数理解析研究所講究録
797巻 1992年 49-65

Grant による Eisenstein の積公式の一般化について

東大教養 伊藤 博 (Hiroshi Ito)

§0. Introduction.

ここで積公式と言っているのは，次のようなタイプの式のことである：

(0.1) $$\prod_{r=1}^{p-1} 2i\sin\frac{2\pi r}{p} = p \qquad (p:\text{奇素数}),$$

(0.2) $$\prod_{\substack{r \bmod \omega \\ r\not\equiv 0\ (\omega)}} \wp\left(\frac{r\theta}{\omega}\right) = \frac{1}{\omega^2}.$$

但し，(0.2) では，$\wp$ は $\wp'^2 = 4\wp^3 - 1$ をみたす Weierstraß の $\wp$-関数，θ は $\mathbb{Z}[e^{2\pi i/3}]\theta$ が $\wp$ の周期格子となるような正の実数，ω は $\mathbb{Z}[e^{2\pi i/3}]$ の1次の素 ideal の生成元で $\omega \equiv 1\ (3)$ をみたすものとし，r は $\mathbb{Z}[e^{2\pi i/3}]$ を mod ω で動く．最近，Grant は，(0.2) の一般化として次のような結果を発表した ([G2])．C を，$\mathbb{Q}$ 上

(0.3) $$y^2 = x^5 + \frac{1}{x}$$

で定義された種数2の曲線とし，J を C の Jacobian とする．

∞ で C の無限遠点，O で J の原点を表わす．C の J への埋め込み

(0.4) $$C \ni P \longmapsto (P-\infty \text{ の類}) \in J$$

の像を Θ とする．$\zeta = e^{2\pi i/5}$ は

$$(x, y) \longmapsto (\zeta x, y)$$

により C の自己同型を定め，これは $\mathbb{Z}[\zeta]$ の $\mathrm{End}(J)$ への埋め込みをひき起こす．Jacobian J の具体的な記述（Grant [G] に従った）については，次節で記すが，そこで J 上のある有理関数の zero divisor $(X)_0$ が定義される．$\alpha \in \mathbb{Z}[\zeta]$ と J 上の divisor D について，$(\alpha)^{-1}D$ で D の α によるひきもどしを表わす．$\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ を $\sigma(\zeta) = \zeta^2$ で定める．

<u>定理 1.</u>（[G2]）．β を $\mathbb{Z}[\zeta]$ の 1 次の素 ideal の生成元で $\beta \equiv \pm 1 \pmod{(1-\zeta)^2}$ をみたすものとする．このとき，

(0.5) $$\prod_{\substack{P \in \Theta \cap (\beta\sigma^{-1}(\beta))^{-1}(X)_0 \\ 2P \neq O}} x(P) = \frac{1}{(\beta\sigma(\beta))^2}.$$

ここで，$x(P)$ は，P の (0.4) による逆像の x 座標という意味である．

さて，以下 β は上の定理のようなものとし，

$$G(\beta) = \{P \in \Theta \cap (\beta\sigma^{-1}(\beta))^{-1}(X)_0 \ ; \ 2P \neq O\},$$

$$L = L_\beta = \mathbb{Q}(\zeta)(x(P), y(P)\,;\ P \in G(\beta)),$$
$$K = K_\beta = \mathbb{Q}(\zeta)(x(P)^5\,;\ P \in G(\beta)/\mu_{10})$$

とおく（$\mu_{10} = \langle -\zeta \rangle$）．この小論では，主に $K/\mathbb{Q}(\zeta)$ の Galois 群 $\mathrm{Gal}(K/\mathbb{Q}(\zeta))$ について考察する（動機や背景については後述する）．大西 [O] は，$p = N(\beta) = 11, 31, 41, 61$ のときに，計算機を用いた計算により，$\mathrm{Gal}(K/\mathbb{Q}(\zeta)) \cong \mathfrak{S}_{6m}$ =（$6m$ 次の対称群）となることを確かめ，いつも $\mathrm{Gal}(K/\mathbb{Q}(\zeta)) \cong \mathfrak{S}_{6m}$ となるだろうと予想している（$m = (p-1)/10$ とおく．$\#G(\beta) = 60m$，$\#(G(\beta)/\mu_{10}) = 6m$ である）．筆者は [O] にある計算例を見て，$K/\mathbb{Q}(\zeta)$ における素 ideal (β), $(\sigma(\beta))$ の振る舞いが，ある程度の規則性をもっていて，そのことから $\mathrm{Gal}(K/\mathbb{Q}(\zeta)) \cong \mathfrak{S}_{6m}$ となることが従うという状況になっているのではないか，と考えた．今の所，この方針で議論を進めるためには，いくつかのことを仮定する必要がある．本質的な仮定は，次の2つである（(ii) は少し弱められる）：

(i) $\mathrm{Gal}(K/\mathbb{Q}(\zeta))$ は，集合 $\{x(P)^5\,;\ P \in G(\beta)/\mu_{10}\}$ に可移に作用する．

(ii) $J \bmod p$ の $5p$-分点で $\Theta \bmod p$ 上にあるものは，5-分点のみである（$J \bmod p$ などは，J の mod p の reduction を表わす）．

§2 の定理2は，上の2つと若干の補助的な仮定の下で，$\mathrm{Gal}(K/\mathbb{Q}(\zeta)) \cong \mathfrak{S}_{6m}$ となることを言っている．上で触れた

$K/\mathbb{Q}(\zeta)$ における素 ideal $(\mathfrak{p})$, $(\sigma(\mathfrak{p}))$ の振る舞いの規則性と関係する部分は，§2 の補題 1, 2 である．

この§のしめくくりとして，筆者が Grant の仕事に興味をもった理由を記す．第1は Gauss 和と関係したことである．(0.1) で r を奇数に制限した積は Gauss 和になる：

$$\prod_{\substack{r=1\\2\nmid r}}^{p-1} 2i\sin\frac{2\pi r}{p} = \sum_{a=1}^{p-1}\left(\frac{a}{p}\right)e^{2\pi i a/p}.$$

但し，$\left(\frac{a}{p}\right)$ は $\mathbb{Q}$ の平方剰余記号．同様に (0.2) でも，r を $S\cup e^{2\pi i/3}S\cup e^{4\pi i/3}S$ (disjoint union) が mod ω の既約剰余類の完全代表系となるような集合 $S\ (\subset \mathbb{Z}[e^{2\pi i/3}])$ に制限した積は，3次の Gauss 和を記述する (Matthews [M])：

S が $\prod_{s\in S} s \equiv -1 \pmod{\omega}$ をみたすとき，

$$-p^{1/3}\omega\prod_{s\in S}\wp\left(\frac{s\theta}{\omega}\right) = \sum_{a=1}^{p-1}\left(\frac{a}{\omega}\right)_3 e^{2\pi i a/p}.$$

但し，$\left(\frac{a}{\omega}\right)_3$ は $\mathbb{Q}(e^{2\pi i/3})$ の3乗剰余記号である．これらの式はそれ自体できれいな式であるので，(0.5) を用いて5次の Gauss 和への一般化ができれば喜ばしい．第2に，例えば，素数 p は $\mathbb{Q}(e^{2\pi i/p})$ で $(p)=\mathfrak{p}^{p-1}$ と完全分岐し，$\mathfrak{p}$ の生成元 γ をひとつとると，γ のノルムは p に一致する．(0.1) は，γ として具体的に $2i\sin\frac{2\pi r}{p}$ がとれることを表わしているとも見れる．そしてこのことから，

$$\sin\frac{2\pi t}{p} \Big/ \sin\frac{2\pi}{p}$$

たちが $\mathbb{Q}(e^{2\pi i/p})$ の単数となることがわかる．この単数は円単数と呼ばれ，周知のとおり円分体の整数論において重要な役割を果たす．(0.2) および楕円単数についても同様である．このようなことを念頭に置くと，(0.5) から円単数や楕円単数の何らかの一般化が得られないかという期待が生ずる．以上の2点については，しかしながら，今の所何の見通しもない．また (0.5) が (0.2) の一般化として本当に正統なものであるかどうかもわからない．これらの諸点についていくらかでも見通しを得るためにまず $G(p)$ の性質を調べてみようというのが，ここに記す考察の動機である．

§1. Jacobi 多様体．

Grant [G] の結果のうちで以下の議論に関係する部分をまとめておく．F を標数が 2, 5 と異なる体とし，(0.3) で定義される曲線 C を F 上で考える．[G] によれば，C の Jacobian のひとつのモデルとして，8次元の射影空間 $\mathbb{P}^8$ の中に次の多項式たちの共通零点として定義される多様体がとれる（以下この多様体を J と記すことにする．また $\mathbb{P}^8$ の同次座標を [G] の記法に倣わせて $X_0, X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X$ とかく）[注1]：

$$f_2^h = 2XX_0 - X_{11}X_{22} + X_{12}^2,$$

$$f_3^h = X_{112}X_0 - X_{222}X_{12} + X_{122}X_{22},$$
$$f_4^h = X_{111}X_0 + X_{222}X_{11} + X_{122}X_{12} - 2X_{112}X_{22},$$
$$f_5^h = X_{122}^2X_0 - X_{11}X_{22}^2 + 2XX_{22}X_0 + X_{11}X_{12}X_0 - \frac{1}{4}X_0^3,$$
$$f_6^h = X_{222}^2X_0 - X_{22}^3 - X_{12}X_{22}X_0 - X_{11}X_0^2,$$
$$f_7^h = X_{122}X_{222}X_0 - X_{12}X_{22}^2 + XX_0^2,$$
$$f_8^h = X_{111}^2X_0 - X_{11}^3 + \frac{3}{4}X_{11}X_{22}X_0 + \frac{1}{2}XX_0^2,$$
$$f_9^h = -X_{111}X_{112} + \frac{1}{4}X_{222}^2 - X^2 - \frac{1}{4}X_{12}X_{22} - \frac{1}{2}X_{11}X_0,$$
$$f_{10}^h = X_{112}^2 - X_{111}X_{122} + XX_{11} - \frac{3}{4}X_{22}^2 - \frac{1}{4}X_{12}X_0,$$
$$f_{11}^h = X_{111}X_{222} - X_{112}X_{122} - 2XX_{12} + X_{11}^2 - \frac{1}{4}X_{22}X_0,$$
$$f_{12}^h = X_{122}^2 - X_{112}X_{222} + X_{22}X + 2X_{11}X_{12} - \frac{1}{4}X_0^2,$$
$$f_{13}^h = X_{111}X_{12} - X_{112}X_{11} + \frac{1}{2}X_{222}X_0,$$
$$f_{14}^h = 2X_{122}X_{11} - X_{112}X_{12} - X_{111}X_{22}.$$

記法 f_i^h は，f_i^h で $X_0=1$ としたもの f_i が先にあって，それを X_0 について同次化したものが f_i^h であるという事情に依る．Jacobian の定義により，J の点は $\mathrm{Div}^0(C)=\{C$ 上の次数 0 の因子$\}$ を線型同値 $\sim$ で割った群 $\mathrm{Div}^0(C)/\sim$ の元と 1 対 1 に対応し，さらに $\mathrm{Div}^0(C)/\sim$ の加法はいたる所正則な有理写像 $J\times J\to J$ をひきおこさなければならない．ここでは，この対応を次のように与える（これからひき起される J の加法は，[G] に具体的に記されている）．いま，C の自己同型 $(x,y)\mapsto(x,-y)$ を τ とかくと，$\mathrm{Div}^0(C)/\sim$ の完全代表系として次のような因

子の全体がとれる：

(1.1) $$P_1 + P_2 - 2\infty \quad (P_1 \neq \infty,\ P_2 \neq \infty,\ P_1 \neq \iota P_2),$$

(1.2) $$P - \infty \quad (P \in C).$$

そこで，(1.2) で代表される $\mathrm{Div}^0(C)/\sim$ の元には，$P = \infty$ なら

$$O = (0, 0, 0, 0, 1, 0, 0, 0, 0) \in J$$

を，$P = (x, y) \neq \infty$ なら，

(1.3) $$(0, 0, 0, 0, -x^3, x^2, -x, 1, -y) \in J$$

を対応させる．また，(1.1) には次のような J の点を対応させる（$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$）：

$$\Big(1,\ \frac{(x_1+x_2)(x_1x_2)^2 + \frac{1}{2} - 2y_1y_2}{(x_1-x_2)^2},\ -x_1x_2,\ x_1+x_2,$$
$$\frac{y_2\psi(x_1,x_2) - y_1\psi(x_2,x_1)}{(x_1-x_2)^3},\ \frac{y_1x_2^2 - y_2x_1^2}{x_1-x_2},\ \frac{y_2x_1 - y_1x_2}{x_1-x_2},$$
$$\frac{y_1-y_2}{x_1-x_2},\ \frac{(x_1x_2)^3 + \frac{1}{4}(x_1+x_2) - y_1y_2(x_1+x_2)}{(x_1-x_2)^2}\Big).$$

但し，

$$\psi(x_1, x_2) = 1 + x_1^3 x_2 (3x_1 + x_2).$$

1 の原始10乗根 $-\zeta$ の J への作用（$(-\zeta)\cdot(x, y) = (\zeta x, -y)$ なる C への作用からひきおこされるもの）は，

(1.4) $$(-\zeta)\cdot(X_0, X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X)$$
$$= (X_0, \zeta^3 X_{11}, \zeta^2 X_{12}, \zeta X_{22}, -\zeta^2 X_{111}, -\zeta X_{112}, -X_{122}, -\zeta^4 X_{222}, \zeta^4 X)$$

となる．

ここで，定理1（p.2）に若干の注釈を加えておく．上で$F=\mathbb{Q}$とした状況で考える．ΘはJの原点Oと(1.3)のような点の全体の合併となる．また$(X)_0$は，J上$X=0$で定義される曲線で，よって，

$$G(\beta)=\{P\in\Theta;\ X(\beta\sigma^{-1}(\beta)P)=0,\ 2P\neq O\}$$

となる．(1.4)からわかるように$G(\beta)$は$\mu_{10}=\langle-\zeta\rangle$の作用で閉じている．さらに，$G(\beta)$については，次のことがわかっている（$P\in G(\beta)$とする）：

(1.5)　$\#G(\beta)=6(p-1)=60m$　$\left(p=N(\beta),\ m=\frac{p-1}{10}\right)$，

(1.6)　PはJの等分点ではない，

(1.7)　$x(P)\in\overline{\mathbb{Q}}=$（$\mathbb{Q}$の代数的閉包）で，$x(P)$は$2\beta\sigma(\beta)$の外でintegral，$x(P)^{-1}$は$10$の外でintegralである．

§2. Galois群．

βと$K=K_\beta$，$L=L_\beta$を§0と同様なものとする．

$$\Phi(T)=\Phi(\beta;T)=\prod_{P\in G(\beta)/\mu_{10}}\left(T-\frac{1}{x(P)^5}\right)$$

とおく．$\Phi(T)\in\mathbb{Q}(\zeta)[T]$で，$K$は$\Phi(T)$の$\mathbb{Q}(\zeta)$上の最小分解体である．また，(1.5)と(0.5)（の精密化）から，

$$\deg\Phi(T)=6m,\qquad \Phi(0)=\beta\sigma(\beta)$$

となる．さらに，cも後で説明する（§4, (4.3)）有理数とする．これはβによらない数である．

<u>定理2</u>　次の仮定の下で，$K/\mathbb{Q}(\zeta)$ の Galois群 $\mathrm{Gal}(K/\mathbb{Q}(\zeta))$ は，$6m$ 次の対称群 $\mathfrak{S}_{6m}$ と同型である．

(i)　$\Phi(T)$ は $\mathbb{Q}(\zeta)$ 上既約である．

(ii)　L の $\sigma(\beta)$ 上のある素 ideal $\mathfrak{Q}$ があって，

$$P \in G(\beta) \Rightarrow (1-\zeta)\beta\sigma^{-1}(\beta)P \bmod \mathfrak{Q} \neq 0.$$

(iii)　$\mathbb{Q}(\zeta)$ のある単数 η があって，$\eta\beta \equiv 1 \pmod{10}$.

(iv)　$\left(\frac{2}{\beta}\right)_5 = 1$.　　(v)　$c \not\equiv 0 \pmod{p\mathbb{Z}_p}$.

但し，(ii) の '$\bmod \mathfrak{Q}$' は $\bmod \mathfrak{Q}$ の reduction を表わし，(iv)の左辺は $\mathbb{Q}(\zeta)$ の 5乗剰余記号を表わす．

上の (ii) の 2行目は

$$P \in G(\beta) \Rightarrow \beta\sigma^{-1}(\beta)P \bmod \mathfrak{Q} \notin \{0, (1,0,0,0,0,0,\pm\tfrac{1}{2},0,0)\}$$

でおきかえてもよい．(ここに現れる3点から成る集合は J と $X=0$, $X_{222}=0$ の交わりである)．また，(i)については次のことが後出の補題1からわかる：

$\Phi(T)$ が $\mathbb{Q}(\zeta)$ 上既約でなければ，$\Phi(T)$ は $\mathbb{Q}(\zeta)$ 上で m 次の既約多項式と $5m$ 次の既約多項式の積に分解する．

定理2の証明の概略は次のとおりである．

<u>補題1.</u>　定理2の (iii), (iv) を仮定する．このとき，$\Phi(T)$ は，$\mathbb{Q}(\zeta)$ の (β) での完備化 $\mathbb{Q}(\zeta)_\beta$ 上で m 次の既約多項式 $\Phi_0(T)$

と $5m$ 次の既約多項式 $\Phi_1(T)$ の積に分解する．さらに，$\Phi_0(T)$, $\Phi_1(T)$ の $\mathbb{Q}(\zeta)_\beta$ 上の最小分解体たちは，$\mathbb{Q}(\zeta)_\beta$ 上それぞれ m 次，$5m$ 次の完全分岐巡回拡大である．

<u>補題 2</u>．定理 2 の (ii), (v) を仮定する．また $p \geq 31$ とする．このとき，$\Phi(T)$ は，$\mathbb{Q}(\zeta)$ の $(\sigma(\beta))$ での完備化 $\mathbb{Q}(\zeta)_{\sigma(\beta)}$ 上で次をみたす 2 つの多項式 $\varphi(T)$, $\psi(T)$ の積に分解する：

- $\deg \varphi(T) = 2$ で，$\varphi(T)$ の $\mathbb{Q}(\zeta)_{\sigma(\beta)}$ 上の最小分解体は $\mathbb{Q}(\zeta)_{\sigma(\beta)}$ の 2 次の分岐拡大体である，
- $\psi(T) \bmod \sigma(\beta)$ $(\in \mathbb{F}_p[T])$ は分離多項式で，したがって $\psi(T)$ の $\mathbb{Q}(\zeta)_{\sigma(\beta)}$ 上の最小分解体は不分岐拡大体である．

上で $\varphi(T)$ は $\mathbb{Q}(\zeta)_{\sigma(\beta)}$ 上既約であるが，$\psi(T)$ は既約とは限らない．補題 1, 2 の証明については次節以降で説明する．ここでは，上の 2 つの補題から定理 2 がどのようにして導かれるかを説明する．定理 2 の (i) ～ (v) を仮定する．いま $\Phi(T)$ の根全体の集合を，適当に

$$R = \{1, 2, \cdots, 6m\}$$

と同一視して

$$\Phi_0(T) \text{ の根と } R_0 = \{1, 2, \cdots, m\},$$

$$\Phi_1(T) \text{ の根と } R_1 = \{m+1, m+2, \cdots, 6m\}$$

が対応するようにする．そして，$G = \mathrm{Gal}(K/\mathbb{Q}(\zeta))$ を R 上の対称群 $\mathfrak{S}_{6m}$ の部分群と見なす．まず K の (β) 上の素 ideal $\mathfrak{p}$ をひとつとり，$Z(\subset G)$ を $\mathfrak{p}$ の分解群とすると，自然に

$$Z = \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}(\zeta)_{\beta})$$

と同一視できて，$K_{\mathfrak{p}}$ は $\Phi(T)$ の $\mathbb{Q}(\zeta)_{\beta}$ 上の最小分解体である．よって，補題1から，次がわかる：

(2.1) $\qquad \sigma(R_i) = R_i \qquad (\sigma \in Z,\ i = 1, 2)$,

(2.2) ある $\sigma_0, \sigma_1 \in Z$ があって，$\sigma_0|R_0$ は長さ m の巡回置換で，$\sigma_1|R_1$ は長さ $5m$ の巡回置換となる．

次に，K の $(\alpha(\beta))$ 上の素 ideal $\mathfrak{q}$ をひとつとり，その分解群，惰性群をそれぞれ $Z', T'(\subset G)$ とする．すると，補題2から $\#T' = 2$ で，$T' = \langle\tau\rangle$ とすると，τ は $\psi(T)$ の根を不変にして $\varphi(T)$ の2つの根を入れかえるという互換をひきおこす．定理2は，上のことと次の群論の補題（証明は略す）から直ちに導かれる．

<u>補題3</u>．$R, R_0, R_1, \mathfrak{S}_{6m}$ は上のとおりとし，G を $\mathfrak{S}_{6m}$ の部分群とする．このとき，次の(i)～(iii)が成り立てば，$G = \mathfrak{S}_{6m}$ である：

(i) G は R に可移に作用する．

(ii) G の部分群 Z があって，上の(2.1)，(2.2)が成り立つ．

(iii) G は互換を少なくともひとつ含む．

§3. (β) での局所的考察（補題1の証明の概略）

$\mathbb{C}_p$ で $\mathbb{Q}_p$ の代数的閉包の完備化を表わし，$\mathfrak{m}$ を $\mathbb{C}_p$ の付値 ideal とする．また $\overline{\mathbb{Q}}$ の $\mathbb{C}_p$ への埋め込みで，$(\beta)\subset\mathfrak{m}$ となるものがひとつ固定されているとする．'〜' で mod $\mathfrak{m}$ の reduction を表わす．虚数乗法論の定理により，J の準同型 $\beta\sigma^{-1}(\beta)$ を mod $\mathfrak{m}$ で見たものは，$\tilde{J}$ の p 乗準同型となる．このことと，§1の状況（$ch(F)\neq 2,5$ なる F の上の一般論）で，

$$J\cap(X_0)_0\cap(X)_0 = \Theta\cap J[2]$$

となることから（ここで，$(X_0)_0$ は $X_0=0$ で定義される超平面，$\Theta=J\cap(X_0)_0$，また $J[2]$ は J の2分点の全体），

$$P\in G(\beta)\Rightarrow \tilde{P}\in\tilde{\Theta}\cap\tilde{J}[2]$$

がわかる．いま，$\gamma^5+\frac{1}{\gamma}=0$ なる γ をひとつとり，(1,3) で $y=0$，$x=\gamma$ とした点を W とすると，

$$\Theta\cap J[2]=\{O,\ \zeta^i\cdot W\ (i=0,1,\cdots,4)\}$$

である．そこで，

$$\Phi_0(T)=\prod_{\substack{P\in G(\beta)/\mu_{10}\\ \tilde{P}=\tilde{O}}}\left(T-\frac{1}{x(P)^5}\right),\quad \Phi_1(T)=\prod_{\substack{P\in G(\beta)/\pm1\\ \tilde{P}=\tilde{W}}}\left(T-\frac{1}{x(P)^5}\right)$$

とおくと，$\Phi(T)=\Phi_0(T)\Phi_1(T)$ となる．この Φ_0，Φ_1 が補題1の条件をみたすことを次に見る．Φ_0 については省略し，Φ_1 についてだけ考える．

J の定義方程式 $f_2^h\sim f_{14}^h$ から，

$$t_1=-\frac{X_{11}}{X_{111}},\quad t_2=-\frac{X}{X_{111}}$$

は W での local parameter を与えることがわかる（これも，標数 $\neq 2,5$ なら一般の体上で成り立つ）．よって，W で正則な J 上の有理関数は t_1, t_2 の巾級数に展開されるが，若干の考察により，展開係数について，

$$\frac{X_0}{X_{111}},\ \frac{X_{ij}}{X_{111}},\ \frac{X_{ijk}}{X_{111}},\ t_2(\beta\sigma^{-1}(\beta)u) \in \mathbb{Z}[\zeta, \gamma, \tfrac{1}{10}][[t_1, t_2]] \quad (i, j, k = 1, 2) \tag{3.0}$$

となることがわかる（上の u は J 上の点を一般的に表わしている）．さらに，$t_2(\beta\sigma^{-1}(\beta)u)$ を t_1, t_2 について展開して得られる巾級数を $f(t_1, t_2)$ とすると，

$$f(t_1, t_2) \equiv t_2^p \pmod{\mathfrak{m}}, \tag{3.1}$$

$$f(0, t_2) \equiv \frac{1}{5}(3\sigma^{-1}(\beta) + 2\sigma(\beta))\beta\, t_2 \pmod{\deg 2}, \tag{3.2}$$

(3.3) $f(0, t_2)$ は t_2 の奇数巾の項のみから成る

が成り立つ（(3.2) 以外は容易にわかる）．ここで定理2の仮定 (iii) から

$$3\sigma^{-1}(\beta) + 2\sigma(\beta) \not\equiv 0 \pmod{\beta}$$

が従う（証明略）ことを用いる．すると，定理2の仮定 (iv) より $\mathbb{Q}(\zeta, \gamma)$ の $\mathbb{C}_p$ での閉包は $\mathbb{Q}_p$ に一致し，(3.2) の左辺の t_2 の係数は $\mathbb{Q}_p$ の素元を与えるから，一般論（例えば，Lubin-Tate [LT]）により次がわかる：

$f(0, t_2) = 0$ なる $t_2 \in \mathfrak{m}$ が丁度 p 個存在し，それらを $\lambda_0 = 0, \lambda_1, \cdots, \lambda_{p-1}$ とすると $\mathbb{Q}_p(\lambda_1, \cdots, \lambda_{p-1}) = \mathbb{Q}_p(\lambda_1)$

でこの体は $\mathbb{Q}_p$ の $p-1$ 次完全分岐巡回拡大体である．そこで，先の展開 (3.0) に $(t_1, t_2) = (0, \lambda_j)$ $(1 \leq j \leq p-1)$ を代入すると J の点 P_j ができる．作り方から，

$$X_{111}(P_j) \neq 0, \quad t_1(P_j) = 0, \quad t_2(\beta\sigma^{-1}(\beta)P_j) = f(0, \lambda_j) = 0,$$

よって

$$X_0(P_j) = 0, \quad X(\beta\sigma^{-1}(\beta)P_j) = 0.$$

（前者は，(3.0) の X_0/X_{111} の展開が t_1 で割り切れること（$f_0^h = 0$ から従う）から出る）．したがって，$P_j \in G(\beta)$ $(1 \leq j \leq p-1)$ となり，$\mathbb{Q}_p$ 上 P_j の座標（の商）たちで生成される体は $\mathbb{Q}_p(\lambda_1)$ に一致する．このことにいくらかの考察を付け加えて，

$$\{P \in G(\beta);\ \tilde{P} = \tilde{W}\} = \{P_1, \cdots, P_{p-1}\},$$

$$\mathbb{Q}_p(x(P_j)^5) = \mathbb{Q}_p(\lambda_1^2) \qquad (1 \leq j \leq p-1),$$

$$\Phi_1(T) \in \mathbb{Q}_p[T]$$

となることを確めれば，補題1の証明の Φ_1 に関する部分が完成する（これらについては略す）．

§4. $(\sigma(\beta))$ での局所的考察（補題2の証明の概略）．

$p \geq 31$ とする．定理2の (ii), (v) を仮定し，の Q について $Q \subset \mathfrak{m}$ となるように $\overline{\mathbb{Q}}$ を $\mathbb{C}_p$ に埋め込んで考える（$\mathbb{C}_p$, $\mathfrak{m}$ は前節と同じ）．補題2は次の事実の簡単な系である．

(4.1) mod $\mathfrak{m}$ の reduction map $G(\beta) \ni P \mapsto \tilde{P} \in J$ におい

て，$\tilde{J}$ の原点 $\tilde{O}$ に写るものは 20 個で，これを除けば
この reduction map は 1対1 である．

以下 (4.1) について考える．[G] により，$\mathbb{Z}[\frac{1}{2}]$ 上定義された 2 変数可換形式群 $F(x,y)$ $(x=(x_1,x_2),\ y=(y_1,y_2))$ が存在して，J_0 を $\tilde{P}=\tilde{O}$ となる J の $\mathbb{C}_p$-rational point 全体のなす群とし，

$$\phi : J_0 \longrightarrow \mathfrak{m}^2$$

を $\phi(P)=(t_1(P),t_2(P))$ で定めるとき，ϕ は全単射で，

$$\phi(P+Q)=F(\phi(P),\phi(Q)) \qquad (P,Q\in J_0)$$

が成り立つ（t_1,t_2 は §3 と同じ．これらは O でも J の local parameter を与える）．また，J が $\mathbb{Z}[\zeta]$ による虚数乗法をもつことから，各 $\alpha\in\mathbb{Z}[\zeta]$ に対して，巾級数

$$[\alpha](x)=([\alpha]_1(x_1,x_2),[\alpha]_2(x_1,x_2))\in\left(\mathbb{Z}[\tfrac{1}{2},\zeta][[x_1,x_2]]\right)^2$$

が存在して

$$[\alpha](F(x,y))=F([\alpha](x),[\alpha](y)),$$

$$\phi(\alpha P)=[\alpha](\phi(P)), \qquad P\in J_0$$

が成り立つ．さらに，$f(x)=(f_1(x),f_2(x))\in\mathbb{Q}[[x]]^2$ を

$$f(x)\equiv x \quad (\mathrm{mod}\ \deg 2),$$

$$F(x,y)=f^{-1}(f(x)+f(y))$$

なる条件で一意的に決まるもの（Honda [H] で transformer と呼ばれているもの）とすると，

$$[\alpha](x)=f^{-1}(\alpha f_1(x),\sigma(\alpha)f_2(x)), \qquad \alpha\in\mathbb{Z}[\zeta]$$

となる．これと $f(x)$ の(p-1)次までの係数が p-integral である（cf. [H], Th.1, Prop.1.1）ことから，$g(x)=(g_1(x), g_2(x))=f^{-1}(x)$ とおくとき，

(4.2) $$[\alpha]_2(0,X) = g_2(\alpha f_1(0,X),\ \sigma(\alpha) f_2(0,X))$$
$$\equiv g_2(\alpha f_1(0,X),\ 0) \quad \mathrm{mod}\ (\deg p, \mathfrak{m})$$
$$(\alpha := \beta\sigma^{-1}(\beta))$$

となる．ここで，次を用いる（証明略）：

(4.3) ある $c \in \mathbb{Z}[\frac{1}{2\cdot 3\cdot 7}]$, $c \not\equiv 0$ があって，
$$g_2(f_1(0,X), 0) \equiv c X^{21} \quad \mathrm{mod}\ \deg 22.$$

仮定により $c \not\equiv 0 \pmod{\mathfrak{m}}$，よって，ある $\mathbb{C}_p$ の単数 c' について，

(4.4) $$[\beta\sigma^{-1}(\beta)]_2(0,X) \equiv c' X^{21} \quad \mathrm{mod}\ (\deg 22, \mathfrak{m})$$

となる．

さて，$P \in J_0$ について，

$$\begin{aligned} & P \in G(\beta) \\ \Longleftrightarrow\ & t_1(P) = t_2(\beta\sigma^{-1}(\beta)P) = 0, \quad t_2(P) \not\equiv 0 \\ \Longleftrightarrow\ & t_1(P) = [\beta\sigma^{-1}(\beta)]_2(0, t_2(P)) = 0, \quad t_2(P) \not\equiv 0 \end{aligned}$$

となり，結局

$$\#(G(\beta) \cap J_0) = \#\{\lambda \in \mathfrak{m}\ ;\ [\beta\sigma^{-1}(\beta)]_2(0,\lambda) = 0,\ \lambda \not\equiv 0\}$$

であるが，(4.4) からこれは 20 に等しい．これで (4.1) の前半が示された．

(4.1) の後半については，ポイントを記すに止める．$P \in G(\beta) - J_0$ とする．$\lambda_1 = -\frac{X_{11}}{X_{222}}$，$\lambda_2 = -\frac{X}{X_{222}}$，$\lambda_2' = \lambda_2 - \lambda_2(P)$ と

おくと，s_1, s_2' は P での local parameter を与え，s_1, s_2' による $X_0/X_{222}, \cdots, X/X_{222}$，$(X/X_{222})(\beta\sigma^{-1}(\beta)u)$ の展開の係数はすべて $\mathbb{C}_p$ の整数となる．そこで，

$$(X/X_{222})(\beta\sigma^{-1}(\beta)u) = \sum_{i+j>0} \alpha_{ij} s_1^i s_2'^j$$

とおく．(4.1) の後半についてのポイントは，我々の仮定の下で，

$$\alpha_{01} \not\equiv 0 \pmod{\mathfrak{m}}$$

となることである．

注1) (p.5) 標数 0 で考えるとき，J の $\mathbb{C}$-有理点の全体は，よく知られているように2次元トーラス $\mathbb{C}^2/L$ と同型である．この同型は，適当に L と L に関するテータ関数 $\theta(z)$ をとれば，$\log\theta(z)$ の2階・3階の偏導関数を用いて記述される．$f_2^h \sim f_{14}^h$ はこの偏導関数たちの満たす関係式を考えることから出てきたものである (cf. [G], [O])．

文献

[G] D. Grant, Crelle J., 411 (1990).

[G2] ———, Proc. London Math. Soc. (3), 62 (1991).

[H] T. Honda, J. Math. Soc. Japan, 22 (1970).

[LT] J. Lubin and J. Tate, Ann. Math., 81 (1965).

[M] C.R. Matthews, Invent. Math., 52 (1979).

[O] 大西良博，数理研講究録 759 (1991).