ある微分方程式のモジュラー形式解と楕円曲線の超特異多項式

中屋 智瑛（九州大学大学院数理学府）

概要

Serre 微分と呼ばれる微分作用素の類似物から $M_k(SL_2(\mathbb{Z}))$ の自己準同型を構成し, その固有関数と supersingular polynomial との関係を示すことができたのでそれを紹介する.

1 序

標数 $p>0$ の体 K 上定義された楕円曲線 E に対し, 群 $E(\overline{K})$ が位数 p の元をもたないとき E は supersingular であるという. supersingular な楕円曲線 E の j 不変量は $\mathbb{F}_{p^2}$ に入ることが知られている. したがって E の同型類は有限個であり, その j 不変量を根にもつ monic 多項式

$$ss_p(j)=\prod_{\substack{E/\overline{\mathbb{F}}_p\\ E:\text{supersingular}}}(j-j(E)) \quad \in \mathbb{F}_p[j]$$

は supersingular polynomial と呼ばれる.

偶数 $k\geq 4$ に対して M_k を $SL_2(\mathbb{Z})$ に関する重さ k の正則モジュラー形式のなす $\mathbb{C}$ ベクトル空間とする. k は

$$k=12m+4\delta+6\varepsilon \quad m\in\mathbb{Z}_{\geq 0},\ \ \delta\in\{0,1,2\},\ \ \varepsilon\in\{0,1\}$$

と一意的に書け, $\dim M_k = m+1$ が成り立つ. さらに任意の $f\in M_k$ に対し, $f/(E_4^\delta E_6^\varepsilon \Delta^m)$ は重さ 0 かつ $\mathfrak{H}$ 上正則より, 高々 m 次の $j(\tau)$ の多項式 $\widetilde{f}$ を用いて

$$f(\tau)=E_4(\tau)^\delta E_6(\tau)^\varepsilon \Delta(\tau)^m \widetilde{f}(j(\tau))$$

と書ける. ここで $E_k(\tau)\in M_k$ は Eisenstein 級数と呼ばれ, 次のようなフーリエ展開で定義される (B_k は k 番目のベルヌーイ数).

$$E_k(\tau)=1-\frac{2k}{B_k}\sum_{n=1}^{\infty}\left(\sum_{d|n}d^{k-1}\right)q^n \quad (q=e^{2\pi i\tau},\tau\in\mathfrak{H}=\{\tau\in\mathbb{C}\mid \Im(\tau)>0\})$$

また,

$$\Delta(\tau)=\frac{E_4(\tau)^3-E_6(\tau)^2}{1728}=q\prod_{n=1}^{\infty}(1-q^n)^{24}=q-24q^2+252q^3-1472q^3+\cdots,$$
$$j(\tau)=\frac{E_4(\tau)^3}{\Delta(\tau)}=\frac{1}{q}+744+196884q+21497360q^2+\cdots$$

は各々重さ 12 の尖点形式および楕円モジュラー関数である. $k=2$ に対して,

$$E_2(\tau)=1-24\sum_{n=1}^{\infty}\Big(\sum_{d|n}d\Big)q^n=\frac{1}{2\pi i}\frac{d}{d\tau}\log\Delta(\tau)$$

は $\mathfrak{H}$ 上正則だがモジュラー形式ではないことに注意しておく.

Eisenstein 級数と supersingular polynomial の間には次のような古典的な関係が知られている ($p-1=12m+4\delta+6\varepsilon$).

Theorem 1 (Deligne)**.** 素数 $p\geq 5$ に対して,

$$ss_p(j)\equiv j^{\delta}(j-1728)^{\varepsilon}\widetilde{E}_{p-1}(j)\pmod p.$$

また, supersingular polynomial は超幾何級数を用いて次のように書ける.

Theorem 2 (Deuring)**.** 素数 $p\geq 5$ に対して,

$$ss_p(j)\equiv j^{m+\delta}(j-1728)^{\varepsilon}{}_2F_1\left(\frac{1}{12}+\frac{2\delta+3\varepsilon}{6},\frac{5}{12}-\frac{2\delta-3\varepsilon}{6};1;\frac{1728}{j}\right)\pmod p.$$

さて, $f'(\tau):=(2\pi i)^{-1}df/d\tau=q\,df/dq$ とし, Serre 微分 $\partial_\Delta=\partial_{\Delta,k}:M_k\to M_{k+2}$ を次で定める.

$$\partial_\Delta(f)(\tau):=f'(\tau)-\frac{k}{12}\frac{\Delta'(\tau)}{\Delta(\tau)}f(\tau)=f'(\tau)-\frac{k}{12}E_2(\tau)f(\tau)$$

さらに Serre 微分を二回施した作用素 $\partial_\Delta^2=\partial_{\Delta,k+2}\circ\partial_{\Delta,k}:M_k\to M_{k+4}$ を考える. $k\not\equiv 2\pmod 3$ に対して $\dim M_k=\dim M_{k+4}$ となることから, $M_{k+4}=E_4\cdot M_k$ である. ゆえに $E_4^{-1}\partial_\Delta^2$ は M_k の自己準同型を与えるが, これは $k(k+2)/144$ を固有値の一つとして持つ. そこで固有値問題

$$\partial_\Delta^2(f)=\frac{k(k+2)}{144}E_4f \tag{1}$$

において, その一意的な正規化された解を $F_{\Delta,k}\in M_k$ とする. このとき次が成り立つ.

Theorem 3 (Kaneko, Zagier)**.** 素数 $p\geq 5$ に対して,

$$ss_p(j)\equiv j^{\delta}(j-1728)^{\varepsilon}\widetilde{F}_{\Delta,p-1}(j)\pmod p.$$

証明は (1) が

$$f''(\tau)-\frac{k+1}{6}E_2(\tau)f'(\tau)+\frac{k(k+1)}{12}E_2'(\tau)f(\tau)=0$$

と書き直せることから, $k=p-1$ に対して $F''_{\Delta,p-1}\equiv 0 \pmod p$, よって $F_{\Delta,p-1}\equiv 1+O(q^p) \pmod p$ となることと $E_{p-1}\equiv 1 \pmod p$ という事実から Theorem 1 を通じてなされる. また解は超幾何級数を用いて表示することもできる. 詳細は [1] を参照のこと.

また [2] では Serre 微分の代わりに, 微分作用素

$$\partial_{E_4}(f)(\tau):=f'(\tau)-\frac{k}{4}\frac{E_4'(\tau)}{E_4(\tau)}f(\tau),\quad \partial_{E_6}(f)(\tau):=f'(\tau)-\frac{k}{6}\frac{E_6'(\tau)}{E_6(\tau)}f(\tau)$$

を用いて構成した同様の固有値問題の, 正規化されたモジュラー形式解に対し次が成り立つことが示されている.

Theorem 4 (Baba, Granath)**.** 素数 $p\geq 5$ に対して,

$$ss_p(j)\equiv j^{\delta}(j-1728)^{\varepsilon}\widetilde{F}_{E_4,p-1}(j)\equiv j^{\delta}(j-1728)^{\varepsilon}\widetilde{F}_{E_6,p-1}(j)\pmod p.$$

同じ方針でより一般的な形で微分作用素を構成しても, やはり supersingular polynomial との関係が得られるというのが主結果である.

2 主結果

$r,s,t\in\mathbb{Z}, 2r+3s+6t\neq 0$ に対して $g(\tau):=E_4(\tau)^rE_6(\tau)^s\Delta(\tau)^t$ とおく. さらに $k=12m+4\delta+6\varepsilon$ とし, $1\leq n\leq m$ なる整数 n に対して $t(k+1)\neq n(2r+3s+6t)$ であるとする. このとき

$$\partial_g(f)(\tau)=\partial_{g,k}(f)(\tau):=f'(\tau)-\frac{k}{4r+6s+12t}\frac{g'(\tau)}{g(\tau)}f(\tau)$$

と定める. この作用素は M_k の元を M_{k+2} の元にうつすとは限らず, r,s,t の値によっては行き先が $\mathfrak{H}$ に極をもつ. そこで M_k の基底にこの作用素を二回作用させ, non-holomorphic term がどこから生じているかを具体的に計算する. それと打ち消しあうような項を加えることで M_k の自己準同型を構成できる. さらに適当な固有値を選んで固有値問題を考えると, それは以下のような微分方程式に書き換えることができる:

$$f''-\frac{k+1}{u}\frac{g'}{g}f'+\frac{k(k+1)}{2u}\left(\frac{g'}{g}\right)'f+\frac{s(k+1)(k+2\varepsilon)}{8u}\frac{E_4(E_4^3-E_6^2)}{E_6^2}f$$
$$-\left\{\frac{r(k+1)(k+2\delta)}{18u}-\frac{\delta(\delta-1)}{9}\right\}\frac{E_4^3-E_6^2}{E_4^2}f=0.$$

ここで $u=2r+3s+6t$ である. モジュラー形式解を $F_{g,k}(\tau)$ とし, $F_{g,k}(i\infty)=1$ と正規化する.

Theorem 5. 素数 $p \geq 5$ に対して, $u \not\equiv 0 \pmod{p}$ とすると

$$ss_p(j) \equiv j^{\delta}(j-1728)^{\varepsilon}\widetilde{F}_{g,p-1}(j) \pmod{p}.$$

証明は Theorem 3 と同様で, $k = p-1$ に対して $F''_{g,p-1} \equiv 0 \pmod{p}$ となることから示される (今の場合 $\delta \in \{0,1\}$ であることに注意). また, $F_{g,k}(\tau)$ は超幾何級数を用いて具体的に表示することもできる.

$$F_{g,k} = E_4^{3m+\delta}E_6^{\varepsilon}\ {}_2F_1\left(-\frac{k}{12}+\frac{2\delta+3\varepsilon}{6}, \frac{5}{12}+\frac{(2r-3s-6t)(k+1)}{12u}-\frac{2\delta-3\varepsilon}{6}; 1-\frac{t(k+1)}{u}; \frac{1728}{j}\right)$$

これより $k = p-1$ に対し $\widetilde{F}_{g,p-1}(j) \pmod{p}$ は Theorem 2 の右辺に還元されるので, 確かに supersingular polynomial を与えている.

3 今後の課題

今のところ non-holomorphic term を消すという構成方法が, なぜ supersingular polynomial との関係を導くのかはよくわかっていない. また微分作用素を三回以上施して固有値問題を考えることもできる. 例えば [3] では $k \equiv 0 \pmod{4}$ のとき M_k の自己準同型

$$E_6^{-1}(\partial_{\Delta}^3(f) + cE_4\partial_{\Delta}(f))$$

の固有関数から構成される多項式が supersingular polynomial を与えることが示されている. あるいは $SL_2(\mathbb{Z})$ の合同部分群に対しても同様の問題を考えることができるだろう.

参考文献

[1] M. Kaneko, D. Zagier, Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, AMS/IP Studies in Advanced Mathematics, vol. **7** (1998), 97–126

[2] S. Baba, H. Granath, Orthogonal systems of modular forms and supersingular polynomials, International Journal of Number Theory, vol. 7, no. 1 (2011), 249–259

[3] M. Kaneko, N. Todaka, Hypergeometric modular forms and supersingular elliptic curves, Centre de Recherches Mathématiques, CRM Proceedings and Lecture Notes, vol. **30** (2001), 79–83