連分数と整数係数2元2次形式

MATHEMATICS.PDF

2010-12-10

目 次

1　連分数

連分数とは,

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{\ddots \\ + \cfrac{b_{n-1}}{a_{n-1} + \cfrac{b_n}{a_n}}}}} \tag{1}$$

という形の式である. 記述を簡単にするため, 式 (1) を次のような省略形で表す：

$$a_0 + \frac{b_1}{a_1} + \frac{b_2}{a_2} + \cdots + \frac{b_n}{a_n}. \tag{2}$$

[定理 1.1] a_0 が整数であり, a_1, ..., a_n, b_1, b_2, ..., b_n が 0 でない整数であるとき, 連分数 (1) は有理数である.

[証明] n に関する数学的帰納法によって証明する. まず,

$$a_0 + \frac{b_1}{a_1} = \frac{a_0 a_1 + b_1}{a_1}$$

は有理数である.

$n = k - 1$ のとき, 式 (1) の形の連分数がすべて有理数であると仮定する.

$$\cfrac{b_{k-1}}{a_{k-1} + \cfrac{b_k}{a_k}} = \frac{a_k b_{k-1}}{a_{k-1} a_k + b_k}$$

なので,

$$\begin{aligned} a_0 + \frac{b_1}{a_1} + \frac{b_2}{a_2} + \cdots + \frac{b_{k-2}}{a_{k-2}} + \frac{b_{k-1}}{a_{k-1}} + \frac{b_k}{a_k} \\ = a_0 + \frac{b_1}{a_1} + \frac{b_2}{a_2} + \cdots + \frac{b_{k-2}}{a_{k-2}} + \frac{a_k b_{k-1}}{a_{k-1} a_k + b_k}. \end{aligned}$$

すなわち, $n = k$ としたときの式 (1) は $n = k - 1$ のときの形に変形できる. ゆえに $n = k$ のときも連分数 (1) は有理数である.

以上より, すべての番号 n に対して, 連分数 (1) が有理数であることが示された. □

以後, 分子がすべて 1 の連分数

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} \tag{3}$$

を扱う. これを省略形で表すと

$$a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

となるが, これ以外にも

$$[a_0, a_1, a_2, \ldots, a_n]$$

という記号で表すこともある[1)].

各々の a_0, a_1, a_2, …, a_n を連分数 (3) の**部分商**という.

記号の意味を考えれば,

$$\begin{aligned}
[a_0, a_1, a_2, \ldots, a_n] &= [a_0, [a_1, a_2, \ldots, a_n]] \\
&= [a_0, a_1, [a_2, \ldots, a_n]] \\
&= \cdots\cdots \\
&= [a_0, a_1, a_2, \ldots, a_{n-2}, [a_{n-1}, a_n]]
\end{aligned}$$

が成り立つことがわかる.

連分数 $[a_0, a_1, a_2, \ldots, a_n]$ が定義されるためには, 分母が 0 にならないことが必要である. すなわち, 条件

$$[a_1, a_2, \ldots, a_n] \neq 0, \quad [a_2, \ldots, a_n] \neq 0, \quad \ldots, \quad [a_{n-1}, a_n] \neq 0, \quad a_n \neq 0 \tag{4}$$

を満たすことが必要である. 逆に, この条件を満たしていれば, 連分数 $[a_0, a_1, a_2, \ldots, a_n]$ を定義することができる.

少なくとも, a_1, a_2, …, a_n がすべて正の実数であるとき, (4) は満たされるから, 連分数 $[a_0, a_1, a_2, \ldots, a_n]$ が定義できる.

a_0 が整数で, a_1, a_2, …, a_n が正の整数であるとき, 連分数 $[a_0, a_1, a_2, \ldots, a_n]$ を**単純連分数**という.

[1)] 高木 [1] 第 2 章で用いられている記号 $[k_0, k_1, \ldots, k_n]$ が表しているものと, この文書で用いる記号 $[a_0, a_1, \ldots, a_n]$ が表しているものとは, 一般には一致しないので注意せよ.

$a_1,\ a_2,\ \ldots,\ a_{n-1}$ のうちのいくつかが 0 のとき, 連分数はより簡単な形になる. 例えば $n = 3$, $a_1 = 0$ のとき,

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}} = a_0 + \cfrac{1}{\cfrac{1}{a_2 + \cfrac{1}{a_3}}} = a_0 + a_2 + \frac{1}{a_3}$$

となる.

[例 1.2]

$$[1,2,3] = 1 + \cfrac{1}{2 + \cfrac{1}{3}} = 1 + \frac{1}{\cfrac{7}{3}} = 1 + \frac{3}{7} = \frac{10}{7}.$$

[例 1.3]

$$[-4,3,2] = -4 + \cfrac{1}{3 + \cfrac{1}{2}} = -4 + \frac{1}{\cfrac{7}{2}} = -4 + \frac{2}{7} = -\frac{26}{7}.$$

[定理 1.4] $n \geq 0$ を整数とする. a_0 は整数, $a_1,\ a_2,\ \ldots,\ a_n$ は正の整数であるとする. このとき, 連分数 $[a_0,\ a_1,\ a_2,\ \ldots,\ a_n]$ が整数ならば, 「$n = 0$」または「$n = 1,\ a_1 = 1$」である.

[証明] $n \geq 2$ と仮定する.

$$s = a_1 + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

とおくと,

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{s} \tag{5}$$

である. ところが, $n \geq 2$ のとき, $s > 1$ となるので, 式 (5) の右辺は整数ではない. これは矛盾である. したがって, $n \leq 1$ でなければならない.

よって, もし $n \neq 0$ であれば, $n = 1$ であり,

$$[a_0, a_1] = a_0 + \frac{1}{a_1}$$

かつ左辺は整数である. もし $a_1 > 1$ ならば, 右辺は整数ではない. これは矛盾である. したがって, $n \neq 0$ ならば, $n = 1$ かつ $a_1 = 1$ でなければならない. □

[補題 1.5] $a,\ b$ を整数, $\alpha,\ \beta$ を実数とし, $0 < \alpha < 1,\ 0 < \beta < 1$ とする. このとき, $a + \alpha = b + \beta$ ならば, $a = b$ かつ $\alpha = \beta$ が成り立つ.

[証明] $0 < \alpha < 1$, $0 < \beta < 1$ より,

$$-1 < \beta - 1 < \beta - \alpha < 1 - \alpha < 1.$$

$a + \alpha = b + \beta$ より, $a - b = \beta - \alpha$ だから,

$$-1 < a - b < 1.$$

$a - b$ は整数だから, $a - b = 0$ でなければならない. 同時に, $\beta - \alpha = 0$ も得られる. □

[定理 1.6] m, n を負でない整数とし, $n \leq m$ であるとする. a_0, b_0 は整数, a_1, a_2, …, a_n, b_1, b_2, …, b_m は正の整数であるとする. このとき,

$$[a_0, a_1, \ldots, a_n] = [b_0, b_1, \ldots, b_m]$$

ならば, 次のどちらか一方が成り立つ.

(i) $m = n$, $a_0 = b_0$, $a_1 = b_1$, …, $a_n = b_n$

(ii) $m = n + 1$, $a_0 = b_0$, $a_1 = b_1$, …, $a_n = b_n + 1$, $b_{n+1} = 1$

[証明] $0 \leq i \leq n - 1$ なる正の整数 i に対して,

$$s_i = a_{i+1} + \frac{1}{a_{i+2}} + \cdots + \frac{1}{a_n}$$
$$t_i = b_{i+1} + \frac{1}{a_{i+2}} + \cdots + \frac{1}{b_m}$$

とおく.

$1 \leq i \leq n - 2$ のときは, $s_i > 1$, $t_i > 1$ なので, 補題 1.5 より

$$a_i + \frac{1}{s_i} = b_i + \frac{1}{t_i} \Longrightarrow a_i = b_i$$

となる. よって,

$$a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2, \quad \ldots, \quad a_{n-2} = b_{n-2}$$

が次々といえる. また,

$$a_{n-1} + \frac{1}{a_n} = b_{n-1} + \frac{1}{t_{n-1}} \tag{6}$$

が成り立つ.

$a_n > 1$ のとき, 式 (6) の左辺は整数ではないので, $t_{n-1} > 1$ でなければならない. よって補題 1.5 より

$$a_{n-1} = b_{n-1}, \quad a_n = t_{n-1}$$

となる. a_n は整数なので, 定理 1.4 より, 「$m = n$, $a_n = b_n$」または「$m = n + 1$, $a_n = b_n + 1$, $b_{n+1} = 1$」でなければならない.

$a_n = 1$ のとき, 式 (6) の左辺は整数なので, $t_{n-1} = 1$ でなければならない. もし $m \geq n + 1$ ならば $t_{n-1} > 1$ となってしまうので, $m = n$, $b_n = 1$ でなければならない. □

[定理 1.7] m, n を負でない整数とし, $n \leq m$ であるとする. a_0, b_0 は整数, a_1, a_2, …, a_n, b_1, b_2, …, b_m は正の整数であるとする. また, s, t を 1 より大きい実数とする. このとき,

$$[a_0, a_1, \ldots, a_n, s] = [b_0, b_1, \ldots, b_m, t]$$

ならば,

$$a_0 = b_0, \quad a_1 = b_1, \quad \ldots, \quad a_n = b_n$$

かつ

$$s = [b_{n+1}, b_{n+2}, \ldots, b_m, t]$$

である. 特に, $m = n$ ならば $s = t$ である.

[証明] $0 \leq i \leq n-1$ なる正の整数 i に対して,

$$s_i = a_{i+1} + \frac{1}{a_{i+2}} + \cdots + \frac{1}{a_n} + \frac{1}{s}$$
$$t_i = b_{i+1} + \frac{1}{a_{i+2}} + \cdots + \frac{1}{b_m} + \frac{1}{t}$$

とおくと, $s_i > 1$, $t_i > 1$ なので, 補題 1.5 より

$$a_i + \frac{1}{s_i} = b_i + \frac{1}{t_i} \Longrightarrow a_i = b_i,\ s_i = t_i$$

となる. よって,

$$a_0 = b_0, \quad a_1 = b_1, \quad a_2 = b_2, \quad \ldots, \quad a_{n-1} = b_{n-1}$$

が次々といえる. また,

$$a_n + \frac{1}{s} = b_n + \frac{1}{b_{n+1}} + \cdots + \frac{1}{b_m} + \frac{1}{t}$$

が成り立つ. $s > 1$, $t > 1$ だから, 再び補題 1.5 が適用できて, $a_n = b_n$ かつ

$$s = b_{n+1} + \frac{1}{b_{n+2}} + \cdots + \frac{1}{b_m} + \frac{1}{t}$$

となる. 特に, $m = n$ ならば $s = t$ である. □

2 数列 (p_n), (q_n)

実数列 (a_n) に対して, 実数列 (p_n), (q_n) を, 漸化式

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \quad p_{-1} = 1, \quad p_{-2} = 0, \\ q_n &= a_n q_{n-1} + q_{n-2}, \quad q_{-1} = 0, \quad q_{-2} = 1 \end{aligned} \tag{7}$$

によって定義する.

$n \geq 1$ を整数とする. a_1, a_2, …, a_n が整数であれば, p_1, p_2, …, p_n および q_1, q_2, …, q_n もまた整数であることが, p_n, q_n の定め方からわかる.

[定理 2.1] すべての番号 $n \geq 1$ に対して $a_n \geq 1$ であるとする. このとき, すべての番号 $n \geq 1$ に対して

(i) $n \leq q_n$

(ii) $q_n < q_{n+1}$

が成り立つ.

[証明] (i)　n に関する数学的帰納法により証明する. まず, $q_{-2} = 1$, $q_{-1} = 0$ より,

$$q_0 = a_0 q_{-1} + q_{-2} = 1.$$

これと $a_1 \geq 1$, $a_2 \geq 1$ より,

$$q_1 = a_1 q_0 + q_{-1} = a_1 \geq 1,$$
$$q_2 = a_2 q_1 + q_0 = a_1 a_2 + 1 \geq 2.$$

$n \geq 3$ のとき, $1 \leq k < n$ なるすべての番号 k について $k \leq q_k$ であると仮定すると, $a_n \geq 1$ より

$$\begin{aligned} q_n &= a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} \\ &\geq (n-1) + (n-2) = 2n - 3 \\ &\geq n. \end{aligned} \tag{8}$$

以上より, すべての番号 $n \geq 1$ に対して $n \leq q_n$ が成り立つことが示された.

(ii)　まず,

$$q_1 = a_1 q_0 + q_{-1} = a_1,$$
$$q_2 = a_2 q_1 + q_0 = a_1 a_2 + 1.$$

$a_1 \geq 1$, $a_2 \geq 1$ より, $q_1 < q_2$ が成り立つ.

$n \geq 3$ のとき, $a_n \geq 1$ であり, (i) より $n - 2 \leq q_{n-2}$ であるから,

$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + (n-2) > q_{n-1}.$$

□

[注意 2.2] $1 = q_0 \leq q_1$ なので, すべての番号 $n \geq 0$ に対して $q_n \leq q_{n+1}$ が成り立つ. また, $n \geq 4$ のとき (8) において $2n - 3 > n$ だから, すべての番号 $n \geq 4$ に対して $n < q_n$ が成り立つ.

[定理 2.3] $a_0 \geq 1$ とし, すべての番号 $n \geq 1$ に対して $a_n \geq 1$ であるとする. このとき, すべての番号 $n \geq 0$ に対して

(i) $n < p_n$

(ii) $p_n < p_{n+1}$

が成り立つ.

[証明] (i)　n に関する数学的帰納法により証明する. まず, $p_{-2} = 0$, $p_{-1} = 1$ より,

$$p_0 = a_0 p_{-1} + p_{-2} = a_0 \geq 1.$$

これと $a_1 \geq 1$, $a_2 \geq 1$ より,

$$p_1 = a_1 p_0 + p_{-1} = a_1 a_0 + 1 \geq 2.$$

$n \geq 2$ のとき, $1 \leq k < n$ なるすべての番号 k について $k < p_k$ であると仮定すると, $a_n \geq 1$ より

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \geq p_{n-1} + p_{n-2} \\ &> (n-1) + (n-2) = 2n - 3 \\ &\geq n. \end{aligned}$$

以上より, すべての整数 $n \geq 0$ に対して $n < p_n$ が成り立つことが示された.

(ii)　まず, $p_0 = a_0$, $p_1 = a_1 a_0 + 1$ であり, $a_1 \geq 1$ だから, $p_0 < p_1$ が成り立つ.

$n \geq 2$ のとき, $a_n \geq 1$ であり, (ii) より $n - 2 < p_{n-2}$ であるから,

$$p_n = a_n p_{n-1} + p_{n-2} > p_{n-1} + (n-2) > p_{n-1}.$$

□

[定理 2.4] すべての番号 $n \geq 1$ に対して $a_n \geq 1$ であるとする. このとき,

$$\lim_{n \to \infty} q_n = \infty.$$

さらに $a_0 \geq 1$ という仮定を追加すれば,

$$\lim_{n \to \infty} p_n = \infty.$$

[証明] 定理 2.1 より, すべての番号 $n \geq 1$ に対して $q_n \geq n$ が成り立つ. ゆえに $n \to \infty$ のとき $q_n \to \infty$ である.

さらに $a_0 \geq 1$ であれば, 定理 2.3 より, すべての番号 $n \geq 1$ に対して $p_n \geq n$ が成り立つ. ゆえに $n \to \infty$ のとき $p_n \to \infty$ である. □

[定理 2.5] すべての番号 $n \geq -2$ に対して,

(i) $p_n q_{n+1} - p_{n+1} q_n = (-1)^n$

(ii) p_n, q_n が整数ならば $\gcd(p_n, q_n) = 1$

が成り立つ.

[証明] (i)　n に関する数学的帰納法によって証明する. まず,

$$p_{-1}q_{-2} - p_{-2}q_{-1} = 1$$

なので, $n = -2$ のとき (i) は正しい.

$n = k - 1$ のとき (i) が正しいと仮定すると,

$$\begin{aligned} p_{k+1}q_k - p_kq_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) \\ &= -(p_kq_{k-1} - p_{k-1}q_k) = -(-1)^{k-1} = (-1)^k. \end{aligned}$$

よって $n = k$ のときも (i) が成り立つ.

以上より, すべての番号 n に対して (i) は正しい.

(ii)　もし仮に $g = \gcd(p_n, q_n) > 1$ であれば, (i) の左辺は g の倍数なので, 右辺も g の倍数でなければならない. ところが, 右辺は g の倍数ではないので, 矛盾である. したがって $g = 1$ でなければならない. □

[定理 2.6] すべての番号 $n \geq 1$ に対して $a_n > 0$ であるとする. このとき,

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_{2k}}{q_{2k}} < \frac{p_{2k+2}}{q_{2k+2}} < \cdots < \frac{p_{2k+3}}{q_{2k+3}} < \frac{p_{2k+1}}{q_{2k+1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$$

が成り立つ. ただし, k は負でない整数である.

[証明]

$$\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} = \frac{p_{n+2}q_n - p_nq_{n+2}}{q_nq_{n+2}}.$$

定理 2.5 より

$$p_{n+1}q_n - p_nq_{n+1} = (-1)^n \tag{9}$$

であるから,

$$\begin{aligned} p_{n+2}q_n - p_nq_{n+2} &= (a_{n+2}p_{n+1} + p_n)q_n - p_n(a_{n+2}q_{n+1} + q_n) \\ &= (p_{n+1}q_n - p_nq_{n+1})a_{n+2} \\ &= (-1)^n a_{n+2}. \end{aligned}$$

ゆえに

$$\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} = \frac{(-1)^n a_{n+2}}{q_nq_{n+2}}.$$

$q_n > 0$, $q_{n+2} > 0$, $a_{n+2} > 0$ なので,

$$n \text{ が偶数} \Longrightarrow \frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} > 0 \Longrightarrow \frac{p_{n+2}}{q_{n+2}} > \frac{p_n}{q_n}, \tag{10}$$

$$n \text{ が奇数} \Longrightarrow \frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} < 0 \Longrightarrow \frac{p_{n+2}}{q_{n+2}} < \frac{p_n}{q_n} \tag{11}$$

である. つまり, 番号 n が偶数の場合は大きい番号ほど p_n/q_n は大きくなり, 番号 n が奇数の場合は大きい番号ほど p_n/q_n は小さくなる.

また, 式 (9) より

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}} = \frac{(-1)^n}{q_n q_{n+1}}.$$

$q_n > 0$, $q_{n+1} > 0$ なので,

$$n \text{ が偶数} \Longrightarrow \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} > 0 \Longrightarrow \frac{p_{n+1}}{q_{n+1}} > \frac{p_n}{q_n}, \tag{12}$$

$$n \text{ が奇数} \Longrightarrow \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} < 0 \Longrightarrow \frac{p_{n+1}}{q_{n+1}} < \frac{p_n}{q_n} \tag{13}$$

である.

したがって, 任意の偶数 $u \geq 0$ と任意の奇数 $v \geq 1$ に対して, $u < v$ のときは, $u < v + 1$ なので, 式 (10) と式 (13) より

$$\frac{p_u}{q_u} < \frac{p_{v+1}}{q_{v+1}} < \frac{p_v}{q_v}$$

であり, $v < u$ のときは, $v < u + 1$ なので, 式 (11) と式 (12) より

$$\frac{p_u}{q_u} < \frac{p_{u+1}}{q_{u+1}} < \frac{p_v}{q_v}$$

が成り立つ. つまり, 奇数番号のものはすべての偶数番号のものより大きく, 逆に偶数番号のものはすべての奇数番号のものより小さい.

以上で定理が証明された. □

3 近似分数

(a_n) を整数列とし, 数列 (p_n), (q_n) は (a_n) に対して §2 の漸化式 (7) によって定まるものとする.

[定理 3.1] 任意の整数 $n \geq 0$ と, 0 でも負の有理数でもない任意の実数 t に対して,

$$[a_0, a_1, \ldots, a_{n-1}, t] = \frac{tp_{n-1} + p_{n-2}}{tq_{n-1} + q_{n-2}} \tag{14}$$

が成り立つ. ただし, $n \geq 2$ のとき, a_1, a_2, …, a_{n-1} はすべて正であるとする.

[証明] n に関する数学的帰納法によって証明する.

$p_{-1} = 1$, $p_{-2} = 0$, $q_{-1} = 0$, $q_{-2} = 1$ だから,

$$[t] = \frac{tp_{-1} + p_{-2}}{tq_{-1} + q_{-2}}.$$

また,

$$p_0 = a_0 p_{-1} + p_{-2} = a_0,$$
$$q_0 = a_0 q_{-1} + q_{-2} = 1$$

なので,

$$[a_0, t] = a_0 + \frac{1}{t} = \frac{ta_0 + 1}{t} = \frac{tp_0 + p_{-1}}{tq_0 + q_{-1}}.$$

よって, $n = 0$, 1 のとき (14) は正しい. また

一般の整数 $n \geq 2$ について, $n-1$ のとき (14) が正しいと仮定すると, 定理 3.1 より,

$$\begin{aligned}[a_0, a_1, \ldots, a_{n-2}, a_{n-1}, t] &= \left[a_0, a_1, \ldots, a_{n-2}, a_{n-1} + \frac{1}{t}\right] \\ &= \frac{(a_{n-1} + 1/t)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/t)q_{n-2} + q_{n-3}}.\end{aligned}$$

さらに計算すると,

$$\begin{aligned}\frac{(a_{n-1} + 1/t)p_{n-2} + p_{n-3}}{(a_{n-1} + 1/t)q_{n-2} + q_{n-3}} &= \frac{(ta_{n-1} + 1)p_{n-2} + tp_{n-3}}{(ta_{n-1} + 1)q_{n-2} + tq_{n-3}} \\ &= \frac{t(a_{n-1}p_{n-2} + p_{n-3}) + p_{n-2}}{t(a_{n-1}q_{n-2} + q_{n-3}) + q_{n-2}} \\ &= \frac{tp_{n-1} + p_{n-2}}{tq_{n-1} + q_{n-2}}.\end{aligned}$$

ゆえに, n のときも (14) が成り立つ.

最後に, t や a_1, a_2, …, a_n についての定理の仮定により, 計算の途中で現れた分数の分母は決して 0 にならないことに注意せよ.

以上より, すべての番号 $n \geq 0$ に対して (14) が正しいことが示された. □

[定理 3.2] 任意の整数 $n \geq 0$ と, 0 でも負の有理数でもない任意の実数 s, t に対して,

$$\begin{aligned}&[a_0, a_1, \ldots, a_{n-1}, s] - [a_0, a_1, \ldots, a_{n-1}, t] \\ &= \frac{(-1)^n (s - t)}{(sq_{n-1} + q_{n-2})(tq_{n-1} + q_{n-2})}.\end{aligned}$$

ただし, $n \geq 2$ のとき, a_1, a_2, …, a_{n-1} はすべて正であるとする.

[証明] 定理 2.5 より,

$$p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^{n-2} = (-1)^n.$$

よって, 定理 3.1 より,

$$\begin{aligned}
&[a_0, a_1, \ldots, a_{n-1}, s] - [a_0, a_1, \ldots, a_{n-1}, t] \\
&\quad = \frac{sp_{n-1} + p_{n-2}}{sq_{n-1} + q_{n-2}} - \frac{tp_{n-1} + p_{n-2}}{tq_{n-1} + q_{n-2}} \\
&\quad = \frac{(sp_{n-1} + p_{n-2})(tq_{n-1} + q_{n-2}) - (sq_{n-1} + q_{n-2})(tp_{n-1} + p_{n-2})}{(sq_{n-1} + q_{n-2})(tq_{n-1} + q_{n-2})} \\
&\quad = \frac{\begin{array}{c} stp_{n-1}q_{n-1} + sp_{n-1}q_{n-2} + tp_{n-2}q_{n-1} + p_{n-2}q_{n-2} \\ -(stp_{n-1}q_{n-1} + tp_{n-1}q_{n-2} + sp_{n-2}q_{n-1} + p_{n-2}q_{n-2}) \end{array}}{(sq_{n-1} + q_{n-2})(tq_{n-1} + q_{n-2})} \\
&\quad = \frac{(s-t)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1})}{(sq_{n-1} + q_{n-2})(tq_{n-1} + q_{n-2})} \\
&\quad = \frac{(-1)^n (s-t)}{(sq_{n-1} + q_{n-2})(tq_{n-1} + q_{n-2})}.
\end{aligned}$$

□

[定理 3.3] $n \geq 0$ を整数とする. $n \geq 2$ のとき, a_1, a_2, …, a_{n-1} はすべて正であるとする. また, s, t を正の実数とする.

(a)

$$[a_0, a_1, \ldots, a_{n-1}, s] = [a_0, a_1, \ldots, a_{n-1}, t] \Longleftrightarrow s = t.$$

(b) n が偶数のとき,

$$[a_0, a_1, \ldots, a_{n-1}, s] < [a_0, a_1, \ldots, a_{n-1}, t] \Longleftrightarrow s < t.$$

(c) n が奇数のとき,

$$[a_0, a_1, \ldots, a_{n-1}, s] < [a_0, a_1, \ldots, a_{n-1}, t] \Longleftrightarrow s > t.$$

[証明] 定理 3.2 から直ちに導かれる. □

[定理 3.4] $n \geq 0$ を整数とする. また, $n \geq 1$ のとき, a_1, a_2, …, a_n はすべて正であるとする. このとき,

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}$$

が成り立つ.

[証明] $n \geq 1$ のとき, 定理 3.1 において, $t = a_n$ を代入すれば,

$$[a_0, a_1, \ldots, a_n] = \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n}$$

が成り立つ.

また, $p_{-1}=1$, $p_{-2}=0$, $q_{-1}=0$, $q_{-2}=1$ であり,

$$p_0 = a_0 p_{-1} + p_{-2} = a_0,$$
$$q_0 = a_0 q_{-1} + q_{-2} = 1$$

なので,

$$\frac{p_0}{q_0} = a_0 = [a_0]$$

である. よって $n=0$ のときも定理が成り立つ. □

$0 \le n \le m$ とするとき, 連分数 $\omega = [a_0, a_1, a_2, \ldots, a_m]$ に対して, 連分数

$$[a_0, a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}$$

を ω の n 次の**近似分数**という. $\gcd(p_n, q_n) = 1$ かつ $q_n > 0$ なので, p_n/q_n は既約分数である.

[定理 3.5] すべての番号 $n \ge 1$ に対して $a_n \ge 1$ であるとする.

$$c_n = [a_0, a_1, a_2, \ldots, a_n], \quad n = 0, 1, 2, \ldots$$

とおくことによって連分数の列 (c_n) を定めると, ある実数 ω が存在して

$$\lim_{n\to\infty} c_n = \omega$$

が成り立つ.

[証明] 定理 3.4 より, すべての番号 $n \ge 0$ に対して

$$c_n = [a_0, a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}$$

が成り立つ.

m, n を正の整数とし, $n \le m$ とする. 定理 2.6 より,

$$\left|\frac{p_m}{q_m} - \frac{p_n}{q_n}\right| \le \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|.$$

また, 定理 2.5 より

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}} = \frac{(-1)^n}{q_n q_{n+1}}.$$

ゆえに,

$$\left|\frac{p_m}{q_m} - \frac{p_n}{q_n}\right| \le \frac{(-1)^n}{q_n q_{n+1}}.$$

定理 2.1 より, $q_n \ge n$, $q_{n+1} \ge n+1$ であるから,

$$\frac{(-1)^n}{q_n q_{n+1}} \le \frac{1}{n(n+1)} \le \frac{1}{n^2}.$$

ゆえに,

$$\left|\frac{p_m}{q_m}-\frac{p_n}{q_n}\right|\leq\frac{1}{n^2}.$$

実数 $\varepsilon>0$ を任意にとる. $\delta=1/\sqrt{\varepsilon}$ とおくと, $n>\delta$ を満たすすべての番号 n に対して

$$\frac{1}{n^2}<\frac{1}{\delta^2}=\varepsilon$$

となる. ゆえに

$$m\geq n>\delta\Longrightarrow\left|\frac{p_m}{q_m}-\frac{p_n}{q_n}\right|<\varepsilon$$

が成り立つ. よって数列 (c_n) はコーシー列である. 実数の完備性から, ある実数 ω が存在して, $\lim_{n\to\infty}c_n=\omega$ となる. □

[補題 3.6] $f(x)$ を区間 $[a,\,\infty)$ で連続な実数値関数とし, $\lim_{x\to\infty}f(x)=l$ であるとする.

(i) $f(a)<l$ であるとし, c を $f(a)<c<l$ なる任意の実数とするとき, $f(\xi)=c$ かつ $\xi>a$ となるよう実数 ξ が存在する.

(ii) $l<f(a)$ であるとし, c を $l<c<f(a)$ なる任意の実数とするとき, $f(\xi)=c$ かつ $\xi>a$ となるよう実数 ξ が存在する.

[証明] (i) ある実数 b が存在して $a<b$ かつ $l\leq f(b)$ であるとき, 閉区間 $[a,\,b]$ に対して中間値の定理を適用すると, ある実数 ξ が存在して $f(\xi)=c$ かつ $a<\xi<b$ が成り立つ.

$x>a$ を満たす任意の実数 x に対して $f(x)<l$ であるとき, 仮定より $\lim_{x\to\infty}f(x)=l$ なので, 任意の実数 $\varepsilon>0$ に対して, ある実数 δ が存在して, 任意の実数 x に対して

$$x>\delta\Longrightarrow|f(x)-l\,|<\varepsilon.$$

$\varepsilon=(l-c)/2$ とおくと,

$$x>\delta\Longrightarrow l-f(x)<\frac{l-c}{2}\Longrightarrow f(x)>\frac{l+c}{2}>c.$$

$t=\max\{\delta,\,a\}$ とおけば, $f(a)<c<f(t)$ となる. 閉区間 $[a,\,t]$ に対して中間値の定理を適用すると, ある実数 ξ が存在して $f(\xi)=c$ かつ $a<\xi<t$ が成り立つ.

(ii) (i) と同様にして証明できる. □

[定理 3.7] $n\geq0$ を整数とする. $n\geq1$ のとき, $a_1,\,a_2,\,\ldots,\,a_n$ はすべて正であるとする. また, ω を実数とする.

(i)

$$[a_0,a_1,\ldots,a_n,a_{n+1}]<\omega<[a_0,a_1,\ldots,a_n]$$

ならば, ある実数 s が存在して, $s>a_{n+1}$ かつ

$$\omega=[a_0,a_1,\ldots,a_n,s]$$

が成り立つ.

(ii)

$$[a_0, a_1, \ldots, a_n] < \omega < [a_0, a_1, \ldots, a_n, a_{n+1}]$$

ならば, ある実数 s が存在して, $s > a_{n+1}$ かつ

$$\omega = [a_0, a_1, \ldots, a_n, s]$$

が成り立つ.

[証明] $f(x) = [a_0, a_1, \ldots, a_n, x]$ とおく. $f(x)$ は $a_j + x$ $(j = 0, 1, \ldots, n)$ と $1/x$ との合成によって構成されるから, 区間 $(0, \infty)$ における実数値連続関数である. さて,

$$f(a_{n+1}) = [a_0, a_1, \ldots, a_n, a_{n+1}].$$

また, $f(x) = [a_0, a_1, \ldots, a_{n-1}, a_n + 1/x]$ だから,

$$\lim_{x \to \infty} f(x) = [a_0, a_1, \ldots, a_n].$$

したがって, ある実数 s が存在して $s > a_{n+1}$ かつ $\omega = [a_0, a_1, \ldots, a_n, s]$ となることが, 求める定理の (i), (ii) それぞれの場合に応じて, 補題 3.6 (i), (ii) よりいえる. □

4 連分数展開

ω を実数とする. ω が整数でないとき, ω を超えない最大の整数を a_0 とすると,

$$\omega = a_0 + \frac{1}{\omega_1} \tag{15}$$

を満たす ω_1 が定まる. ω_1 は

$$\omega_1 = \frac{1}{\omega - a_0} > 1$$

であるような実数である.

同様に, ω_1 が整数でないとき, ω_1 を超えない最大の整数を a_1 とすると,

$$\omega_1 = a_1 + \frac{1}{\omega_2} \tag{16}$$

を満たす ω_2 が定まる. ω_2 は

$$\omega_2 = \frac{1}{\omega_1 - a_1} > 1$$

であるような実数である.

式 (16) を式 (15) に代入すれば,

$$\omega = a_0 + \frac{1}{a_1 + \dfrac{1}{\omega_2}} = [a_0, a_1, \omega_2]$$

となる. 同じような計算を繰り返せば, 正の整数の列 a_1, a_2, …, a_{n-1} と, 実数 $\omega_n > 1$ と, 関係式

$$\omega = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{n-1}} + \frac{1}{\omega_n} = [a_0, a_1, a_2, \ldots, a_{n-1}, \omega_n] \tag{17}$$

が得られる.

各番号 $n \geq 0$ に対する式 (17) を, ω の**連分数展開**という. また, ω_n を連分数展開 (17) の n 次の**全商**という.

ω が整数のとき, $a_0 = q$ とすれば,

$$q = a_0 = [a_0].$$

これが整数の場合の連分数展開である.

ω が有理数のとき, ある整数 m, n が存在して, $\omega = m/n$, $n > 0$ と表すことができる. ω が整数ではないとすると, ユークリッドの互除法によって,

$$\begin{aligned}
m &= a_0 n + r_1, && 0 < r_1 < n,\\
n &= a_1 r_1 + r_2, && 0 < r_2 < r_1,\\
r_1 &= a_2 r_2 + r_3, && 0 < r_3 < r_2,\\
&\cdots\cdots, &&\\
r_{n-1} &= a_n r_n + r_{n+1}, && 0 < r_{n+1} < r_n,\\
r_n &= a_{n+1} r_{n+1} &&
\end{aligned}$$

となるような整数 a_0, a_1, …, a_n, a_{n+1}, r_1, r_2, …, r_n, r_{n+1} が存在する. ここで, n, r_1, r_2, …, r_n はすべて正なので, a_1, a_2, …, a_n も正である. 上の式を書き直せば,

$$\begin{aligned}
\frac{m}{n} &= a_0 + \frac{r_1}{n} = a_0 + \frac{1}{n/r_1},\\
\frac{n}{r_1} &= a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{r_1/r_2},\\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{r_2/r_3},\\
&\cdots\cdots,\\
\frac{r_{n-1}}{r_n} &= a_n + \frac{r_{n+1}}{r_n} = a_n + \frac{1}{r_n/r_{n+1}},\\
\frac{r_n}{r_{n+1}} &= a_{n+1}
\end{aligned}$$

となる. したがって, 下から上に式を次々に代入していけば,

$$\omega = \frac{m}{n} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{n+1}} = [a_0, a_1, \ldots, a_{n+1}]$$

が得られる. よって, 次の定理が成り立つ.

[定理 4.1] 任意の有理数 q に対して, ある整数 a_0 と正の整数 a_1, a_2, …, a_n, a_{n+1} が存在して

$$q = [a_0, a_1, \ldots, a_n, a_{n+1}]$$

が成り立つ.

今の場合, $\omega_1 = n/r_1$, $\omega_2 = r_1/r_2$, $\omega_3 = r_2/r_3$, …, $\omega_n = r_{n-1}/r_n$, $\omega_{n+1} = r_n/r_{n+1}$ である. したがって, ω が有理数の場合, 連分数展開は必ず有限で止まることがわかる.

[例 4.2]

$$\frac{10}{7} = 1 + \frac{3}{7} = 1 + \cfrac{1}{\cfrac{7}{3}} = 1 + \cfrac{1}{2 + \cfrac{1}{3}} = [1, 2, 3].$$

[例 4.3]

$$-\frac{26}{7} = -4 + \frac{2}{7} = 1 + \cfrac{1}{\cfrac{7}{2}} = -4 + \cfrac{1}{3 + \cfrac{1}{2}} = [-4, 3, 2].$$

[例 4.4]

$$3.14 = 3 + \frac{14}{100} = 3 + \frac{7}{50} = 3 + \cfrac{1}{\cfrac{50}{7}} = 3 + \cfrac{1}{7 + \cfrac{1}{7}} = [3, 7, 7].$$

ω が無理数の場合, もし仮にある番号 n について ω_{n+1} が整数になるとすると,

$$\omega = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n + \cfrac{1}{\omega_{n+1}}}}}$$

が成り立つので, 定理 1.1 に反する. ゆえに, 任意の番号 $n \geq 1$ に対して ω_n は整数にはならない. したがって, ω が無理数の場合, ω の連分数展開は無限に続く.

[例 4.5 ($\sqrt{2}$ の連分数展開)]

$$\begin{aligned}
\sqrt{2} &= 1 + (\sqrt{2} - 1) = 1 + \cfrac{1}{\sqrt{2} + 1} \\
&= 1 + \cfrac{1}{2 + (\sqrt{2} - 1)} = 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2} + 1}} \\
&= \cdots\cdots
\end{aligned}$$

［例 4.6（$\sqrt{3}$ の連分数展開）］

$$\sqrt{3} = 1 + (\sqrt{3} - 1) = 1 + \frac{2}{\sqrt{3}+1} = 1 + \cfrac{1}{\cfrac{\sqrt{3}+1}{2}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{\sqrt{3}-1}{2}} = 1 + \cfrac{1}{1 + \cfrac{1}{\sqrt{3}+1}}$$

$$= 1 + \cfrac{1}{1 + \cfrac{1}{2 + (\sqrt{3}-1)}}$$

$$= \cdots\cdots$$

［定理 4.7］ ω を実数とする．ある整数列 (a_n) が存在して，すべての番号 $n \geq 1$ に対して $a_n \geq 1$ であり，数列 (c_n) を

$$c_n = [a_0, a_1, a_2, \ldots, a_n] \quad (n = 0, 1, 2, \ldots)$$

によって定めるとき，

$$\lim_{n\to\infty} c_n = \omega$$

が成り立つとする．このとき，ω は無理数である．

［証明］ もし仮に ω が有理数ならば，定理 4.1 より，ある整数 b_0 と正の整数 b_1, b_2, …, b_m が存在して

$$\omega = [b_0, b_1, \ldots, b_m]$$

が成り立つ．

$\lim_{n\to\infty} c_n = \omega$ のとき，偶数番号のみの列 (c_{2k}) と奇数番号のみの列 (c_{2k+1}) は (c_n) の部分列であり，これらもまた ω に収束する．定理 2.6 より，任意の整数 $k \geq 0$ に対して

$$c_{2k} < \omega < c_{2k+1}$$

でなければならない．定理 3.7 より，$n > m$ を満たす番号 n に対して，ある実数 s が存在して，$s > a_{n+1} \geq 1$ かつ

$$[b_0, b_1, \ldots, b_m] = [a_0, a_1, \ldots, a_n, s]$$

となる．したがって定理 1.7 より

$$b_m = [a_m, a_{m+1}, \ldots, a_n, s]$$

が得られる．ところが，b_m は整数であると同時に $[a_m, a_{m+1}, \ldots, a_n, s]$ は整数ではない．これは矛盾である．したがって ω は無理数でなければならない． □

5　無理数の連分数による近似

この節では, ω を無理数とし,

$$\omega = [a_0, a_1, \ldots, a_{n-1}, \omega_n] \quad (n = 0, 1, 2, \ldots)$$

を ω の連分数展開とする. ω の連分数展開によって整数列 (a_n) が定まる. このとき, すべての番号 $n \geq 1$ に対して $a_n \geq 1$, $\omega_n > 1$ である. 数列 (a_n) に対して, 数列 (p_n), (q_n) を, 漸化式

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \quad p_{-1} = 1, \quad p_{-2} = 0, \\ q_n &= a_n q_{n-1} + q_{n-2}, \quad q_{-1} = 0, \quad q_{-2} = 1 \end{aligned}$$

によって定義する. 定理 3.4 より,

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}$$

が成り立つ. p_n/q_n を ω の n 次の**近似分数**という.

[定理 5.1] すべての番号 $n \geq 0$ に対して

$$\omega - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(q_n\omega_{n+1} + q_{n-1})} \tag{18}$$

が成り立つ.

[証明] 定理 3.1 より,

$$[a_0, a_1, \ldots, a_n, \omega_{n+1}] = \frac{\omega_{n+1}p_n + p_{n-1}}{\omega_{n+1}q_n + q_{n-1}}$$

である. よって

$$\begin{aligned} \omega - \frac{p_n}{q_n} &= [a_0, a_1, \ldots, a_n, \omega_{n+1}] - \frac{p_n}{q_n} \\ &= \frac{\omega_{n+1}p_n + p_{n-1}}{\omega_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \\ &= \frac{q_n(\omega_{n+1}p_n + p_{n-1}) - p_n(\omega_{n+1}q_n + q_{n-1})}{q_n(\omega_{n+1}q_n + q_{n-1})}. \end{aligned}$$

さらに分子を計算すると, 定理 2.5 より,

$$\begin{aligned} &q_n(\omega_{n+1}p_n + p_{n-1}) - p_n(\omega_{n+1}q_n + q_{n-1}) \\ &\quad = -(p_n q_{n-1} - q_n p_{n-1}) = -(-1)^{n-1} = (-1)^n. \end{aligned}$$

ゆえに式 (18) が成り立つ. □

[定理 5.2]

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < \frac{p_{2k}}{q_{2k}} < \frac{p_{2k+2}}{q_{2k+2}} < \cdots < \omega < \cdots < \frac{p_{2k+3}}{q_{2k+3}} < \frac{p_{2k+1}}{q_{2k+1}} < \cdots < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

[証明] $n \geq 0$ を整数とする. 定理 5.1 より,

$$\omega - \frac{p_n}{q_n} = \frac{(-1)^n}{q_n(q_n\omega_{n+1} + q_{n-1})}.$$

$q_{n-1} > 0$, $q_n > 0$, $\omega_{n+1} > 1$ なので,

$$n \text{ が偶数} \Longrightarrow \omega - \frac{p_n}{q_n} > 0 \Longrightarrow \omega > \frac{p_n}{q_n},$$
$$n \text{ が奇数} \Longrightarrow \omega - \frac{p_n}{q_n} < 0 \Longrightarrow \omega < \frac{p_n}{q_n}$$

となる. つまり, n が偶数のとき p_n/q_n は常に ω より小さく, n が奇数のとき p_n/q_n は常に ω より大きい. このことと定理 2.6 と合わせれば, 求める定理が得られる. □

[定理 5.3] 任意の整数 $n \geq 1$ に対して

$$\left|\omega - \frac{p_n}{q_n}\right| < \left|\omega - \frac{p_{n-1}}{q_{n-1}}\right| \tag{19}$$

が成り立つ.

[証明] 定理 3.1 より,

$$\omega = \frac{\omega_{n+1}p_n + p_{n-1}}{\omega_{n+1}q_n + q_{n-1}}.$$

両辺に $\omega_{n+1}q_n + q_{n-1}$ を掛けると,

$$(\omega_{n+1}q_n + q_{n-1})\omega = \omega_{n+1}p_n + p_{n-1}.$$

よって,

$$\omega_{n+1}(\omega q_n - p_n) = -(\omega q_{n-1} - p_n) = -q_{n-1}\left(\omega - \frac{p_{n-1}}{q_{n-1}}\right).$$

$\omega_{n+1}q_n$ で割り, 絶対値をとると,

$$\left|\omega - \frac{p_n}{q_n}\right| = \left|\frac{q_{n-1}}{\omega_{n+1}q_n}\right| \cdot \left|\omega - \frac{p_{n-1}}{q_{n-1}}\right|.$$

$0 < q_{n-1} < q_n$ かつ $1 < \omega_{n+1}$ より

$$0 < \frac{q_{n-1}}{\omega_{n+1}q_n} < 1.$$

したがって式 (19) が成り立つ. □

[定理 5.4] 任意の整数 $n \geq 0$ に対して

$$\left|\omega - \frac{p_n}{q_n}\right| > \frac{1}{2q_nq_{n+1}} \tag{20}$$

が成り立つ.

[証明] 定理 5.3 より

$$\left|\omega - \frac{p_{n+1}}{q_{n+1}}\right| < \left|\omega - \frac{p_n}{q_n}\right|$$

なので,

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \leq \left|\omega - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\omega - \frac{p_n}{q_n}\right| < 2\left|\omega - \frac{p_n}{q_n}\right|.$$

また, 定理 2.5 より

$$p_{n+1}q_n - p_nq_{n-1} = (-1)^n$$

なので,

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{|p_{n+1}q_n - p_nq_{n-1}|}{q_nq_{n+1}} = \frac{1}{q_nq_{n+1}}.$$

ゆえに, 式 (20) が得られる. □

[定理 5.5] 任意の番号 $n \geq 0$ に対して

$$\left|\omega - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}} \leq \frac{1}{q_n^2}$$

が成り立つ.

[証明] $q_n > 0$, $q_{n+1} > 0$, $\omega_{n+1} > a_{n+1}$ であるから,

$$q_n\omega_{n+1} + q_{n-1} > q_na_{n+1} + q_{n-1} = q_{n+1}.$$

よって, 定理 5.1 より,

$$\begin{aligned}\left|\omega - \frac{p_n}{q_n}\right| &= \left|\frac{(-1)^n}{q_n(q_n\omega_{n+1} + q_{n-1})}\right| \\ &= \frac{1}{q_n(q_n\omega_{n+1} + q_{n-1})} < \frac{1}{q_nq_{n+1}}.\end{aligned}$$

また, 定理 2.1 (および注意 2.2) より, すべての番号 $n \geq 0$ に対して $1 \leq q_n \leq q_{n+1}$ だから, 後半の不等式も成り立つ. □

[定理 5.6] 任意の番号 $n \geq 0$ に対して, ある δ_n が存在して,

$$p_n = q_n\omega + \frac{\delta_n}{q_n}, \quad |\delta_n| < 1$$

が成り立つ.

[証明] $\delta_n = q_n(p_n - q_n\omega)$ とおく. この両辺を q_n で割ったのち $q_n\omega$ を移項すると定理の前半の等式が得られる.

さて, 定理 5.5 より,

$$\left|\omega - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

$q_n \geq 1$ より, 両辺を q_n で割ると,

$$|q_n\omega - p_n| < \frac{1}{q_n}.$$

絶対値を外すと,

$$-\frac{1}{q_n} < p_n - q_n\omega < \frac{1}{q_n}.$$

各辺に q_n を掛ければ,

$$-1 < q_n(p_n - q_n\omega) < 1.$$

すなわち, $-1 < \delta_n < 1$. したがって, 定理の後半の不等式が成り立つ. □

[定理 5.7]

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \omega.$$

[証明] 定理 5.5 より, 任意の番号 $n \geq 0$ に対して

$$\left|\omega - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$$

が成り立つ. 一方, 定理 2.4 より $q_n \to \infty$ $(n \to \infty)$ であるから, $1/q_n^2 \to \infty$ $(n \to \infty)$ である. したがって, $\omega - p_n/q_n \to 0$ $(n \to \infty)$ となる. □

[定理 5.8] ω を無理数, p_n/q_n $(n \geq 0)$ を ω の近似分数とする. p, q を整数とし, $q > 0$ とする. このとき,

$$|q\omega - p| < |q_n\omega - p_n| \Longrightarrow q_{n+1} \leq q$$

が成り立つ.

[証明] 背理法により証明する. $|q\omega - p| < |q_n\omega - p_n|$ かつ $1 \leq q < q_{n+1}$ と仮定して矛盾を導く.
まず, 連立方程式

$$\begin{aligned} p_n x + p_{n+1} y &= p, \\ q_n x + q_{n+1} y &= q \end{aligned} \tag{21}$$

を解く. 1 番目の方程式に q_n を掛け, 2 番目の方程式に p_n を掛けたのち, 後者から前者を引くと,

$$(p_{n+1}q_n - p_n q_{n+1})y = pq_n - qp_n.$$

定理 2.5 より $p_{n+1}q_n - p_n q_{n+1} = (-1)^n$ だから,

$$y = (-1)^n(pq_n - qp_n).$$

同様に, 1 番目の方程式に q_{n+1} を掛け, 2 番目の方程式に p_{n+1} を掛けたのち, 前者から後者を引くと,

$$(p_{n+1}q_n - p_n q_{n+1})x = qp_{n+1} - pq_{n+1}.$$

よって,

$$x = (-1)^n(qp_{n+1} - pq_{n+1}).$$

が得られる. しがたって, 連立方程式 (21) は解 (x, y) を持つ.

次に, $x \neq 0$, $y \neq 0$ を示す. もし仮に $x = 0$ とすると, $qp_{n+1} = pq_{n+1}$. 定理 2.5 より $\gcd(p_n, q_n) = 1$ であるから, $q_{k+1} \mid q$. これは $q \leq q_{n+1}$ を意味するから背理法の仮定に反する. ゆえに, $x \neq 0$. また, これより $|x| \geq 1$ だから,

$$|x||q_n\omega - p_n| \geq |q_n\omega - p_n|.$$

もし $y = 0$ ならば, $p_n x = p$, $q_n x = q$ なので,

$$q\omega - p = x(q_n\omega - p_n).$$

ゆえに,

$$|q\omega - p| = |x||q_n\omega - p_n| \geq |q_n\omega - p_n|.$$

これは仮定に反する. ゆえに $y \neq 0$.

x と y の符号は互いに異なる. 実際,

$$\begin{aligned} y < 0 &\Longrightarrow q_n x = q - q_{n+1}y > 0 \\ &\Longrightarrow x > 0, \\ y > 0 &\Longrightarrow q_{n+1}y \geq q_{n+1} > q \\ &\Longrightarrow q_n x = q - q_{n+1}y < 0 \\ &\Longrightarrow x < 0. \end{aligned}$$

ω は無理数なので, 定理 5.2 より $p_n/q_n < \omega < p_{n+1}/q_{n+1}$ または $p_{n+1}/q_{n+1} < \omega < p_n/q_n$. どちらの場合からも, $q_n\omega - p_n$ と $q_{n+1}\omega - p_n$ の符号が異なることがいえる.

x, y は連立方程式 (21) の解だったので,

$$\begin{aligned} |q\omega - p| &= |(q_n x + q_{n+1}y)\omega - (p_n x + p_{n+1}y)| \\ &= |x(q_n\omega - p_n) + y(q_{n+1}\omega - p_{n+1})|. \end{aligned}$$

先に述べたことから, $x(q_n\omega - p_n)$ と $y(q_{n+1}\omega - p_n)$ の符号は同じである. このことと $|x| \geq 1$ より,

$$\begin{aligned} |q\omega - p| &= |x||q_n\omega - p_n| + |y||q_{n+1}\omega - p_{n+1}| \\ &\geq |x||q_n\omega - p_n| \\ &\geq |q_n\omega - p_n|. \end{aligned}$$

これは仮定に反する. 背理法の仮定から矛盾が導かれたので, 定理の主張は示された. □

[定理 5.9] ω を無理数, p_n/q_n $(n \geq 1)$ を ω の近似分数とする. また, p/q を既約分数とする. すなわち, p, $q \in \mathbb{Z}$, $q > 0$, $\gcd(p, q) = 1$ とする. このとき,

$$\left|\omega - \frac{p}{q}\right| < \left|\omega - \frac{p_n}{q_n}\right| \Longrightarrow q_n < q$$

が成り立つ.

[証明] 背理法により証明する.

$n \geq 1$ とし, $|\omega - p/q| < |\omega - p_n/q_n|$ かつ $1 \leq q \leq q_n$ と仮定すると,

$$|q\omega - p| = q\left|\omega - \frac{p}{q}\right| < q_n\left|\omega - \frac{p_n}{q_n}\right| = |q_n\omega - p_n|.$$

よって, 定理 5.8 より, $q_{n+1} \leq q$. ゆえに, $q_{n+1} \leq q_n$. 仮定より $n \geq 1$ だから, これは定理 2.1 に反する. □

[定理 5.10] ω を無理数, p/q を既約分数とする. すなわち, p, $q \in \mathbb{Z}$, $q > 0$, $\gcd(p, q) = 1$ とする. このとき,

$$\left|\omega - \frac{p}{q}\right| < \frac{1}{2q^2}$$

ならば, p/q は ω の近似分数である.

[証明] 背理法により証明する. $|\omega - p/q| < 1/2q^2$ かつ p/q が ω の近似分数に一致しないと仮定すると, 任意の番号 $n \geq 0$ に対して, $p/q \neq p_n/q_n$ より $|qp_n - pq_n| \geq 1$ だから,

$$\begin{aligned}
\frac{1}{qq_n} \leq \frac{|qp_n - pq_n|}{qq_n} &= \left|\frac{qp_n - pq_n}{qq_n}\right| = \left|\frac{p_n}{q_n} - \frac{p}{q}\right| \\
&= \left|\left(\frac{p_n}{q_n} - \omega\right) + \left(\omega - \frac{p}{q}\right)\right| \\
&\leq \left|\omega - \frac{p_n}{q_n}\right| + \left|\omega - \frac{p}{q}\right| \\
&< \left|\omega - \frac{p_n}{q_n}\right| + \frac{1}{2q^2}.
\end{aligned}$$

$q_0 = 1$ であり, 定理 2.1 より数列 (q_n) は $n \geq 1$ で単調増加だから, ある番号 $k \geq 0$ が存在して, $q_k \leq q < q_{k+1}$. よって, 定理 5.8 と仮定より,

$$\begin{aligned}
\left|\omega - \frac{p_k}{q_k}\right| &= \frac{|q_k\omega - p_k|}{q_k} \\
&\leq \frac{|q\omega - p|}{q_k} = \frac{q}{q_k}\left|\omega - \frac{p}{q}\right| \\
&< \frac{1}{2qq_k}.
\end{aligned}$$

ゆえに,

$$\frac{1}{qq_k} < \left|\omega - \frac{p_k}{q_k}\right| + \frac{1}{2q^2} < \frac{1}{2qq_k} + \frac{1}{2q^2}.$$

したがって, $q < q_k$ が得られるが, これは $q_k \leq q$ に反する. □

[定理 5.11] ω を無理数とする. ω の任意の 2 つの連続した近似分数 p_n/q_n, p_{n+1}/q_{n+1} について,

$$\left|\omega - \frac{p_n}{q_n}\right| < \frac{1}{2q_n^2} \quad \text{または} \quad \left|\omega - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2q_{n+1}^2} \tag{22}$$

が成り立つ.

[証明] 番号 $n \geq 0$ を 1 つ固定する.

定理 5.2 より, $p_n/q_n < \omega < p_{n+1}/q_{n+1}$ または $p_{n+1}/q_{n+1} < \omega < p_n/q_n$. 前者の場合,

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} = \left(\frac{p_{n+1}}{q_{n+1}} - \omega\right) + \left(\omega - \frac{p_n}{q_n}\right)$$

かつ

$$\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} > 0, \quad \frac{p_{n+1}}{q_{n+1}} - \omega > 0, \quad \omega - \frac{p_n}{q_n} > 0$$

より,

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\omega - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\omega - \frac{p_n}{q_n}\right|.$$

後者の場合にも, これと同じ等式が得られる. 一方, 定理 2.5 より $p_{n+1}q_n - p_nq_{n+1} = (-1)^n$ だから,

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{|p_{n+1}q_n - p_nq_{n+1}|}{q_nq_{n+1}} = \frac{1}{q_nq_{n+1}}.$$

ゆえに,

$$\left|\omega - \frac{p_{n+1}}{q_{n+1}}\right| + \left|\omega - \frac{p_n}{q_n}\right| = \frac{1}{q_nq_{n+1}}.$$

さて, (22) が成り立たないとすると,

$$\frac{1}{2q_{n+1}^2} + \frac{1}{2q_n^2} \leq \frac{1}{q_nq_{n+1}}.$$

両辺に $2q_n^2q_{n+1}^2$ を掛けて整理すると, $(q_n - q_{n+1})^2 \leq 0$ が得られる. すなわち, $q_n = q_{n+1}$.

もし $n \geq 1$ ならば, 定理 2.1 より $q_n < q_{n+1}$ だから, これは不可能である. ゆえに, $n = 0$ でなければならないが, このとき, $q_1 = q_0 = 1$. さらに, $q_1 = a_1q_0 + q_{-1} = a_1$ より $a_1 = 1$. 定理 5.2 より

$$\frac{p_2}{q_2} < \omega < \frac{p_1}{q_1}$$

であり,

$$\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} = a_0 + 1,$$
$$\frac{p_2}{q_2} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = a_0 + \frac{1}{1 + \dfrac{1}{a_2}} = a_0 + \frac{a_2}{a_2 + 1}$$

であるから,

$$0 < \frac{p_1}{q_1} - \omega < \frac{p_1}{q_1} - \frac{p_2}{q_2} = \frac{a_2}{a_2 + 1} \leq \frac{1}{2}.$$

したがって, 不等式 (22) が成り立つことになって, 矛盾が生じる. □

[定理 5.12] $\omega > 0$ を無理数とし, x/y を既約分数とするとき, x/y が ω の近似分数ならば, y/x は $1/\omega$ の近似分数である.

[証明] まず, $\omega > 1$ のとき, ω の連分数展開を

$$\omega = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

とすると, $1/\omega$ の連分数展開は

$$\frac{1}{\omega} = 0 + \frac{1}{a_0} + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

となる. ここで, $\omega > 1$ より $a_0 \geq 1$ であることに注意せよ. x/y を ω の n 番目の近似分数とすると,

$$\frac{x}{y} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

である. このとき, y/x は

$$\frac{y}{x} = 0 + \frac{1}{a_0} + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n}$$

となり, $1/\omega$ の $n+1$ 番目の近似分数である.

$0 < \omega < 1$ のときは, $\omega > 1$ の場合を $1/\omega$ に適用すればよい. つまり, $1/\omega$ の連分数展開を

$$\frac{1}{\omega} = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

とすれば, $1/(1/\omega) = \omega$ の連分数展開は

$$\omega = 0 + \frac{1}{a_0} + \frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} + \cdots$$

となる. x/y を ω の n 番目の近似分数とすれば, y/x は $1/\omega$ の $n-1$ 番目の近似分数である. □

6 $GL_2(\mathbb{Z})$ と $SL_2(\mathbb{Z})$

整数成分の 2 次正方行列でその行列式が ± 1 のもの全体を $GL_2(\mathbb{Z})$ とおく:

$$GL_2(\mathbb{Z}) = \left\{ P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \;\middle|\; p, q, r, s \in \mathbb{Z},\ \det P = ps - qr = \pm 1 \right\}.$$

[定理 6.1] $GL_2(\mathbb{Z})$ は群をなす.

[証明] 任意の 2 つの行列 P, $Q \in GL_2(\mathbb{Z})$ に対して,

$$\det PQ = \det P \det Q = \pm 1$$

より, 積 PQ も $GL_2(\mathbb{Z})$ に属する.

$GL_2(\mathbb{Z})$ の単位元は単位行列 $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ である.

任意の $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$ に対して, その逆行列 $P^{-1} = \dfrac{1}{\det P} \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}$ が $GL_2(\mathbb{Z})$ における P の逆元である. □

整数成分の 2 次正方行列でその行列式が 1 のもの全体を $SL_2(\mathbb{Z})$ とおく:

$$SL_2(\mathbb{Z}) = \left\{ P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \;\middle|\; p, q, r, s \in \mathbb{Z},\ \det P = ps - qr = 1 \right\}$$
$$= \{ P \in GL_2(\mathbb{Z}) \mid \det P = 1 \}.$$

[定理 6.2] $SL_2(\mathbb{Z})$ は $GL_2(\mathbb{Z})$ の指数 2 の部分群である.

[証明] 任意の $P, Q \in GL_2(\mathbb{Z})$ に対して $\det PQ = \det P \det Q$ が成り立つことから, 写像

$$GL_2(\mathbb{Z}) \to \{\pm 1\}, \quad P \mapsto \det P$$

は群の準同型である. その核は $SL_2(\mathbb{Z})$ である. さらに, 準同型定理により,

$$GL_2(\mathbb{Z})/SL_2(\mathbb{Z}) \cong \{\pm 1\}.$$

ゆえに, $[GL_2(\mathbb{Z}) : SL_2(\mathbb{Z})] = 2$. □

[定理 6.3] $SL_2(\mathbb{Z})$ は $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ によって生成される.

[証明] $S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ とおく.

$$\det S = \det T = 1$$

より, $S, T \in SL_2(\mathbb{Z})$.

S, T で生成される $SL_2(\mathbb{Z})$ の部分群を Γ とおく. $SL_2(\mathbb{Z}) \neq \Gamma$ と仮定して矛盾を導く.

$\begin{bmatrix} p & q \\ 0 & s \end{bmatrix} \in SL_2(\mathbb{Z})$ とすると, $ps - q \cdot 0 = 1$ より $p = s = \pm 1$. 一方,

$$\begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} = S^q, \quad \begin{bmatrix} -1 & q \\ 0 & -1 \end{bmatrix} = S^{-q} T^2$$

であるから, $\begin{bmatrix} p & q \\ 0 & s \end{bmatrix} \in \Gamma$ となる. よって,

$$r_0 = \min \left\{ |r| \;\middle|\; \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{Z}) \setminus \Gamma \right\}$$

とおくと, $r_0 \geq 1$ である. $SL_2(\mathbb{Z}) \setminus \Gamma$ の元で $(2,1)$-成分が r_0 のものをとり, $P_0 = \begin{bmatrix} p_0 & q_0 \\ r_0 & s_0 \end{bmatrix}$ とおく. 除法の原理により, ある n, $n' \in \mathbb{Z}$ が存在して,

$$s_0 = r_0 n + n', \quad 0 \leq n' < r_0.$$

よって,

$$0 \leq |s_0 - r_0 n| < r_0.$$

このとき, r_0 の最小性から,

$$P_0 S^{-1} T = \begin{bmatrix} q_0 - p_0 n & -p_0 \\ s_0 - r_0 n & -r_0 \end{bmatrix} \in \Gamma.$$

一方, $S^{-1}T \in \Gamma$ より, $P_0 \in \Gamma$. これは矛盾である. ゆえに, $SL_2(\mathbb{Z}) = \Gamma$. □

7 複素数の対等関係

$GL_2(\mathbb{Z})$ の $\mathbb{C} \cup \{\infty\}$ への作用を, 各々の $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$, $x \in \mathbb{C} \cup \{\infty\}$ に対して, $r \neq 0$ のとき,

$$P \cdot x = \begin{cases} \dfrac{px+q}{rx+s}, & x \neq \infty,\ x \neq -s/r \text{ のとき} \\ \dfrac{p}{r}, & x = \infty \text{ のとき} \\ \infty, & x = -s/r \text{ のとき} \end{cases}$$

$r = 0$ のとき,

$$P \cdot x = \begin{cases} \dfrac{px+q}{s}, & x \neq \infty \text{ のとき} \\ \infty, & x = \infty \text{ のとき} \end{cases}$$

とおくことによって定める.

[例 7.1] $\begin{bmatrix} 1 & \pm q \\ 0 & 1 \end{bmatrix} \cdot x = x \pm q$. ただし, $\pm$ は複号同順.

$P \in GL_2(\mathbb{Z})$ ならば $-P \in GL_2(\mathbb{Z})$ である. また一般に, 作用の定め方から, 任意の $x \in \mathbb{C} \cup \{\infty\}$ に対して $P \cdot x = (-P) \cdot x$ であることはすぐにわかる.

[例 7.2] $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot x = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot x = -1/x.$

[定理 7.3] $GL_2(\mathbb{Z})$ は実際に $\mathbb{C} \cup \{\infty\}$ に作用する.

[証明] $x \in \mathbb{C} \cup \{\infty\}$ とする. $E \cdot x = x$ は明らかである.
$P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$, $Q = \begin{bmatrix} p' & q' \\ r' & s' \end{bmatrix} \in GL_2(\mathbb{Z})$ とする.
$x \neq \infty$, $r'x + s' \neq 0$, $(rp' + sr')x + (rq' + ss') \neq 0$ のとき,

$$\begin{aligned} PQ \cdot x &= \begin{bmatrix} pp' + qr' & pq' + qs' \\ rp' + sr' & rq' + ss' \end{bmatrix} \cdot x \\ &= \frac{(pp' + qr')x + (pq' + qs')}{(rp' + sr')x + (rq' + ss')}, \end{aligned}$$

$$\begin{aligned} P \cdot (Q \cdot x) = P \cdot \frac{p'x + q'}{r'x + s'} &= \frac{p \cdot \dfrac{p'x + q'}{r'x + s'} + q}{r \cdot \dfrac{p'x + q'}{r'x + s'} + s} \\ &= \frac{p(p'x + q') + q(r'x + s')}{r(p'x + q') + s(r'x + s')} \\ &= \frac{(pp' + qr')x + (pq' + qs')}{(rp' + sr')x + (rq' + ss')}. \end{aligned}$$

$x = \infty$ のとき,

$$PQ \cdot \infty = \begin{cases} \dfrac{pp' + qr'}{rp' + sr'}, & r' \neq 0 \text{ のとき} \\ \dfrac{p}{r}, & r' = 0 \text{ かつ } r \neq 0 \text{ のとき} \\ \infty, & r' = r = 0 \text{ のとき} \end{cases}$$

一方,

$$Q \cdot \infty = \begin{cases} \dfrac{p'}{r'}, & r' \neq 0 \text{ のとき} \\ \infty, & r' = 0 \text{ のとき} \end{cases}$$

であり, さらに,

$$P \cdot \infty = \begin{cases} \dfrac{p}{r}, & r \neq 0 \text{ のとき} \\ \infty, & r = 0 \text{ のとき} \end{cases}$$

$$P \cdot \frac{p'}{r'} = \frac{pp' + qr'}{rp' + sr'}$$

である.

$r'x+s'=0$ のとき, もし仮に $r'=0$ とすると, 同時に $s'=0$ となるが,

$$p's'-q'r'=\det Q\neq 0$$

より不可能である. よって, $x=-s'/r'$. このとき, $P\cdot(Q\cdot x)=P\cdot\infty=p/r$. 一方, 直接計算すると $PQ\cdot x=p/r$ となることがわかる.

$(rp'+sr')x+(rq'+ss')=0$ のとき, もし仮に $rp'+sr'=0$ とすると, 同時に $rq'+ss'=0$ となるが,

$$(pp'+qr')(rq'+ss')-(pq'+qs')(rp'+sr')=\det PQ\neq 0$$

より不可能である. よって, $x=-(rq'+ss')/(rp'+sr')$. このとき, $PQ\cdot x=\infty$. 一方, 直接計算すると $Q\cdot x=-s/r$ となることがわかり, $P\cdot(Q\cdot x)=\infty$ となる.

以上より, いずれの場合においても $PQ\cdot x=P\cdot(Q\cdot x)$ が成り立つことが示された. したがって, $P\cdot x$ によって $GL_2(\mathbb{Z})$ は実際に $\mathbb{C}\cup\{\infty\}$ に作用している. □

$x,\,y\in\mathbb{C}\cup\{\infty\}$ とするとき, x が y に**対等**であるとは, ある行列 $P\in GL_2(\mathbb{Z})$ が存在して

$$x=P\cdot y$$

が成り立つことをいう. $x,\,y\in\mathbb{C}$ のとき, x が y に対等であることは, ある整数 $p,\,q,\,r,\,s$ が存在して

$$x=\frac{py+q}{ry+s},\quad ps-qr=\pm 1$$

が成り立つことと言い換えられる.

特に, $\det P=1$ のとき**正に対等**であるといい, $\det P=-1$ のとき**負に対等**であるという.

$z,\,w\in\mathbb{C}\cup\{\infty\}$ が正に対等であることは, ある $P\in SL_2(\mathbb{Z})$ が存在して $w=P\cdot z$ となることと同値である.

[注意 7.4] 2 つの数が正に対等かつ負に対等になることもある. 例えば, $\sqrt{2}+1$ は $\sqrt{2}$ に正にも負にも対等である. 実際,

$$\sqrt{2}+1=\frac{\sqrt{2}+1}{0\cdot\sqrt{2}+1},\quad \begin{vmatrix}1 & 1\\ 0 & 1\end{vmatrix}=1$$

かつ

$$\sqrt{2}+1=\frac{1}{\sqrt{2}-1},\quad \begin{vmatrix}0 & 1\\ 1 & -1\end{vmatrix}=-1.$$

[定理 7.5] 対等および正に対等なる関係は $\mathbb{C}\cup\{\infty\}$ 上の同値関係である.

[証明] $x, y, z \in \mathbb{C} \cup \{\infty\}$ を任意にとる.

(反射)　$x = E \cdot x$ より, x は x 自身に対等である.

(対称)　x が y に対等ならば, ある $P \in GL_2(\mathbb{Z})$ が存在して, $x = P \cdot y$. このとき,

$$y = E \cdot y = (P^{-1}P) \cdot y = P^{-1} \cdot (P \cdot y) = P^{-1} \cdot x.$$

ゆえに, y は x に対等である.

(推移)　x が y に対等かつ y が z に対等ならば, ある $P, Q \in GL_2(\mathbb{Z})$ が存在して, $x = P \cdot y$ かつ $y = Q \cdot z$. このとき, $x = P \cdot (Q \cdot z) = PQ \cdot z$ となり, x は z に対等である.

以上より, 対等関係は同値関係であることが示された.

$GL_2(\mathbb{Z})$ を $SL_2(\mathbb{Z})$ に置き換えれば, 正に対等な関係が $\mathbb{C} \cup \{\infty\}$ 上の同値関係であることも同様にして証明できる. □

[定理 7.6]　(i) 有理数か ∞ に対等なものは有理数か ∞ である.

(ii) 無理数に対等なものは無理数である.

(iii) 虚数に対等なものは虚数である.

[証明] 対等関係の定め方から, 任意の $P \in GL_2(\mathbb{Z})$, $x \in \mathbb{Q} \cup \{\infty\}$ に対して, $P \cdot x \in \mathbb{Q} \cup \{\infty\}$. すなわち, 有理数か ∞ に対等なものは有理数か ∞ である. 対偶を考えれば, 無理数か虚数に対等なものは無理数か虚数である.

$x, y \in \mathbb{C}$ が互いに対等であるとき, ある $P \in GL_2(\mathbb{Z})$ が存在して $x = P \cdot y$ となる. もし仮に x が虚数, y が無理数だとすれば, 右辺は実数であり, x が虚数であることに反する. また, もし仮に x が無理数, y が虚数だとすれば, $y = P^{-1} \cdot x$ よりやはり矛盾が生じる. □

[定理 7.7] $\mathbb{Q} \cup \{\infty\}$ に属する任意の 2 つの元は互いに正に対等である.

[証明] 有理数を任意にとり, 既約分数 p/r で表すと, $\gcd(p, r) = 1$ より, $ps - qr = 1$ を満たすような $q, s \in \mathbb{Z}$ が存在する.

$$P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$$

とおくと, $P \in SL_2(\mathbb{Z})$ であり,

$$\frac{p}{r} = P \cdot \infty.$$

ゆえに, 任意の有理数と ∞ とは正に対等である.

有理数をもう 1 つ任意にとり, 既約分数 p'/r' で表すと, p/r のときと同様にして, ある $Q \in SL_2(\mathbb{Z})$ が存在して

$$\frac{p'}{r'} = Q \cdot \infty.$$

ゆえに,

$$\frac{p}{r} = PQ^{-1} \cdot \frac{p'}{r'}, \quad PQ^{-1} \in SL_2(\mathbb{Z}).$$

すなわち, p/r は p'/r' に対等である. したがって, 任意の 2 つの有理数は正に対等である. □

[例 7.8] 2 次方程式 $x^2 + bx + c = 0$ の 2 つの解

$$\theta = \frac{-b + \sqrt{b^2 - 4c}}{2}, \quad \overline{\theta} = \frac{-b - \sqrt{b^2 - 4c}}{2}$$

は互いに対等である. 実際, $P = \begin{bmatrix} -1 & -b \\ 0 & 1 \end{bmatrix}$ とおくと, $\det P = -1$ かつ $\theta = P \cdot \overline{\theta}$ が成り立つ.

[定理 7.9] $x \in \mathbb{C} \cup \{\infty\}$ とし,

$$GL_2(\mathbb{Z})_x = \{P \in GL_2(\mathbb{Z}) \mid x = P \cdot x\},$$
$$SL_2(\mathbb{Z})_x = \{P \in SL_2(\mathbb{Z}) \mid x = P \cdot x\}$$

とおく. このとき,

(i) $GL_2(\mathbb{Z})_x$ は $GL_2(\mathbb{Z})$ の部分群である.

(ii) $SL_2(\mathbb{Z})_x$ は $SL_2(\mathbb{Z})$ の部分群である.

[証明] (i) E を単位行列とすると, $E \in GL_2(\mathbb{Z})_x$. よって, $GL_2(\mathbb{Z})_x$ は空集合でない.
任意の $P, Q \in GL_2(\mathbb{Z})_x$ に対して,

$$PQ \cdot x = P \cdot (Q \cdot x) = P \cdot x = x,$$
$$P^{-1} \cdot x = P^{-1} \cdot (P \cdot x) = (P^{-1}P) \cdot x = E \cdot x = x.$$

ゆえに, PQ, $P^{-1} \in GL_2(\mathbb{Z})_x$.

(ii) (i) と同様にして示せる. □

[定理 7.10] $S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $T' = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ とおく. また, E を単位行列とする. このとき,

(i) $GL_2(\mathbb{Z})_\infty$ は S, T', $-E$ で生成される $GL_2(\mathbb{Z})$ の部分群である.

(ii) $SL_2(\mathbb{Z})_\infty$ は S, $-E$ で生成される $SL_2(\mathbb{Z})$ の部分群である.

[証明] (i) まず, $P = S$, T', $-E$ のとき, $P \in GL_2(\mathbb{Z})$ であり, $P \cdot \infty = \infty$ は成り立つ.

$P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$ とし, $P \cdot \infty = \infty$ とする. 作用の定め方から, $r = 0$ でなければならない. また,

$$ps = ps - qr = \det P = \pm 1$$

より,

$$p = \pm 1, \quad d = \pm 1 \quad \text{(複号任意)}.$$

すなわち,

$$P = \begin{bmatrix} \pm 1 & q \\ 0 & \pm 1 \end{bmatrix} \quad \text{(複号任意)}.$$

一方,

$$\begin{bmatrix} 1 & q \\ 0 & 1 \end{bmatrix} = S^q, \quad \begin{bmatrix} -1 & q \\ 0 & 1 \end{bmatrix} = T'S^{-q},$$
$$\begin{bmatrix} -1 & q \\ 0 & -1 \end{bmatrix} = -S^{-q}, \quad \begin{bmatrix} 1 & q \\ 0 & -1 \end{bmatrix} = -T'S^q.$$

ゆえに, P は S, T', $-E$ の積で表される.

(ii) $\det P = \pm 1$ を $\det P = 1$ として (i) と同様の議論を行えば, $P \in SL_2(\mathbb{Z})$ の中で $P \cdot \infty = \infty$ となるもの全体 $SL_2(\mathbb{Z})_\infty$ が S, $-E$ で生成されることがいえる. □

[定理 7.11] $x \in \mathbb{C}$ とし, x は 2 次以下の方程式の解ではないとする. このとき, 任意の $P \in GL_2(\mathbb{Z})$ に対して, $x = P \cdot x$ ならば $P = \pm E$ が成り立つ. したがって,

$$GL_2(\mathbb{Z})_x = SL_2(\mathbb{Z})_x = \{\pm E\}.$$

ただし, E は単位行列である.

[証明] $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$ とし,

$$x = P \cdot x = \frac{px + q}{rx + s}$$

であるとする. 分母を払って整理すると,

$$rx^2 + (s - p)x - q = 0.$$

x は 2 次以下の方程式の解ではないと仮定したので,

$$r = s - p = q = 0.$$

$ps - qr = \det P = \pm 1$ より, $p = s = \pm 1$. ゆえに, $P = \pm E$. よって, 定理の前半の主張が示された. また, このことから, $GL_2(\mathbb{Z})_x$, $SL_2(\mathbb{Z})_x$ が $\{\pm E\}$ に含まれることがいえる. 逆の包含関係は明らかなので, 定理の後半の主張も成り立つ. □

8 $SL_2(\mathbb{Z})$ に関する基本領域

複素数 z に対して, その実部, 虚部を $\mathrm{Re}\, z$, $\mathrm{Im}\, z$ で表す: $z = \mathrm{Re}\, z + \mathrm{Im}\, z\sqrt{-1}$.

[補題 8.1] 任意の $z \in \mathbb{C}$, $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$ に対して,

$$\mathrm{Im}\,(P \cdot z) = \frac{\det P \cdot \mathrm{Im}\, z}{|rz + s|^2}$$

が成り立つ.

[証明] ここでは, $\overline{z}$ は z の複素共役を表すものとする.

$$w = P \cdot z = \frac{pz + q}{rz + s}$$

とおく. 複素共役の性質から,

$$\overline{w} = \frac{p\overline{z} + q}{r\overline{z} + s}.$$

よって,

$$\begin{aligned} w - \overline{w} &= \frac{pz + q}{rz + s} - \frac{p\overline{z} + q}{r\overline{z} + s} \\ &= \frac{(pz + q)(r\overline{z} + s) - (p\overline{z} + q)(rz + s)}{(rz + s)(r\overline{z} + s)} \\ &= \frac{(psz + qr\overline{z}) - (ps\overline{z} + qrz)}{(rz + s)\overline{(rz + s)}} \\ &= \frac{(ps - qr)(z - \overline{z})}{|rz + s|^2}. \end{aligned}$$

$\det P = ps - qr$, $z - \overline{z} = 2\,\mathrm{Im}\, z$, $w - \overline{w} = 2\,\mathrm{Im}\, w$ より,

$$\mathrm{Im}\, w = \frac{\det P \cdot \mathrm{Im}\, z}{|rz + s|^2}.$$

□

[補題 8.2] z を虚数とする. また, S を $\mathbb{Z}\times\mathbb{Z}$ の部分集合とし, $(0,0)$ 以外の元を少なくとも 1 つはもつとする. このとき $\mathbb{R}$ の部分集合

$$\left\{|rz+s| \;\middle|\; (r,s)\in S\setminus\{(0,0)\}\right\} \tag{23}$$

は正の最小元をもつ.

[証明] まず,

$$\begin{aligned} |rz+s|=0 &\Longleftrightarrow rz+s=0\\ &\Longleftrightarrow r=s=0\\ &\Longleftrightarrow (r,s)=(0,0)\end{aligned}$$

であるから, 0 は (23) に属さない. よって, (23) のすべての元は正の値をとる.

$x=\operatorname{Re} z$, $y=\operatorname{Im} z$ とおくと,

$$rz+s=(s+rx)+ry\sqrt{-1}$$

であるから,

$$|rz+s|^2=(s+rx)^2+r^2y^2.$$

$S\setminus\{(0,0)\}\neq\emptyset$ だから, S の元 $(r_0,s_0)\neq(0,0)$ が存在する. $R=|r_0z+s_0|$ とおく. R は (23) に属するから, (23) の最小元はもし存在すれば R 以下の実数である. したがって, $|rz+s|<R$ を満たす整数の組 (r,s) が高々有限個しかないことをいえば十分である.

もし $|rz+s|<R$ ならば,

$$|s+rx|<R,\quad |ry|<R. \tag{24}$$

z は虚数だから, $y\neq 0$. よって, (24) の 2 番目の式より,

$$|r|<\frac{R}{|y|}. \tag{25}$$

さらに, (24) の 1 番目の式と三角不等式から,

$$|s|-|rx|<|s+rx|<R.$$

ゆえに, (25) より

$$|s|<R+|rx|<R\left(1+\frac{|x|}{|y|}\right). \tag{26}$$

(25), (26) より, $|rz+s|<R$ を満たす整数の組 (r,s) は高々有限個しかない. □

[注意 8.3] z が無理数のとき, $|rz+s|$ はいくらでも小さい正の値をとる. したがって, 補題 8.2 の (23) は最小値をもたない.

実際, 以下の定理が成り立つことが知られている:

任意の実数 z と自然数 n とが与えられたとき,

$$|rz - s| < \frac{1}{n}, \quad 0 < r \leq n$$

となる r, $s \in \mathbb{Z}$ が必ず存在する.

この定理は, Dirichlet の部屋割り論法の応用例としてよく知られている.

虚部が正であるような複素数全体からなる $\mathbb{C}$ の部分集合

$$\mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}$$

を**上半平面**という. また, $\mathbb{C}$ の部分集合

$$\begin{aligned}\mathcal{F} = &\{z \in \mathbb{C} \mid |z| > 1 \text{ かつ } -1/2 \leq \operatorname{Re} z < 1/2\} \\ &\cup \{z \in \mathbb{C} \mid |z| = 1 \text{ かつ } -1/2 \leq \operatorname{Re} z \leq 0\}\end{aligned}$$

を $SL_2(\mathbb{Z})$ に関する**基本領域**という. $z \in \mathcal{F}$ ならば必ず $\operatorname{Im} z > 0$ であるため, $\mathcal{F}$ は $\mathcal{H}$ の部分集合である.

[例 8.4] $|\sqrt{-1}| = 1$, $\operatorname{Re}\sqrt{-1} = 0$ であるから, 虚数単位 $\sqrt{-1}$ は $\mathcal{F}$ に属する.

$\rho = (-1 + \sqrt{-3})/2$ を 1 の原始 3 乗根とする. このとき, $|\rho| = 1$, $\operatorname{Re} z = -1/2$ であるから, ρ は $\mathcal{F}$ に属する. また, $\rho + 1 = (1 + \sqrt{-3})/2$ は 1 の原始 6 乗根であり, $|\rho + 1| = 1$, $\operatorname{Re} z = 1/2$ であるから, $\rho + 1$ は $\mathcal{F}$ に属さない.

[定理 8.5] 任意の $z \in \mathcal{H}$ に対して, ある $w \in \mathcal{F}$ が存在して, z と w とは正に対等である.

[証明] $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in SL_2(\mathbb{Z})$ を任意にとると, 補題 8.1 と $z \in \mathcal{H}$ から,

$$\operatorname{Im}(P \cdot z) = \frac{\operatorname{Im} z}{|rz + s|^2} > 0.$$

$S = \{(r, s) \mid P \in SL_2(\mathbb{Z})\}$ として補題 8.2 を適用すれば, $|rz + s|$ が正のもののうちで最小となるような P の存在がいえる. そのような P をとり, $w_0 = P \cdot z$ とおく. すると, w_0 は z と正に対等な $\mathcal{H}$ の元のうちで虚部が最大のものである.

a を任意の整数とすると,

$$w_0 + a = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot w$$

より, $w_0 + a$ は w_0 と正に対等である. そこで, $-1/2 \leq \operatorname{Re} w_0 + a < 1/2$ となるように a を選び, $w = w_0 + a$ とおく. このとき, $\operatorname{Re}(w_0 + a) = \operatorname{Re} w_0 + a$, $\operatorname{Im} w = \operatorname{Im} w_0$ である. さらに,

$$w_1 = -\frac{1}{w} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cdot w_1$$

より, w_1 は w と正に対等である. 再び補題 8.1 によって,

$$\operatorname{Im} w_1 = \frac{\operatorname{Im} w}{|w|^2} = \frac{\operatorname{Im} w_0}{|w|^2}.$$

正に対等な関係は推移律を満たすので, w_2 は z に正に対等である. よって, $\operatorname{Im} w_0$ の最大性により,

$$\operatorname{Im} w_1 \leq \operatorname{Im} w_0.$$

ゆえに,

$$|w|^2 = \frac{\operatorname{Im} w_0}{\operatorname{Im} w_1} \geq 1.$$

したがって, $|w| > 1$ のとき, w は基本領域 $\mathcal{F}$ に属する. $|w| = 1$ のときは,

$$\left|-\frac{1}{w}\right| = |w| = 1, \quad \operatorname{Re}\left(-\frac{1}{w}\right) = -\operatorname{Re} w$$

となるので, w または w_1 が基本領域 $\mathcal{F}$ に属する. □

[定理 8.6] $z, w \in \mathcal{F}$, $P \in SL_2(\mathbb{Z})$ とし, $w = P \cdot z$ とする. このとき, $z = w$ が成り立つ. さらに,

$$P = \begin{cases} \pm E, & z \neq \sqrt{-1}, \rho \text{ のとき} \\ \pm E, \pm T, & z = \sqrt{-1} \text{ のとき} \\ \pm E, \pm TS, \pm (TS)^2 & z = \rho \text{ のとき} \end{cases}$$

が成り立つ. ここで, $S = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $T = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ とおくと

$$TS = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, \quad (TS)^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix}$$

である. また, $\rho = (-1 + \sqrt{-3})/2$ は 1 の原始 3 乗根である.

[証明] $\operatorname{Im} w < \operatorname{Im} z$ のときは P の代わりに P^{-1} を考えればよいので, $\operatorname{Im} z \leq \operatorname{Im} w$ と仮定しても一般性を失わない. $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ とおくと,

$$w = P \cdot z = \frac{pz + q}{rz + s}. \tag{27}$$

$\det P = 1$ であるから, 補題 8.1 より,

$$\operatorname{Im} w = \frac{\operatorname{Im} z}{|rz + s|^2}.$$

$\operatorname{Im} z \leq \operatorname{Im} w$ より,

$$|rz + s| = \frac{\operatorname{Im} z}{\operatorname{Im} w} \leq 1. \tag{28}$$

$\operatorname{Im}(rz+s) = r\operatorname{Im} z$ であるから,

$$|r\operatorname{Im} z| = |\operatorname{Im}(rz+s)| \leq |rz+s| \leq 1.$$

$\mathcal{F}$ の元のうちで虚部が最小のものは ρ であるから,

$$\frac{\sqrt{3}}{2} = \operatorname{Im}\rho \leq \operatorname{Im} z.$$

ゆえに,

$$\frac{\sqrt{3}}{2}|r| \leq 1.$$

したがって,

$$|r| \leq \frac{2}{\sqrt{3}}.$$

$r \in \mathbb{Z}$ だから, $r = 0$ または ± 1.

$\underline{r = 0 \text{ のとき}}$, $ps - qr = 1$ から, $p = s = \pm 1$. ゆえに (27) から

$$w = z \pm q.$$

$z, w \in \mathcal{F}$ より, $q = 0$. したがって, $z = w$.

$\underline{r = -1 \text{ のとき}}$, P の代わりに $-P$ をとることで $r = 1$ とすることができる. よって, $r = 1$ のときに帰着する.

$\underline{r = 1 \text{ のとき}}$, (28) から

$$|z+s| \leq 1. \tag{29}$$

$z \in \mathcal{F}$ かつ $s \in \mathbb{Z}$ だから, もし仮に $|z| > 1$ とすると $|z+s| > 1$ となって (29) と矛盾する. ゆえに, $|z| = 1$. また, もし $s \neq 0$ ならば, (29) が満たされるのは $z = \rho$ かつ $s = 1$ のときのみである. したがって, 「$|z| = 1$, $s = 0$」または「$z = \rho$, $s = 1$」である.

$|z| = 1$, $s = 0$ の場合, $ps - qr = 1$, $r = 1$ から $q = -1$. よって (27) から

$$w = p - \frac{1}{z}.$$

$|z| = 1$ より,

$$\left|-\frac{1}{z}\right| = |z| = 1, \quad \operatorname{Re}\left(-\frac{1}{z}\right) = -\operatorname{Re} z.$$

$z, w \in \mathcal{F}$ より, 「$p = 0$, $-1/z = \sqrt{-1}$」または「$p = -1$, $-1/z = \rho + 1$」である. 前者の場合, $z = w = \sqrt{-1}$ となり, 後者の場合, $\rho + 1 = -\rho^2 = -1/\rho$ より, $z = w = \rho$ となる.

$z = \rho$, $s = 1$ の場合, $ps - qr = 1$, $r = 1$ から $p - q = 1$. すなわち $p = q + 1$ である. (27) から

$$w = \frac{(q+1)\rho + q}{\rho + 1} = q + \frac{\rho}{\rho+1} = q + (\rho + 1).$$

ここで, 最後の等式において

$$\frac{\rho}{\rho+1} = \frac{\rho}{-\rho^2} = -\frac{1}{\rho} = -\rho^2 = \rho + 1$$

を用いた. $w \in \mathcal{F}$ より, $q = -1$. ゆえに, $p = 0$, $z = w = \rho$. □

[定理 8.7] $z, w \in \mathcal{H}$ とする. このとき, z と w とが正に対等であるための必要十分条件は, z と w がある共通の $z_0 \in \mathcal{F}$ と正に対等であることである.

[証明] (必要性)　定理 8.5 より, ある $z_0 \in \mathcal{F}$ が存在して z は z_0 と正に対等である. 同様に, ある $w_0 \in \mathcal{F}$ が存在して w は w_0 と正に対等である. z と w とは正に対等であるから, z_0 と w_0 とは正に対等である. 定理 8.6 より, $z_0 = w_0$ となる.

(十分性)　z が z_0 と正に対等で, z_0 が w と正に対等であれば, z は w と正に対等である.　□

9　2 次代数的数

複素数 θ が **2 次代数的数**であるとは, ある整数係数の 2 次方程式

$$ax^2 + bx + c = 0, \quad \gcd(a, b, c) = 1, \quad a > 0 \tag{30}$$

の解であり, かつ $\theta \notin \mathbb{Q}$ であるときにいう. このとき, θ は無理数か虚数である. 無理数の 2 次代数的数を **2 次無理数**, 虚数の 2 次代数的数を **2 次虚数**という.

2 次代数的数 θ を解とする (30) の形の 2 次方程式が 2 つあったとし, それらを

$$\begin{aligned} &ax^2 + bx + c = 0, \quad \gcd(a, b, c) = 1, \quad a > 0, \\ &a'x^2 + b'x + c' = 0, \quad \gcd(a', b', c') = 1, \quad a' > 0 \end{aligned}$$

とする. $a' = au$ $(u \in \mathbb{Q})$ とおくと,

$$\begin{aligned} 0 &= a'\theta^2 + b'\theta + c' - u(a\theta^2 + b\theta + c) \\ &= (b' - bu)\theta + (c' - cu). \end{aligned}$$

$\theta \notin \mathbb{Q}$ なので,

$$b' - bu = c' - cu = 0.$$

すなわち, $b' = bu$, $c' = cu$ となる. u を, $u = m/n$, $\gcd(m, n) = 1$, $n > 0$ のように既約分数で表せば,

$$a'n = am, \quad b'n = bm, \quad c'n = cm.$$

このとき, n は a, b, c の公約数である. $\gcd(a, b, c) = 1$ より, $n = 1$ でなければならない. ゆえに, u は整数である. またこのとき, m は a', b', c' の公約数である. $\gcd(a', b', c') = 1$ より, $m = \pm 1$. すなわち, $u = \pm 1$. さらに, $a > 0$, $a' > 0$ より $u = 1$ がいえる. したがって, $a = a'$, $b = b'$, $c = c'$ となり, θ を解とする (30) の形の 2 次方程式はただ 1 つ定まる.

2 次代数的数 θ を解とする (30) の形の 2 次方程式の判別式 D を θ の**判別式**という. また, θ を**判別式 D に属する** 2 次代数的数という.

方程式 (30) の解は,

$$\frac{-b+\sqrt{D}}{2a}, \quad \frac{-b-\sqrt{D}}{2a} \tag{31}$$

の 2 つである. これらを互いに**共役**な 2 次代数的数という. また, 2 次代数的数 θ に対して, それと共役なもう 1 つの 2 次代数的数を θ の**共役**といい, $\overline{\theta}$ で表す.

複素数 θ が 2 次代数的数であるためには, θ がある整数係数の 2 次方程式 (30) の解であり, かつその判別式

$$D = b^2 - 4ac$$

が 0 でも平方数でもないことが必要十分である.

2 次無理数の共役は 2 次無理数であり, 2 次虚数の共役は 2 次虚数である. また, θ が 2 次無理数であるとき, その共役 $\overline{\theta}$ は複素共役とは異なる. 実際, $\theta \neq \overline{\theta}$ であるのに対し, θ の複素共役は θ 自身である. 一方, 2 次虚数の共役は複素共役と一致する.

[定理 9.1] 複素数 θ について, 次の 3 つの条件は同値である:

(i) θ は 2 次代数的数である.

(ii) θ はある整数係数 2 次方程式 $ax^2+bx+c=0$, $a \neq 0$ の解であって, その判別式 $D = b^2 - 4ac$ は 0 でも平方数でもない.

(iii) θ はある最高次係数が 1 の有理数係数 2 次方程式 $x^2 + b'x + c' = 0$ の解であって, その判別式 $D' = b'^2 - 4c'$ は 0 でも有理数の平方でもない.

また, 2 つの複素数 θ, θ' について, 次の 3 つの条件は同値である:

(i) θ, θ' は共役な 2 次代数的数である.

(ii) θ, θ' はある整数係数 2 次方程式 $ax^2+bx+c=0$, $a \neq 0$ の相異なる解であって, その判別式 $D = b^2 - 4ac$ は 0 でも平方数でもない.

(iii) θ, θ' はある最高次係数が 1 の有理数係数 2 次方程式 $x^2 + b'x + c' = 0$ の相異なる解であって, その判別式 $D' = b'^2 - 4c'$ が 0 でも有理数の平方でもない.

[証明] まず, 前半の同値を証明する.

(i)⇒(ii)　明らかである.

(ii)⇒(iii)　$ax^2+bx+c=0$ の解を θ とすると,

$$a\theta^2 + b\theta + c = 0.$$

両辺を a で割ると,

$$\theta^2 + b'\theta + c' = 0, \quad b', c' \in \mathbb{Q}.$$

ただし, $b' = b/a$, $c' = c/a$ と置いた. また,

$$D' = b' - 4a'c' = \frac{b^2 - 4ac}{a^2} = \frac{D}{a^2}$$

であるから, D が 0 でも平方数でもなければ, D' は 0 でも有理数の平方でもない.

(iii)⇒(i)　$x^2+b'x+c'=0$ の解を θ をすると,

$$\theta^2+b'\theta+c'=0.$$

$b'=b_1/b_2$, $c'=c_1/c_2$ (b_1, b_2, c_1, $c_2\in\mathbb{Z}$, $b_2>0$, $c_2>0$) と表すとき, 上の方程式の両辺に b_2c_2 を掛けると, 整数係数の 2 次方程式

$$\begin{aligned}&a\theta^2+b\theta+c=0,\\&a=b_2c_2>0,\quad b=b_1c_2,\quad c=b_2c_1\end{aligned}$$

が得られる. $g=\gcd(a,b,c)$ とおくと, $g>1$ のときは, $a\theta^2+b\theta+c=0$ の両辺を g で割って係数の最大公約数を 1 にできる. また,

$$\begin{aligned}\frac{b^2-4ac}{g^2}&=\frac{b_1^2c_2^2-4b_2^2c_1c_2}{g^2}\\&=\frac{b_2^2c_2^2}{g^2}\cdot\left(\frac{b_1^2}{b_2^2}-4\cdot\frac{c_1}{c_2}\right)\\&=\frac{b_2^2c_2^2}{g^2}\cdot D'\end{aligned}$$

であるから, D' が 0 でも有理数の平方でもなければ, $(b^2-4ac)/g^2$ は 0 でも平方数でもない.

後半の同値については, 例えば (iii)⇒(i) の場合, 前半の同値の証明を見ればわかるように, θ, θ' は (30) の形をした同じ 2 次方程式の (相異なる) 解になる. 他の場合についても同様である.　□

[定理 9.2] 整数 D がある 2 次代数的数 θ の判別式であるための必要十分条件は, D は 0 でも平方数でもない整数であって, $D\equiv0$ または $1\pmod4$ であることである.

[証明] D が 2 次代数的数 θ の判別式ならば, ある整数 a, b, c が存在して,

$$\begin{aligned}&a\theta^2+b\theta+c=0,\quad \gcd(a,b,c)=1,\quad a>0,\\&\theta=\frac{-b\pm\sqrt{D}}{2a},\quad D=b^2-4ac.\end{aligned}$$

θ は 2 次代数的数なので, D は 0 でも平方数でもない. また,

$$D\equiv b^2\equiv\begin{cases}0\pmod4, & b\text{ が偶数のとき}\\1\pmod4, & b\text{ が奇数のとき}\end{cases}$$

となる.

逆に, $D\equiv0\pmod4$ のとき, b を任意の偶数とすれば, $D-b^2$ は 4 の倍数である.

$$a=1,\quad c=\frac{b^2-D}{4},\quad \theta=\frac{-b+\sqrt{D}}{2}$$

とおけば, $b^2-4ac=D$ であり, かつ

$$a\theta^2+b\theta+c=0,\quad \gcd(a,b,c)=1,\quad a>0.$$

D は 0 でも平方数でもないので, θ は無理数か虚数である. よって, θ は判別式 D に属する 2 次代数的数である.

$D\equiv 1 \pmod 4$ のとき, b を任意の奇数とすれば同様にして証明できる. □

(30) の解であるような 2 次代数的数 θ に対して, $-\theta$ は方程式 $ax^2-bx+c=0$ の解である. また, $1/\theta$ は方程式 $cx^2+bx+a=0$ の解である. すなわち, $-\theta$ および $1/\theta$ もまた 2 次代数的数である.

より一般に, 次の定理が成り立つ.

[定理 9.3] θ を 2 次代数的数とし, ある $P\in GL_2(\mathbb{Z})$ が存在して $\omega=P\cdot\theta$ であるとする. このとき, ω もまた 2 次代数的数であって, $\overline{\omega}=P\cdot\overline{\theta}$ となる.

[証明] $P=\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ とおき, $\omega=P\cdot\theta=\dfrac{p\theta+q}{r\theta+s}$, $\omega'=P\cdot\overline{\theta}=\dfrac{p\overline{\theta}+q}{r\overline{\theta}+s}$ とする. θ は無理数か虚数だから, ω も無理数か虚数である.

$$\begin{aligned}\omega+\omega' &= \frac{p\theta+q}{r\theta+s}+\frac{p\overline{\theta}+q}{r\overline{\theta}+s}\\ &= \frac{(p\theta+q)(r\overline{\theta}+s)+(p\overline{\theta}+q)(r\theta+s)}{(r\theta+s)(r\overline{\theta}+s)}\\ &= \frac{2pr\theta\overline{\theta}+qr(\theta+\overline{\theta})+2qs}{r^2\theta\overline{\theta}+rs(\theta+\overline{\theta})+s^2}.\end{aligned}$$

また,

$$\begin{aligned}\omega\omega' &= \frac{(p\theta+q)(p\overline{\theta}+q)}{(r\theta+s)(r\overline{\theta}+s)}\\ &= \frac{p^2\theta\overline{\theta}+pq(\theta+\overline{\theta})+q^2}{r^2\theta\overline{\theta}+rs(\theta+\overline{\theta})+s^2}.\end{aligned}$$

解と係数の関係より $\theta+\overline{\theta}$, $\theta\overline{\theta}\in\mathbb{Q}$ だから, $\omega+\omega'$, $\omega\omega'\in\mathbb{Q}$. ゆえに, ω, ω' はともに同一の有理数係数の 2 次方程式

$$x^2+bx+c=0,\quad b=-(\omega+\omega'),\quad c=\omega\omega'$$

の解である. ω は無理数か虚数だから, 上の 2 次方程式の判別式は 0 でも平方数でもない. したがって, 定理 9.1 より, ω, ω' は 2 次代数的数である. もし仮に $\omega=\omega'$ とすると,

$$\theta=P^{-1}\cdot\omega=P^{-1}\cdot\omega'=\overline{\theta}$$

となる. 一方, θ は 2 次代数的数だから, $\theta\neq\overline{\theta}$. これは矛盾であるから, $\omega\neq\omega'$ でなければならない. したがって, ω, ω' は互いに共役である. □

［注意 9.4］ θ, θ' をそれぞれある整数係数 2 次方程式の解とするとき, それらの和 $\theta+\theta'$ と積 $\theta\theta'$ は, 一般には整数係数 2 次方程式の解ではない. 例えば, $1+\sqrt{2}$, $\sqrt{3}$ はそれぞれ $x^2-2x-1=0$, $x^2-3=0$ の解であるが, それらの和 $1+\sqrt{2}+\sqrt{3}$ と積 $\sqrt{2}+\sqrt{6}$ を解に持つ整数係数 2 次方程式は存在しない.

［定理 9.5］ D を 0 でも平方数でもない整数とし, $D\equiv 0$ または $1 \pmod 4$ であるとする. θ を, 判別式 D を持つ 2 次方程式

$$ax^2+bx+c=0, \quad D=b^2-4ac$$

の解とし,

$$\theta=\frac{-b+e\sqrt{D}}{2a}, \quad e=\pm 1$$

であるとする. また, ω は θ と対等な複素数であるとし, ある $P=\begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$ が存在して

$$\theta=P\cdot\omega=\frac{p\omega+q}{r\omega+s} \tag{32}$$

とする. このとき,

$$\begin{aligned} a' &= ap^2+bpr+cr^2, \\ b' &= 2apq+b(ps+qr)+2crs, \\ c' &= aq^2+bqs+cs^2 \end{aligned} \tag{33}$$

とおけば, ω は判別式 D を持つ 2 次方程式

$$a'x^2+b'x+c'=0, \quad D=b'^2-4a'c'$$

の解であって,

$$\omega=\frac{-b'+e'\sqrt{D}}{2a'}, \quad e'=e\cdot\det P$$

が成り立つ. また, $\gcd(a,b,c)=1$ ならば $\gcd(a',b',c')=1$ である.

［証明］ 最初の D に関する仮定は, D がある代数的数の判別式であるための条件である (定理 9.2).
$A=\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$ とおくと,

$$\begin{bmatrix} \theta & 1 \end{bmatrix} A \begin{bmatrix} \theta \\ 1 \end{bmatrix} = a\theta^2+b\theta+c=0.$$

また, (32) より,

$$P\begin{bmatrix} \omega \\ 1 \end{bmatrix} = \begin{bmatrix} p\omega+q \\ r\omega+s \end{bmatrix} = (r\omega+s)\begin{bmatrix} \theta \\ 1 \end{bmatrix}.$$

さらに, $A' = \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix}$ とおくと, (33) より,

$$ {}^tPAP = A'. \tag{34}$$

ゆえに,

$$\begin{aligned} a'\omega^2 + b'\omega + c' &= \begin{bmatrix} \omega & 1 \end{bmatrix} A' \begin{bmatrix} \omega \\ 1 \end{bmatrix} = \begin{bmatrix} \omega & 1 \end{bmatrix} {}^tPAP \begin{bmatrix} \omega \\ 1 \end{bmatrix} \\ &= {}^t\left(P \begin{bmatrix} \omega \\ 1 \end{bmatrix} \right) A \left(P \begin{bmatrix} \omega \\ 1 \end{bmatrix} \right) \\ &= (r\omega + s)^2 \begin{bmatrix} \theta & 1 \end{bmatrix} A \begin{bmatrix} \theta \\ 1 \end{bmatrix} \\ &= 0. \end{aligned}$$

すなわち, ω は 2 次方程式

$$a'x^2 + b'x + c' = 0.$$

の解である. この 2 次方程式の判別式を計算すると,

$$\begin{aligned} b'^2 - 4a'c' &= -4 \det A' = -4 \det {}^tPAP \\ &= -4(\det P)^2 \det A \\ &= -4 \det A = b^2 - 4ac \\ &= D. \end{aligned}$$

$P^{-1} = \dfrac{1}{\det P} \begin{bmatrix} s & -q \\ -r & p \end{bmatrix} = \pm \begin{bmatrix} s & -q \\ -r & p \end{bmatrix}$ と (32) より,

$$\omega = P^{-1} \cdot \theta = \frac{s\theta - q}{-r\theta + p}.$$

$\overline{\theta}, \overline{\omega}$ をそれぞれ θ, ω と共役な 2 次代数的数とすれば, 定理 9.3 より,

$$\begin{aligned} \omega - \overline{\omega} &= \frac{s\theta - q}{-r\theta + p} - \frac{s\overline{\theta} - q}{-r\overline{\theta} + p} \\ &= \frac{(ps - qr)(\theta - \overline{\theta})}{(p - r\theta)(p - r\overline{\theta})} \\ &= \frac{\det P \cdot a(\theta - \overline{\theta})}{a'}. \end{aligned}$$

ここで, 最後の等式において

$$\begin{aligned}(p-r\theta)(p-r\overline{\theta}) &= p^2 - pr(\theta+\overline{\theta}) + r^2\theta\overline{\theta} \\ &= p^2 - pr\cdot\left(-\frac{b}{a}\right) + r^2\cdot\frac{c}{a} \\ &= \frac{ap^2+bpr+cr^2}{a} \\ &= \frac{a'}{a}\end{aligned}$$

を用いた. したがって, $e' = e\cdot\det P$ とおくと,

$$a'(\omega-\overline{\omega}) = \det P\cdot a(\theta-\overline{\theta}) = e'\sqrt{D}.$$

ゆえに,

$$\omega = \frac{-b'+e'\sqrt{D}}{2a'},\quad \overline{\omega} = \frac{-b'-e'\sqrt{D}}{2a'}.$$

最後に, (34) より,

$$A = {}^t(P^{-1})A'P^{-1},\quad P^{-1} = \frac{1}{\det P}\begin{bmatrix} s & -q \\ -r & p\end{bmatrix}.$$

成分ごとに比較すると, 関係式

$$\begin{aligned}a &= a's^2 - b'rs + c'r^2, \\ b &= -2a'qs + b'(ps+qr) - 2c'pr, \\ c &= a'q^2 - b'pq + c'p^2\end{aligned}$$

が得られる. $g = \gcd(a',b',c')$ とおくと, 上の関係式から g は a, b, c の公約数である. ゆえに, $g>1$ ならば $\gcd(a,b,c)>1$ である. よって, 対偶を考えると, $\gcd(a,b,c)=1$ ならば $g=1$ である. □

[定理 9.6] 2 次代数的数に対等なものは 2 次代数的数である. もっと詳しく言うと, 2 次無理数に対等なものは 2 次無理数であり, 2 次虚数に対等なものは 2 次虚数である. また, 対等な 2 次代数的数の判別式は一致する.

[証明] 定理 9.5 より直ちに導かれる. □

10 簡約 2 次無理数

2 次無理数 θ が**簡約 2 次無理数**であるとは, θ 自身およびそれと共役な $\overline{\theta}$ について, 不等式

$$-1 < \overline{\theta} < 0,\quad 1 < \theta$$

が成り立つときにいう.

[定理 10.1] D を平方数でない正の整数とし, $D \equiv 0$ または $1 \pmod 4$ であるとする.

(i) $D \equiv 0 \pmod 4$ のとき, r を $\sqrt{D/4}$ より小さい最大の整数とすれば, $\theta = r + \sqrt{D/4}$ は判別式 D に属する簡約 2 次無理数である.

(ii) $D \equiv 1 \pmod 4$ のとき, r を $\sqrt{D/4}$ より小さい最大の奇数とすれば, $\theta = (r + \sqrt{D})/2$ は判別式 D に属する簡約 2 次無理数である.

[証明] (i) θ は 2 次方程式 $x^2 - 2rx + r^2 - D/4 = 0$ の解であり, $(-2r)^2 - 4(r^2 - D/4) = D$ となる. この 2 次方程式のもう 1 つの解は $\overline{\theta} = r - \sqrt{D/4}$ であり, r の定め方から $-1 < \overline{\theta} < 0$ かつ $1 < \theta$ が成り立つことは明らかである.

(ii) θ は 2 次方程式 $x^2 - rx + (r^2 - D)/4 = 0$ の解であり, $(-r)^2 - 4(r^2 - D)/4 = D$ となる. この 2 次方程式のもう 1 つの解は $\overline{\theta} = (r - \sqrt{D})/2$ であり, r と ω の定め方から $\theta > 0$ は明らか. また, $0 < \sqrt{D} - r < 2$ より, $-1 < \overline{\theta} < 0$ もいえる. □

[例 10.2] m を平方数でない正の整数とする.

$\sqrt{m}$ は 2 次方程式 $x^2 - m = 0$ の解で, その判別式は $4m$ である. もう 1 つの解は $-\sqrt{m}$ であり, $\sqrt{m}$ と $-\sqrt{m}$ は互いに共役な 2 次無理数である.

また, $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ は 2 次方程式 $(x - \lfloor\sqrt{m}\rfloor)^2 - m = 0$ の解で, その判別式は同じく $4m$ である. もう 1 つの解は $\lfloor\sqrt{m}\rfloor - \sqrt{m}$ であり, 2 つの解は互いに共役な 2 次無理数である.

$\sqrt{m}$ と $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ は同じ判別式に属する 2 次無理数である.

さらに, $\lfloor\sqrt{m}\rfloor + \sqrt{m}$ は

$$-1 < \lfloor\sqrt{m}\rfloor - \sqrt{m} < 0, \quad 1 < \lfloor\sqrt{m}\rfloor + \sqrt{m}$$

を満たすので, 簡約 2 次無理数である.

[定理 10.3] 判別式 $D > 0$ が与えられたとき, ある整数係数の 2 次方程式

$$ax^2 + bx + c = 0, \quad D = b^2 - 4ac \tag{35}$$

の解となるような簡約 2 次無理数は有限個しかない.

[証明] θ を簡約 2 次無理数とし, 整数係数の 2 次方程式 (35) の解であるとする. $a < 0$ のとき, θ は両辺に -1 を掛けた方程式の解でもあり, $(-b)^2 - 4(-a)(-c) = b^2 - 4ac = D$ である. よって, $a > 0$ と仮定してもよい.

$\overline{\theta}$ を θ と共役な 2 次無理数とすれば,

$$-1 < \overline{\theta} < 0, \quad 1 < \theta. \tag{36}$$

一方, $a>0$ だから, $(-b-\sqrt{D})/2a<(-b+\sqrt{D})/2a$. ゆえに,

$$\theta=\frac{-b+\sqrt{D}}{2a},\quad \overline{\theta}=\frac{-b-\sqrt{D}}{2a}. \tag{37}$$

(37) より,

$$-\frac{b}{a}=\theta+\overline{\theta}>0,\quad \frac{c}{a}=\theta\overline{\theta}<0.$$

これと $a>0$ より, $b<0$, $c<0$. したがって, $|c|=-c$ なので,

$$D=|b|^2+4a|c|>|b|^2.$$

ゆえに,

$$|b|<\sqrt{D}. \tag{38}$$

また, $|b|=-b$ なので, (37) から,

$$\theta=\frac{|b|+\sqrt{D}}{2a},\quad \overline{\theta}=\frac{|b|-\sqrt{D}}{2a}.$$

さらに, (36) より,

$$-\overline{\theta}<1<\theta$$

なので, $a>0$ より,

$$-a\overline{\theta}<a<a\theta.$$

すなわち,

$$\frac{\sqrt{D}-|b|}{2}<a<\frac{\sqrt{D}+|b|}{2}.$$

(38) より,

$$0<a<\sqrt{D}. \tag{39}$$

判別式 D を 1 つ固定したとき, (38), (39) より $|b|$ および a の取り得る値は有限個に限られる. したがって, $\theta=(|b|+\sqrt{D})/2a$ は有限個しかない. □

11 実数の対等関係と連分数展開

[定理 11.1] $A=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL_2(\mathbb{Z})$ とし, $0<d<c$ を満たすと仮定する. また, 有理数 a/c を

$$\frac{a}{c}=[a_0,a_1,\ldots,a_n]$$

と連分数で表し, n の偶奇は

$$\det A=ad-bc=(-1)^{n-1}$$

を満たすようにする. さらに, a/c の近似分数を p_k/q_k $(0 \leq k \leq n)$ とする. このとき,

$$A = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

が成り立つ.

[証明] まず, 有理数を連分数で表すとき, n が偶数になる表し方と奇数になる表し方の両方が可能である. 実際, $a_n = 1$ のとき,

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = [a_0, a_1, \ldots, a_{n-1} + 1]$$

であり, $a_n \geq 2$ のとき,

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_n - 1, 1]$$

である. よって,

$$ad - bc = (-1)^{n-1}$$

となるように n をとることができる.

近似分数 p_n/q_n は既約分数であり, $q_n > 0$. 一方, $ad - bc = \pm 1$ より $\gcd(a, c) = 1$ であり, 仮定より $c > 0$ だから, $a = p_n$, $c = q_n$.

また,

$$p_n d - b q_n = ad - bc = (-1)^{n-1} = p_n q_{n-1} - p_{n-1} q_n.$$

すなわち,

$$p_n(d - q_{n-1}) = q_n(b - p_{n-1}). \tag{40}$$

$\gcd(p_n, q_n) = 1$ だから, $q_n \mid (d - q_{n-1})$. すなわち,

$$q_n \leq d - q_{n-1} \quad \text{または} \quad d - q_{n-1} = 0.$$

一方, 仮定より $0 < d < c$ であり, $q_{n-1} > 0$ であるから,

$$d - q_{n-1} < d < c = q_n.$$

ゆえに, $d - q_{n-1} = 0$ でなければならない. ゆえに, $d = q_{n-1}$. さらに, $q_n > 0$ だから, (40) より $b = p_{n-1}$. □

[定理 11.2] $\theta > 1$ を実数, a, b, c, d を

$$0 < d < c, \quad ad - bc = \pm 1$$

を満たす整数とし,

$$\omega = \frac{a\theta + b}{c\theta + d}$$

とする. このとき, θ は ω の連分数展開における全商である.

[証明] 定理 11.1 と定理 3.1 より,

$$\begin{aligned}\omega &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \theta = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \cdot \theta \\ &= \frac{p_n\theta + p_{n-1}}{q_n\theta + q_{n-1}} \\ &= [a_0, a_1, \ldots, a_n, \theta].\end{aligned}$$

仮定より $\theta > 1$ だから, θ は ω の連分数展開における全商である. □

[定理 11.3] 2 つの無理数 θ, ω が対等であるための必要十分条件は, θ と ω とを連分数展開するとき, 両方の展開が最後には一致すること, すなわち, ある実数 $\zeta > 1$ と整数 $n \geq 0$, $m \geq 0$ が存在して

$$\begin{aligned}\theta &= [a_0, a_1, \ldots, a_n, \zeta], \\ \omega &= [b_0, b_1, \ldots, b_m, \zeta]\end{aligned} \tag{41}$$

が成り立つことである.

[証明] (十分性) θ が (41) によって与えられるとする. p_n/q_n を θ の n 次の近似分数とすれば,

$$\theta = [a_0, a_1, \ldots, a_n, \zeta] = \frac{p_n\zeta + p_{n-1}}{q_n\zeta + q_{n-1}}$$

および

$$p_nq_{n-1} - p_{n-1}q_n = \pm 1$$

であるから, θ は ζ と対等である. 同様に, ω も ζ と対等である. ゆえに, θ は ω と対等である.

(必要性) θ と ω とが互いに対等であるとすると, ある整数 a, b, c, d が存在して,

$$\omega = \frac{a\theta + b}{c\theta + d}, \quad ad - bc = \pm 1. \tag{42}$$

a, b, c, d の符号をすべて変えたものについても上式は成り立つから, $c\theta + d > 0$ と仮定してもよい.

θ を連分数展開すると,

$$\theta = [a_0, a_1, \ldots, a_{n-1}, \theta_n] = \frac{p_{n-1}\zeta + p_{n-2}}{q_{n-1}\zeta + q_{n-2}}.$$

ただし, $\theta_n > 1$ であり, p_n/q_n は θ の n 次の近似分数である. これを (42) に代入すると,

$$\omega = \frac{a'\theta_n + b'}{c'\theta_n + d'}.$$

ここで,

$$\begin{aligned}a' &= ap_{n-1} + bq_{n-1}, \quad b' = ap_{n-2} + bq_{n-2}, \\ c' &= cp_{n-1} + dq_{n-1}, \quad d' = cp_{n-2} + dq_{n-2}.\end{aligned}$$

a', b', c', d' は整数であり,

$$a'd' - b'c' = (ad - bc)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = \pm 1$$

を満たす.

定理 5.6 より, ある実数 δ, δ' が存在して,

$$p_{n-1} = q_{n-1}\theta + \frac{\delta}{q_{n-1}}, \quad |\delta| < 1,$$
$$p_{n-2} = q_{n-2}\theta + \frac{\delta'}{q_{n-2}}, \quad |\delta'| < 1.$$

ゆえに,

$$c' = (c\theta + d)q_{n-1} + \frac{c\delta}{q_{n-1}},$$
$$d' = (c\theta + d)q_{n-2} + \frac{c\delta'}{q_{n-2}}.$$

$c\theta + d > 0$ かつ $0 < q_{n-2} < q_{n-1}$ だから, 十分大きな n に対して

$$0 < c' < d'$$

となる. そのような n に対して $\zeta = \theta_n$ とおけば, ζ は, θ の連分数展開の全商であると同時に, 定理 11.2 より ω の連分数展開の全商である. □

12　2 次無理数と循環連分数

連分数展開が途中から循環するものを循環連分数という. 循環の最小の周期のことを, その連分数の周期という. 特に, 最初から循環しているものを純循環連分数という.

これらの用語を厳密に定義しよう.

無理数 ω が

$$\omega = [a_0, a_1, a_2, \ldots, a_{n-1}, \omega_n] \quad (n = 0, 1, 2, \ldots) \tag{43}$$

と連分数展開され, ある整数 $n_0 \geq 1$ と $m \geq 1$ が存在して,

$$\omega_{n_0} = \omega_{n_0+m} = \cdots = \omega_{n_0+jm} = \cdots \quad (j = 0, 1, 2, \ldots) \tag{44}$$

が成り立つとき, ω を**循環連分数**という. あるいは, ω は循環連分数に展開されるという. (44) を満たす最小の m を循環連分数 ω の**周期**という. 特に, $n_0 = 0$ のとき, ω を**純循環連分数**という. あるいは, ω は純循環連分数に展開されるという.

ω が (43), (44) を満たす (必ずしも m が周期とは限らない) 循環連分数であるとき, ω_{n_0} は純循環連分数である. また,

$$\begin{aligned}\omega &= [a_0, a_1, a_2, \ldots, a_{n_0-1}, \omega_{n_0}] \\ &= [a_0, a_1, a_2, \ldots, a_{n_0-1}, a_{n_0}, \ldots, a_{n_0+m-1}, \omega_{n_0}] \\ &= [a_0, a_1, a_2, \ldots, a_{n_0-1}, a_{n_0}, \ldots, a_{n_0+m-1}, a_{n_0}, \ldots, a_{n_0+m-1}, \omega_{n_0}] \\ &= \cdots\cdots\end{aligned}$$

という具合に, a_{n_0}, ..., a_{n_0+m-1} が繰り返し現れる. そのことを

$$\omega = [a_0, a_1, \ldots, a_{n_0-1}, \dot{a}_{n_0}, \ldots, \dot{a}_{n_0+m-1}]$$

と表す. 特に, ω が純循環連分数であるときには,

$$\omega = [\dot{a}_0, \ldots, \dot{a}_{m-1}]$$

のように表される.

[例 12.1] $\sqrt{7}$ の連分数展開は

$$\begin{aligned}\sqrt{7} &= 2 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{4} + \cdots \\ &= [2, \dot{1}, 1, 1, \dot{4}] \\ &= [2, 1, 1, 1, \dot{4}, 1, 1, \dot{1}]\end{aligned}$$

である. $\sqrt{7}$ は循環連分数に展開され, 周期は 4 である.

$\lfloor\sqrt{7}\rfloor + \sqrt{7}$ の連分数展開は

$$\begin{aligned}\lfloor\sqrt{7}\rfloor + \sqrt{7} &= 4 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \frac{1}{4} + \cdots \\ &= [\dot{4}, 1, 1, \dot{1}]\end{aligned}$$

である. これは周期 4 の純循環連分数である.

[定理 12.2] 純循環連分数は簡約 2 次無理数である.

[証明] ω を純循環連分数として,

$$\omega = [\dot{a}_0, a_1, \ldots, \dot{a}_{n-1}], \quad n \geq 1$$

とする. a_0 は連分数展開の途中に現れるから, $a_0 \geq 1$. ゆえに, $\omega > 1$. また,

$$\omega = [a_0, a_1, \ldots, a_{n-1}, \omega] = \frac{p_{n-1}\omega + p_{n-2}}{q_{n-1}\omega + q_{n-2}}$$

であるから,

$$q_{n-1}\omega^2 + (q_{n-2} - p_{n-1})\omega - p_{n-2} = 0.$$

ゆえに, ω は 2 次無理数である. さらに,

$$f(x) = q_{n-1}x^2 + (q_{n-2} - p_{n-1})x - p_{n-2}$$

とおくと, $n > 1$ のときは, 定理 2.1, 定理 2.2 により

$$0 < p_{n-2} < p_{n-1}, \quad 0 < q_{n-2} \leq q_{n-1}$$

であり, $n = 1$ のときは, $p_{-1} = 1$, $p_0 = a_0$, $q_{-1} = 0$, $q_0 = 1$ であるから,

$$f(0) = -p_{n-2} < 0,$$
$$f(-1) = q_{n-1} - q_{n-2} + p_{n-1} - p_{n-2} > 0.$$

中間値の定理により, 方程式 $f(x) = 0$ は $-1 < x < 0$ の範囲に実数解を持つ. 一方, 方程式 $f(x) = 0$ の実数解は ω およびそれと共役な $\overline{\omega}$ の 2 つである. $\omega > 1$ だったから, $-1 < \overline{\omega} < 0$ でなければならない. ゆえに, ω は簡約 2 次無理数である. □

[定理 12.3] 循環連分数は 2 次無理数である.

[証明] ω を循環連分数として,

$$\omega = [a_0, a_1, \ldots, a_{n-1}, \dot{a}_n, a_{n+1}, \ldots, \dot{a}_{n+k}]$$

とする. ω の連分数展開は無限だから, 定理 4.7 より ω は無理数である. また,

$$\omega' = [\dot{a}_n, a_{n+1}, \ldots, \dot{a}_{n+k}]$$

とすると, ω' は純循環連分数なので, 定理 12.2 より 2 次無理数である. さらに, 定理 3.1 により

$$\omega = [a_0, a_1, \ldots, a_{n-1}, \omega'] = \frac{p_{n-1}\omega' + p_{n-2}}{q_{n-1}\omega' + q_{n-2}}.$$

すなわち, ω は ω' に対等である. したがって, 定理 9.6 により, ω もまた 2 次無理数である. □

無理数 ω の連分数展開

$$\omega = [a_0, a_1, a_2, \ldots, a_{n-1}, \omega_n] \quad (n = 0, 1, 2, \ldots)$$

において, ある番号 n_1, n_2 が存在して

$$\omega_{n_1} = \omega_{n_2}, \quad n_1 < n_2$$

が成り立てば, ω は循環連分数である. 実際,

$$\begin{aligned}\omega_{n_1} &= [a_{n_1}, a_{n_1+1}, a_{n_1+2}, \ldots, a_{n_2-1}, \omega_{n_2}] \\ &= [a_{n_1}, a_{n_1+1}, a_{n_1+2}, \ldots, a_{n_2-1}, \omega_{n_1}] \\ &= [\dot{a}_{n_1}, a_{n_1+1}, a_{n_1+2}, \ldots, \dot{a}_{n_2-1}]\end{aligned}$$

であるから,

$$\begin{aligned}\omega &= [a_0, a_1, a_2, \ldots, a_{n_1-1}, \omega_{n_1}] \\ &= [a_0, a_1, a_2, \ldots, a_{n_1-1}, \dot{a}_{n_1}, a_{n_1+1}, a_{n_1+2}, \ldots, \dot{a}_{n_2-1}].\end{aligned}$$

[定理 12.4] 2 次無理数は循環連分数である.

[証明] θ を 2 次無理数とし, 整数係数の 2 次方程式

$$ax^2 + bx + c = 0, \quad \gcd(a, b, c) = 1, \quad D = b^2 - 4ac > 0$$

の解であるとする. また, θ の連分数展開を

$$\theta = [a_0, a_1, a_2, \ldots, a_{n-1}, \theta_n] \quad (n = 0, 1, 2, \ldots)$$

とし, p_n/q_n を θ の近似分数とすると,

$$\theta = \frac{p_{n-1}\theta_n + p_{n-2}}{q_{n-1}\theta_n + q_{n-2}}.$$

定理 9.5 より,

$$\begin{aligned}A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2, \\ B_n &= 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2}, \\ C_n &= ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2\end{aligned}$$

とおくと, θ_n は 2 次方程式

$$A_n x^2 + B_n x + C_n = 0, \quad B_n^2 - 4A_nC_n = D$$

の解である.

各番号 n に対して, 定理 5.6 より, ある定数 δ_{n-1} が存在して,

$$p_{n-1} = q_{n-1}\theta + \frac{\delta_{n-1}}{q_{n-1}}, \quad |\delta_{n-1}| < 1.$$

ゆえに,

$$\begin{aligned}A_n &= a\left(q_{n-1}\theta + \frac{\delta_{n-1}}{q_{n-1}}\right)^2 + bq_{n-1}\left(q_{n-1}\theta + \frac{\delta_{n-1}}{q_{n-1}}\right) + cq_{n-1}^2 \\ &= (a\theta^2 + b\theta + c)q_{n-1}^2 + 2a\theta\delta_{n-1} + a\frac{\delta_{n-1}^2}{q_{n-1}^2} + b\delta_{n-1} \\ &= 2a\theta\delta_{n-1} + a\frac{\delta_{n-1}^2}{q_{n-1}^2} + b\delta_{n-1}.\end{aligned}$$

よって,

$$|A_n| < 2|a\theta| + |a| + |b|.$$

また, $C_n = A_{n-1}$ だから,

$$|C_n| < 2|a\theta| + |a| + |b|.$$

さらに, $B_n^2 - 4A_nC_n = D > 0$ より,

$$\begin{aligned} B_n^2 &\leq 4|A_n||C_n| + D \\ &< 4(2|a\theta| + |a| + |b|)^2 + D. \end{aligned}$$

すなわち,

$$|B_n| < \sqrt{4(2|a\theta| + |a| + |b|)^2 + D}.$$

$|A_n|$, $|B_n|$, $|C_n|$ が n に依存しない値で上から評価されたので, 相異なる組 (A_n, B_n, C_n) は有限個しかない. よって, 番号 n_1, n_2, n_3 が存在して, $n_1 < n_2 < n_3$ かつ

$$(A_{n_1}, B_{n_1}, C_{n_1}) = (A_{n_2}, B_{n_2}, C_{n_2}) = (A_{n_3}, B_{n_3}, C_{n_3}).$$

これを (A, B, C) とおく. すると, θ_{n_1}, θ_{n_2}, θ_{n_3} はすべて 2 次方程式 $Ax^2 + Bx + C = 0$ の解であるから, 少なくとも 2 つは等しくなければならない. したがって, θ は循環連分数である. □

[補題 12.5] θ を簡約 2 次無理数とし, その連分数展開を

$$\theta = [a_0, a_1, a_2, \ldots, a_{n-1}, \theta_n] \quad (n = 0, 1, 2, \ldots)$$

とすれば, 各々の全商 θ_n もまた簡約 2 次無理数である.

[証明] θ を解にもつ 2 次方程式を

$$f(x) = ax^2 + bx + c = 0$$

とし, もう 1 つの解を $\overline{\theta}$ とする. θ は簡約 2 次無理数なので,

$$-1 < \overline{\theta} < 0, \quad 1 < \theta.$$

多項式列 $(f_n(x))$ を

$$f_0(x) = f(x), \quad f_n(x) = x^2 f_{n-1}\left(a_{n-1} + \frac{1}{x}\right) \quad (n = 1, 2, \ldots)$$

によって定めると, 各番号 $n \geq 0$ に対して, $f_n(x)$ は整数係数の 2 次多項式であり,

$$f_n(\theta_n) = 0$$

を満たす. さらに, 実数列 $(\overline{\theta}_n)$ を

$$\overline{\theta}_0 = \overline{\theta}, \quad \overline{\theta}_n = \frac{1}{\overline{\theta}_{n-1} - a_{n-1}} \quad (n = 1, 2, \ldots)$$

と定めると, 各番号 $n \geq 0$ に対して

$$f_n(\overline{\theta}_n) = 0$$

が成り立つ.

さて, 補題の主張を n に関する数学的帰納法により証明しよう. すべての番号 $n \geq 0$ に対して, $\theta_n > 1$ であることは θ_n が連分数展開の全商であることにより明らかであるから, $-1 < \overline{\theta}_n < 0$ であることを示せば十分である.

$n = 0$ のときは $\overline{\theta}_0 = \overline{\theta}$ より明らかである.

θ_{n-1} が簡約された無理数であると仮定すると, $-1 < \overline{\theta}_{n-1} < 0$ が成り立つ. $a_{n-1} \geq 1$ より,

$$\overline{\theta}_{n-1} - a_{n-1} < -1.$$

ゆえに,

$$-1 < \frac{1}{\overline{\theta}_{n-1} - a_{n-1}} < 0.$$

すなわち,

$$-1 < \overline{\theta}_n < 0.$$

したがって, θ_n は簡約 2 次無理数である.

以上より, すべての番号 $n \geq 0$ に対して定理の主張が証明された. □

[定理 12.6] 簡約 2 次無理数は純循環連分数である.

[証明] θ を簡約 2 次無理数とし, その連分数展開を

$$\theta = [a_0, a_1, a_2, \ldots, a_{n-1}, \theta_n] \quad (n = 0, 1, 2, \ldots)$$

とする. 定理 12.4 より, 2 次無理数は循環連分数だから, ある番号 n, m が存在して

$$\theta_n = \theta_m, \quad n < m$$

が成り立つ. $n \geq 1$ ならば,

$$\theta_{n-1} = a_{n-1} + \frac{1}{\theta_n} = \frac{a_{n-1}\theta_n + 1}{\theta_n},$$
$$\theta_{m-1} = a_{m-1} + \frac{1}{\theta_m} = \frac{a_{m-1}\theta_m + 1}{\theta_m}.$$

$\overline{\theta}_n$ を θ_n と共役な 2 次無理数とし, 他も同様とすると, 定理 9.3 より

$$\overline{\theta}_{n-1} = a_{n-1} + \frac{1}{\overline{\theta}_n},$$
$$\overline{\theta}_{m-1} = a_{m-1} + \frac{1}{\overline{\theta}_m}.$$

$\theta_n = \theta_m$ より $\overline{\theta}_n = \overline{\theta}_m$ だから,

$$\overline{\theta}_{n-1} - \overline{\theta}_{m-1} = a_{n-1} - a_{m-1}.$$

補題 12.5 より, θ_{n-1}, θ_{m-1} は簡約 2 次無理数だから, $\overline{\theta}_{n-1}$, $\overline{\theta}_{m-1}$ はともに -1 と 0 との間にある. ゆえに,

$$-1 < \overline{\theta}_{n-1} < \overline{\theta}_{n-1} - \overline{\theta}_{m-1} < -\overline{\theta}_{m-1} < 1.$$

よって,

$$-1 < a_{n-1} - a_{m-1} < 1.$$

$a_{n-1} - a_{m-1}$ は整数なので, 0 に一致する. すなわち, $a_{n-1} = a_{m-1}$. したがって,

$$\theta_{n-1} = \theta_{m-1}.$$

以上の操作を繰り返すと, 最後には

$$\theta_0 = \theta_{m-n}$$

を得る. すなわち, θ は純循環連分数である. □

[定理 12.7] 任意の 2 次無理数は, ある簡約 2 次無理数と正に対等である.

[証明] θ を 2 次無理数とし, その連分数展開を

$$\theta = [a_0, a_1, a_2, \ldots, a_{n-1}, \theta_n] \quad (n = 0, 1, 2, \ldots)$$

とする. 定理 12.4 より, 2 次無理数は循環連分数だから, ある番号 n, m が存在して

$$\theta_n = \theta_m, \quad n < m$$

が成り立つ. このとき,

$$\begin{aligned}\theta &= [a_0, a_1, a_2, \ldots, a_{n-1}, \theta_n] \\ &= [a_0, a_1, a_2, \ldots, a_{n-1}, a_n, \ldots, a_{m-1}, \theta_m] \\ &= [a_0, a_1, a_2, \ldots, a_{n-1}, a_n, \ldots, a_{m-1}, \theta_n]\end{aligned}$$

であるから, 定理 1.7 より,

$$\theta_n = [a_n, \ldots, a_{m-1}, \theta_n].$$

ゆえに, θ_n は純循環連分数である. 定理 12.2 より, θ_n は簡約 2 次無理数である.

n が偶数のとき, 定理 3.1 より,

$$\theta = \frac{p_{n-1}\theta_n + p_{n-2}}{q_{n-1}\theta_n + q_{n-2}}.$$

また, 定理 2.5 より,

$$p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^{n-2} = 1.$$

ゆえに, θ と θ_n とは正に対等である.

n が奇数のとき, 補題 12.5, 定理 12.2 より, θ_{n+1} も簡約 2 次無理数である. したがって, θ_{n+1} に対して n が偶数のときと同様の議論を行えば, θ と θ_{n+1} とが正に対等であることがいえる. □

13 整数係数 2 元 2 次形式

整数 a, b, c を係数し, x, y を変数とする同次多項式

$$f(x,y) = ax^2 + bxy + cy^2 \tag{45}$$

を**整数係数 2 元 2 次形式**という. 以下, 特に断らない限り, 単に **2 次形式**と呼ぶことにする.

$\gcd(a,b,c) = 1$ のとき, $f(x,y)$ は**原始的**であるという. 任意の 2 次形式は, 係数の最大公約数をくくり出すことにより, 原始的な 2 次形式の整数倍として表せる.

式 (45) を, 行列を用いて

$$\begin{aligned} f(x,y) &= x\left(ax + \frac{b}{2}y\right) + y\left(\frac{b}{2}x + cy\right) \\ &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} ax + \dfrac{b}{2}y \\ \dfrac{b}{2}x + cy \end{bmatrix} \\ &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \end{aligned}$$

と表すとき, 真ん中の 2 次正方行列

$$\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \tag{46}$$

を 2 次形式 f の**行列**という.

$D = b^2 - 4ac$ を 2 次形式 f の**判別式**という. f の行列 (46) を A とおくと,

$$D = -(4ac - b^2) = -\begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = -4\det A \tag{47}$$

が成り立つ.

[定理 13.1] $f(x,y) = ax^2 + bxy + cy^2$ を 2 次形式とし, D をその判別式とする. このとき,

$$4af(x,y) = (2ax + by)^2 - Dy^2$$

が成り立つ.

[証明] $D = b^2 - 4ac$ より,

$$\begin{aligned} 4af(x,y) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (4a^2x^2 + 4abxy + b^2y^2) - (b^2y^2 - 4acy^2) \\ &= (2ax + by^2)^2 - (b^2 - 4ac)y^2 \\ &= (2ax + by)^2 - Dy^2. \end{aligned}$$

□

2 次形式 $f(x,y)$ に対して,

(i) f が**不定符号** $\iff$ $f(x,y)$ が正負両方の値をとる.
(ii) f が**半正値** $\iff$ 任意の $x,\ y \in \mathbb{Z}$ に対して $f(x,y) \geq 0$.
(iii) f が**半負値** $\iff$ 任意の $x,\ y \in \mathbb{Z}$ に対して $f(x,y) \leq 0$.
(iv) f が**正値** $\iff$ f は半正値. かつ, 任意の $x,\ y \in \mathbb{Z}$ に対して, $f(x,y) = 0$ ならば $x = y = 0$.
(v) f が**負値** $\iff$ f は半負値. かつ, 任意の $x,\ y \in \mathbb{Z}$ に対して, $f(x,y) = 0$ ならば $x = y = 0$.

と定義する. また, f が正値または負値のとき, **定値**であるという.

[補題 13.2] $f(x,y) = ax^2 + bxy + cy^2$ を 2 次形式, $D = b^2 - 4ac$ を f の判別式とする.

$a \neq 0$ のとき,

(i) $D > 0 \iff f$ は不定符号.
(ii) $D = 0$ かつ $a > 0 \iff f$ は半正値だが正値ではない.
(iii) $D = 0$ かつ $a < 0 \iff f$ は半負値だが負値ではない.
(iv) $D < 0$ かつ $a > 0 \iff f$ は正値.
(v) $D < 0$ かつ $a < 0 \iff f$ は負値.

$a = 0$ のとき,

(i) $D > 0 \iff f$ は不定符号.
(ii) $D = 0$ かつ $c > 0 \iff f$ は半正値だが正値でなく, 恒等的には 0 にならない.
(iii) $D = 0$ かつ $c < 0 \iff f$ は半負値だが負値でなく, 恒等的には 0 にならない.
(iv) $D = 0$ かつ $c = 0 \iff f$ は恒等的に 0.

[証明] $a \neq 0$ のとき:

(i) ($\Rightarrow$)　定理 13.1 より, $f(x,y)$ は正負両方の値をとる.

(ii) ($\Rightarrow$)　$a > 0$ のとき, $D = 0$ と定理 13.1 より,

$$4af(x,y) = (2ax + by)^2.$$

$a > 0$ より, $f(x,y)$ は半正値である. また, $2ax + by = 0$ ならば $f(x,y) = 0$ なので, f は正値ではない.

(iii) ($\Rightarrow$)　(ii) と同様の議論で示せる.

(iv) ($\Rightarrow$)　定理 13.1 より, $D<0$ かつ $a>0$ のとき, $f(x,y)$ は正値である. また, 任意の $x, y \in \mathbb{Z}$ に対して,

$$f(x,y)=0 \Longrightarrow 2ax+by=y=0 \Longrightarrow x=y=0.$$

したがって, f は正値である.

(v) ($\Rightarrow$)　(iv) と同様の議論で示せる.

(i)〜(v) の各々の条件は互いに両立せず, 左側の条件は全ての場合を網羅しているので, ($\Leftarrow$) も一斉に成り立つ.

$a=0$ のとき:

(i) ($\Rightarrow$)　$D=b^2$ より, $b\neq 0$. よって, $f(x,y)=bxy+cy^2$ は正負両方の値をとる.

(ii) ($\Rightarrow$)　$D=b^2$ より, $b=0$. よって, $f(x,y)=cy^2$ は常に負でない. また, $y=0$ ならば任意の x に対して $f(x,y)=0$ なので, f は正値ではない. さらに, $y\neq 0$ ならば $f(x,y)\neq 0$ なので, f は恒等的には 0 にならない.

(iii) ($\Rightarrow$)　(ii) と同様の議論で示せる.

(iv) ($\Rightarrow$)　$D=b^2$ より, $b=0$. よって, $a=b=c=0$. したがって, f は恒等的に 0 である.

(i)〜(iv) の各々の条件は互いに両立しない. また, $a=0$ ならば $D=b^2\geq 0$ である. よって, 左側の条件は全ての場合を網羅している. したがって, ($\Leftarrow$) も一斉に成り立つ.　□

[定理 13.3] $f(x,y)=ax^2+bxy+cy^2$ を 2 次形式, $D=b^2-4ac$ を f の判別式とする. このとき, 次が成り立つ.

(i) f は不定符号 $\Longleftrightarrow D>0$.

(ii) f は半正値だが正値ではなく, 恒等的には 0 でない $\Longleftrightarrow D=0$ かつ「$a>0$ または $c>0$」.

(iii) f は半負値だが負値ではなく, 恒等的には 0 でない $\Longleftrightarrow D=0$ かつ「$a<0$ または $c<0$」.

(iv) f は恒等的に 0 $\Longleftrightarrow D=0$ かつ $a=c=0$.

(v) f は正値 $\Longleftrightarrow D<0$ かつ $a>0$.

(vi) f は負値 $\Longleftrightarrow D<0$ かつ $a<0$.

[証明] (ii) の ($\Leftarrow$) について, $D=0$ かつ $c>0$ のとき, 2 次形式 $f(x,y)$ が x, y について対称であることから, $D=0$ かつ $a>0$ のときと同様にして左側の条件が導かれる. (iii) の ($\Leftarrow$) についても同様である.

残りは, 補題 13.2 より直ちに得られる.　□

2 次形式

$$f(x,y)=ax^2+bxy+cy^2$$

に対して, $y=1$ を代入することにより, x に関する 2 次多項式

$$g(x)=f(x,1)=ax^2+bx+c \tag{48}$$

が得られる. 逆に, 多項式 $g(x) = ax^2 + bx + c$ が与えられたとき,

$$f(x,y) = y^2 \cdot g\left(\frac{x}{y}\right) = ax^2 + bxy + cy^2$$

となる. このように互いに対応しているので, $g(x)$ を $f(x,y)$ **に対応する 2 次多項式**といい, $f(x,y)$ を $g(x)$ **に対応する 2 次形式**という. またこのとき, $f(x,y)$ の判別式と $g(x)$ の判別式とは等しい.

14　2 次形式の対等関係

2 次形式

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} A \begin{bmatrix} x \\ y \end{bmatrix}, \quad A = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

に対して, $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$ による変数変換

$$\begin{bmatrix} x \\ y \end{bmatrix} = P \begin{bmatrix} x' \\ y' \end{bmatrix}, \tag{49}$$

すなわち,

$$\begin{aligned} x &= px' + qy', \\ y &= rx' + sy' \end{aligned}$$

を施すと,

$$\begin{aligned} f(x,y) &= \begin{bmatrix} x' & y' \end{bmatrix} {}^tPAP \begin{bmatrix} x' \\ y' \end{bmatrix} \\ &= a'x'^2 + b'x'y' + c'y'^2. \end{aligned}$$

ただし,

$$\begin{aligned} a' &= ap^2 + bpr + cr^2 \,(= f(p,r)), \\ b' &= 2apq + b(ps + qr) + 2crs, \\ c' &= aq^2 + bqs + cs^2 \,(= f(q,s)). \end{aligned} \tag{50}$$

特に, a', b', c' は整数である. つまり, 変数変換 (49) によって, 整数係数 2 元 2 次形式は整数係数 2 元 2 次形式に変換される. $a'x'^2 + b'x'y' + cy'^2$ のことを, $f(x,y)$ から P による**変数変換によって得られる 2 次形式**と呼ぶことにする.

2 つの 2 次形式

$$f(x,y) = ax^2 + bxy + cy^2 = \begin{bmatrix} x & y \end{bmatrix} A \begin{bmatrix} x \\ y \end{bmatrix}, \quad A = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}, \tag{51}$$

$$f(x',y') = a'x'^2 + b'x'y' + c'y'^2 = \begin{bmatrix} x' & y' \end{bmatrix} A' \begin{bmatrix} x' \\ y' \end{bmatrix}, \quad A' = \begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix} \tag{52}$$

が**等しい**ことを $f = f'$ で表し,

$$f = f' \Longleftrightarrow a = a',\ b = b',\ c = c'$$

と定義する. この定義によれば, $f = f'$ であることは $A = A'$ と同値である.

また, f が f' に**対等**であるとは, ある $P \in GL_2(\mathbb{Z})$ が存在して

$$A' = {}^tPAP \tag{53}$$

が成り立つことをいう. ただし, ${}^tP$ は P の転置行列を表す. $f(x,y)$ が $f'(x',y')$ に対等であることを記号 $f \sim f'$ で表す. またこのとき, 変数変換 (49) によって $f(x,y)$ は $f'(x',y')$ に変換される.

$P = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ とおけば, 2 次形式が対等であることの条件 (53) は関係式 (50) が成り立つことと言い換えることができる.

特に, $\det P = 1$ のとき**正に対等**であるといい, $\det P = -1$ のとき**負に対等**であるという.

[定理 14.1] 2 次形式 $f(x,y) = ax^2 + bxy + cy^2,\ f'(x',y') = a'x'^2 + b'x'y' + c'y'^2$ について, $f = f'$ であるための必要十分条件は, すべての $n_1,\ n_2 \in \mathbb{Z}$ に対して

$$f(n_1, n_2) = f'(n_1, n_2)$$

が成り立つことである.

[証明] (必要性)　$f = f'$ とすると, $a = a',\ b = b',\ c = c'$ なので, すべての $n_1,\ n_2 \in \mathbb{Z}$ に対して

$$\begin{aligned} f(n_1, n_2) &= an_1^2 + bn_1n_2 + cn_2^2 \\ &= a'n_1^2 + b'n_1n_2 + c'n_2^2 \\ &= f'(n_1, n_2). \end{aligned}$$

(十分性)　まず,

$$\begin{aligned} a &= f(1,0) = f'(1,0) = a', \\ c &= f(0,1) = f'(0,1) = c'. \end{aligned}$$

さらに,

$$a + b + c = f(1,1) = f'(1,1) = a' + b' + c'.$$

より, $b = b'$. □

[定理 14.2] $f,\ f'$ を 2 次形式とする. $f \sim f'$ かつ f' が原始的ならば, f もまた原始的である.

[証明] f, f' およびそれらの行列 A, A' を (51), (52) のように表すと, $f \sim f'$ という仮定より, ある $P = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \in GL_2(\mathbb{Z})$ が存在して, 関係式 (50) を満たす.

$g = \gcd(a, b, c)$ とおく. (50) から g は a', b', c' の公約数である. もし仮に $g > 1$ とすれば, f' が原始的であることに反する. ゆえに, $g = 1$ でなければならない. □

[定理 14.3] 対等な 2 次形式の判別式は一致する.

[証明] f, f' を対等な 2 次形式とし, D, D' をそれぞれ f, f' の判別式とする. また, A, A' をそれぞれ f, f' の行列とする. $f \sim f'$ より, ある $P \in GL_2(\mathbb{Z})$ が存在して $A' = {}^tPAP$. よって, (47) より,

$$\begin{aligned} D' &= -4 \det A' = -4 \det {}^tPAP \\ &= -4 \det {}^tP \det A \det P \\ &= -4 (\det P)^2 \det A = -4 \det A \\ &= D. \end{aligned}$$

□

[定理 14.4] 2 次形式における対等関係は同値関係である.

[証明] $f(x, y)$, $f'(x', y')$, $f''(x'', y'')$ を 2 次形式とし, それらの行列をそれぞれ A, A', A'' とおく.

(反射)　単位行列 $E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ により, $A = {}^tEAE$.

(対称)　$f \sim f'$ とすると, ある $P \in GL_2(\mathbb{Z})$ が存在して, $A' = {}^tPAP$. このとき, $A = {}^tPA'P$ となるから, $f' \sim f$.

(推移)　$f \sim f'$ かつ $f' \sim f''$ とする. 前者より, ある $P \in GL_2(\mathbb{Z})$ が存在して, $A' = {}^tPAP$. 同様に, 後者より, ある $P' \in GL_2(\mathbb{Z})$ が存在して, $A'' = {}^tPA'P$. ゆえに, $A'' = {}^t(PP')A(PP')$ となるから, $f \sim f''$. □

D を 0 でも平方数でもない整数とし, $D \equiv 0$ または $1 \pmod 4$ であるとする. 判別式 D を持つ 2 次多項式

$$ax^2 + bx + c, \quad D = b^2 - 4ac$$

の根, すなわち 2 次方程式 $ax^2 + bx + c = 0$ の解

$$\frac{-b + \sqrt{D}}{2a}, \quad \frac{-b - \sqrt{D}}{2a}$$

について, 最初のものを**第 1 根**といい, 残りのもう 1 つを**第 2 根**という. 定理 9.1 より, 第 1 根と第 2 根は互いに共役である.

[定理 14.5] $f(x,y)=ax^2+bxy+cy^2$, $f'(x',y')=a'x'^2+b'x'y'+c'y'^2$ を同じ判別式 D を持つ 2 次形式とする. また, θ を f に対応する 2 次多項式 ax^2+bx+c の第 1 根とし, θ' を f' に対応する 2 次多項式 $a'x'^2+b'x'+c'$ の第 1 根とする.

(i) f と f' とが等しい $\Longleftrightarrow$ $\theta=\theta'$.

(ii) f と f' とが正に対等 $\Longleftrightarrow$ θ と θ' とが正に対等.

(iii) f と f' とが負に対等 $\Longleftrightarrow$ θ と $\overline{\theta'}$ とが負に対等.

[証明] まず, $\theta=(-b+\sqrt{D})/2a$, $\theta'=(-b'+\sqrt{D})/2a'$ である.

(i) ($\Rightarrow$) f と f' とが等しければ, それぞれに対応する 2 次方程式の係数は等しいから, $\theta=\theta'$ である.

($\Leftarrow$) $\theta=\theta'$ とすると,

$$\frac{-b+\sqrt{D}}{2a}=\frac{-b'+\sqrt{D}}{2a'}.$$

分母を払って整理すると,

$$(a'b-ab')+(a-a')\sqrt{D}=0.$$

a, b, a', $b'\in\mathbb{Z}$ かつ $\sqrt{D}\notin\mathbb{Q}$ だから,

$$a'b-a'b'=a-a'=0.$$

ゆえに, $a=a'$, $b=b'$ となる. また, f と f' の判別式は同じだから,

$$b^2-4ac=b'^2-4a'c'.$$

これより, $c=c'$ が得られる. したがって, $f=f'$.

(ii) A, A' をそれぞれ f, f' の行列とすると, $A=\begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$, $A'=\begin{bmatrix} a' & b'/2 \\ b'/2 & c' \end{bmatrix}$ である.

($\Rightarrow$) f と f' とが正に対等であるとする. このとき, ある $P=\begin{bmatrix} p & q \\ r & s \end{bmatrix}\in SL_2(\mathbb{Z})$ が存在して, $A'={}^tPAP$. これより関係式 (33) が得られる. $\omega=P^{-1}\cdot\theta$ とおくと, 定理 9.5 より $\omega=\theta'$ がいえる. ゆえに, $\theta=P\cdot\theta'$.

($\Leftarrow$) θ と θ' とが正に対等である. このとき, ある $P=\begin{bmatrix} p & q \\ r & s \end{bmatrix}\in SL_2(\mathbb{Z})$ が存在して, $\theta=P\cdot\theta'$. また,

$$\begin{aligned} a'' &= ap^2+bpr+cr^2, \\ b'' &= 2apq+b(ps+qr)+2crs, \\ c'' &= aq^2+bqs+cs^2 \end{aligned} \tag{54}$$

とおくと, 定理 9.5 より, $\theta'=(-b''+\sqrt{D})/2a''$. すなわち,

$$\frac{-b'+\sqrt{D}}{2a'}=\frac{-b''+\sqrt{D}}{2a''}.$$

分母を払って整理すると,

$$(a''b' - a'b'') + (a' - a'')\sqrt{D} = 0.$$

a', b', a'', $b'' \in \mathbb{Z}$ かつ $\sqrt{D} \notin \mathbb{Q}$ だから,

$$a''b' - a'b'' = a' - a'' = 0.$$

ゆえに, $a' = a''$, $b' = b''$ となる. よって, (54) から $A' = {}^tPAP$ が得られる. したがって, f と f' とは正に対等である.

(iii) (ii) と同様にして示せる. □

15 負の判別式をもつ 2 次形式

定理 13.3 より, f が正値 (負値) であることと, 判別式が負で $a > 0$ (判別式が負で $a < 0$) であることとは同値であった. よって, 判別式が負の 2 次形式は正値か負値かのどちらかである.

また, 対等な 2 つの 2 次形式について, 一方が正値 (負値) ならばもう一方も正値 (負値) である. 実際, §14 の関係式 (50) より, 任意の $P \in GL_2(\mathbb{Z})$ に対して, 正値 (負値) 2 次形式から P による変数変換によって得られる 2 次形式もまた正値 (負値) である.

さらに, $f(x, y)$ が正値 2 次形式のとき, $-f(x, y)$ は負値 2 次形式である. $f(x, y)$ が P による変数変換によって $f'(x', y')$ に対等であれば, 同じ P による変数変換によって $-f(x, y)$ は $-f'(x', y')$ に対等である. 実際, f, f' の行列をそれぞれ A, A' とすると,

$$A' = {}^tPAP \Longleftrightarrow -A' = {}^tP(-A)P$$

が成り立つ.

したがって, 負値 2 次形式の対等関係に関する議論は正値の場合に帰着する.

2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ が正値のとき, $a > 0$ であり, もし仮に $c \leq 0$ とすると $b^2 - 4ac \geq 0$ となって矛盾が生じるから, $c > 0$ である.

正値 2 次形式 $f(x, y) = ax^2 + bxy + cy^2$ が**簡約 2 次形式**であるとは, 条件

$$-a < b \leq a < c \quad \text{または} \quad 0 \leq b \leq a = c \tag{55}$$

が成り立つときにいう.

[定理 15.1] 正値 2 次形式 $f(x, y)$ に対応する 2 次多項式 $g(x)$ の第 1 根を θ とする. このとき, f が簡約 2 次形式であるための必要十分条件は,

$$|\theta| > 1, -\frac{1}{2} \leq \mathrm{Re}\,\theta < \frac{1}{2} \quad \text{または} \quad |\theta| = 1, -\frac{1}{2} \leq \mathrm{Re}\,\theta \leq 0$$

が成り立つことである. すなわち, $\mathcal{F}$ を $SL_2(\mathbb{Z})$ に関する基本領域とすれば,

$$f \text{ は簡約 2 次形式} \Longleftrightarrow \theta \in \mathcal{F}$$

である.

[証明] $\overline{\theta}$ を θ の共役, すなわち $g(x)$ の第 2 根とする. 解と係数の関係より,

$$2\operatorname{Re}\theta = \theta + \overline{\theta} = -\frac{b}{a}, \quad |\theta| = \theta\overline{\theta} = \frac{c}{a}. \tag{56}$$

f が簡約ならば, (55) より

$$0 \leq \frac{b}{a} \leq 1 = \frac{c}{a} \quad \text{または} \quad -1 < \frac{b}{a} \leq 1 < \frac{c}{a}. \tag{57}$$

よって, (56) より $\theta \in \mathcal{F}$. 逆に, $\theta \in \mathcal{F}$ ならば, (56) より (57) が成り立つ. よって, (55) が成り立ち, f は簡約である. □

[定理 15.2] 与えられた判別式 $D < 0$ をもつ簡約 2 次形式は有限個しかない.

[証明] $f(x, y) = ax^2 + bxy + cy^2$ を判別式が D の簡約 2 次形式とすると, (55) より

$$|b| \leq a \leq c.$$

したがって,

$$|D| = 4ac - b^2 \geq 4b^2 - b^2 = 3b^2.$$

ゆえに,

$$|b| \leq \sqrt{\frac{|D|}{3}}.$$

が得られる. よって, b の取り得る整数値は有限個である. さらに, 各 b に対して, $4ac = b^2 - D$ を満たす整数の組 (a, c) は有限個である. したがって, a, c の取り得る整数値もまた有限個である. ゆえに, D が与えられたとき, D を判別式にもつ簡約 2 次形式の個数は有限である. □

[定理 15.3] 任意の正値 2 次形式 f に対して, f と正に対等な簡約 2 次形式が存在する.

[証明] $f(x, y) = ax^2 + bxy + cy^2$ とおく. また, $D = b^2 - 4ac$ を f の判別式, $g(x) = ax^2 + bx + c$ を f に対応する 2 次多項式, $\theta = (-b + \sqrt{D})/2a$ を $g(x)$ の第 1 根とする.

$D < 0$ かつ $a > 0$ だから, θ は上半平面 $\mathcal{H}$ に属する. $\mathcal{F}$ を $SL_2(\mathbb{Z})$ に関する基本領域とすると, θ はある $\theta_0 \in \mathcal{F}$ と正に対等である (定理 8.5). 定理 9.5 より, θ_0 もまたある整数係数 2 次多項式 $g_0(x')$ の第 1 根である. $g_0(x')$ に対応する 2 次形式を $f_0(x', y')$ とすれば, 定理 15.1 より, f_0 は簡約である. また, θ と θ_0 とが正に対等であることから, 定理 14.5 より, f と f_0 とは正に対等である. □

[定理 15.4] 2 つの簡約 2 次形式は, 正に対等ならば等しい.

[証明] $f(x,y)=ax^2+bxy+cy^2$ と $f'(x',y')=a'x'^2+b'x'y'+c'y'^2$ を互いに正に対等な簡約 2 次形式とする. また, $g(x)$, $g'(x')$ をそれぞれ f, f' に対応する 2 次多項式とし, θ を $g(x)$ の第 1 根, θ' を $g'(x')$ の第 1 根とする.

f と f' は正に対等だから, 定理 14.5 より, θ と θ' とは正に対等である. また, $\mathcal{F}$ を $SL_2(\mathbb{Z})$ に関する基本領域とすると, 定理 15.1 より, θ, $\theta' \in \mathcal{F}$. ゆえに, 定理 8.6 より, $\theta=\theta'$. したがって, 定理 14.5 より, $f=f'$. □

[定理 15.5] f, f' を正値 2 次形式とする. このとき, f と f' とが正に対等であるための必要十分条件は, f と f' がある共通の簡約 2 次形式 f_0 と正に対等であることである.

[証明] (必要性)　定理 15.3 より, ある簡約 2 次形式 f_0 が存在して f は f_0 と正に対等である. 同様に, ある簡約 2 次形式 f_0' が存在して f' は f_0' と正に対等である. 定理 15.4 より, $f_0=f_0'$ となる.

(十分性)　f が f_0 と正に対等で, f_0 が f' と正に対等であれば, f は f' と正に対等である.　□

16　正の判別式をもつ 2 次形式

D を正の整数で, 0 も平方数でもないものとする. 判別式 D の 2 次形式 $f(x,y)=ax^2+bxy+cy^2$ が**簡約 2 次形式**あるとは, f が条件

$$a>0, \quad a-b+c>0, \quad a+b+c<0, \quad c<0 \tag{58}$$

を満たすときにいう. $f(x,y)$ に対応する 2 次多項式を $g(x)=ax^2+bx+c$ とすれば,

$$g(0)=c, \quad g(1)=a+b+c, \quad g(-1)=a-b+c$$

であるから, (58) は

$$a>0, \quad g(-1)>0, \quad g(0)<0, \quad g(1)<0 \tag{59}$$

と同値である. また, $2b=g(1)-g(-1)$ であるから, f が簡約ならば $b<0$ である.

f の判別式が正であり, かつ 0 でも平方数でもないという条件は, g の根が無理数であることと同値である.

[定理 16.1] $f(x,y)$ を判別式が正でも平方数でもない 2 次形式, $g(x)$ を f に対応する 2 次多項式, θ を $g(x)$ の第 1 根とする. このとき, $f(x,y)$ が簡約 2 次形式であるための必要十分条件は, θ が簡約 2 次無理数であること, すなわち,

$$-1<\overline{\theta}<0, \quad 1<\theta \tag{60}$$

が成り立つことである. ただし, $\overline{\theta}$ は θ の共役, すなわち $g(x)$ の第 2 根である.

[証明] $f(x,y)=ax^2+bxy+cy^2$, $D=b^2-4ac$ とおくと, $g(x)=ax^2+bx+c$, $\theta=(-b+\sqrt{D})/2a$, $\overline{\theta}=(-b-\sqrt{D})/2a$ と表せる. また, $g(x)$ を実数の範囲で因数分解すれば,

$$g(x)=a(x-\theta)(x-\overline{\theta}). \tag{61}$$

f が簡約ならば, (59) が成り立つ. $\overline{\theta}<\theta$ かつ $a>0$ だから, (61) より, 任意の実数 x に対して,

$$g(x)=\begin{cases} <0, & \overline{\theta}<x<\theta, \\ =0, & x=\theta \text{ または } x=\overline{\theta}, \\ >0, & x<\overline{\theta} \text{ または } \theta<x \end{cases}$$

が成り立つ. これと $g(-1)>0$, $g(0)<0$, $g(1)<0$ より, $-1<\overline{\theta}<0$ と $1<\theta$ が得られる. すなわち, (60) が成り立つ.

逆に, (60) が成り立てば,

$$\frac{\sqrt{D}}{a}=\theta-\overline{\theta}>0$$

より $a>0$ が得られる. さらに, (61) より, $g(-1)>0$, $g(0)<0$, $g(1)<0$ が得られる. したがって, (59) が成り立つ. □

[定理 16.2] D を 0 でも平方数でもない正の整数とする. このとき, 判別式 D の簡約 2 次形式は有限個しかない.

[証明] f を判別式 D の簡約 2 次形式とし, $f(x,y)=ax^2+bxy+cy^2$ とおくと, 定理 16.1 より

$$0<\frac{b+\sqrt{D}}{2a}<1<\frac{-b+\sqrt{D}}{2a}$$

であるから,

$$0<b+\sqrt{D}<2a<-b+\sqrt{D}.$$

これより,

$$|b|<\sqrt{D}$$

が得られる. よって, b の取り得る整数値は有限個である. さらに, 各 b に対して, $4ac=b^2-D$ を満たす整数の組 (a,c) は有限個である. したがって, a, c の取り得る整数値もまた有限個である. ゆえに, D が与えられたとき, D を判別式にもつ簡約 2 次形式の個数は有限である. □

[定理 16.3] 0 でも平方数でもない判別式 $D>0$ をもつ任意の 2 次形式 f に対して, f と正に対等な簡約 2 次形式が存在する.

[証明] $f(x,y)=ax^2+bxy+cy^2$ とおく. また, $D=b^2-4ac$ を f の判別式, $g(x)=ax^2+bx+c$ を f に対応する 2 次多項式, $\theta=(-b+\sqrt{D})/2a$ を $g(x)$ の第 1 根とする.

D は 0 でも平方数でもない正の整数なので, θ は 2 次無理数である. 定理 12.7 より, θ と正に対等なある簡約 2 次無理数 θ_0 が存在する. 定理 9.5 より, θ_0 もまたある整数係数 2 次多項式 $g_0(x')$ の第 1 根である. $g_0(x')$ に対応する 2 次形式を $f_0(x',y')$ とすれば, 定理 16.1 より, f_0 は簡約である. また, θ と θ_0 とが正に対等であることから, 定理 14.5 より, f と f_0 とは正に対等である. □

17　2 次形式による整数の表現

n を整数, $f(x,y)=ax^2+bxy+cy^2$ を 2 次形式とする. x, y に関する不定方程式

$$ax^2+bxy+cy^2=n \tag{62}$$

が整数解 (x,y) を持つとき, n は 2 次形式 f によって**表現される**という. また, $\gcd(x,y)=1$ なる解があるとき, それを**原始解**といい, n は f によって**原始的に表現される**という.

方程式 (62) が $g=\gcd(x,y)>1$ なる整数解 (x,y) を持つとき, $g^2 \mid n$ であるから, (62) の両辺を g^2 で割ることにより,

$$a\left(\frac{x}{g}\right)^2+b\cdot\frac{x}{g}\cdot\frac{y}{g}+c\left(\frac{y}{g}\right)^2=\frac{n}{g^2}$$

となって, n/g^2 が $f(x,y)$ によって原始的に表現される.

$P=\begin{bmatrix}p & q\\ r & s\end{bmatrix}\in GL_2(\mathbb{Z})$ とし, 変数変換

$$\begin{bmatrix}x\\ y\end{bmatrix}=P\begin{bmatrix}x'\\ y'\end{bmatrix}$$

を考えると, (50) より $f(x,y)=ax^2+bxy+cy^2$ は整数係数 2 元 2 次形式

$$f'(x',y')=a'x'^2+b'x'y'+c'y'^2$$

に変換されるのであった. このとき, 逆の変換

$$\begin{bmatrix}x'\\ y'\end{bmatrix}=P^{-1}\begin{bmatrix}x\\ y\end{bmatrix},\quad P^{-1}=\frac{1}{\det P}\begin{bmatrix}s & -q\\ -r & p\end{bmatrix},\quad \det P=\pm1$$

によって, 方程式 $f(x,y)=n$ の整数解 (x,y) は方程式 $f'(x',y')=n$ の整数解 (x',y') に移される.

したがって, 整数 n が 2 次形式 f で表現されるならば, n は f から P による変数変換によって得られる 2 次形式 f' でも表現される.

特に, n を整数とし, $f(x,y)$, $f'(x',y')$ を互いに対等な 2 次形式とするとき, n が f で表現されることと, f' で表現されることとは同値である.

［定理 17.1］ 正の整数 n が判別式 D の 2 次形式によって原始的に表現されるための必要十分条件は, z に関する合同方程式

$$z^2 \equiv D \pmod{4n} \tag{63}$$

が解を持つことである.

［証明］ (x_0, y_0) を方程式 (62) の原始解とする. $\gcd(x_0, y_0) = 1$ より, ある z_0, $w_0 \in \mathbb{Z}$ が存在して

$$x_0 z_0 + y_0 w_0 = 1.$$

ここで, 変数変換

$$\begin{bmatrix} x \\ y \end{bmatrix} = P \begin{bmatrix} x' \\ y' \end{bmatrix}, \quad P = \begin{bmatrix} x_0 & -w_0 \\ y_0 & z_0 \end{bmatrix}$$

を考えると, $P \in GL_2(\mathbb{Z})$ であり, §14 の関係式 (50) より $f(x, y) = ax^2 + bxy + cy^2$ は整数係数 2 元 2 次形式

$$f'(x', y') = nx'^2 + b'x'y' + c'y'^2$$

に変換される. $f \sim f'$ だから, 定理 14.3 より f, f' の判別式は一致する. すなわち,

$$b'^2 - 4nc' = D.$$

よって, $z = b'$ が合同方程式 (63) の解になる.

逆に, 合同方程式 (63) に解 $z = b$ が存在すれば, ある $c \in \mathbb{Z}$ が存在して $b^2 - 4nc = D$ が成り立つ. このとき, $f(x, y) = nx^2 + bxy + cy^2$ とおけば, f の判別式は D であり, 方程式 (62) は原始解 $(x, y) = (1, 0)$ を持つ. □

参考文献

[1] 高木貞治: 初等整数論講義 第 2 版, 岩波書店, 1971.

[2] 遠山啓: 初等整数論, 日本評論社, 1972.

[3] 和田秀男: 数の世界—整数論への道, 岩波書店, 1981.

[4] 河田敬義: 数論—古典数論から類体論へ, 岩波書店, 1992.

[5] 木田祐司, 牧野潔夫: UBASIC によるコンピュータ整数論, 日本評論社, 1994.

[6] G. M. ハーディ, E. M. ライト: 数論入門 I, シュプリンガー・フェアラーク東京, 2001.

索 引