数理解析研究所講究録
513巻 1984年 97-108

相互法則と重さ1の保型形式について

神戸大理　平松　豊一　(Toyokazu Hiramatsu)
大阪府大　石井　伸郎　(Noburo Ishii)
神戸大理　味村　良雄　(Yoshio Mimura)

§0. 序

多項式 $f(x)=x^4-12$ について、$f(x) \bmod p$ が相異なる一次式の積になるような素数 p の集合を $Spl\{f(x)\}$ と書く。これは次のように特徴づけられる：

$$Spl\{f(x)\}$$
$$=\{p:\text{素数} \mid p=a^2+36b^2\}$$
$$=\{p:\text{素数} \mid p=(6c+1)^2+12d^2,\ c\equiv d \bmod 2\}$$
$$=\{p:\text{素数} \mid 2p=3(2k+1)^2-(6l+1)^2,\ k\equiv l \bmod 2\}.$$

一方，この $Spl\{f(x)\}$ は，重さ1の cusp form $\eta(12\tau)^2$ の Fourier 係数 $a(p)$ で決まり（$\eta(\tau)$ は Dedekind の η 関数），次のようになる：

$$Spl\{f(x)\}=\{p:\text{素数} \mid a(p)=2\}.$$

上の三つの条件は，$\eta(12\tau)^2$ の三つの表現に対応している：

$$\eta(12\tau)^2 = \frac{1}{2}\sum_{a,b}(-1)^b q^{a^2+9b^2} \quad ((a,3)=1,\ a \not\equiv b \bmod 2)$$
$$= \sum_{c,d}(-1)^{c+d} q^{(6c+1)^2+12d^2}$$
$$= \sum_{k,l}(-1)^{k+l} q^{\frac{3(2k+1)^2-(6l+1)^2}{2}} \quad (k \geqq 2|l|).$$

ところで，この最後の等式は，Kac-Moody の Lie 環の方から Kac-Peterson [3] により，与えられたものである。また、今の場合，$Spl\{f(x)\}$ は，式の形からみて，法 p に関して 12 が 4 乗剰余となる素数 p の集合ともみることができる。

このように，ある多項式については，その Spl が三つの同値な条件で決まり，それはまた，重さ 1 の cusp form の三つの表現（2つは definite 型，1つは indefinite 型）に関係し、さらに，4 乗剰余とも関連する。以下では，この事情を，整数論的に解明し，Kac-Peterson によって与えられた残りの等式を説明し，新しい等式を付け加えよう．最後に，相互法則との関連についても少しふれる。

§1.

実 2 次体 $F = \mathbb{Q}(\sqrt{D})$ （D は平方因子を含まない正整数）をとり，その整数環を $\mathcal{O}_F$ とする．$\mathcal{O}_F$ の ambig な整イデアル $\mathfrak{f}$ を法とする狭義 ray class 群を $H_F(\mathfrak{f})$ とかく。$\mathcal{O}_F$ の単数群を $\mathcal{O}_F^\times$ として

（仮定1）　任意の総正な単数 ε に対して，$\varepsilon+1 \notin \mathfrak{f}$.

のもとで，$H_F(\mathfrak{f})$ の指標 χ で次をみたすものが存在する：

$$\chi((x)) = \operatorname{sgn} x \quad (又は \ \operatorname{sgn} x')$$

$$\forall x \in \mathcal{O}_F, \quad x \equiv 1 \bmod \mathfrak{f}$$

この χ について F の L 関数が定まる：

$$L_F(s,\chi) = \sum_{c \in H_F(\mathfrak{f})} \chi(c) \sum_{\mathfrak{a} \in c,\, \mathfrak{a} \subset \mathcal{O}_F} N\mathfrak{a}^{-s}.$$

K を F 上の極大狭義 ray class field とする．

（仮定2）　$[H_F(\mathfrak{f}) : H_F(\mathfrak{f})_0] = 2$

ただし，$H_F(\mathfrak{f})_0 = \{c \in H_F(\mathfrak{f}) \mid c = c'\}$,

のもとで，虚2次体 k で，K が k 上アーベル拡大となるものが存在する．K/k に対応する類群の指標で，χ からきまるものを ξ_χ とかくとき，

$$L_F(s,\tilde{\chi}) = L_k(s,\tilde{\xi}_\chi)$$

となる．ここで，$\tilde{\chi}$，$\tilde{\xi}_\chi$ はそれぞれ．χ，ξ_χ からきまる原始指標であり，$L_k(s,\tilde{\xi}_\chi)$ は，k の L 関数である．（以上については Shintani [4] を参照されたい。）

以下，これら $L_F(s,\tilde{\chi})$，$L_k(s,\tilde{\xi}_\chi)$ を実際に書き下すことになる。

先ず，F において考える。上の仮定から，

$$\mu \in \mathcal{O}_F, \quad \mu < 0, \quad \mu' > 0, \quad \mu \equiv 1 \bmod \mathfrak{f}$$

となるμが存在し，単項イデアル(μ)を含むray classをμと書くことにして，

$$H_F(\mathfrak{f}) = R \cup R\mu \cup R\mu' \cup R\mu\mu'$$

となる。ここで，Rは$H_F(\mathfrak{f})_0/\langle\mu\mu'\rangle$の完全代表系である。したがって，

$$L_F(s,\chi) = \sum_{\sigma\in R}\chi(\sigma)\sum_{\alpha}(\mathrm{sgn}\,\alpha)(N\alpha/N\mathfrak{a}_\sigma)^{-s},$$

ただし，$\mathfrak{a}_\sigma$はσ^{-1}に属する整イデアル，$\rho_\sigma\in\mathfrak{a}_\sigma$，$\rho_\sigma\equiv 1 \bmod \mathfrak{f}$。$\alpha$は，$\mathcal{O}_F/E_{\mathfrak{f}}^+$，$N\alpha>0$，$\alpha\equiv\rho_\sigma \bmod \mathfrak{a}_\sigma\mathfrak{f}$，を走る。ここで，$E_{\mathfrak{f}}^+ = \{\varepsilon\in\mathcal{O}_F^\times \mid \varepsilon\gg 0,\ \varepsilon\equiv 1 \bmod \mathfrak{f}\}$。

この式を，逆Mellin変換して，

$$\theta_F(\tau) = \sum_{\sigma\in R}\chi(\sigma)\ \theta\,(QD_1\tau;\ \rho_\sigma,\mathfrak{a}_\sigma,\mathfrak{f})$$

を得る．ただし，$\mathfrak{f}=Q\mathfrak{f}_1$，$\mathfrak{f}_1 \mid \sqrt{D}$，$D_1=N\mathfrak{f}_1$，Q：正整数，また，$\theta(\tau;\rho,\mathfrak{a},\mathfrak{f}) = \sum_{\alpha}(\mathrm{sgn}\,\alpha)\,q^{N\alpha/N\mathfrak{a}\cdot QD_1}$

とくに，$\mathfrak{f}_1=\sqrt{D}$なら，このθは，Heckeの定義したindefiniteテータ関数となる[1，2]。

次にkで考える。ここでK/kは巡回拡大とし，その導手を$\mathfrak{c}$とすると，$H_k(\mathfrak{c})/C = \langle\lambda\rangle$，$\lambda^{4m}=1$，とかける（Cは，Kに対応する類群）。$\chi$からきまるGal(K/Q)の表現のGal(K/k)への制限は$\xi_\chi+\xi'_\chi$と直和に分解し，ξをξ_χあるいはξ'_χとして，kのL関数$L_k(s,\xi)$は次の形にかける：

$$L_k(s,\xi) = \sum_{\mathfrak{a} \subset \mathcal{O}_k} \xi(\mathfrak{a}) N\mathfrak{a}^{-s} = \sum_{j=0}^{4m-1} \xi(\lambda)^j \sum_{\mathfrak{a} \in \lambda^j} N\mathfrak{a}^{-s}$$
$$= \sum_{j=0}^{m-1} \xi(\lambda^2)^j \left\{ \sum_{\mathfrak{a} \in \lambda^{2j}} N\mathfrak{a}^{-s} - \sum_{\mathfrak{a} \in \lambda^{2j+2m}} N\mathfrak{a}^{-s} \right\}.$$

再び逆Mellin変換して

$$\theta_k(\tau) = \sum_{j=0}^{m-1} \xi(\lambda^2)^j \{ \theta_{2j}(\tau) - \theta_{2j+2m}(\tau) \}$$

ただし，$\theta_j(\tau) = \sum_{\mathfrak{a} \in \lambda^j} q^{N\mathfrak{a}}$.

ここで，更に，$K/\mathbb{Q}$ は dihedral 拡大であるとすると，$m = 1$, $R = \{1\}$ となり，

$$\theta_F(\tau) = \theta(QD_1\tau\,;\,1, \mathcal{O}_F, \mathfrak{f}) = \frac{1}{t}\vartheta_\pm(QD_1\tau\,;\,\rho, Q\sqrt{D})$$

ただし，$\pm N\rho > 0$, $\mathfrak{f}\rho = (Q\sqrt{D})$, $t = [E^+_{\mathfrak{f}} : E^+_{Q\sqrt{D}}]$

$\vartheta_\pm$ は Hecke のテータ関数。

$$\theta_k(\tau) = \theta_0(\tau) - \theta_2(\tau)$$

を得る．すなわち，

Prop. $\frac{1}{t}\vartheta_\pm(QD_1\tau\,;\,\rho, Q\sqrt{D}) = \theta_0(\tau) - \theta_2(\tau)$.

§2. 例

以下では，F，k を具体的に与える．

例 1. $F = \mathbb{Q}(\sqrt{3})$, $k = \mathbb{Q}(\sqrt{-1})$, $K = k(\sqrt[4]{12})$

$\mathfrak{f} = (2\sqrt{3})$, $\mathfrak{c} = (6)$

$$\begin{tikzcd}
 & K \arrow[d, dash] & \\
 & L \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
F \arrow[dr, dash] & k \arrow[d, dash] & E = \mathbb{Q}(\sqrt{-3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$H_F(f) = \{1, \mu, \mu', \mu\mu'\}$

$H_k(f) = \{1, \lambda, \lambda^2, \lambda^3\}$

$\mu = (7-6\sqrt{3})$, $\lambda = (2+\sqrt{-1})$

$\varepsilon = 2+\sqrt{3}$, $\varepsilon^2 \equiv 1 \mod f$

(i) $\theta_k(\tau)$ について.

$\mathfrak{a} \in \{1, \lambda^2\}$ のとき, $\mathfrak{a} = (\alpha)$, $\alpha = a + 3b\sqrt{-1}$, $(a, 3) = 1$, とかけるが, 更に,

$$\begin{cases} (\alpha) \in 1 \iff a \equiv 1,\ b \equiv 0 \mod 2 \\ (\alpha) \in \lambda \iff a \equiv 0,\ b \equiv 1 \mod 2 \end{cases}$$

となるから

$$\theta_k(\tau) = \frac{1}{2}\sum_{a,b} (-1)^b q^{a^2+9b^2} \qquad (a, 3) = 1,\ a \not\equiv b \mod 2$$
$$= \eta(12\tau)^2$$

(ii) $\theta_F(\tau)$ について.

$$\begin{cases} \mathfrak{a} \in 1 \iff \mathfrak{a} = (\alpha),\ \alpha \equiv 1 \mod f,\ \alpha \gg 0 \\ \mathfrak{a} \in \mu\mu' \iff \mathfrak{a} = (\alpha),\ \alpha \equiv -1 \mod f,\ \alpha \gg 0 \end{cases}$$

となるので, $\alpha = x + 2\sqrt{3}y \gg 0$, $x \equiv \pm 1 \mod 6$ として,

$$\begin{cases} (\alpha) \in 1 \iff x \equiv 1 \mod 3 \\ (\alpha) \in \mu\mu' \iff x \equiv -1 \mod 3 \end{cases}$$

となる.

$$\alpha\varepsilon^{\pm 2} = (7x \pm 24y) + (14y \pm 4x)\sqrt{3}$$

だから，α の動く基本領域として，$7x \pm 24y \geqq x$，則ち，$x \geqq 4|y|$ をとることができて，

$$\theta_F(\tau) = \vartheta_+(12\tau; 1, \sqrt{12}) = \sum \left(\frac{x}{3}\right) q^{x^2-12y^2}$$

ただし，$x \geqq 4|y|$，$(x, 6) = 1$，

を得る。今，Kac-Peterson の等式を得るために，θ_F の別の表現を考える。 $\rho \in \theta_F$，$\rho > 0$ として，

$$\theta_F(\tau) = \sum_{\beta} (\mathrm{sgn}\,\beta)\, q^{N\beta/N\rho}$$

ただし，β は，θ_F/E_f^+，$N\beta \cdot N\rho > 0$，$\beta \equiv \rho \bmod f\rho$，を走る。そこで，$\rho = 1 + \sqrt{3}$ ととり，$\beta = x \pm y\sqrt{3}$，（$\pm$ は $\mathrm{sgn}\,\beta$ と同じ）とおく。$\beta > 0$ のとき，$y > 0$，$x \equiv 1 \bmod 6$，$x \equiv y \bmod 4$ となり，$x = 6l+1$，$y = 2k+1$ とおくと $k \equiv l \bmod 2$ を得る。

$$\beta\varepsilon^{\pm 2} = (7x \pm 12y) + (7y \pm 4x)\sqrt{3}$$

だから，β の動く基本領域として，$7y \pm 4x \geqslant y$，すなわち，$3y \geqq 2|x|$，結局 $k \geqq 2|l|$ がとれる．$\beta < 0$ のときも，同様であるが，$k \not\equiv l \bmod 2$ となる。つまり，$\mathrm{sgn}\,\beta = (-1)^{k+l}$ となり，

$$\theta_F(\tau) = \sum_{k \geqslant 2|l|} (-1)^{k+l} q^{\frac{3(2k+1)^2 - (6l+1)^2}{2}}$$

となる。これは，Kac-Peterson の得たものである。

なお，もう一つの2次体 E についても，k のときと同じよ

うにして

$$\Theta_E(\tau) = \sum_{c,d} (-1)^{c+d} q^{(6c+1)^2+12d^2} = \eta(24\tau)\,\theta_0(24\tau)$$

が得られる。（K/E は導手 $(4\sqrt{-3})$ をもつ）

例 2. $F=\mathbb{Q}(\sqrt{2})$, $k=\mathbb{Q}(\sqrt{-2})$, $K=k(\sqrt{\varepsilon})$ $E=\mathbb{Q}(\sqrt{-1})$

$\mathfrak{f}=(4)$, $\mathfrak{c}=(4)$ $\varepsilon = 1+\sqrt{2}$ $(4(1+\sqrt{-1}))$

$$\Theta_k(\tau) = \sum (-1)^n q^{(4m+1)^2+8n^2} = \eta(8\tau)\,\eta(16\tau)$$

$$\Theta_F(\tau) = \sum_{n\geq 3|m|} (-1)^n q^{(2n+1)^2-32m^2} = \vartheta_+(8\tau;\, 2+\sqrt{2},\, 2\sqrt{8})$$

$$\Theta_E(\tau) = \sum (-1)^{m+n} q^{(4m+1)^2+16n^2}$$

例 3. $F=\mathbb{Q}(\sqrt{5})$, $k=\mathbb{Q}(\sqrt{-5})$, $E=\mathbb{Q}(\sqrt{-1})$, $K=k(\sqrt{\varepsilon})$

$\mathfrak{f}=(4)$, $\mathfrak{c}=(2)$ (10), $\varepsilon=\frac{1+\sqrt{5}}{2}$

$$\Theta_k(\tau) = \sum (-1)^{m+n} q^{\frac{(6n+1)^2+5(6m+1)^2}{6}} = \eta(4\tau)\,\eta(20\tau)$$

$$\Theta_F(\tau) = \sum_{2k\geq l\geq 0} (-1)^k q^{\frac{5(2k+1)^2-(2l+1)^2}{4}} = \frac{1}{2}\vartheta_+\left(4\tau;\, \frac{5+\sqrt{5}}{2},\, 4\sqrt{5}\right)$$

例 4. $F=\mathbb{Q}(\sqrt{21})$, $k=\mathbb{Q}(\sqrt{-7})$, $K=k(\sqrt{\alpha})$

$\mathfrak{f}=(\alpha)$ $\mathfrak{c}=(3)$ $\alpha=\frac{3+\sqrt{21}}{2}$

$$\Theta_k(\tau) = \sum (-1)^{m+n} q^{\frac{(6m+1)^2+7(6n+1)^2}{8}} = \eta(3\tau)\,\eta(21\tau)$$

$$\Theta_F(\tau) = \sum_{\substack{x\geq 7|y| \\ x\equiv y \bmod 2}} \left(\frac{-x}{3}\right) q^{\frac{x^2-21y^2}{4}} = \frac{1}{2}\vartheta_+\left(3\tau;\, \frac{7+\sqrt{21}}{2},\, \sqrt{21}\right)$$

注1. 上の例1～3は，Kac-Peterson [3] によって見い出された等式である。

注2. $\eta(\tau)\eta(23\tau)$, $\eta(2\tau)\eta(22\tau)$, $\eta(6\tau)\eta(18\tau)$ は D_3 型であり，従って，indefiniteテータ級数で表わされない。

注3. 例2からの等式

$$\sum(-1)^n q^{(4m+1)^2+8n^2} = \sum(-1)^{m+n} q^{(4m+1)^2+16n^2}$$

は，2の4乗剰余に対するGaussの2つの判別条件の同値性の一般化を与えている。判別条件そのものは，類体Kの代りに，$K' = \mathbb{Q}(\sqrt{-1}, \sqrt[4]{2})$ をとって，得られる。

§3. Higher Reciprocity Law

Splに戻る。仮定1, 2を満たす実2次体Fをとる。§1のとおり，虚2次体kがあって，Fとkに対するL関数が一致する。K/kが巡回拡大，K/Qがdihedral拡大とする。$f(x)$ を，実2次体Fを通してのK/Qの定義多項式（有理整係数）とする。次を得る。

<u>定理</u>　$\mathrm{Spl}\{f(x)\} = \{p : \text{整数} \mid p \nmid \Delta_f,\ a(p) = 2\}$

ただし，f の判別式を Δ_f，$a(p)$ は，Fに対するHeckeのindefinite modular form $\theta_F(\tau)$ の p 番目のFourier係数である。

(証) $\theta_k(\tau)=\sum_{\mathfrak{a}\subset\mathcal{O}_k}\xi(\mathfrak{a})q^{N\mathfrak{a}}=\sum b(n)q^n$

とおく。kの素イデアルで，K/kで不分岐なもの$\mathfrak{p}$をとる。次が成り立つ．($L=F\cdot k$)。

(i) $\xi(\mathfrak{p})=1 \iff \mathfrak{p}\in(1) \iff \mathfrak{p}$は$K$で完全分解する。

(ii) $\xi(\mathfrak{p})=-1 \iff \mathfrak{p}\in\lambda^2 \iff \mathfrak{p}$は$L/k$で完全分解し，
K/Lで惰性する

(iii) $\xi(\mathfrak{p})=i$ or $-i \iff \mathfrak{p}\in\lambda$ or $\lambda^3 \iff \mathfrak{p}$は$K/k$で惰性的。

pを有理素数で，kで $p=\mathfrak{p}\mathfrak{p}'$，$\mathfrak{p}\neq\mathfrak{p}'$，とする。このとき，

$$\mathfrak{p}\in(1) \iff b(p)=2$$

である。$F(x)$をK/kの定義多項式（有理整数係数）とする。あきらかに

$$\mathrm{Spl}\{F(x)\}=\{p:\text{素数}\mid b(p)=2,\ p\nmid\Delta_F\}$$

である。他方，

$$\mathrm{Spl}\{f(x)\}\cup\{p:\text{素数}\mid p\text{は不分岐},\ p\mid\Delta_f\}$$
$$=\mathrm{Spl}\{F(x)\}\cup\{p:\text{素数}\mid p\text{は不分岐},\ p\mid\Delta_F\}$$

であり，Prop. より $a(p)=b(p)$ であったから，

$$\mathrm{Spl}\{f(x)\}=\{p:\text{素数}\mid a(p)=2,\ p\nmid\Delta_f\}$$

を得る。 Q.E.D.

§2の例1をとりあげる。K/kの定義多項式として，

$F_1(x)=x^4-12$ または，$F_2(x)=x^4-6x^2-3$

をとる。他方，K/F の定義多項式

$$f_1(x) = x^4 - 4(1+\sqrt{3})x^2 + 4(2+\sqrt{3})^2$$

から，

$$f(x) = f_1(x) f_1(x)' = x^8 - 8x^6 + 24x^4 + 160x^2 + 16$$

とおくと，

$$\begin{aligned} \mathrm{Spl}\{F_1(x)\} = \mathrm{Spl}\{F_2(x)\} &= \mathrm{Spl}\{f(x)\} \\ &= \{p : \text{素数} \mid a(p) = 2\} \\ &= \{p : \text{素数} \mid p = u^2 + v^2,\ u \equiv 0 \bmod 6\}, \end{aligned}$$

ただし，

$$\Theta_F(\tau) = \vartheta_+(12\tau; 1, \sqrt{12}) = \sum a(n) q^n .$$

注） Spl だけでなく，定理の f について次が言える．

(i) $f(x) \bmod p$ が相異なる2つの4次多項式の積でかける $\iff$ $a(p) = 0$，$a(p^2) = -1$

(ii) $f(x) \bmod p$ が相異なる4つの2次多項式の積でかける $\iff \begin{cases} a(p) = -2 \\ \text{又は}\quad a(p) = 0,\ a(p^2) = 1. \end{cases}$

参考文献

[1] E.Hecke, Uber einen neuen Zusammenhang zwischen elliptischen und indefiniten quadratischen Formen, Mathematische Werke,

Vandenhoeck und Reprecht, Gottingen, 1959, pp.418-427.

[2] E.Hecke, Zur Theorie def elliptischen Modulfunktionen, Ibid., pp.428-460.

[3] V.G.Kac and Peterson, Infinite-dimensional Lie algebras, theta functions and modular forms (preprint).

[4] T.Shintani, On certain ray class invariants of real quadratic fields, J.Math.Soc.Japan 30 (1978), pp.139-167.