}(p)$  と同型である:

- (i)  $\deg h_0 = 2$ .
- (ii)  $1 \leq i \leq r$  に対して,  $2 \nmid \deg h_i$ .

次に, 前田芳孝によって 1997 年に以下が成り立つことが示されている [8].

**定理 3.7.**  $k \leq 468$  のとき, 予想 3.2 は成り立つ.

上の定理 3.7 は以下の命題 3.8 を用いて確認されている.

**命題 3.8.** モニックな整数係数多項式を  $\phi(x)$  ( $\deg \phi(x) = n$ ) とする. 次の条件を満たす素数  $p_1, p_2, p_3$  が存在するならば,  $\phi(x)$  は  $\mathbb{Q}$  上既約で,  $\text{Gal}(f_k)$  は  $p$  次対称群  $\text{Sym}(n)$  と同型である:

- (i)  $\phi(x) \pmod{p_1}$  は  $\mathbb{F}_{p_1}$  上既約.
- (ii)  $\phi(x) \equiv \chi_0(x) \cdots \chi_h(x) \pmod{p_2}$   
(ただし,  $\chi_i(x) \in \mathbb{F}_{p_2}$  は,  $\deg \chi_0 = 2$ ,  $2 \nmid \deg \chi_i(x)$  ( $1 \leq i \leq h$ ) をみたす).
- (iii)  $\phi(x) \equiv \psi_1(x)\psi_2(x) \pmod{p_3}$ .  
(ただし,  $\psi_1(x), \psi_2(x) \in \mathbb{F}_{p_3}$  は,  $\deg \psi_1 = 1$ ,  $\deg \psi_2(x) = n - 1$  をみたす).

次に, Conrey-Farmer によって 1999 年に以下が成り立つことが示されている [9].

**定理 3.9.**  $k \leq 500$  ( $k \equiv 0 \pmod{4}$ ) のとき, 予想 3.2 は成り立つ.

上の定理 3.9 は, 後に紹介する Algorithm 3.1 で確認した. そこで必要となるものを準備する.

**定義 3.10.** 4 以上の整数  $k$  と  $z \in \mathbb{H}$  に対して,

$$G_k(z) = \sum_{m,n \in \mathbb{Z}} \frac{1}{(mz+n)^k} \quad (m, n \text{ は } mz+n \neq 0 \text{ をみたす})$$

を**アイゼンシュタイン級数**という. さらに,

$$E_k(z) = \frac{(k-1)!}{2 \cdot (2\pi i)^k} G_k(z)$$

を**正規化されたアイゼンシュタイン級数**という.

ここで, 必要のため以下を定義する:

$$F_j = \Delta^j E_4^{\frac{k}{4}-3j} = \sum_{m=j}^{\infty} A_j(m) q^m.$$

また,  $A_j(m)$  は  $F_j$  を  $q$ -展開した  $q^m$  の係数を表し,

$$\Delta = \frac{(60G_4(z))^3 - 27(140G_6(z))^2}{(2\pi)^{12}}$$

とする.

---

**Algorithm 3.1**


---

- 1:  $d = \dim(S_k)$  とし, 基底  $\{F_1 \dots F_d\}$  を計算する.
  - 2: 行列  $A, B$  を次のように定義する:  
 $A = (a_{j,l}) = A(2l) + 2^{k-1}A_j(l/2), B = (A_j(l)).$
  - 3:  $x$  を整数とし,  $\det(A - xB) \in \mathbb{Z}[x]$  を計算する.
  - 4:  $\det(A - xB) \pmod{p}$  の素因数分解を考える.
  - 5: 命題 3.8 の条件 (i)(ii)(iii) を満たす素数を見つけるまで繰り返す.
- 

次に, Farmer-James によって 2001 年に以下が成り立つことが示されている [10].

**定理 3.11.**  $k \leq 2000$  のとき, 予想 3.2 は成り立つ.

次に, Buzzard-Stein, Kleinerman によって 2004 年に以下が成り立つことが示されている [11].

**定理 3.12.**  $k \leq 3000$  のとき, 予想 3.2 は成り立つ.

上の定理 3.12 は命題 3.8 を用いず, 違う方法で確認されている.

次に, Chu-Wee Lim によって 2005 年に以下が成り立つことが示されている [12].

**定理 3.13.**  $k \leq 6000$  のとき, 予想 3.2 は成り立つ.

次に, Ghitza-McAndrew によって 2012 年に以下が成り立つことが示されている [13].

**定理 3.14.**  $k \leq 12000$  のとき, 予想 3.2 は成り立つ.

予想 3.2 に関して, 現在 (2022 年 12 月) では上の定理 3.14 が最高記録である. 定理 3.14 は命題 3.8 を用いて確認された. また, 以下のアルゴリズムが用いられた.

---

**Algorithm 3.2**


---

- 1:  $S_k$  の基底の集合  $B$  を求める.
  - 2:  $B$  に対するヘッケ作用素  $T_2$  の行列  $M$  を求める.
  - 3:  $2^{20}$  以下の素数  $p$  をとる.
  - 4:  $M \pmod{p}$  の固有多項式  $F_p \in \mathbb{F}_p$  を計算する.
  - 5: 命題 3.8 の条件 (i)(ii)(iii) を満たす素数を見つけるまで繰り返す.
-

## 第 4 章

# ヘッケ体の判別式に関する予想

### 4.1 ヘッケ体の判別式に関する予想

この章では、重さ  $k$  ( $k \in \mathbb{Z}$ ), レベル 1 のカスプ形式を考える. 第 3 章で予想 3.2 が正しいとすると, 同じ次元の代数体が 6 つずつ得られることを確認した. そして, それぞれの代数体に関係性があるのではないかと考えられた. そこで, それぞれの代数体の判別式に着目し, 前田芳孝によって以下の予想が提唱された [2].

**予想 4.1** (ヘッケ体の判別式に関する予想). 奇素数  $p$  が  $\mathbb{Q}(f_k)$  で分岐するとき, 以下の 2 つが成り立つ.

- (1)  $p \mid d(k + p \pm 1)$ . (弱予想)
- (2)  $p$  は  $\mathbb{Q}(f_{k+p \pm 1})$  でも分岐する. (強予想)

**注意 4.2.** 弱予想は,  $p \mid D(\mathbb{Q}(f_{k+p \pm 1}))$  であるので, 命題 2.21 より, 強予想が成り立てば, 弱予想も成り立つ. さらに, ヘッケ体の判別式  $d(k)$  の素因子  $p$  に対して,  $p$  が奇数乗であれば,  $p$  は  $\mathbb{Q}(f_k)$  で分岐することもわかる.

**注意 4.3.** 判別式の計算において,  $D(k)$  の計算 (より正確には  $\mathcal{O}_{\mathbb{Q}(f_k)}$  の計算) は  $d(k)$  の計算より難しいことが知られている. 実際,  $D(k)$  の計算は  $k \approx 80$  程度で限界をむかえる. 例えば,  $k = 70$  の時, 数式処理ソフト Magma [1] を用いて時間を計測すると,  $D(70)$  の計算に 27.550 秒,  $d(70)$  の計算は 0.01 秒未満であった. (Magma のバージョンは 2.27-3 で, PC 環境は以下の通りである:

OS 環境: Mac OS Monterey 12.5, CPU: Intel Core i7-1068NG7, メモリ: 32GB, プロセッサ速度: 2.3GHz.)

**例 4.4.** 例 2.22 より, 131 は  $\mathbb{Q}(f_{28})$  で分岐する. そこで, 131 が重さ  $k = 28 + 131 \pm 1 = 158, 160$  のヘッケ固有形式で定義されたヘッケ体で分岐するかどうかを調べる.  $d(158), d(160)$  を求めると,

$$d(158) \doteq 5.91 \cdot 10^{3124}, d(160) \doteq 7.26 \cdot 10^{3741}$$

となる．そして，131 で何回割れるのかを計算すると，

$$131 \mid d(158), 131^2 \nmid d(158), 131 \mid d(160), 131^2 \nmid d(160)$$

となり，分岐することがわかる．

次に，131 の  $k = 158 + 131 \pm 1 = 288, 290, k = 160 + 131 \pm 1 = 290, 292$  のヘッケ固有形式で定義されたヘッケ体での分岐を同様に調べると，分岐することがわかる．さらに，同様に  $k = 418, 420, 422, 424$  について調べると，131 は  $\mathbb{Q}(f_{418}), \mathbb{Q}(f_{422}), \mathbb{Q}(f_{424})$  で分岐することがわかる．また， $d(418)$  は 131 で 2 回割れるので，分岐するかどうかは  $D(418)$  を実際に計算しないとわからない．

現在 (2022 年 12 月) の記録として横山俊一と前田芳孝によって，以下の定理が成り立つことが知られている．

**定理 4.5.**  $p$  を奇素数とする．この時，弱予想について以下が成り立つ．

- (i)  $k \leq 74, p \leq 1009$  で， $p$  は  $\mathbb{Q}(f_k)$  で分岐するとする．この時，弱予想は成り立つ．
- (ii)  $k \leq 100, p \leq 1009$  で， $p$  は  $d(k)$  を奇数回割りきれるとする．この時，弱予想は成り立つ．
- (iii)  $k \leq 500, k + p + 1 \leq 500$  で， $p$  は  $d(k)$  を奇数回割りきれるとする．この時，弱予想は成り立つ．

## 4.2 素数 2 の分岐に関する考察

本論文では  $p = 2$  の分岐について考えた．2 が分岐する重さ  $k$  は奇素数と比べ，多く存在することが計算によってわかった．

まず， $p = 2$  の場合は予想 4.1 は成り立たない．

**例 4.6.** 2 はヘッケ体  $\mathbb{Q}(f_{46})$  で分岐する．実際，2 は  $D(46)$  を 3 回割る．しかし， $k = 46 + 2 \pm 1 = 47, 49$  は奇数なので，対応する固有形式は存在しない．

そこで，2 が分岐する重さについて特有の性質を調べた結果，重さに規則性を見つけ，以下のような予想をたてた．

**予想 4.7.** 2 は  $\mathbb{Q}(f_k)$  で分岐するとする．この時，以下が成り立つ．

- (i)  $k \equiv 2 \pmod{4}$  のとき，2 は  $\mathbb{Q}(f_{k+6})$  でも分岐する．
- (ii)  $k \equiv 2 \pmod{4}$  のとき，2 は  $\mathbb{Q}(f_{2k+5 \pm 3})$  でも分岐する．
- (iii)  $k \equiv 0 \pmod{4}$  のとき，2 は  $\mathbb{Q}(f_{k-6})$  でも分岐する．
- (iv)  $k \equiv 0 \pmod{4}$  のとき，2 は  $\mathbb{Q}(f_{2k-7 \pm 3})$  でも分岐する．

**注意 4.8.** 式  $2k - 7 \pm 3$  は  $2(k - 6) + 5 \pm 3$  と変形できるので，(iii)，(iv) は本質的に (i)，(ii) と同じである．また，(i)，(iii) より差が 6 のペアで出現することがわかる．

**例 4.9.** 2 は  $\mathbb{Q}(f_{46})$  で分岐する. 実際 2 は  $d(46)$  を 39 回割る.

(i)  $46 \equiv 2 \pmod{4}$  より,  $\mathbb{Q}(f_{52})$  で分岐すると予想される. 実際, 2 は  $d(52)$  を 75 回割るので, 2 は  $\mathbb{Q}(f_{52})$  で分岐する.

(iii)  $2 \cdot 46 + 5 \pm 3 = 94, 100$  を調べると, 2 は  $d(94)$  を 469 回割り, 2 は  $d(100)$  を 637 回割るので, 2 は  $\mathbb{Q}(f_{94}), \mathbb{Q}(f_{100})$  で分岐する.

しかし, 例 4.4 の様に, 実際に  $D(k)$  を計算しなければわからない例も存在する.

**例 4.10.** 2 は  $\mathbb{Q}(f_{278})$  で分岐する. 実際, 2 は  $d(278)$  を 14371 回割る.  $278 \equiv 2 \pmod{4}$  で, 2 は  $284 (= 278 + 6)$  で分岐するが, 重さ  $558, 564 (= 2 \cdot 278 + 5 \pm 3)$  のヘッケ体の判別式  $d(558), d(564)$  はそれぞれ 2 で 130610 回, 137096 回割られる. よって, 分岐するかどうかは実際に  $D(558), D(564)$  を計算しなければわからない.

Magma [1] を用いて, (i), (iii) は  $k \leq 704$  のとき, 正しいことを確認した. また, (ii), (iv) は  $k \leq 276$  のとき, 正しいことを確認した. さらに,  $2k + 5 \pm 3 \leq 704$  のとき,  $d(k)$  の計算だけでは予想が成り立つかがわからない重さ  $k$  は, 278, 284, 294, 300 の 4 つであった.  $p = 2$  の場合は奇素数に比べ, 多くの重さで分岐することと, 定理 4.5 に比べ, 大きな重さでの分岐を考え, 成り立つことがわかった.

今後の課題として, データの記録を伸ばすことと, 数式の意味や根拠を探すことが挙げられる.



# 謝辞

本論文は筆者が東京都立大学大学院理学研究科数理科学専攻博士前期課程に在学中の研究成果をまとめたものである。修士課程より2年間、他大学からの入学を受け入れていただいた上、数学を手取り足取り教えていただき、さらに公私ともにご支援していただきました指導教員である横山俊一准教授に深謝申し上げます。そしてご多用の中、本論文の副査を快諾していただきました内山成憲教授と内田幸寛准教授に深く感謝いたします。加えて、いつも心配をしてくれる家族、輪講でともに数学をしてくれたゼミのメンバー、息抜き等にいろいろな場所へ連れて行ってくれた友人、朝起きるのが苦手な私を起こしてくれた友人など、関わってくださったすべての方一人一人に感謝を記します。

# 付録

例 2.10 及び例 2.14

---

```
1 > M:=ModularForms(1,12); #重さ 12, レベル 1 のモジュラー形式
2 > M;
3 Space of modular forms on Gamma_0(1) of weight 12 and dimension 2
4 over Integer Ring.
5 > Basis(M); #M の基底
6 [
7     1 + 196560*q^2 + 16773120*q^3 + 398034000*q^4 +
8         4629381120*q^5 +
9         34417656000*q^6 + 187489935360*q^7 + 814879774800*q^8 +
10        2975551488000*q^9 +
11        9486551299680*q^10 + 27052945920000*q^11 + 0(q^12),
12    q - 24*q^2 + 252*q^3 - 1472*q^4 + 4830*q^5 - 6048*q^6 -
13    16744*q^7 +
14    84480*q^8 - 113643*q^9 - 115920*q^10 + 534612*q^11 + 0(q
15    ^12)
16 ]
17 >T:=HeckeOperator(M,2); #M の T_2 ヘッケ作用素
18 >T;
19 [2049 196560]
20 [0 -24]
```

---

---

```

1 > C:=CuspForms(1,28);
2 > T:=HeckeOperator(C,2);
3 > cp:=CharacteristicPolynomial(T);
4 > K:=NumberField(cp); #ヘッケ体
5 > d:=Discriminant(K); #ヘッケ体の判別式
6 > d;
7 849559104
8 > Factorization(d); #ヘッケ体の判別式の素因数分解
9 [ <2, 6>, <3, 6>, <131, 1>, <139, 1> ]
10 > OK:=MaximalOrder(K); #ヘッケ体の整数環
11 > D:=Discriminant(OK); #ヘッケ体の整数環の判別式
12 > D;
13 18209
14 > Factorization(D); #ヘッケ体の整数環の判別式の素因数分解
15 [ <131, 1>, <139, 1>, ]

```

---



---

```

1 > C:=CuspForms(1,70);
2 > T:=HeckeOperator(C,2);
3 > f:=CharacteristicPolynomial(T);
4 > K:=NumberField(f);
5 > time MaximalOrder(K);
6 Maximal Order of Equation Order with defining polynomial x^5 +
   18005734368*x^4 - 1942747456996431618048*x^3 -
7   14539211744046993293953166475264*x^2 +
8   613518461067953168654246762332094963122176*x +
9   4169744246282611427836654706819235757668276180615168 over
   its ground order
10 Time: 27.550 #整数環を生成するにかかった時間
11 > time Discriminant(K);
12 4653661038408060497923465868056338614856767474332438845594902\
13 9358009865675538162444814229839778978104740321515966791468940\
14 2405011456932972907118227770113011782990150281417427223101321\
15 3969964363793039360000000000
16 Time: 0.000 #ヘッケ体の判別式を計算するにかかった時間

```

---

```
1 #第 4.2節では 131を 2に変えて使用した.
2 > f:=function(x); #重さを入力するとヘッケ体の判別式が 131で何回割れる
   かを出力する関数
3 function> C:=CuspForms(1,x);
4 function> T:=HeckeOperator(C,2);
5 function> cp:=CharacteristicPolynomial(T);
6 function> K:=NumberField(cp);
7 function> d:=Discriminant(K);
8 function> k:=0;
9 function> if d mod 131 eq 0 then
10 function|if> repeat
11 function|if|repeat> k:=k+1;
12 function|if|repeat> d:=d div 131;
13 function|if|repeat> until d mod 131 ne 0;
14 function|if> end if;
15 function> return k;
16 function> end function;
17 > f(28);
18 1
19 > f(158);
20 1
21 > f(160);
22 1
23 > f(288);
24 1
25 > f(290);
26 1
27 > f(292);
28 1
29 > f(418);
30 2
31 > f(420);
32 3
33 > f(422);
34 1
35 > f(424);
36 1
```

---

素数 2 が分岐する重さ  $k$  のヘッケ固有形式で作られたヘッケ体と  $d(k)$  を割り切る回数  $n$  ( $k \leq 704$ , 139 個)

$(k, n) = (46, 39), (52, 75), (78, 299), (84, 425), (100, 637), (116, 917), (142, 1809),$   
 $(148, 2205), (150, 2357), (156, 2825), (158, 2349), (164, 2817), (166, 2989),$   
 $(172, 3535), (190, 4579), (196, 5299), (214, 6655), (220, 7573), (222, 7887),$   
 $(228, 8913), (230, 7883), (236, 8909), (238, 9281), (244, 10421), (270, 14371),$   
 $(276, 15889), (278, 14371), (282, 16401), (284, 15889), (286, 16421), (288, 18507),$   
 $(290, 16931), (292, 18077), (294, 18651), (296, 18047), (300, 20451), (302, 18633),$   
 $(308, 20433), (310, 21067), (316, 23017), (318, 23695), (324, 25801), (326, 23683),$   
 $(332, 25789), (334, 26501), (340, 28769), (342, 29567), (346, 29529), (348, 32003),$   
 $(352, 32809), (354, 32809), (358, 32821), (360, 35419), (364, 35431), (382, 40061),$   
 $(388, 43037), (406, 48295), (410, 48273), (412, 51661), (416, 51639), (418, 52777),$   
 $(422, 52819), (424, 56347), (428, 56389), (430, 57589), (436, 61369), (438, 62693),$   
 $(444, 66689), (446, 62681), (452, 66677), (454, 68027), (460, 72245), (462, 73701),$   
 $(468, 78147), (470, 73701), (474, 79637), (476, 78147), (478, 79637), (480, 84317),$   
 $(482, 79629), (484, 84317), (486, 85951), (488, 84309), (492, 90871), (494, 85937),$   
 $(500, 90857), (526, 106691), (532, 112367), (534, 114347), (538, 114275),$   
 $(540, 120287), (542, 114331), (544, 120215), (546, 122263), (548, 120271),$   
 $(550, 122275), (552, 128473), (556, 128485), (570, 139265), (572, 137093),$   
 $(574, 139281), (576, 146033), (578, 139243), (580, 146049), (582, 148371),$   
 $(584, 146011), (588, 155427), (598, 157793), (602, 157745), (604, 165143),$   
 $(606, 167647), (608, 165095), (610, 167589), (612, 175297), (614, 167627),$   
 $(616, 175239), (620, 175277), (622, 177867), (628, 185823), (630, 188541),$   
 $(636, 196809), (638, 188517), (644, 196785), (646, 199603), (652, 208189),$   
 $(654, 211075), (660, 219985), (666, 222959), (670, 222997), (672, 232199),$   
 $(674, 222927), (676, 232237), (680, 232167), (686, 235323), (692, 244899),$   
 $(694, 248175), (698, 248097), (700, 258093), (704, 258015).$

素数 2 が分岐するかどうか判定できなかった重さ  $k$  のヘッケ固有形式で作られたヘッケ体と  $d(k)$  を割り切る回数  $n$  ( $k \leq 704$ , 4 個)

$(k, n) = (558, 130610), (564, 137096), (590, 148332), (596, 155388).$

# 参考文献

- [1] W. Bosma, J. Cannon, and C. Playoust: The Magma algebra system. I: The user language, J. Symbolic Comput. 24 , 235–265(1997).
- [2] Yoshitaka Maeda: Maeda’s conjecture and related topics, RIMS Kokyuroku Bessatsu B53, pp. 305-324 (2015).
- [3] L. Calic: Modular forms and Maeda’s conjecture: University OF Luxembourg.
- [4] W. A. Stein (with an appendix by Paul E. Gunnells): Modular Forms: A Computational Approach , AMS (2007).
- [5] J.-P. Serre: A Course in Arithmetic: Graduate Texts in Mathematics , Springer (1973).
- [6] H.-C. Lee and W.-H. Hung: Galois groups of Hecke eigenforms, Chinese J. Math. 23.4 pp.329-342 (1995)
- [7] K.Buzzard: On the eigenvalues of the Hecke operator  $T_2$ : J.Number theory57 (1996).
- [8] Haruzo Hida and Yoshitaka Maeda: Non-abelian base change for totally real field: Pacific J. Math. Special Issue (1997).
- [9] J.B.Conrey and D.W.Farmer: Hecke opetarots and the nonvanishing of L-functions: Topics in number theorem, Kluwer Academic Publishers pp.143-150 (1999).
- [10] D.W.Farmer and K.James: The irreducibility of some level 1 Hecke polynomials: Mathmatics of computation71 pp.1263-1270 (2001).
- [11] S.Kleinerman: Some computations in support of Maeda’s conjecture: preprint (2004).
- [12] C.-W. Lim: Decomposition of spaces of cusp forms over  $\mathbb{Q}$ , and variants of partical Nim: Thesis (Ph.D.)-University of California, Berkeley: ProQuest LLC, Ann Arbor, MI p.111 (2005)
- [13] A.Ghitza and A.McAndrew: Experimental evidence for Maeda’s conjecture on modular forms: University of Melbourne (2012).