数理解析研究所講究録
第 572 巻 1985 年 84-108

Dedekind和の除外値について

静岡大 浅井哲也 (Tetsuya Asai)
京都大 齋藤 裕 (Hiroshi Saito)
九州大 長坂千秋 (Chiaki Nagasaka)

この稿は講演に従って つぎのように分担して述べる.

§1. 問題と歴史 (A.)

§2. 定理の証明 (S.)

§3. 新たな観察 (N.)

(ただし長坂氏はこの締切を前にして急逝されたので十分な原稿が用意できなかったこと また各節の間の統一性が不完全であることを予めお断りしたい. これらの責任はA.にある.)

文献

[1] T. Asai, Some arithmetic on Dedekind sums, to appear.

[2] T. Asai, The multiplier system of eta function and traces of unimodular matrices, to appear.

[3] H. Hijikata, Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$, J.Math.Soc.Japan, 26(1974), 56-82.

[4] Ch. Nagasaka, Exceptional values of the Dedekind symbol, to appear.

[5] H. Rademacher, "Topics of Analytic Number Theory", Springer, 1973.

[6] H. Saito, On missing trace values for the eta multipliers, to appear.

[7] H. Salié, Zum Wertvorrat der Dedekindschen Summen, Math.Z., 72(1959), 61-75.

[8] D. Zagier, Nombres de classes et fractions continues, Astérisque, 24/25(1975), 81-97.

§1. 問題と歴史

この節では問題の由来と最近の経過について解説する.

eta関数とその変換公式については周知である.([5])

$$\eta(z) = e^{\frac{\pi i z}{12}}\prod_{n=1}^{\infty}(1 - e^{2\pi i n z}), \quad \mathrm{Im}\, z > 0.$$

$$\eta(\sigma z) = \varepsilon(\sigma)(cz+d)^{\frac{1}{2}}\eta(z), \quad \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

ここで平方根を $w^{\frac{1}{2}} = \sqrt{|w|}\, e^{\frac{1}{2} i \arg w}$, $-\pi \leq \arg w < \pi$ と決めておけば $\varepsilon(\sigma)$ は z によらない値として確定する. これを eta multiplier と呼ぶ. $\varepsilon(\sigma)^{24} = 1$ である. われわれの問題をもし一言で云うならば

『$\varepsilon(\sigma)$ と $tr(\sigma)$ との関係や如何?』

ということになる. $tr(\sigma)$ は行列 σ の跡である. しかし問題はこのように一直線に進行したのではない.

Dedekind は $\eta(z)$ の対数関数とその変換公式を扱った.

$$L(z) = \frac{\pi i z}{12} - \sum_{m,n=1}^{\infty} \frac{1}{m} e^{2\pi i m n z}$$

$$L(\sigma z) = L(z) + \frac{1}{2}\log(cz+d) + \frac{\pi i}{12} V(\sigma).$$

彼は加法的因子 $V(\sigma)$ を新しい算術的和によって表した. ここでも $\log w = \log|w| + i \arg w$, $-\pi \leq \arg w < \pi$ のように対数の枝を定めておく必要がある. このとき $V(\sigma)$ は有理整数値をとる定数であって明らかに $\varepsilon(\sigma) = e^{\frac{\pi i}{12}V(\sigma)}$.

($\varepsilon(\sigma)$ や $V(\sigma)$ は本質的には $SL_2(\mathbb{Z})$ の適当な被覆群のアーベル指標として捉えられるものであり必ずしも解析関数を持ち出す必要はない. またこれらの因子がそのまま他の数論的な量との関連ではっきりと登場することもある. ― Hardy-Ramanujan-Rademacher の公式([5]) や C. Meyer の公式([8]に簡潔な記述がある)などである.)

Dedekind の与えた公式は, ($\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$)

$$V(\sigma) = \begin{cases} \dfrac{a+d}{c} - 3\,\mathrm{sgn}\,c - 12\,\mathrm{sgn}\,c \cdot s(d,|c|) & \cdots\ c \neq 0, \\ (b-3)\,\mathrm{sgn}\,d + 3 & \cdots\ c = 0, \end{cases}$$

というものである. ここに現われた $s(d,|c|)$ がいわゆる Dedekind 和である. これの定義と性質については他の稿で触れられることと思われるのでここでは詳細をのべない. 最も基本的な性質はつぎのように要約することができる.

互いに素な有理整数の組 h, k $(k>0)$ について

$$D(h, k) = 12k \cdot s(h, k),$$

および便利のために $D(\pm 1, 0) = \pm 2$ とおく.（今は $k<0$ については $D(h, k)$ を定義しない.）これを D-関数と呼ぶ.

このときつぎの性質 ①（相互法則）, ② が成立つ.

① $hD(h, k) + kD(k, h) = h^2 + k^2 - 3hk + 1$,

② $D(h', k) = D(h, k)$ ⋯ $h' \equiv h \pmod{k}$ のとき.

逆にこの2つの性質が D-関数を完全に特徴づける. さらに,

③ $D(\dot{h}, k) = D(h, k)$ ⋯ $\dot{h}h \equiv 1 \pmod{k}$ のとき.

④ $D(-h, k) = -D(h, k)$.

D-関数の値と値域を注意深く観察したのは Salié が最初であろう. 性質 ④ によって正値のみを対象としてよい.

0 2 6 12 16 18 20 $\square$ 30 $\square$ 36 38 42 48 52 54

2 4 6 4 2 2 4 6 4 2 2 4 6 4 2

56 60 66 70 72 74 78 84 $\square$ 90 92 96 102 106 ⋯

2 4 6 4 2 2 4 6 4 2 2 4 6 4 ⋯

階差から明らかなつぎの合同式は証明も容易である.

$$D(h, k) \equiv 0, 2, 6, 12 \text{ or } 16 \pmod{18}.$$

Salié の注目したのはところどころに抜けた値, すなわち, この合同式は満たすが D-関数の値とはならぬ数である.

このような値をいま除外値(exceptional or missing value)と呼ぶ．Saliéは300以下の除外値として証明なしでつぎの4個の数を挙げている．(1959)

$$24,\ 34,\ 88,\ 214.$$

除外値を確定するために筆者はつぎの基準(1982)を示した．

「合同式($s \equiv 0, \pm 2, \pm 6 \pmod{18}$)を満たすような $s\,(>2)$ に対して すべての $1 < t < s$ ($1 \leq t < k/2$)について $D(t, k) \neq s$ ならば この s は除外値である」

(その後改良されて $s > 52$ ならば $k < s/2$ について調べれば十分であることがわかっている．(1984)) これは，相互法則①を用いたひとつの"descent"の考え方に基くものである．この基準によってSaliéの観察を確認するとともに数個の除外値を追加したが依然として正体不明であった．

$$304,\ 344,\ 394,\ 1060.$$

(ここまでについては [7] と [1] を参照されたい．)

さて除外値の計算はその後も少しづつ進んでいたが，1984年の夏までに長坂氏は大型計算機を用いて k 変数を76000まで，従って合わせて877848679個の $D(t, k)$ の値を計算されて，上記8個に加えて

つぎの数を除外値として確定した.(カッコ内は新基準後に.)

1924, 2050, 3364, 4804, 9250, 17674, 21220, 25090, 25540, 49930, 55780, 67714, 74500, 75274, (113290, 114244, 123010, 131074, 150154.)

同時に長坂氏は鋭い観察によってつぎの発見をされた!

(長坂氏の予想, 1984) つぎの形の s は除外値である: $s=2(n^2+1)$ ただし $n\equiv\pm4 \pmod 9$ かつ n の任意の素因子 p は $p=2$ または $p\equiv\pm1 \pmod 8$ を満たす. そして $s>344$ なる除外値はこれらで尽きる.

このうち $n\equiv\pm4 \pmod 9$ の条件は先の合同式に基くものであるが s の特異な形と素因子に関する条件が興味を惹きつける.

この年の終る頃筆者は D-関数を拡張してみるのが自然であると感じた. いま各整数 $l\in\mathbb{Z}$ に対して形式的に

$$D_l(h,k)=(l+3)k+D(h,k)$$

と定義する. 基本性質によってこれをのべればつぎの通り.

① $hD_l(h,k)+kD_l(k,h)=h^2+k^2+(2l+3)hk+1$,

② $D_l(h',k)=D_l(h,k)$ $\cdots$ $h'\equiv h \pmod k$ のとき,

③ $D_l(\dot{h},k)=D_l(h,k)$ $\cdots$ $\dot{h}h\equiv 1 \pmod k$ のとき,

④ $D_\ell(-h, k) = -D_{-(\ell+6)}(h, k)$.

この一般化の根拠は先述の $V(\sigma)$ に関する Dedekind の公式から直ちに導くことのできるつぎの公式にある.

(跡公式, Dedekind)

$\sigma = \begin{pmatrix} h & H \\ k & K \end{pmatrix} \in SL_2(\mathbb{Z})$ について $V(\sigma) = \ell$ のとき

$$tr(\sigma) = \begin{cases} D_\ell(h, k) & \cdots \quad k \geqq 0, \\ D_{-\ell}(h, |k|) & \cdots \quad k < 0. \end{cases}$$

すなわち D-関数の値域とは $V(\sigma) = -3$ (および 3) となる σ についての trace values に他ならない. ± 3 にとどまらず各 ℓ について観察する必要がこうして生じた. D_ℓ-関数の除外値の概念を得るためには, D-関数についての基本合同式: $D(h, k) \equiv 0, \pm 2$ or $\pm 6 \pmod{18}$ に相当するものを知る必要がある. つぎの補題から D_ℓ-関数の基本合同式は容易に得られるのである.

(D-関数の合同式(詳形)) $D = D(h, k)$ と略記する.

$k \equiv \pm 1 \pmod 3 \Rightarrow D \equiv 0 \pmod 3$, $k \equiv 0 \pmod 3 \Rightarrow D \equiv \pm 2 \pmod 9$,

$k \equiv 1 \pmod 4 \Rightarrow D \equiv 0 \pmod 4$, $k \equiv -1 \pmod 4 \Rightarrow D \equiv 2 \pmod 4$,

$k \equiv 2 \pmod 8 \Rightarrow D \equiv 0 \pmod 8$, $k \equiv -2 \pmod 8 \Rightarrow D \equiv 4 \pmod 8$,

$k \equiv 0, -4 \pmod{16} \Rightarrow D \equiv \pm 2 \pmod{16}$, $k \equiv 4, 8 \pmod{16} \Rightarrow D \equiv \pm 6 \pmod{16}$.

この補題自身の証明は相互法則を用いて例えば帰納法でできる.

ところで、結果からいうと各 D_ℓ-関数の規則的な除外値は $\ell \pmod{24}$ によって共通であることが観察されるのである。このことは $\varepsilon(\sigma) = \zeta^{V(\sigma)}$ (以下 $\zeta = e^{\frac{\pi i}{12}}$) に注意するならば各 $\ell \pmod{24}$ について $\varepsilon(\sigma) = \zeta^\ell$ となる σ についての $tr(\sigma)$ の除外値ともいうべき概念が一層自然であることを意味する。これによって、D_ℓ-関数の基本合同式を述べる代わりにつぎの形でこれを表しておく。

(<u>$tr(\sigma)$ の基本合同式</u>) $\varepsilon(\sigma) = \zeta^\ell$ $(\sigma \in SL_2(\mathbb{Z}))$ のとき:

- $\ell \equiv \pm 1 \pmod 6 \Rightarrow tr(\sigma) \equiv \pm 1 \pmod 3$ かつ, $\equiv 0 \pmod 2$,
- $\ell \equiv 3 \pmod 6 \Rightarrow tr(\sigma) \equiv 0, \pm 2, \pm 3 \pmod 9$ かつ, $\equiv 0 \pmod 2$,
- $\ell \equiv \pm 2 \pmod{12} \Rightarrow tr(\sigma) \equiv \pm 1 \pmod 3$ かつ, $\equiv 1, 2, 5, 9, 10, 13, 14 \pmod{16}$,
- $\ell \equiv \pm 4 \pmod{12} \Rightarrow tr(\sigma) \equiv \pm 1 \pmod 3$ かつ, $\equiv 2, 3, 6, 7, 11, 14, 15 \pmod{16}$,
- $\ell \equiv 6 \pmod{12} \Rightarrow tr(\sigma) \equiv 0, \pm 2, \pm 3 \pmod 9$ かつ $\equiv 1, 2, 5, 9, 10, 13, 14 \pmod{16}$,
- $\ell \equiv 0 \pmod{12} \Rightarrow tr(\sigma) \equiv 0, \pm 2, \pm 3 \pmod 9$ かつ $\equiv 2, 3, 6, 7, 11, 14, 15 \pmod{16}$.

上の合同式で $tr(\sigma)$ を s で置き換えたものを "$\varepsilon(\sigma) = \zeta^\ell$ に対応する基本合同式" と呼ぼう。例えば $\varepsilon(\sigma) = \zeta^3$ に対応する基本合同式とは、$s \equiv 0, \pm 2, \pm 3 \pmod 9$ かつ $\equiv 0 \pmod 2$, すなわち $s \equiv 0, \pm 2$ or $\pm 6 \pmod{18}$ を意味する。$tr(\sigma)$ の除外値という概念を定義しよう。

$s>2$ とする.(この場合が本質的である.) s が $\varepsilon(\sigma)=\zeta^l$ に関する <u>$tr(\sigma)$ の除外値</u> (missing trace value) とは, 第一に s が対応する基本合同式を満たし, かつ第二に, $\varepsilon(\sigma)=\zeta^l$, $tr(\sigma)=s$ となる $\sigma\in SL_2(\mathbb{Z})$ が存在しない, ときをいう. 注意すべきことは, $s(>2)$ が $\varepsilon(\sigma)=\zeta^{l_0}$ に関する $tr(\sigma)$ の除外値であることは, すべての $l\equiv l_0 \pmod{24}$ について s が D_l-関数の除外値であることと同義であるということである. 例えば $D(=D_{-3})$-関数の除外値であっても D_{21}-関数の値であれば, それは $\varepsilon(\sigma)=\zeta^{-3}$ に関する $tr(\sigma)$ の除外値ではない. [こうして結果としては不規則な除外値(この場合は 24, 88, 214, 304, 344)が一掃される!]

S_l で $\varepsilon(\sigma)=\zeta^l$ に関する missing trace value 全体の集合を表そう. $tr(\sigma)>2$ のとき $\varepsilon(\sigma^{-1})=\varepsilon(\sigma)^{-1}$ が成立つことから $S_l=S_{-l}$. 従って 13 個の集合 $S_0, S_1, \cdots, S_{12}$ が問題となる.

与えられた $s(>2)$ が S_l に属するか否かは先述の基準によって有限回の計算により判定が可能であるので S_l の観察を試ることができる. 結果を述べるために幾つかの特別な数列を定義せねばならない. 以下に $A\sim O$ の集合を定義するが, 読み方はつぎのようである. 例えば C は, 2つの条件: $n\equiv\pm4 \pmod 9$ と素因子に関する条件: $p=2$ または $\left(\frac{2}{p}\right)=1$ すなわち $p\equiv\pm1 \pmod 8$ を満たすような n によって $2n^2+2$ と表わされる数(>2)の全体の集合を意味する. $\left(\frac{*}{p}\right)$ は Legendre 記号.

A : n^2-2 ; $n \equiv \pm 2 \pmod 9$, $n \not\equiv \pm 2 \pmod{16}$, $p \mid n \Rightarrow p = 2$ or $\left(\frac{-1}{p}\right) = 1$.

B : $2n^2-2$; $n \equiv 0 \pmod 3$, $p \mid n \Rightarrow p = 2$ or $\left(\frac{-2}{p}\right) = 1$.

C : $2n^2+2$; $n \equiv \pm 4 \pmod 9$, $p \mid n \Rightarrow p = 2$ or $\left(\frac{2}{p}\right) = 1$.

D : n^2+2 ; $n \equiv 0 \pmod 3$, $n \not\equiv 0 \pmod 8$.

E : $2n^2+2$; $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{2}{p}\right) = 1$.

F : $6n^2-2$; $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{-6}{p}\right) = 1$.

G : $6n^2+2$; $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{6}{p}\right) = 1$.

H : n^2-2 ; $n \not\equiv \pm 2 \pmod{16}$, $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{-1}{p}\right) = 1$.

I : $2n^2-2$; $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{-2}{p}\right) = 1$.

J : $2n^2+2$; $n \equiv \pm 3 \pmod 9$, $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{2}{p}\right) = 1$.

K : $3n^2-2$; $n \not\equiv 0 \pmod 4$, $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{-3}{p}\right) = 1$.

L : $3n^2+2$; $n \not\equiv \pm 6, \pm 22 \pmod{48}$, $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{3}{p}\right) = 1$.

M : n^2-2 ; $n \equiv \pm 3 \pmod 9$, $n \not\equiv \pm 2 \pmod{16}$, $p \mid n \Rightarrow p = 2, 3$ or $\left(\frac{-1}{p}\right) = 1$.

N : n^2+2 ; $n \not\equiv 0 \pmod 8$.

O : $12n^2+2$; $12n^2+2 = m^2-2$ for an integer m,
$p \mid mn \Rightarrow p = 2, 3$ or $p \equiv \pm 1 \pmod{12}$.

以上の準備によって，missing trace values の集合 S_ℓ ($0 \leq \ell \leq 12$) を記述することができる. つぎの命題は筆者が観察の結果として得たもので予想として提出した. しかし僅か1ヶ月足らずの後に齋藤裕氏によって証明が完成した. ここでは予想＝定理とするゆえんである.

(<u>予想</u>＝<u>定理</u>)

$S_0 = A$, $S_1 = B$, $S_2 = \phi$ (empty), $S_3 = C$,
$S_4 = D$, $S_5 = E \cup O$, $S_6 = \phi$,
$S_7 = B \cup F \cup G \cup O$, $S_8 = H$, $S_9 = I \cup J$,
$S_{10} = K \cup L$, $S_{11} = E \cup F \cup G$, $S_{12} = M \cup N$.

ただし集合 O については筆者の予想では単に $O = \{14\}$ であった。齋藤氏によれば数列 O において 14 に続く数は $142821501076 84^2 - 2$ という大きなものであって，高々5万程度の数値を観察していた筆者にとっては到底予想し得ることではなかった．しかしながらこの問題でパソコンの果たした役割は大きく，対象としては Euler の五角数定理と並ぶほどの素朴かつ初等的な現象ではあるが，手計算のみでは気付き難いことに思われる．その意味ではこの結果もまたパソコン、すなわち核兵器産業のおこぼれと知り胸が痛む．

こうして 1985年3月末までには除外値の問題が一応の解決をみた．次節で述べられるように齋藤氏の証明は $\xi(\sigma)$ についてのもうひとつのよく知られた公式，いわゆる (Weber–) Petersson の公式に基くもので Dedekind 和は Jacobi 記号に退化している．なお長坂氏の予想については正確には後半は未解決であることを念のために付言しておく．

§2. 定理の証明

この節では，§1 で述べられた予想＝定理の証明を略述する。我々の方法で定理の完全な証明を与えるには，かなり個別の計算が必要になるので，ここでは集合 $A \sim O$ を定める条件のうち主な二条件 (I) $s = an^2 \pm 2$，(II) $p | n \Rightarrow \left(\frac{\pm a}{p}\right) = 1$ $(a = 1, 2, 3, 6)$ が，どのようにして出て来るかということに主眼をおいて述べることにする。

$X = \mathbb{Z}/24\mathbb{Z}$ とし，$\sigma \in SL_2(\mathbb{Z})$ に対して $l(\sigma) \in X$ を

$$\varepsilon(\sigma) = \zeta^{l(\sigma)}, \qquad \zeta = e^{\pi i/12},$$

で定める。$l(\sigma)$ に対して次の Petersson の公式が成り立つ。([5] 参照)

$$(1)\quad l(\sigma) = \begin{cases} bd(1-c^2) + c(tr(\sigma)-3) + 6\left(\left(\frac{d}{c}\right)-1\right), & c \text{ 奇数} \\ ac(1-d^2) + d(b-c) + 3(d-1) + 6\left(\left(\frac{c}{|d|}\right)-1\right), & d \text{ 奇数}. \end{cases}$$

まず，次のことに注意する。

Lemma 1. $\sigma \in SL_2(\mathbb{Z})$ に対し

(i) $tr(\sigma) > 2 \Longrightarrow l(\gamma^{-1}\sigma\gamma) = l(\sigma)$, $\gamma \in SL_2(\mathbb{Z})$.

（実は $tr(\sigma) > 2 \Longrightarrow \nu(\gamma^{-1}\sigma\gamma) = \nu(\sigma)$ が成り立つ。）

即ち，$\ell(\sigma)$ は σ の $SL_2(\mathbb{Z})$ 共役類で決まる。そこで，各共役類の中から公式 (1) を用いて計算するのに都合がよい元を選ぶことを考える。

Lemma 2. 各 $\tau \in SL_2(\mathbb{Z})$ に対し，τ と $SL_2(\mathbb{Z})$ に関して共役な元 $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ で，次の条件を満たすものが存在する。

(2) $v_p(b),\ v_p(a-d) \geqq v_p(c),\quad p = 2, 3$.

ここで v_p は $v_p(p) = 1$ である p 進加法付値。

これは，[3] の Th. 2.3 と $SL_2(\mathbb{Z})$ が $SL_2(\mathbb{Z}_2) \times SL_2(\mathbb{Z}_3)$ の中で稠密であることを用いて示される。この条件の下では，$\ell(\sigma) \in X_1$ なる $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ は，$(c, 6) = 1$ を満たす。また，次の Lemma が成り立つ。

Lemma 3. $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ が (2) を満たし，$c = 2^u 3^v N$，$(N, 6) = 1$，$c > 0$ とする。

(1) 2, 3 と異なる素数 p に対し

$$p^2 \mid N \implies l(\sigma) = l\left(\begin{pmatrix} a & p^2 b \\ c/p^2 & d \end{pmatrix}\right).$$

$$\text{(ii)}\quad u \geqq 5 \implies l(\sigma) = l\left(\begin{pmatrix} a & 2^2 b \\ c/2^2 & d \end{pmatrix}\right).$$

$$\text{(iii)}\quad v \geqq 3 \implies l(\sigma) = l\left(\begin{pmatrix} a & 3^2 b \\ c/3^2 & d \end{pmatrix}\right).$$

これは公式(1)と $p^2 \equiv 1 \mod 24$, $2^u \equiv 2^{u-2} \mod 24$ $u \geqq 5$, $3^v \equiv 3^{v-2} \mod 24$, $v \geqq 3$ により容易にわかる。このLemmaにより，$s>2$ に対し，X の部分集合 $\{l(\sigma) \mid tr(\sigma)=s\}$ を決めるには，考察を条件(2)及び次の条件(3)を満たす σ に制限してよいことがわかる。

(3) $c = 2^u 3^v N$, $u \leq 4$, $v \leq 2$, $(N,6)=1$, N square-free.

一般の場合を扱うには(1)の二番目の式も必要になり，叙述が繁雑になるので，以下 $l(\sigma) = X_1 = (\mathbb{Z}/24\mathbb{Z})^\times$ の場合に限ることにする。このときには前述のように $(c,6)=1$, $c=N$ である。$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ に対し $\sigma_0 = \begin{pmatrix} a & Nb \\ 1 & d \end{pmatrix}$ と置く。σ_0 は $\begin{pmatrix} s-1 & s-2 \\ 1 & 1 \end{pmatrix}$ と共役で，$l(\sigma_0) = s-3$ $(s = tr(\sigma))$ である。$l(\sigma)$ と $l(\sigma_0)$ の関係を表すために，群 G と G の X への作用を

$$G = (\mathbb{Z}/24\mathbb{Z})^\times \times \{\pm 1\},$$

$$(a,b)x = ax + 6(b-1), \quad (a,b) \in G,\ x \in X,$$

で定める。[このとき $X = \bigcup X_i$ が G の作用に関する X

の軌道分解を与えている。）G の元 g_N を $g_N=(N,(\frac{d}{N}))$ で定めると，(1) により

$$l(\sigma)=g_N\,l(\sigma_0)=g_N(tr(\sigma)-3)$$

が成り立つ。ここで次のことに注意する。$f(X)=X^2-sX+1$ $(s=tr(\sigma))$ と置くと

$$a=s-d\quad,\quad b=-f(d)/N$$

である。b は整数だから $f(d)\equiv 0 \mod N$ であり，従って

$$(4)\quad p\,|\,N \implies p\,|\,D\,(=s^2-4) \ \text{又は}\ \left(\frac{D}{p}\right)=1$$

であり，$(\frac{d}{N})$ の値は N にのみ依存している。（即ち，$f(d)\equiv f(d')\equiv 0 \mod N \implies (\frac{d}{N})=(\frac{d'}{N})$）これから g_N の定義が well-defined であることがわかる。

逆に (4) を満たす平方因子を含まない整数 N に対しては，

$$f(d)\equiv 0 \mod N$$

を満たす整数 d が存在し，$\sigma=\begin{pmatrix} s-d & -f(d)/N \\ N & d\end{pmatrix}$ とすれば，σ は $SL_2(\mathbb{Z})$ の元で

$$l(\sigma)=g_N\,l(\sigma_0)=g_N(s-3)$$

が成り立つ。(4) を満たし，平方因子を含まない整数 M, N に対し，$(M, N) = 1$ ならば

$$g_{MN} = g_M g_N$$

が成り立つ。以上の考察により次のことがわかる。

Proposition 4. $s > 2$, $s \equiv \pm 2 \mod 6$ なる s に対し G の部分群 Z_s, T_s を

$$Z_s = \{ g_N \mid (N, 6) = 1,\ p \mid N \Rightarrow \left(\tfrac{D}{p}\right) = 1 \}$$
$$T_s = \{ g_N \mid (N, 6) = 1,\ p \mid N \Rightarrow p \mid D \}$$

で定義すると

$$\{ \ell(\sigma) \mid tr(\sigma) = s \} \cap X_1 = Z_s T_s (s-3)$$

が成立する。

Z_s を記述するために，整数 M に対し G の部分群

$$Z(M) = \{ (m, \left(\tfrac{M}{m}\right)) \mid (m, 6M) = 1 \}$$

を考える。容易にわかるように $\mathbb{Q}(\sqrt{M}) \neq \mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$ ならば，$Z(M) = G$ である。

Proposition 5. $D_{\pm 1} = s \pm 2$（複号同順）と置くと

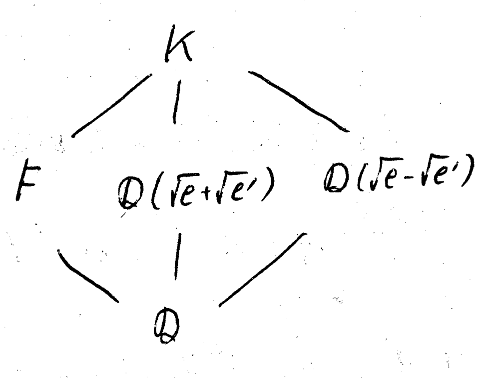
$$Z_s = Z(D_1) \cap Z(D_{-1})$$

が成り立つ。

Corollary 6. $\{\mathbb{Q}(\sqrt{D_1}), \mathbb{Q}(\sqrt{D_{-1}})\} \cap \{\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})\} = \phi$ ならば $Z_s = G$ であり従って s は除外値ではない。

s が除外値であるならば、$\mathbb{Q}(\sqrt{D_1})$ 又は $\mathbb{Q}(\sqrt{D_{-1}})$ が $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$ のいずれかと一致しなければならず、$s = an^2 \pm 2$ となり条件 (I) が出て来る。

Proposition の証明には、$F = \mathbb{Q}(\sqrt{D})$ と、F の元 e で $f(e) = 0$ となるものから得られる拡大 $K = F(\sqrt{e})$ を考える。e の $\mathbb{Q}$ 上の共役を e' とし $\sqrt{e'}$ を $\sqrt{e}\sqrt{e'} = 1$ となるように定めると、$(\sqrt{e} \pm \sqrt{e'})^2 = s \pm 2 = D_{\pm 1}$（複号同順）であり、$K$ は $\mathbb{Q}(\sqrt{D_{\pm 1}})$ を含む。p が $F/\mathbb{Q}$ で分解する素数であるとき、ξ を



$f(\xi) \equiv 0 \mod p$ を満たす整数とすると

$$\left(\frac{\xi}{p}\right) = \left(\frac{D_1}{p}\right) = \left(\frac{D_{-1}}{p}\right)$$

が成り立つ。Proposition はこれから容易に導かれる。

次に T_s について考える。

$$T_{s,\pm 1} = \left\langle \left(p, \left(\frac{2s}{p}\right)\right) \;\middle|\; p \mid s \pm 2,\ (p,6)=1 \right\rangle$$

（複号同順）

とすれば　$T_s = T_{s,1}\, T_{s,-1}$ であり，次の命題が容易に証明できる。

Proposition 7.　$\lambda = \pm 1$ とし，$s + 2\lambda = a n^2$, $a = 1, 2, 3, 6$, とする。

(i)　$Z(D_\lambda) \supset T_{s,-\lambda}$。

(ii)　$Z(D_\lambda) \supset T_{s,\lambda} \iff \left(\frac{-a\lambda}{p}\right) = 1$,　$p \mid s + 2\lambda$ (i.e. $p \mid n$), $(p,6) = 1$.

これから条件 (III) が出てくる。

s が除外値であるときどの ℓ に対して除外値になるかは，$Z_s T_s (s-3)$ を個別に計算して決める。例えば，B の元は Prop. 5, Prop. 7 により除外値であるが、$s \in B$ に対しては　$Z_s T_s = Z(2)$ で

$$Z_s T_s(s-3) = Z(2)(s-3) = \{\pm 5, \pm 11\}$$

である。従って B の元は ± 1 と ± 7 に対して除外値になっている。

詳細については [6] を御参照下さい。

§3. 新たな観察

長坂氏はこの節のための原稿をはっきりとは遺されなかったのであるが研究集会に先立って筆者(A.)のもとに送って頂いたひとつの草稿がここにある。内容は講演のものとほぼ同じであり、かつ記録に残す価値の高いものと考えられるので、誰の了解を得べきかとまどうのであるけれど、これをそのまま掲載させて頂きたいと思う。はじめに小さな導入を試ることをお赦し願いたい。

例えば 30 という数は D-関数の値となるのであるが:

$$\begin{aligned} 30 &= D(1,7) = D(2,11) = D(3,16) = D(5,31) = D(7,32) \\ &= D(8,35) = D(12,43) = D(13,44) = D(9,47) = D(13,55) \end{aligned}$$

というように 値30を実現する (h, k) の組は h を

$1 \leqq h < k$ の範囲に限っても（性質②を参照），無限に存在する．明らかに最小の k（この場合は $k=7$）にひとつの興味がある．長坂氏はつぎのような定義をされた．

$$\mathrm{ord}(s) = \inf\{k : s = D(h, k) \text{ for some } h\}.$$

ここで s は，$s>0$ で $s \equiv 0, \pm 2$ or $\pm 6 \pmod{18}$ を満たすもののみについて考えるのである．上の例では $\mathrm{ord}(30)=7$．除外値とは $\mathrm{ord}(s)=\infty$ となる s を意味することになる．先述の筆者の基準はつぎのように換言される．

$$s > 52 \Rightarrow \mathrm{ord}(s) < \frac{s}{2} \text{ or } \infty.$$

他方 k を定めたときの最大の D-値は $D(1,k)=k^2-3k+2$ であるから下からの評価としては $\mathrm{ord}(s) > \sqrt{s}+\frac{3}{2}$．しかしこれらの評価は甚だしく雑なので，長坂氏はより正確な $\mathrm{ord}(s)$ の評価に情熱を抱かれていた．氏は大計算によって $\mathrm{ord}(s)$ の表や graph（[4] にある）を作成されていた．それによると s がたとひ除外値でなくても $s=2(n^2+1)$ の形のとき $\mathrm{ord}(s)$ が著るしく大きくなるという傾向がある．このことから氏はつぎの「方程式」を「解く」ことに執心された．

$$\text{(イ)} \qquad D(h, k) = 2(n^2+1).$$

沢山の実例を観察された結果，(イ) の解，とりわけ n が素数の場合には $h \equiv 1 \pmod{n}$，$k \equiv 0 \pmod{n}$ を

満たす特徴のあることに注目された．従って(イ)より強く，

$$(\text{ロ})\quad D(\lambda n+1,\ \mu n)=2(n^2+1)$$

を考察の対象にすべく進んでおられたのである．(ロ)を群論的(?)に云えば，(n：素数として)

$$tr(\sigma)=2(n^2+1),\ V(\sigma)=\pm 3 \overset{?}{\Longrightarrow} \sigma\in\Gamma(n)$$

ということになろう．$\Gamma(n)$は主合同部分群である．また $ord(s)$ の問題は $V(\sigma)$ が σ の共役類の不変量([5]) であることを考慮すると $\sigma=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ が与えられたとき共役類の中から最小正の c を見出すことと関連している．(しかし $tr(\sigma)=s$ が大きくなると類数が大きくなるので $ord(s)$ はこのことだけで片付くのでもなかろう．)

最後に記号であるが長坂氏は D-関数よりは伝統を主んじて，$(h,k)=\frac{1}{2}D(h,k)$ を好まれ，これを Dedekind 記号と呼んでおられる．粗雑な導入であるが関心のある人の眼に氏の遺稿が親しく触れられることを祈ってやまない．

思えば，除外値の問題は最後は齋藤氏の明晰に助けられたのであったが，最も重要な step は長坂氏の直観による発見であったのは明らかである．この素朴な問題がさらに深く解明されて発展することを氏とともに強く願いまた努力したい．

Some facts and observations on the Dedekind symbol

Chiaki Nagasaka May 22, 1985

Let us consider the equation in $n, \mu \in \mathbb{N}$ and $\lambda \in \mathbb{Z}$:

$$(\lambda n + 1, \mu n) = n^2 + 1. \qquad (1)$$

I. Obvious congruences for λ, μ, n with (1).

1. $3 \nmid n \implies 3 \mid \mu$.
2. $\lambda \equiv n \pmod 3$.
3. i) $n \equiv 1 \pmod 4 \implies \mu \equiv 1$ or $2 \pmod 4$,
   ii) $n \equiv 2 \pmod 4 \implies \mu$ even,
   iii) $n \equiv 3 \pmod 4 \implies \mu \equiv 2$ or $3 \pmod 4$,
   iv) $\mu \equiv 0 \pmod 4 \implies n$ even,
   v) $\mu \equiv 1 \pmod 4 \implies n \equiv 0$ or $1 \pmod 4$,
   vi) $\mu \equiv 3 \pmod 4 \implies n \equiv 0$ or $3 \pmod 4$.

II. Solutions (λ, μ, n) of (1).

Let m be in $\mathbb{N}$. The followings are solutions of (1):

1. $(\pm 2, 2m, 3m)$.
2.* $(\alpha m + \beta, 3(Am + B), 18(am^2 + bm + c) + (-1)^{d(a)} \cdot 5)$ with
   $a, b, c, A, B, \alpha, \beta$ in the Table and
   $d(a) = 1$ if $a \equiv 1 \pmod 3$; $d(a) = 0$ if $a \equiv -1 \pmod 3$.

III. Observations.

1. Let (λ, μ, n) satisfy (1) and $n = 2^e \nu$ with ν odd.

   i) The 2-ordinal of μ is equal to e or $e + 1$.

   ii) If $\nu \equiv \pm 1 \pmod 8$, then μ and n have a common prime divisor $\equiv \pm 3 \pmod 8$.

For such n that $n^2 + 1$ is not missing we define

$$M(n) = \inf \left\{ \mu \mid (\lambda, \mu, n) \text{ satisfies } (1) \right\}.$$

2. Let p be a prime $\equiv \pm 5, \pm 13 \pmod{72}$.

   i)** If $p > 13$, then $M(p) \geq \sqrt{2(p + 5)} + 3$, where the equality holds only when p is of the form $18m^2 - 5$.

   ii) If $p > 1733$, then $M(p)$ is odd.

3. For any positive integer m, a triple $(\lambda, 2m, 3m)$ satisfies (1) if and only if $\lambda = 2\ell$ with ℓ prime to m.

The statement i) in Observation 1 is true for n odd. Observation 2 is true up to $p = 19949$. Observation 3 is true up to $m = 1000$.

**) $w \equiv 0, \pm 1, \pm 3 \pmod{g}$, not missing

$\rho = \inf\{ r \mid \mathrm{ord}(w) = O(w^r) \}$ とおきます．先生の結果とSaliéの結果から $\frac{1}{2} \leq \rho \leq 1$ ですが，2のi) は $\rho \geq \frac{3}{4}$ であることを示唆しております．私の数値実験では，$\frac{3}{4} < \rho < \frac{7}{8}$ という感じです．

a	b	c	A	B	(α, β)
1	0	0	2	1	(0, 1), (0, -2)
2	-2	0	4	-1($\cancel{0}$)1	(0, -4), (6, -1)
2	2	-1	4	5($\cancel{1}$)0	(0, -4), (6, 8)
4	0	0	8	1(0)	(0, -8), (6, 1)
4	-4	1	8	-5(1)	(0, -8), (-6, 4)
4	4	-4	8	13(2)	(0, -8), (6, 10)
4	0	-3	8	7(3)	(0, -8), (-6, -5)
5	2	-4	10	11(0)	(0, 5), (-6, -7)
5	-8	3	10	-7(1)	(0, 5), (-12, 8)
5	8	-1	10	17(3)	(0, 5), (12, 20)
5	-2	0	10	-1(4)	(0, 5), (6, -1)
5	-4	-1	10	1(0)	(0, -10), (-12, -10)
5	10	-4	10	23(1)	(0, -10), (6, 14)
5	0	1	10	-3(3)	(0, -10), (-6, 2)
5	4	-1	10	9(4)	(0, -10), (12, 11)
7	-6	0	14	1(0)	(0, 7), (18, 1)
7	-10	4	14	-11(1)	(0, 7), (6, -5)
7	4	-7	14	19(2)	(0, 7), (12, 16)
7	-4	1	14	-5(4)	(0, 7), (-12, 4)
7	10	-4	14	25(5)	(0, 7), (-12, -11)
7	6	0	14	13(6)	(0, 7), (-18, -17)
7	2	0	14	1(0)	(0, -14), (12, 1)
7	2	-8	14	17(1)	(0, -14), (18, 22)
7	0	-3	14	-9(2)	(0, -14), (-6, 4)

a	b	c	A	B	(α, β)
7	14	-12	14	37(4)	(0, -14), (6, 16)
7	-2	0	14	-3(5)	(0, -14), (-18, 4)
7	12	-3	14	27(6)	(0, -14), (-12, -23)
8	-4	-1	16	1(0)	(0, -16), (-18, -1)
				(1)	
8	24	-9	16	53(2)	(0, -16), (6, 20)
8	-4	-4	16	7(3)	(0, -16), (18, 8)
8	4	-1	16	9(4)	(0, -16), (-18, -10)
8	8	-4	16	-5(5)	(0, -16), (-6, 2)
8	0	-1	16	-3(6)	(0, -16), (6, -1)
8	4	-4	16	15(7)	(0, -16), (18, 17)
10	6	0	20	1(0)	(0, -20), (18, 1)
10	-10	1	20	-17(1)	(0, -20), (6, -5)
				(2)	
10	10	-11	20	-13(3)	(0, -20), (-6, 4)
10	-6	0	20	-11(4)	(0, -20), (-18, 10)
10	6	-15	20	31(5)	(0, -20), (18, 28)
10	30	-24	20	73(6)	(0, -20), (6, 22)
				(7)	
10	10	-16	20	37(8)	(0, -20), (-6, -11)
10	14	-11	20	39(9)	(0, -20), (-18, -35)

*) これらは (λ, μ, n) μ odd n prime の data から構成したものの一部です．相互法則を使って確認しました．

(この稿，終)