

# 連分数論入門<sup>\*</sup>

佐藤 篤<sup>†</sup>

## 目 次

|   |              |    |
|---|--------------|----|
| 1 | 有理整数の整除      | 3  |
| 2 | 連分数          | 11 |
| 3 | 実数の連分数展開     | 17 |
| 4 | 連分数展開の一意性    | 24 |
| 5 | 2 次無理数と循環連分数 | 29 |
| 6 | 有理数による実数の近似  | 37 |
| 7 | Pell 方程式     | 44 |
|   | 参考文献         | 51 |
|   | 問題略解         | 52 |

---

<sup>\*</sup>代数学特選題目 (1998 年度, 於 宮城教育大学) 講義ノートに加筆修正 [2024 年 7 月 9 日版]

<sup>†</sup>東北学院大学情報学部 (E-mail: [atsushi@mail.tohoku-gakuin.ac.jp](mailto:atsushi@mail.tohoku-gakuin.ac.jp))

## 記号と用語

- 線型代数学, 微分積分学ならびに集合と位相の基礎は既知であるものとする. また, 集合と写像に関する標準的な記号, 特に次の記号は断りなしに用いる:

$\mathbb{Z}$  有理整数全体のなす集合.

$\mathbb{Q}$  有理数全体のなす集合.

$\mathbb{R}$  実数全体のなす集合.

さらに, 正の実数 (正の有理整数) 全体のなす集合を  $\mathbb{R}_+$  ( $\mathbb{Z}_+$ ) で表す.

- $X, Y$  を集合とすると,  $Y$  が  $X$  の部分集合であることを  $Y \subset X$  または  $X \supset Y$  で表す. また, 差集合  $\{x \in X; x \notin Y\}$  を  $X \setminus Y$  で表す. さらに, 空集合を  $\emptyset$  で表す.
- $\alpha \in \mathbb{R}$  に対し,  $\alpha$  以下の有理整数のうちで最大のものを  $\lfloor \alpha \rfloor$  で表す:

$$\lfloor \alpha \rfloor := \max\{a \in \mathbb{Z}; a \leq \alpha\}.$$

$\lfloor \alpha \rfloor$  を  $\alpha$  の整数部分という. これは不等式  $0 \leq \alpha - \lfloor \alpha \rfloor < 1$  をみたす (ただ 1 つの) 有理整数に他ならない.  $\alpha$  の整数部分を  $\lfloor \alpha \rfloor$  と表している文献も多いが, 本稿では角括弧  $\lfloor \cdot \rfloor$  は別の意味に用いる.

## 1 有理整数の整除

### 1.1 約数と倍数

$a, b \in \mathbb{Z}$  に対し,  $b = ak$  となるような  $k \in \mathbb{Z}$  が存在するとき,  $a$  は  $b$  の約数 ( $a$  は  $b$  を割り切る),  $b$  は  $a$  の倍数 ( $b$  は  $a$  で割り切れる) であるといい, そのことを  $a \mid b$  と表す. また,  $a \in \mathbb{Z}$  の倍数全体からなる集合を  $a\mathbb{Z}$  で表す:

$$a\mathbb{Z} := \{b \in \mathbb{Z} ; a \mid b\} = \{ak ; k \in \mathbb{Z}\}.$$

0 は任意の  $a \in \mathbb{Z}$  の倍数であり, 1 は任意の  $b \in \mathbb{Z}$  の約数である. また,

$$a \mid b \iff (-a) \mid b \iff a \mid (-b) \iff (-a) \mid (-b)$$

が成り立つ.

**命題 1.1**  $a, b \in \mathbb{Z}$  に対し:

- (1)  $a \mid b, b \neq 0 \implies |a| \leq |b|$ .
- (2)  $a \mid b \iff b \in a\mathbb{Z} \iff b\mathbb{Z} \subset a\mathbb{Z}$ .
- (3)  $a\mathbb{Z} = b\mathbb{Z} \iff |a| = |b|$ .

[証明] (1)  $b = ak \neq 0$  ( $k \in \mathbb{Z}$ ) とすると,  $k \neq 0$  より  $|k| \geq 1$  となるから,  $|b| = |a| \cdot |k| \geq |a|$ .

(2) まず  $b = ak$  ( $k \in \mathbb{Z}$ ) とすると, 任意の  $l \in \mathbb{Z}$  に対して  $bl = a(kl) \in a\mathbb{Z}$  が成り立つから  $b\mathbb{Z} \subset a\mathbb{Z}$ . 逆に  $b\mathbb{Z} \subset a\mathbb{Z}$  とすると  $b = b \cdot 1 \in b\mathbb{Z} \subset a\mathbb{Z}$ . 従って  $b \in a\mathbb{Z}$  と  $b\mathbb{Z} \subset a\mathbb{Z}$  は同値. なお,  $a \mid b$  と  $b \in a\mathbb{Z}$  が同値であることは明らか.

(3)  $a\mathbb{Z} = b\mathbb{Z}$  とすると, (2) より  $b = ak$  となるような  $k \in \mathbb{Z}$  と  $a = bl$  となるような  $l \in \mathbb{Z}$  が存在することがわかる. 従って,  $ab \neq 0$  ならば (1) より  $|a| \leq |b|$  かつ  $|a| \geq |b|$ . また  $ab = 0$  ならば  $a = b = 0$ . いずれの場合にも  $|a| = |b|$  となる. 逆に  $|a| = |b|$  ならば  $a\mathbb{Z} = b\mathbb{Z}$  となることは容易. □

$A \subset \mathbb{R}, \neq \emptyset$  が加法について閉じている (減法について閉じている) とは, 次が成り立つことをいう:

$$\alpha, \alpha' \in A \implies \alpha + \alpha' \in A \quad (\alpha - \alpha' \in A).$$

**例 1.2** (1)  $\alpha \in \mathbb{R}$  に対し, 集合

$$\alpha\mathbb{Z} := \{\alpha k ; k \in \mathbb{Z}\}$$

は加法についても減法についても閉じている.

(2)  $A_1, A_2, \dots, A_n \subset \mathbb{R}, \neq \emptyset$  が加法 (減法) について閉じているならば, それらの共通部分

$$A_1 \cap A_2 \cap \dots \cap A_n$$

や “和”

$$A_1 + A_2 + \dots + A_n := \{ \alpha_1 + \alpha_2 + \dots + \alpha_n ; \alpha_1 \in A_1, \alpha_2 \in A_2, \dots, \alpha_n \in A_n \}$$

(和集合  $A_1 \cup A_2 \cup \dots \cup A_n$  とは異なることに注意) も加法 (減法) について閉じている.

**問題 1.3**  $A \subset \mathbb{R}, \neq \emptyset$  が減法について閉じているならば, 次が成り立つことを示せ:

- (1)  $0 \in A$ .
- (2)  $\alpha \in A \implies -\alpha \in A$ .
- (3)  $A$  は加法について閉じている.

**定理 1.4**  $A \subset \mathbb{Z}, \neq \emptyset$  が減法について閉じているならば,  $A = a\mathbb{Z}$  となるような  $a \in \mathbb{Z}_+ \cup \{0\}$  がただ 1 つ存在する.

[証明] 一意性は命題 1.1 の (3) より従うから存在を示す. まず, 問題 1.3 の (1) より  $0 \in A$ . もし  $A = \{0\}$  ならば  $a = 0$  とすればよいから, 以下  $A \neq \{0\}$  の場合を考える. このとき, 問題 1.3 の (2) より  $A_+ := A \cap \mathbb{Z}_+$  は空ではない. そこで

$$a := \min A_+$$

と置き,  $A = a\mathbb{Z}$  となることを示す. 明らかに  $a \in A$  であるから, 問題 1.3 の (2) と (3) より  $a\mathbb{Z} \subset A$  となることがわかる. 逆に, 任意の  $a' \in A$  に対し,

$$a'' := a' - a \left\lfloor \frac{a'}{a} \right\rfloor$$

と置くと,  $a' \in A$  と  $a \left\lfloor \frac{a'}{a} \right\rfloor \in a\mathbb{Z} \subset A$  より  $a'' \in A$ . また

$$0 \leq \frac{a'}{a} - \left\lfloor \frac{a'}{a} \right\rfloor < 1$$

より  $0 \leq a'' < a$ . 従って,  $a$  の最小性より  $a'' = 0$  であることがわかる. このとき  $a' = a \left\lfloor \frac{a'}{a} \right\rfloor \in a\mathbb{Z}$ . よって  $A \subset a\mathbb{Z}$  となる. □

**問題 1.5**  $A \subset \mathbb{R}, \neq \emptyset$  が減法について閉じているならば, 次のいずれか一方が成り立つことを示せ:

- (a)  $A = \alpha\mathbb{Z}$  となるような  $\alpha \in \mathbb{R}_+ \cup \{0\}$  がただ 1 つ存在する.
- (b) 任意の開区間  $I \subset \mathbb{R}$  に対して  $A \cap I \neq \emptyset$ .

## 1.2 最大公約数と最小公倍数

$a_1, a_2, \dots, a_n \in \mathbb{Z}$  の共通の約数を公約数という.  $a_1 = a_2 = \dots = a_n = 0$  ならば任意の有理整数は  $a_1, a_2, \dots, a_n$  の公約数であるが, それ以外の場合には, 命題 1.1 の (1) より,  $a_1, a_2, \dots, a_n$  の公約数  $b$  は不等式

$$|b| \leq \min\{|a_i|; 1 \leq i \leq n, a_i \neq 0\}$$

をみたす.  $a_1, a_2, \dots, a_n$  の正の公約数のうち最大のものを最大公約数といい,  $\gcd(a_1, a_2, \dots, a_n)$  で表す. ただし  $a_1 = a_2 = \dots = a_n = 0$  の場合には, それらの最大公約数は 0 と定めることにする.

**命題 1.6**  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  に対し,  $d := \gcd(a_1, a_2, \dots, a_n)$  と置くと,

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = d\mathbb{Z}$$

が成り立つ.

[証明] 例 1.2 と定理 1.4 より,

$$a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = a\mathbb{Z}$$

となるような  $a \in \mathbb{Z}_+ \cup \{0\}$  が (ただ 1 つ) 存在する. ここで  $a = a \cdot 1 \in a\mathbb{Z}$  であるから,

$$a_1k_1 + a_2k_2 + \dots + a_nk_n = a$$

となるような  $k_1, k_2, \dots, k_n \in \mathbb{Z}$  がとれる. 従って  $d = 0$  (i.e.,  $a_1 = a_2 = \dots = a_n = 0$ ) ならば  $a = 0$ . 以下  $d \neq 0$  とする. このとき  $a \in \mathbb{Z}_+$  であって,  $d$  が  $a_1, a_2, \dots, a_n$  の公約数であることより  $d \mid a$ . 他方, 各  $i$  に対して  $a_i \in a_1\mathbb{Z} + a_2\mathbb{Z} + \dots + a_n\mathbb{Z} = a\mathbb{Z}$  が成り立つから,  $a$  は  $a_1, a_2, \dots, a_n$  の正の公約数である. よって  $d$  の最大性より  $a \leq d$ . 以上より  $a = d$  となることがわかる.  $\square$

**系 1.7**  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  とするとき,

$$a_1k_1 + a_2k_2 + \dots + a_nk_n = \gcd(a_1, a_2, \dots, a_n)$$

となるような  $k_1, k_2, \dots, k_n \in \mathbb{Z}$  が存在する.

**系 1.8**  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  とするとき,  $b \in \mathbb{Z}$  に対して次は同値:

- (a)  $b$  は  $a_1, a_2, \dots, a_n$  の公約数.
- (b)  $b \mid \gcd(a_1, a_2, \dots, a_n)$ .

**問題 1.9** (1)  $a, b \in \mathbb{Z}$  に対して次の同値性を示せ:

$$\gcd(a, b) = 1 \iff ak + bl = 1 \text{ となるような } k, l \in \mathbb{Z} \text{ が存在する.}$$

( $a, b \in \mathbb{Z}$  が  $\gcd(a, b) = 1$  をみたすとき,  $a$  と  $b$  は互いに素であるという.)

(2)  $a, a' \in \mathbb{Z}$  と  $b, b' \in \mathbb{Z}_+$  が

$$\frac{a}{b} = \frac{a'}{b'}, \quad \gcd(a, b) = \gcd(a', b') = 1$$

をみたすならば  $a = a'$  かつ  $b = b'$  であることを素因数分解の一意性を用いずに証明せよ.

$a_1, a_2, \dots, a_n \in \mathbb{Z}$  の共通の倍数を公倍数という.  $a_1, a_2, \dots, a_n$  の中に 1 個でも 0 があればそれらの公倍数は 0 に限るが, それ以外の場合には, 命題 1.1 の (1) より,  $a_1, a_2, \dots, a_n$  の公倍数  $b$  は不等式

$$|b| \geq \max\{|a_i|; 1 \leq i \leq n\}$$

をみたす.  $a_1, a_2, \dots, a_n$  の正の公倍数のうち最小のものを最小公倍数といい,  $\text{lcm}(a_1, a_2, \dots, a_n)$  で表す. ただし  $a_1 a_2 \cdots a_n = 0$  の場合には, それらの最小公倍数は 0 と定めることにする.

**命題 1.10**  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  に対し,  $m := \text{lcm}(a_1, a_2, \dots, a_n)$  と置くと,

$$a_1 \mathbb{Z} \cap a_2 \mathbb{Z} \cap \cdots \cap a_n \mathbb{Z} = m \mathbb{Z}$$

が成り立つ.

[証明] 例 1.2 と定理 1.4 より,

$$a_1 \mathbb{Z} \cap a_2 \mathbb{Z} \cap \cdots \cap a_n \mathbb{Z} = a \mathbb{Z}$$

となるような  $a \in \mathbb{Z}_+ \cup \{0\}$  が (ただ 1 つ) 存在する.  $a_1 \mathbb{Z} \cap a_2 \mathbb{Z} \cap \cdots \cap a_n \mathbb{Z}$  は  $a_1, a_2, \dots, a_n$  の公倍数全体のなす集合に他ならないから,  $b \in \mathbb{Z}$  が  $a_1, a_2, \dots, a_n$  の公倍数であるためには  $a \mid b$  となる必要かつ十分である. 以上より  $a = m$  となることがわかる.  $\square$

**系 1.11**  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  とするとき,  $b \in \mathbb{Z}$  に対して次は同値:

(a)  $b$  は  $a_1, a_2, \dots, a_n$  の公倍数.

(b)  $\text{lcm}(a_1, a_2, \dots, a_n) \mid b$ .

**問題 1.12**  $a, b, c \in \mathbb{Z}$  に対し, 次が成り立つことを示せ:

(1)  $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c)) = \gcd(a, b, c)$ .

$$(2) \text{ lcm}(\text{lcm}(a, b), c) = \text{lcm}(a, \text{lcm}(b, c)) = \text{lcm}(a, b, c).$$

$$(3) \text{ gcd}(ab, ac) = |a| \text{ gcd}(b, c).$$

$$(4) \text{ lcm}(ab, ac) = |a| \text{ lcm}(b, c).$$

**命題 1.13**  $a, b \in \mathbb{Z}$  に対し,  $d := \text{gcd}(a, b)$ ,  $m := \text{lcm}(a, b)$  と置くと,

$$dm = |ab|$$

が成り立つ.

[証明]  $ab = 0$  のときは明らか. 以下,  $ab \neq 0$  とする. まず

$$\frac{ab}{d} = a \cdot \frac{b}{d} = b \cdot \frac{a}{d}$$

は  $a$  と  $b$  の公倍数であるから, 系 1.11 より

$$\frac{ab}{d} = mk$$

となるような  $k \in \mathbb{Z}$  が存在する. このとき  $k \neq 0$  であって

$$\frac{a}{dk} = \frac{m}{b}, \quad \frac{b}{dk} = \frac{m}{a}$$

は共に  $\mathbb{Z}$  に属するから,  $dk$  は  $a$  と  $b$  の公約数である. 従って系 1.8 より

$$d = dkl$$

となるような  $l \in \mathbb{Z}$  が存在する. よって  $k = l \in \{1, -1\}$  となり, 求める等式を得る. □

### 1.3 Euclid の互除法

**補題 1.14**  $a, b, c \in \mathbb{Z}$  とすると,

$$\text{gcd}(a, b) = \text{gcd}(a - bc, b)$$

が成り立つ.

[証明] まず, 任意の  $k, l \in \mathbb{Z}$  に対して

$$ak + bl = (a - bc)k + b(ck + l) \in (a - bc)\mathbb{Z} + b\mathbb{Z}$$

が成り立つことより,

$$a\mathbb{Z} + b\mathbb{Z} \subset (a - bc)\mathbb{Z} + b\mathbb{Z}.$$

逆に, 任意の  $k, l \in \mathbb{Z}$  に対して

$$(a - bc)k + bl = ak + b(-ck + l) \in a\mathbb{Z} + b\mathbb{Z}$$

が成り立つことより,

$$(a - bc)\mathbb{Z} + b\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}.$$

従って  $a\mathbb{Z} + b\mathbb{Z} = (a - bc)\mathbb{Z} + b\mathbb{Z}$  となり, 命題 1.6 より求める等式を得る.  $\square$

**定理 1.15 (Euclid の互除法)**  $a \in \mathbb{Z}$  と  $b \in \mathbb{Z}_+$  に対し,  $a_0, b_0, c_0, a_1, b_1, c_1, \dots \in \mathbb{Z}$  を次により定める:

$$\begin{pmatrix} a_0 \\ b_0 \end{pmatrix} := \begin{pmatrix} a \\ b \end{pmatrix}, \quad c_i := \left\lfloor \frac{a_i}{b_i} \right\rfloor \quad (i \geq 0), \quad \begin{pmatrix} a_{i+1} \\ b_{i+1} \end{pmatrix} := \begin{pmatrix} 0 & 1 \\ 1 & -c_i \end{pmatrix} \begin{pmatrix} a_i \\ b_i \end{pmatrix} \quad (i \geq 0).$$

ただし,  $b_i = 0$  の場合には  $c_i, a_{i+1}, b_{i+1}, \dots$  は定義しない (以上を **Euclid のアルゴリズム** という). このとき:

- (1)  $b_n = 0$  となるような  $n$  が  $0 < n \leq b$  という範囲で存在する.
- (2) (1) の  $n$  に対し,  $a_n = \gcd(a, b)$ .

[証明] (1) まず,  $b_i > 0$  ならば

$$b_{i+1} = a_i - b_i c_i = a_i - b_i \left\lfloor \frac{a_i}{b_i} \right\rfloor$$

より

$$0 \leq b_{i+1} < b_i$$

となることがわかる. 従って,  $b_0 = b > 0$  であることより求める  $n$  の存在がわかる.

- (2)  $b_i > 0$  ならば

$$a_{i+1} = b_i, \quad b_{i+1} = a_i - b_i c_i$$

であるから, 補題 1.14 より

$$\gcd(a_i, b_i) = \gcd(a_{i+1}, b_{i+1}).$$

従って,

$$\gcd(a, b) = \gcd(a_0, b_0) = \gcd(a_1, b_1) = \dots = \gcd(a_n, b_n) = \gcd(a_n, 0).$$

$n > 0$  より  $a_n = b_{n-1} > 0$  であるから,  $\gcd(a_n, 0) = a_n$  となり, 主張を得る.  $\square$

注意 1.16 定理より,

$$\begin{pmatrix} a_i \\ b_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -c_{i-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -c_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -c_0 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \quad (0 \leq i \leq n).$$

この等式の右辺を展開することにより

$$a_i = ak_i + bl_i$$

をみたす  $k_i, l_i \in \mathbb{Z}$  が具体的に構成できる. 特に  $i = n$  とすれば

$$\gcd(a, b) = ak_n + bl_n$$

となる (cf. 系 1.7).

例 1.17  $a = 240$ ,  $b = 135$  の場合.

$$\begin{aligned} \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} &= \begin{pmatrix} 240 \\ 135 \end{pmatrix}, & c_0 &= \left\lfloor \frac{240}{135} \right\rfloor = 1; \\ \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 240 \\ 135 \end{pmatrix} = \begin{pmatrix} 135 \\ 105 \end{pmatrix}, & c_1 &= \left\lfloor \frac{135}{105} \right\rfloor = 1; \\ \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 135 \\ 105 \end{pmatrix} = \begin{pmatrix} 105 \\ 30 \end{pmatrix}, & c_2 &= \left\lfloor \frac{105}{30} \right\rfloor = 3; \\ \begin{pmatrix} a_3 \\ b_3 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 105 \\ 30 \end{pmatrix} = \begin{pmatrix} 30 \\ 15 \end{pmatrix}, & c_3 &= \left\lfloor \frac{30}{15} \right\rfloor = 2; \\ \begin{pmatrix} a_4 \\ b_4 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 30 \\ 15 \end{pmatrix} = \begin{pmatrix} 15 \\ 0 \end{pmatrix} \end{aligned}$$

より  $n = 4$  で,

$$\gcd(240, 135) = a_4 = 15.$$

また,

$$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 4 & -7 \\ * & * \end{pmatrix}$$

より,

$$15 = 240 \cdot 4 + 135 \cdot (-7).$$

注意 1.18 上の計算は次のように書いてもよい:

$$240 = 135 \cdot 1 + 105,$$

$$135 = 105 \cdot 1 + 30,$$

$$105 = 30 \cdot 3 + 15,$$

$$30 = 15 \cdot 2 + 0$$

より,

$$\gcd(240, 135) = 15.$$

このときには

$$15 = 240k + 135l$$

となるような  $k, l \in \mathbb{Z}$  は次のように計算される:

$$\begin{aligned} 15 &= 105 - 30 \cdot 3 = 105 \cdot 1 + 30 \cdot (-3) \\ &= 105 \cdot 1 + (135 - 105 \cdot 1) \cdot (-3) = 135 \cdot (-3) + 105 \cdot 4 \\ &= 135 \cdot (-3) + (240 - 135 \cdot 1) \cdot 4 = 240 \cdot 4 + 135 \cdot (-7). \end{aligned}$$

**問題 1.19**  $a \in \mathbb{Z}, \geq 2$  とするとき, 相異なる  $e, f \in \mathbb{Z}_+$  に対して次が成り立つことを示せ:

$$\gcd(a^{2^e} + 1, a^{2^f} + 1) = \begin{cases} 1 & (a \text{ が偶数の場合}) \\ 2 & (a \text{ が奇数の場合}) \end{cases}.$$

## 2 連分数

次のような形の分数を (有限) 連分数という:

$$\gamma_0 + \frac{1}{\gamma_1 + \frac{1}{\gamma_2 + \frac{1}{\ddots + \frac{1}{\gamma_i}}}} \quad (i \geq 0)$$

(正確な名称は正則連分数だが, 本稿では正則な連分数しか扱わないので単に連分数と呼ぶ). このような数は, 通常の分数に簡約する際に 0 による除法が現れない限り意味をもつ. 例えば,  $\gamma_0 \in \mathbb{R}$  かつ  $\gamma_1, \gamma_2, \dots, \gamma_i \in \mathbb{R}_+$  ( $\gamma_0$  は 0 や負の数でもよい) ならば, 通分の際に分母に現れる数は全て正であり, 上の分数は 1 つの実数を定める (通分には加法, 乗法と除法しか用いないことに注意). 以下, 上の分数を次のように略記する:

$$[\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_i].$$

この記号は, 厳密には次のように定義される:

$$[\gamma_0] := \gamma_0, \quad [\gamma_0, \gamma_1, \dots, \gamma_i] := \gamma_0 + \frac{1}{[\gamma_1, \dots, \gamma_i]} \quad (i \geq 1).$$

ただし,  $[\gamma_1, \dots, \gamma_i] = 0$  の場合には  $[\gamma_0, \gamma_1, \dots, \gamma_i]$  を定義することはできない.

**例 2.1** (1)  $i = 1$  のとき,

$$[\gamma_0, \gamma_1] = \gamma_0 + \frac{1}{[\gamma_1]} = \gamma_0 + \frac{1}{\gamma_1} = \frac{\gamma_0\gamma_1 + 1}{\gamma_1}$$

は  $\gamma_1 \neq 0$  ならば意味をもつ.

(2)  $i = 2$  のとき,

$$[\gamma_0, \gamma_1, \gamma_2] = \gamma_0 + \frac{1}{[\gamma_1, \gamma_2]} = \gamma_0 + \frac{1}{\frac{\gamma_1\gamma_2 + 1}{\gamma_2}} = \gamma_0 + \frac{\gamma_2}{\gamma_1\gamma_2 + 1} = \frac{\gamma_0\gamma_1\gamma_2 + \gamma_0 + \gamma_2}{\gamma_1\gamma_2 + 1}$$

は  $\gamma_2 \neq 0$  かつ  $\gamma_1\gamma_2 + 1 \neq 0$  ならば意味をもつ.

**注意 2.2** 容易にわかるように,  $[\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_i]$  が定義できるならば, 次が成り立つ:

$$\begin{aligned} [\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_i] &= [\gamma_0, [\gamma_1, \gamma_2, \dots, \gamma_i]] = [\gamma_0, \gamma_1, [\gamma_2, \dots, \gamma_i]] \\ &= \dots = [\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_{i-2}, [\gamma_{i-1}, \gamma_i]] = [\gamma_0, \gamma_1, \gamma_2, \dots, \gamma_{i-1}, [\gamma_i]]. \end{aligned}$$

## 2.1 連分数の“分子”と“分母”

連分数  $[\gamma_0, \gamma_1, \dots, \gamma_i]$  を形式的に通分すると,  $\gamma_0, \gamma_1, \dots, \gamma_i$  の  $\mathbb{Z}$  係数の多項式の商に簡約することができる. 以下しばらく, これらの多項式の性質を調べることを考える.

$i \geq 0$  に対し,  $i+1$  個の文字  $x_0, x_1, \dots, x_i$  を変数とする  $\mathbb{Z}$  係数の多項式  $P_i = P_i(x_0, x_1, \dots, x_i)$  と  $Q_i = Q_i(x_0, x_1, \dots, x_i)$  を次により定める:

$$\begin{pmatrix} P_i \\ Q_i \end{pmatrix} := \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

例 2.3

$$\begin{pmatrix} P_0 \\ Q_0 \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_0 \\ 1 \end{pmatrix},$$

$$\begin{pmatrix} P_1 \\ Q_1 \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ 1 \end{pmatrix} = \begin{pmatrix} x_0 x_1 + 1 \\ x_1 \end{pmatrix},$$

$$\begin{pmatrix} P_2 \\ Q_2 \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 x_2 + 1 \\ x_2 \end{pmatrix} = \begin{pmatrix} x_0 x_1 x_2 + x_0 + x_2 \\ x_1 x_2 + 1 \end{pmatrix}.$$

命題 2.4  $i \geq 1$  に対し,

$$\begin{pmatrix} P_i \\ Q_i \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} P_{i-1}(x_1, \dots, x_i) \\ Q_{i-1}(x_1, \dots, x_i) \end{pmatrix}.$$

[証明]

$$\begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} P_{i-1}(x_1, \dots, x_i) \\ Q_{i-1}(x_1, \dots, x_i) \end{pmatrix}$$

より明らか. □

系 2.5  $i \geq 0$  に対し,

$$\frac{P_i}{Q_i} = [x_0, x_1, \dots, x_i].$$

[証明]  $i = 0$  の場合は明らか.  $i \geq 1$  のときには命題より,

$$\frac{P_i}{Q_i} = x_0 + \frac{Q_{i-1}(x_1, \dots, x_i)}{P_{i-1}(x_1, \dots, x_i)} = x_0 + \frac{1}{\frac{P_{i-1}(x_1, \dots, x_i)}{Q_{i-1}(x_1, \dots, x_i)}}.$$

これより求める等式を得る. □

命題 2.6  $i \geq 1$  に対し,

$$\begin{pmatrix} P_i & P_{i-1} \\ Q_i & Q_{i-1} \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix}.$$

[証明]

$$\begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_i & * \\ Q_i & * \end{pmatrix}$$

となることは定義から明らか. また,

$$\begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

より

$$\begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & P_{i-1} \\ * & Q_{i-1} \end{pmatrix}$$

となることがわかる. □

系 2.7  $i \geq 1$  に対し:

(1)

$$P_i Q_{i-1} - P_{i-1} Q_i = (-1)^{i-1}.$$

(2)

$$(-1)^{i-1} \begin{pmatrix} Q_{i-1} & -P_{i-1} \\ -Q_i & P_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -x_i \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -x_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -x_0 \end{pmatrix}.$$

[証明] 命題の等式において, 両辺の行列式と逆行列をとればよい. □

命題 2.8  $i \geq 2$  に対し,

$$\begin{pmatrix} P_i \\ Q_i \end{pmatrix} = x_i \begin{pmatrix} P_{i-1} \\ Q_{i-1} \end{pmatrix} + \begin{pmatrix} P_{i-2} \\ Q_{i-2} \end{pmatrix}.$$

[証明] 命題 2.6 より

$$\begin{pmatrix} P_i \\ Q_i \end{pmatrix} = \begin{pmatrix} x_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} x_{i-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} P_{i-1} & P_{i-2} \\ Q_{i-1} & Q_{i-2} \end{pmatrix} \begin{pmatrix} x_i \\ 1 \end{pmatrix}$$

となることによる. □

系 2.9  $i \geq 2$  に対し,

$$P_i Q_{i-2} - P_{i-2} Q_i = (-1)^i x_i.$$

[証明] 命題より

$$\begin{aligned} P_i Q_{i-2} - P_{i-2} Q_i &= (x_i P_{i-1} + P_{i-2}) Q_{i-2} - P_{i-2} (x_i Q_{i-1} + Q_{i-2}) \\ &= x_i (P_{i-1} Q_{i-2} - P_{i-2} Q_{i-1}) \end{aligned}$$

となるから, 系 2.7 の (1) より求める等式を得る. □

問題 2.10  $\begin{pmatrix} P_{-2} \\ Q_{-2} \end{pmatrix} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ ,  $\begin{pmatrix} P_{-1} \\ Q_{-1} \end{pmatrix} := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  と置くとき:

- (1) 命題 2.6 と系 2.7 の主張は  $i = 0$  でも成り立つことを示せ.
- (2) 命題 2.8 と系 2.9 の主張は  $i = 0, 1$  でも成り立つことを示せ.

問題 2.11  $i \geq 1$  に対し, 次が成り立つことを示せ:

$$Q_i = P_{i-1}(x_1, x_2, \dots, x_i).$$

問題 2.12  $i \geq 0$  に対し, 次が成り立つことを示せ:

$$P_i = P_i(x_i, \dots, x_1, x_0).$$

問題 2.13  $i \geq 0$  に対し, 次が成り立つことを示せ:

$$P_i = \begin{vmatrix} x_0 & 1 & & & 0 \\ -1 & x_1 & 1 & & \\ & -1 & \ddots & \ddots & \\ & & \ddots & \ddots & 1 \\ 0 & & & -1 & x_i \end{vmatrix}.$$

## 2.2 連分数の基本的性質

以下しばらく  $\gamma_0 \in \mathbb{R}$  かつ  $\gamma_1, \gamma_2, \dots \in \mathbb{R}_+$  とする. このとき:

命題 2.14  $i \geq 0$  に対し,

$$Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) > 0, \quad [\gamma_0, \gamma_1, \dots, \gamma_i] = \frac{P_i(\gamma_0, \gamma_1, \dots, \gamma_i)}{Q_i(\gamma_0, \gamma_1, \dots, \gamma_i)}.$$

[証明] まず,  $Q_0(\gamma_0) = 1$ ,  $Q_1(\gamma_0, \gamma_1) = \gamma_1$ . また, 命題 2.8 より

$$Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) = \gamma_i Q_{i-1}(\gamma_0, \gamma_1, \dots, \gamma_{i-1}) + Q_{i-2}(\gamma_0, \gamma_1, \dots, \gamma_{i-2}) \quad (i \geq 2).$$

これより  $Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) > 0$  がわかる. 後者の等式は系 2.5 より明らか. □

注意 2.15 上の証明と同様にして,  $\gamma_1, \gamma_2, \dots \geq 1$  ならば  $Q_0(\gamma_0) \leq Q_1(\gamma_0, \gamma_1)$  ならびに  $i \geq 1$  に対して

$$Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) + 1 \leq Q_{i+1}(\gamma_0, \gamma_1, \dots, \gamma_{i+1})$$

が成り立つことが示せる.

命題 2.16 (1)  $i \geq 1$  に対し,

$$[\gamma_0, \gamma_1, \dots, \gamma_i] - [\gamma_0, \gamma_1, \dots, \gamma_{i-1}] = \frac{(-1)^{i-1}}{Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) Q_{i-1}(\gamma_0, \gamma_1, \dots, \gamma_{i-1})}.$$

(2)  $i \geq 2$  に対し,

$$[\gamma_0, \gamma_1, \dots, \gamma_i] - [\gamma_0, \gamma_1, \dots, \gamma_{i-2}] = \frac{(-1)^i \gamma_i}{Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) Q_{i-2}(\gamma_0, \gamma_1, \dots, \gamma_{i-2})}.$$

[証明] 系 2.7 の (1) と系 2.9 より明らか. □

系 2.17

$$[\gamma_0] < [\gamma_0, \gamma_1, \gamma_2] < [\gamma_0, \gamma_1, \dots, \gamma_4] < \dots < [\gamma_0, \gamma_1, \dots, \gamma_5] < [\gamma_0, \gamma_1, \gamma_2, \gamma_3] < [\gamma_0, \gamma_1].$$

系 2.18  $\gamma_1, \gamma_2, \dots \geq 1$  ならば,  $0 \leq i < j$  をみたす  $i, j$  に対し,

$$|[\gamma_0, \gamma_1, \dots, \gamma_i] - [\gamma_0, \gamma_1, \dots, \gamma_j]| < \frac{1}{Q_i(\gamma_0, \gamma_1, \dots, \gamma_i)^2}.$$

また,

$$\lim_{i \rightarrow \infty} Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) = \infty.$$

[証明] 命題より

$$\begin{aligned} |[\gamma_0, \gamma_1, \dots, \gamma_i] - [\gamma_0, \gamma_1, \dots, \gamma_j]| &\leq |[\gamma_0, \gamma_1, \dots, \gamma_i] - [\gamma_0, \gamma_1, \dots, \gamma_{i+1}]| \\ &= \frac{1}{Q_i(\gamma_0, \gamma_1, \dots, \gamma_i) Q_{i+1}(\gamma_0, \gamma_1, \dots, \gamma_{i+1})} \end{aligned}$$

となることがわかるから, 注意 2.15 より主張が得られる. □

系 2.18 より,  $\gamma_1, \gamma_2, \dots \geq 1$  ならば, 数列  $\{[\gamma_0, \gamma_1, \dots, \gamma_i]\}_{i=0}^{\infty}$  は Cauchy 列であることがわかる:

$$\lim_{i, j \rightarrow \infty} |[\gamma_0, \gamma_1, \dots, \gamma_i] - [\gamma_0, \gamma_1, \dots, \gamma_j]| = 0.$$

この数列の極限值  $\lim_{i \rightarrow \infty} [\gamma_0, \gamma_1, \dots, \gamma_i] \in \mathbb{R}$  を

$$[\gamma_0, \gamma_1, \gamma_2, \dots] = \gamma_0 + \frac{1}{\gamma_1 + \frac{1}{\gamma_2 + \frac{1}{\ddots}}}$$

で表す. このような形の数をも無限連分数という.

## 2.3 単純連分数

以下  $c_0 \in \mathbb{Z}$  かつ  $c_1, c_2, \dots \in \mathbb{Z}_+$  とし,  $[c_0, c_1, c_2, \dots]$  という形の有限または無限の連分数を考える (このような連分数を単純連分数という). 任意の  $c \in \mathbb{Z}_+$  は  $c \geq 1$  をみたすから, 単純な無限連分数は常に意味をもつ. より正確には:

**定理 2.19** (1) 任意の有限単純連分数は 1 つの有理数を定める.

(2) 任意の無限単純連分数は 1 つの実数を定める.

**注意 2.20** 単純連分数  $[c_0]$  は  $[c_0 - 1, 1]$  と書ける. また,  $i \geq 1$  かつ  $c_i \geq 2$  ならば, 単純連分数  $[c_0, c_1, \dots, c_i]$  は  $[c_0, c_1, \dots, c_{i-1}, c_i - 1, 1]$  (これも単純な連分数) と書ける. よって, 有理数が有限単純連分数で表せたとしても, その方法は 1 通りではない.

次の命題は, 命題 2.14, 注意 2.15, 命題 2.16 ならびに系 2.17 より明らか:

**命題 2.21**  $p_i, q_i \in \mathbb{Z}$  ( $i \geq -2$ ) を

$$\begin{pmatrix} p_{-2} \\ q_{-2} \end{pmatrix} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} p_{-1} \\ q_{-1} \end{pmatrix} := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} p_i \\ q_i \end{pmatrix} := \begin{pmatrix} P_i(c_0, c_1, \dots, c_i) \\ Q_i(c_0, c_1, \dots, c_i) \end{pmatrix} \quad (i \geq 0)$$

により定める. このとき:

(1)

$$1 = q_0 \leq q_1 < q_2 < \dots.$$

(2)  $i \geq 0$  に対し,

$$[c_0, c_1, \dots, c_i] = \frac{p_i}{q_i}.$$

(3)  $i \geq 1$  に対し,

$$p_i q_{i-1} - p_{i-1} q_i = (-1)^{i-1}, \quad \frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^{i-1}}{q_i q_{i-1}}.$$

(4)

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

**問題 2.22** 上の命題と同じ記号の下で,  $i \geq -2$  に対して次が成り立つことを示せ:

$$\gcd(p_i, q_i) = 1.$$

**問題 2.23** 注意 1.16 における  $k_i, l_i \in \mathbb{Z}$  ( $0 \leq i \leq n$ ) は

$$k_i = (-1)^i q_{i-2}, \quad l_i = (-1)^{i-1} p_{i-2}$$

により与えられることを示せ.

### 3 実数の連分数展開

#### 3.1 有理数の場合

**命題 3.1**  $a \in \mathbb{Z}$  と  $b \in \mathbb{Z}_+$  に対し,  $a_0, b_0, c_0, a_1, b_1, c_1, \dots \in \mathbb{Z}$  を Euclid のアルゴリズム (定理 1.15) により定め,  $b_n = 0$  とする. このとき:

(1)  $i \geq 0$  に対し,

$$b_i = a_{i+1} \geq 1, \quad \frac{a_i}{b_i} = c_i + \frac{b_{i+1}}{a_{i+1}}.$$

(2)  $i \geq 1$  ならば  $c_i \geq 1$ .

(3)  $n \geq 2$  ならば  $c_{n-1} \geq 2$ .

**注意 3.2**  $b_n = 0$  としたことより  $c_n, a_{n+1}, b_{n+1}, \dots$  は定義されないから, 命題の主張が意味をもつのは  $i \leq n-1$  の場合に限られる. 以下, 定理や命題などにおける  $i$  の上限は, 特に断らない限り “主張が意味をもつような最大の値” (いまの場合には  $n-1$ ) と規約する.

**注意 3.3** 定理 1.15 で述べたように  $0 < n \leq b$  であつて,

$$n = 1 \iff \left\lfloor \frac{a}{b} \right\rfloor = \frac{a}{b} \iff \frac{a}{b} \in \mathbb{Z}$$

が成り立つ.

[命題 3.1 の証明] (1) 前者の主張は

$$b_0 = a_1 > b_1 = a_2 > \dots > b_{n-1} = a_n > b_n = 0$$

から明らか. また,  $b_{i+1} = a_i - b_i c_i$  より

$$\frac{b_{i+1}}{a_{i+1}} = \frac{a_i - b_i c_i}{b_i} = \frac{a_i}{b_i} - c_i$$

と後者の主張を得る.

(2) 定理 1.15 の証明で述べたように,  $i \geq 1$  に対して

$$0 < b_i < b_{i-1} = a_i$$

が成り立つから,

$$c_i = \left\lfloor \frac{a_i}{b_i} \right\rfloor \geq 1.$$

(3)  $b_n = a_{n-1} - b_{n-1} c_{n-1}$  が 0 であることより,

$$c_{n-1} = \frac{a_{n-1}}{b_{n-1}}$$

は 1 より大きい有理整数になる. □

命題 3.1 と同じ記号の下で,  $\frac{a}{b} \in \mathbb{Q}$  の有限単純連分数への展開が得られる:

$$\frac{a}{b} = [c_0, c_1, \dots, c_{n-1}].$$

注意 2.20 より, 右辺の連分数は

$$[c_0, c_1, \dots, c_{n-2}, c_{n-1} - 1, 1]$$

(これも単純な連分数) と書ける. 以上より:

定理 3.4 任意の有理数は有限単純連分数に (少なくとも 2 通りに) 展開される.

例 3.5 (1)  $a \in \mathbb{Z}$  とするとき,

$$\frac{a}{1} = [a] = [a - 1, 1].$$

(2) 例 1.17 より,

$$\frac{16}{9} = \frac{240}{135} = [1, 1, 3, 2] = [1, 1, 3, 1, 1].$$

### 3.2 一般の場合

命題 3.6  $\alpha \in \mathbb{R}$  に対し,  $\alpha_0, \alpha_1, \dots \in \mathbb{R}$  と  $c_0, c_1, \dots \in \mathbb{Z}$  を次により定める:

$$\alpha_0 := \alpha, \quad c_i := \lfloor \alpha_i \rfloor \quad (i \geq 0), \quad \alpha_{i+1} := \frac{1}{\alpha_i - c_i} \quad (i \geq 0).$$

ただし,  $\alpha_i \in \mathbb{Z}$  (i.e.,  $c_i = \alpha_i$ ) の場合には  $\alpha_{i+1}, c_{i+1}, \dots$  は定義しない (以上を連分数アルゴリズム  $\Delta$  という). このとき,  $i \geq 1$  に対し,

$$\alpha_i > 1, \quad c_i \geq 1.$$

また,  $i \geq 0$  に対し,

$$\alpha = [c_0, c_1, \dots, c_{i-1}, \alpha_i]$$

( $\alpha_i, c_i$  をそれぞれ  $\alpha$  の  $i$  次全商, 部分商という).

注意 3.7 (1)  $\alpha \in \mathbb{Q}$  の場合,  $\alpha = \frac{a}{b}$  ( $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}_+$ ) として  $a_0, b_0, c_0, a_1, b_1, c_1, \dots$  を Euclid のアルゴリズムにより定めると, この  $c_i$  は連分数アルゴリズムで定めた  $c_i$  と一致し, さらに  $\alpha_i = \frac{a_i}{b_i}$  が成り立つ. 実際, 定理 1.15 の  $c_i$  を  $c_i^{\text{old}}$ , 命題 3.6 の  $c_i$  を  $c_i^{\text{new}}$  と書くことにすると,

$$\alpha_0 = \alpha = \frac{a}{b} = \frac{a_0}{b_0}$$

であって,  $\alpha_i = \frac{a_i}{b_i}$  ならば

$$c_i^{\text{new}} = \lfloor \alpha_i \rfloor = \left\lfloor \frac{a_i}{b_i} \right\rfloor = c_i^{\text{old}}$$

および

$$\alpha_{i+1} = \frac{1}{\alpha_i - c_i^{\text{new}}} = \frac{b_i}{a_i - b_i c_i^{\text{old}}} = \frac{a_{i+1}}{b_{i+1}}$$

が成り立つ.

また,

$$\alpha_i \in \mathbb{Z} \iff b_i \mid a_i \iff b_{i+1} = 0$$

であるから, 定理 1.15 のように  $n$  をとると,  $\alpha_{n-1} \in \mathbb{Z}$  となる.

(2)  $\alpha \notin \mathbb{Q}$  の場合, 容易にわかるように  $\alpha_i \in \mathbb{Z}$  となることはない.

[命題 3.6 の証明] 定義より,  $i \geq 0$  かつ  $\alpha_i \notin \mathbb{Z}$  ならば

$$0 < \alpha_i - c_i < 1$$

であるから,

$$\alpha_{i+1} = \frac{1}{\alpha_i - c_i} > 1, \quad c_{i+1} = \lfloor \alpha_{i+1} \rfloor \geq 1.$$

また,

$$\alpha_i = c_i + \frac{1}{\alpha_{i+1}} = [c_i, \alpha_{i+1}] \quad (i \geq 0)$$

より,

$$\alpha = [\alpha_0] = [c_0, \alpha_1] = [c_0, c_1, \alpha_2] = \cdots = [c_0, c_1, \dots, c_{i-1}, \alpha_i] = \cdots$$

がわかる. □

**命題 3.8** 命題 3.6 と同じ記号の下で,  $p_i, q_i \in \mathbb{Z}$  ( $i \geq -2$ ) を命題 2.21 と同様に

$$\begin{pmatrix} p_{-2} \\ q_{-2} \end{pmatrix} := \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} p_{-1} \\ q_{-1} \end{pmatrix} := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} p_i \\ q_i \end{pmatrix} := \begin{pmatrix} P_i(c_0, c_1, \dots, c_i) \\ Q_i(c_0, c_1, \dots, c_i) \end{pmatrix} \quad (i \geq 0)$$

により定める. このとき:

(1)  $i \geq 0$  に対し,

$$\alpha = \frac{p_{i-1}\alpha_i + p_{i-2}}{q_{i-1}\alpha_i + q_{i-2}}, \quad \alpha_i = \frac{q_{i-2}\alpha - p_{i-2}}{-q_{i-1}\alpha + p_{i-1}}.$$

(2)  $i \geq 0$  に対し,

$$\alpha - \frac{p_i}{q_i} = \frac{(-1)^i}{(q_i\alpha_{i+1} + q_{i-1})q_i}$$

( $p_i, q_i$  をそれぞれ  $\alpha$  の  $i$  次近似分子, 近似分母といい,  $\frac{p_i}{q_i}$  ( $i \geq 0$ ) を  $\alpha$  の  $i$  次近似分数という).

[証明] (1) 命題 2.14 より

$$\alpha = [c_0, c_1, \dots, c_{i-1}, \alpha_i] = \frac{P_i(c_0, c_1, \dots, c_{i-1}, \alpha_i)}{Q_i(c_0, c_1, \dots, c_{i-1}, \alpha_i)}.$$

ここで, 命題 2.8 と問題 2.10 より

$$\left( \frac{P_i(c_0, c_1, \dots, c_{i-1}, \alpha_i)}{Q_i(c_0, c_1, \dots, c_{i-1}, \alpha_i)} \right) = \alpha_i \binom{p_{i-1}}{q_{i-1}} + \binom{p_{i-2}}{q_{i-2}}$$

であるから, 前者の等式が得られる. これから後者を導くのは容易 (cf. 問題 3.10).

(2) 命題 2.16 の (1) より,  $i \geq 1$  ならば

$$\frac{P_i(c_0, c_1, \dots, c_{i-1}, \alpha_i)}{Q_i(c_0, c_1, \dots, c_{i-1}, \alpha_i)} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^{i-1}}{Q_i(c_0, c_1, \dots, c_{i-1}, \alpha_i) q_{i-1}}$$

が成り立つから, 上で述べたことより求める等式を得る. □

**注意 3.9** 近似分子, 近似分母という言葉は筆者の造語なので本稿の外では通用しない. なお, 便宜上  $i = -2, -1$  に対してもこのように呼ぶことにする.

**問題 3.10**  $\alpha, \beta, \gamma, \delta \in \mathbb{R}$  ( $\alpha\delta - \beta\gamma \neq 0$ ) とするとき,  $\gamma\xi + \delta \neq 0$  をみたす  $\xi \in \mathbb{R}$  に対して

$$\eta := \frac{\alpha\xi + \beta}{\gamma\xi + \delta}$$

と置くと,  $-\gamma\eta + \alpha \neq 0$  ならびに

$$\xi = \frac{\delta\eta - \beta}{-\gamma\eta + \alpha}$$

が成り立つことを示せ.

**系 3.11** 命題 3.8 と同じ記号の下で:

(1)  $i \geq 0$  に対し,

$$\left| \alpha - \frac{p_i}{q_i} \right| \leq \frac{1}{q_i q_{i+1}} \leq \frac{1}{q_i^2}.$$

(2)  $i \geq 1$  に対し,

$$\left| \alpha - \frac{p_i}{q_i} \right| < \left| \alpha - \frac{p_{i-1}}{q_{i-1}} \right|.$$

(3)

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \dots \leq \alpha \leq \dots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

[証明] (1) 命題の (2) より

$$\left| \alpha - \frac{p_i}{q_i} \right| = \frac{1}{(q_i \alpha_{i+1} + q_{i-1}) q_i}$$

であって,  $\alpha_{i+1} \geq c_{i+1}$  より

$$q_i \alpha_{i+1} + q_{i-1} \geq q_i c_{i+1} + q_{i-1} = q_{i+1} \geq q_i.$$

これより求める不等式を得る.

(2)  $\alpha_{i+1} > 1$  より,

$$q_i \alpha_{i+1} + q_{i-1} > q_i + q_{i-1} \geq 2q_{i-1}.$$

従って, 命題の (2) より,

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{2q_i q_{i-1}}.$$

他方, 命題 2.21 の (3) より

$$\frac{1}{q_i q_{i-1}} = \left| \frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} \right| \leq \left| \alpha - \frac{p_i}{q_i} \right| + \left| \alpha - \frac{p_{i-1}}{q_{i-1}} \right|$$

が成り立つから, 求める不等式が得られる.

(3) 命題 2.21 の (4) と命題の (2) による. □

**注意 3.12** 上の系の (1) において,  $\alpha = \frac{p_i}{q_i}$  だと  $q_{i+1}$  は定義されないが, その場合でも  $\left| \alpha - \frac{p_i}{q_i} \right| \leq \frac{1}{q_i^2}$  は明らかに成り立つ.

**問題 3.13** 命題 3.8 と同じ記号の下で,  $i \geq 0$  に対して

$$\frac{1}{q_i q_{i+2}} < \left| \alpha - \frac{p_i}{q_i} \right|$$

が成り立つことを示せ.

無理数  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$  の  $i$  次部分商  $c_i$  は全ての  $i \geq 0$  に対して定義される.  $p_i, q_i$  ( $i \geq -2$ ) をそれぞれ  $\alpha$  の  $i$  次近似分子, 近似分母とすると, 系 3.11 の (1) は

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{q_i q_{i+1}} \leq \frac{1}{q_i^2}$$

となる. つまり, 第 1 の不等号において等号は成立しない. なお,  $i \geq 1$  ならば  $q_{i+1} > q_i$  であるから第 2 の不等号においても等号は成立しない. また, 既に述べたように

$$\lim_{i \rightarrow \infty} q_i = \infty.$$

これより  $\alpha$  の無限単純連分数への展開が得られる:

$$\alpha = \lim_{i \rightarrow \infty} \frac{p_i}{q_i} = [c_0, c_1, c_2, \dots].$$

以上より:

定理 3.14 任意の無理数は無限単純連分数に展開される.

例 3.15 (1)  $\alpha = \frac{16}{9}$  の場合.

$$\alpha_0 = \frac{16}{9}, \quad c_0 = \left\lfloor \frac{16}{9} \right\rfloor = 1;$$

$$\alpha_1 = \frac{9}{16 - 9 \cdot 1} = \frac{9}{7}, \quad c_1 = \left\lfloor \frac{9}{7} \right\rfloor = 1;$$

$$\alpha_2 = \frac{7}{9 - 7 \cdot 1} = \frac{7}{2}, \quad c_2 = \left\lfloor \frac{7}{2} \right\rfloor = 3;$$

$$\alpha_3 = \frac{2}{7 - 2 \cdot 3} = 2, \quad c_3 = \lfloor 2 \rfloor = 2.$$

これより:

$$\frac{p_0}{q_0} = \frac{1}{1} = 1,$$

$$\frac{p_1}{q_1} = \frac{1 \cdot 1 + 1}{1} = \frac{2}{1} = 2,$$

$$\frac{p_2}{q_2} = \frac{3 \cdot 2 + 1}{3 \cdot 1 + 1} = \frac{7}{4} = 1.75,$$

$$\frac{p_3}{q_3} = \frac{2 \cdot 7 + 2}{2 \cdot 4 + 1} = \frac{16}{9} = 1.77 \dots$$

(2)  $\alpha = \sqrt{2}$  の場合.

$$\alpha_0 = \sqrt{2}, \quad c_0 = \lfloor \sqrt{2} \rfloor = 1;$$

$$\alpha_1 = \frac{1}{\sqrt{2} - 1} = 1 + \sqrt{2}, \quad c_1 = \lfloor 1 + \sqrt{2} \rfloor = 2;$$

$$\alpha_2 = \frac{1}{(1 + \sqrt{2}) - 2} = 1 + \sqrt{2}, \quad c_2 = \lfloor 1 + \sqrt{2} \rfloor = 2;$$

$$\alpha_3 = \frac{1}{(1 + \sqrt{2}) - 2} = 1 + \sqrt{2}, \quad c_3 = \lfloor 1 + \sqrt{2} \rfloor = 2.$$

以下同様に, 任意の  $i \geq 1$  に対し,

$$\alpha_i = 1 + \sqrt{2}, \quad c_i = 2.$$

これより:

$$\frac{p_0}{q_0} = \frac{1}{1} = 1,$$

$$\frac{p_1}{q_1} = \frac{2 \cdot 1 + 1}{2} = \frac{3}{2} = 1.5,$$

$$\frac{p_2}{q_2} = \frac{2 \cdot 3 + 1}{2 \cdot 2 + 1} = \frac{7}{5} = 1.4,$$

$$\frac{p_3}{q_3} = \frac{2 \cdot 7 + 3}{2 \cdot 5 + 2} = \frac{17}{12} = 1.4166 \dots$$

なお, 上の計算より  $\sqrt{2}$  が無理数であることもわかる. また,

$$\sqrt{2} = [1, 2, 2, \dots, 2, \dots].$$

(3)  $\alpha = \pi$  の場合.

$$\alpha_0 = 3.1415926535 \dots, \quad c_0 = 3;$$

$$\alpha_1 = \frac{1}{0.1415926535 \dots} = 7.0625133 \dots, \quad c_1 = 7;$$

$$\alpha_2 = \frac{1}{0.0625133 \dots} = 15.9965 \dots, \quad c_2 = 15;$$

$$\alpha_3 = \frac{1}{0.9965 \dots} = 1.003 \dots, \quad c_3 = 1.$$

これより:

$$\frac{p_0}{q_0} = \frac{3}{1} = 3,$$

$$\frac{p_1}{q_1} = \frac{7 \cdot 3 + 1}{7} = \frac{22}{7} = 3.1428 \dots,$$

$$\frac{p_2}{q_2} = \frac{15 \cdot 22 + 3}{15 \cdot 7 + 1} = \frac{333}{106} = 3.141509 \dots,$$

$$\frac{p_3}{q_3} = \frac{1 \cdot 333 + 22}{1 \cdot 106 + 7} = \frac{355}{113} = 3.14159292 \dots$$

なお,

$$\frac{1}{0.003} = 333.3 \dots, \quad \frac{1}{0.004} = 250$$

であるから, 上の計算を続けても  $c_4$  を求めることはできない.

**問題 3.16** 次が成り立つことを示せ:

$$\sqrt{3} = [1, 1, 2, 1, 2, \dots, 1, 2, \dots],$$

$$\sqrt{5} = [2, 4, 4, \dots, 4, \dots],$$

$$\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \dots, 1, 1, 1, 4, \dots].$$

## 4 連分数展開の一意性

### 4.1 単純連分数と実数との対応

本節を通して

$$\mathbf{c} = (c_0, c_1, c_2, \dots) \quad (c_0 \in \mathbb{Z}, c_1, c_2, \dots \in \mathbb{Z}_+)$$

という形の有限数列 (無限数列) 全体のなす集合を  $\mathcal{C}_0$  ( $\mathcal{C}_\infty$ ) で表し,  $\mathcal{C}_0$  の部分集合  $\mathcal{C}'_0, \mathcal{C}''_0$  をそれぞれ

$$\mathcal{C}'_0 := \{(c_0, c_1, \dots, c_i) \in \mathcal{C}_0 ; i = 0 \text{ または } c_i \geq 2\},$$

$$\mathcal{C}''_0 := \{(c_0, c_1, \dots, c_i) \in \mathcal{C}_0 ; i \geq 1 \text{ かつ } c_i = 1\}$$

により定める. このとき  $\mathcal{C}_0 = \mathcal{C}'_0 \cup \mathcal{C}''_0$  かつ  $\mathcal{C}'_0 \cap \mathcal{C}''_0 = \emptyset$  となっている. また明らかに  $\mathcal{C}_0 \cap \mathcal{C}_\infty = \emptyset$ .

これらの記号を用いて §2.3 と §3 で述べたことを整理することを考える.

まず, 定理 2.19 で述べたことより, 写像

$$\varphi : \mathcal{C}_0 \cup \mathcal{C}_\infty \ni (c_0, c_1, c_2, \dots) \mapsto [c_0, c_1, c_2, \dots] \in \mathbb{R}$$

が定義できて,

$$\varphi(\mathcal{C}_0) \subset \mathbb{Q}$$

が成り立つ. また,

$$\delta : \mathcal{C}'_0 \ni (c_0, c_1, \dots, c_i) \mapsto (c_0, c_1, \dots, c_{i-1}, c_i - 1, 1) \in \mathcal{C}''_0$$

は明らかに全単射で, 注意 2.20 で述べたように, 任意の  $\mathbf{c} \in \mathcal{C}'_0$  に対して

$$\varphi(\delta(\mathbf{c})) = \varphi(\mathbf{c})$$

をみたす. 他方, 連分数アルゴリズム (命題 3.6) により写像

$$\psi : \mathbb{R} \ni \alpha \mapsto (c_0, c_1, c_2, \dots) \in \mathcal{C}_0 \cup \mathcal{C}_\infty \quad (c_i \text{ は } \alpha \text{ の } i \text{ 次部分商})$$

が定義できて, 命題 3.1 と注意 3.7 より

$$\psi(\mathbb{Q}) \subset \mathcal{C}'_0, \quad \psi(\mathbb{R} \setminus \mathbb{Q}) \subset \mathcal{C}_\infty$$

が成り立つ. さらに, 任意の  $\alpha \in \mathbb{R}$  に対して

$$\varphi(\psi(\alpha)) = \alpha$$

が成り立つ (定理 3.4, 定理 3.14). 逆に,  $\mathbf{c} \in \mathcal{C}_0 \cup \mathcal{C}_\infty$  に対して

$$\psi(\varphi(\mathbf{c})) = \begin{cases} \mathbf{c} & (\mathbf{c} \in \mathcal{C}'_0 \cup \mathcal{C}_\infty \text{ の場合}) \\ \delta(\mathbf{c}) & (\mathbf{c} \in \mathcal{C}''_0 \text{ の場合}) \end{cases}$$

が成り立つことは次の命題より従う:

命題 4.1 (1)  $\mathbf{c} = (c_0^*, c_1^*, \dots, c_j^*) \in \mathcal{C}_0$  とし,

$$\alpha := \varphi(\mathbf{c}) = [c_0^*, c_1^*, \dots, c_j^*]$$

の  $i$  次全商, 部分商をそれぞれ  $\alpha_i, c_i$  とする. このとき  $0 \leq i \leq j-1$  に対し,

$$\alpha_i = [c_i^*, c_{i+1}^*, \dots, c_j^*] \notin \mathbb{Z}, \quad c_i = c_i^*.$$

また,

$$\alpha_j = c_j = c_j^* \in \mathbb{Z}.$$

ただし,  $\mathbf{c} \in \mathcal{C}_0''$  の場合には

$$\alpha_{j-1} = c_{j-1} = c_{j-1}^* + 1 \in \mathbb{Z}$$

となる.

(2)  $\mathbf{c} = (c_0^*, c_1^*, c_2^*, \dots) \in \mathcal{C}_\infty$  とし,

$$\alpha := \varphi(\mathbf{c}) = [c_0^*, c_1^*, c_2^*, \dots]$$

の  $i$  次全商, 部分商をそれぞれ  $\alpha_i, c_i$  とする. このとき  $i \geq 0$  に対し,

$$\alpha_i = [c_i^*, c_{i+1}^*, c_{i+2}^*, \dots] \notin \mathbb{Z}, \quad c_i = c_i^*.$$

従って特に  $\alpha \notin \mathbb{Q}$ .

上の命題を証明するために, まず次の補題を示す:

補題 4.2  $c_0^* \in \mathbb{Z}$  かつ  $c_1^*, c_2^*, \dots, c_{j-1}^* \in \mathbb{Z}_+$  ( $j \geq 1$ ) とし,  $\beta \in \mathbb{R}, > 1$  に対して

$$\alpha := [c_0^*, c_1^*, \dots, c_{j-1}^*, \beta]$$

の  $i$  次全商, 部分商をそれぞれ  $\alpha_i, c_i$  とする. このとき  $0 \leq i \leq j-1$  に対し,

$$\alpha_i = [c_i^*, c_{i+1}^*, \dots, c_{j-1}^*, \beta] \notin \mathbb{Z}, \quad c_i = c_i^*.$$

また,

$$\alpha_j = \beta, \quad c_j = \lfloor \beta \rfloor.$$

[証明]  $0 \leq i \leq j$  をみたす  $i$  に対して

$$\alpha_i^* := [c_i^*, c_{i+1}^*, \dots, c_{j-1}^*, \beta]$$

と置く. このとき  $0 \leq i \leq j-1$  ならば,

$$\alpha_i^* > c_i^*.$$

また,

$$\alpha_j^* = \beta.$$

これより,  $0 \leq i \leq j-1$  に対して  $\alpha_{i+1}^* > 1$ , 従って

$$c_i^* < \alpha_i^* = c_i^* + \frac{1}{\alpha_{i+1}^*} < c_i^* + 1$$

が成り立つことがわかり,

$$\alpha_i^* \notin \mathbb{Z}, \quad [\alpha_i^*] = c_i^*.$$

よって  $\alpha_0 = \alpha = \alpha_0^*$  より主張を得る. □

[命題 4.1 の証明] (1)  $j = 0$  の場合は明らか.  $j \geq 1$  かつ  $c_j^* \geq 2$  の場合には, 補題において  $\beta := c_j^*$  と置けばよい. また,  $j \geq 1$  かつ  $c_j^* = 1$  の場合には

$$\alpha = [c_0^*, c_1^*, \dots, c_{j-2}^*, c_{j-1}^* + 1]$$

であるから, 既を示した場合に帰着される.

(2) 各  $i \geq 0$  に対して

$$\alpha_i^* := [c_i^*, c_{i+1}^*, c_{i+2}^*, \dots]$$

と置くと,

$$\alpha = [c_0^*, c_1^*, \dots, c_{i-1}^*, \alpha_i^*].$$

また,  $i \geq 1$  ならば

$$\alpha_i^* > c_i^* \geq 1.$$

従って補題より, 任意の  $i \geq 0$  に対して

$$\alpha_i = \alpha_i^* \notin \mathbb{Z}, \quad c_i = c_i^*$$

が成り立つ. □

以上より, 写像  $\varphi$  と  $\psi$  によって  $\mathcal{C}'_0 \cup \mathcal{C}_\infty$  と  $\mathbb{R}$  の間には 1 対 1 の対応がつくことがわかった. まとめると次のようになる:

**定理 4.3** 有理数はちょうど 2 通りに有限単純連分数に展開され, 無理数はただ 1 通りに無限単純連分数に展開される. また, 有限単純連分数の値は有理数で, 無限単純連分数の値は無理数である.

## 4.2 連分数展開と大小関係

連分数で与えられた数の大小を比べるのには次の命題が有効である:

**命題 4.4**  $c_0 \in \mathbb{Z}$  かつ  $c_1, c_2, \dots, c_{j-1} \in \mathbb{Z}_+$  ( $j \geq 1$ ) とし, 関数  $f: \mathbb{R}_+ \rightarrow \mathbb{R}$  を

$$f(\xi) := [c_0, c_1, \dots, c_{j-1}, \xi]$$

により定める. このとき,  $j$  が偶数 (奇数) ならば  $f$  は狭義単調増加 (減少).

[証明] 命題 2.21 と同様に  $p_{j-1}, p_{j-2}, q_{j-1}, q_{j-2} \in \mathbb{Z}$  を定めると, 命題 3.8 の (1) より,

$$f(\xi) = \frac{p_{j-1}\xi + p_{j-2}}{q_{j-1}\xi + q_{j-2}}.$$

従って  $f$  は  $\mathbb{R}_+$  で微分可能で,

$$f'(\xi) = \frac{p_{j-1}(q_{j-1}\xi + q_{j-2}) - (p_{j-1}\xi + p_{j-2})q_{j-1}}{(q_{j-1}\xi + q_{j-2})^2} = \frac{p_{j-1}q_{j-2} - p_{j-2}q_{j-1}}{(q_{j-1}\xi + q_{j-2})^2} = \frac{(-1)^j}{(q_{j-1}\xi + q_{j-2})^2}.$$

これより主張を得る. □

**系 4.5**  $c_0 \in \mathbb{Z}$  かつ  $c_1, c_2, \dots, c_{j-1} \in \mathbb{Z}_+$  ( $j \geq 1$ ) とし,  $\beta_1, \beta_2 \in \mathbb{R}, > 1$  とするとき,

$$[c_0, c_1, \dots, c_{j-1}, \beta_1] \leq \alpha \leq [c_0, c_1, \dots, c_{j-1}, \beta_2]$$

をみたす  $\alpha \in \mathbb{R}$  の  $i$  次部分商 ( $0 \leq i \leq j-1$ ) は  $c_i$  で与えられる.

[証明]  $\alpha$  が上の不等式をみたすならば, 命題と中間値の定理により

$$\alpha = [c_0, c_1, \dots, c_{j-1}, \beta]$$

となるような  $\beta \in \mathbb{R}, > 1$  が存在することがわかるから, 補題 4.2 より主張を得る. □

**例 4.6**  $\pi = 3.1415926535 \dots$  より

$$3.1415926535 \leq \pi \leq 3.1415926536$$

で,

$$3.1415926535 = \left[3, 7, 15, 1, 292, 1, 1, \frac{27995}{4319}\right], \quad 3.1415926536 = \left[3, 7, 15, 1, 292, 1, 1, \frac{13345}{10989}\right].$$

これより,  $\pi$  の連分数展開は次のようになることがわかる:

$$\pi = [3, 7, 15, 1, 292, 1, 1, \dots].$$

なお,

$$\left\lfloor \frac{27995}{4319} \right\rfloor = 6, \quad \left\lfloor \frac{13345}{10989} \right\rfloor = 1$$

であるから,  $\pi$  の近似値 3.1415926535 からは, この先の部分商を求めることはできない.

**問題 4.7** 近似値 2.7182818 を用いて  $e$  の連分数展開を求めよ.

## 5 2 次無理数と循環連分数

### 5.1 代数的数と超越数

一般に,  $\alpha \in \mathbb{R}$  が代数的数であるとは  $\alpha$  が  $\mathbb{Q}$  係数の 0 でない多項式の根となることをいう.  $\alpha$  を代数的数とすると,  $\alpha$  を根とする  $\mathbb{Q}$  係数のモニックな (i.e., 最高次の係数が 1 の) 多項式のうち次数が最小であるようなものを  $\alpha$  の最小多項式といい, その次数を  $\alpha$  の次数という. また, 代数的でない実数を超越数という (これらの概念は複素数  $\alpha$  に対しても同様に定義される).

**問題 5.1** (1) 代数的数の最小多項式は一意的に定まることを示せ.

(2) 代数的数の最小多項式は  $\mathbb{Q}$  上既約であることを示せ.

次数が 1 であるような代数的数とは有理数に他ならない. 従って,  $\alpha \in \mathbb{R}$  が次数  $d \geq 2$  の代数的数ならば  $\alpha$  は無理数である. このような数を  $d$  次無理数という.

### 5.2 2 次無理数

**問題 5.2**  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$  に対して次の (a)–(c) は互いに同値であることを示せ:

(a)  $\alpha$  は 2 次無理数.

(b)  $a\alpha^2 + b\alpha + c = 0$  となるような  $a, b, c \in \mathbb{Z}$  ( $a \neq 0$ ) が存在する.

(c)  $\alpha + \alpha' \in \mathbb{Q}$  かつ  $\alpha\alpha' \in \mathbb{Q}$  となるような  $\alpha' \in \mathbb{R}$  が存在する.

さらに, このとき  $\alpha \neq \alpha'$  であって,  $\alpha$  の最小多項式は

$$(x - \alpha)(x - \alpha') = x^2 + \frac{b}{a}x + \frac{c}{a}$$

で与えられることを示せ.

上の問題のような  $\alpha'$  を  $\alpha$  の共役元という. 問題からわかるように,  $\alpha'$  は  $\alpha$  とは異なる 2 次無理数である.

**例 5.3** 平方数ではない (i.e., 有理整数の 2 乗では表せない)  $d \in \mathbb{Z}_+$  に対し,  $\sqrt{d}$  は 2 次無理数で,  $x^2 - d$  がその最小多項式を与える. また,  $\sqrt{d}$  の共役元は  $-\sqrt{d}$  となる.

**例 5.4**  $\alpha \in \mathbb{R}$ ,  $r, s, t, u \in \mathbb{Q}$  ( $ru - st \neq 0$ ,  $t\alpha + u \neq 0$ ) とし,

$$\beta := \frac{r\alpha + s}{t\alpha + u}$$

が 2 次無理数であるとする. このとき

$$A\beta^2 + B\beta + C = 0$$

となるような  $A, B, C \in \mathbb{Q}$  ( $A \neq 0$ ) をとると,

$$A(r\alpha + s)^2 + B(r\alpha + s)(t\alpha + u) + C(t\alpha + u)^2 = 0.$$

これを整理して

$$a\alpha^2 + b\alpha + c = 0$$

を得る. ただし,

$$\begin{aligned} a &:= Ar^2 + Brt + Ct^2, \\ b &:= 2Ars + B(ru + st) + 2Ctu, \\ c &:= As^2 + Bsu + Cu^2. \end{aligned}$$

これらの等式は

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} = {}^t \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}$$

とまとめることができる.

さて,  $\beta \notin \mathbb{Q}$  より  $\alpha \notin \mathbb{Q}$ . いま仮に  $a = 0$  であるとする,  $b\alpha + c = 0$  と  $\alpha \notin \mathbb{Q}$  より  $b = c = 0$ , 従って

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} = {}^t \begin{pmatrix} r & s \\ t & u \end{pmatrix}^{-1} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

となり矛盾. よって  $a \neq 0$  であって,  $\alpha$  も 2 次無理数である.

**補題 5.5**  $\alpha$  を 2 次無理数,  $r, s, t, u \in \mathbb{Q}$  ( $ru - st \neq 0$ ) とするとき,

$$\beta := \frac{r\alpha + s}{t\alpha + u}$$

も 2 次無理数で,

$$\beta' := \frac{r\alpha' + s}{t\alpha' + u}$$

がその共役元を与える. ただし  $\alpha'$  は  $\alpha$  の共役元.

[証明] まず,  $t\alpha + u \neq 0$ ,  $t\alpha' + u \neq 0$  ならびに  $\beta \notin \mathbb{Q}$  は容易にわかる. また  $\alpha + \alpha' \in \mathbb{Q}$ ,  $\alpha\alpha' \in \mathbb{Q}$  より

$$\begin{aligned} (r\alpha + s)(r\alpha' + s) &= r^2\alpha\alpha' + rs(\alpha + \alpha') + s^2, \\ (r\alpha + s)(t\alpha' + u) + (r\alpha' + s)(t\alpha + u) &= 2rt\alpha\alpha' + (ru + st)(\alpha + \alpha') + 2su, \\ (t\alpha + u)(t\alpha' + u) &= t^2\alpha\alpha' + tu(\alpha + \alpha') + u^2 \end{aligned}$$

は全て有理数であることがわかる. よって  $\beta + \beta' \in \mathbb{Q}$ ,  $\beta\beta' \in \mathbb{Q}$  となり, 問題 5.2 により主張を得る.  $\square$

2 次無理数  $\alpha$  が簡約 2 次無理数であるとは

$$\alpha > 1, \quad -1 < \alpha' < 0$$

が成り立つことをいう。ここで  $\alpha'$  は  $\alpha$  の共役元。

**例 5.6** 平方数ではない  $d \in \mathbb{Z}_+$  に対し,  $\lfloor \sqrt{d} \rfloor + \sqrt{d}$  は簡約 2 次無理数である。実際, 例 5.3 と補題 5.5 より  $\lfloor \sqrt{d} \rfloor + \sqrt{d}$  の共役元は  $\lfloor \sqrt{d} \rfloor - \sqrt{d}$  であって, これらの数は不等式

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

をみたす。

**補題 5.7**  $\alpha$  を簡約 2 次無理数とすると, 任意の  $i \geq 0$  に対し,  $\alpha$  の  $i$  次全商  $\alpha_i$  もまた簡約 2 次無理数である。

[証明]  $\alpha_i$  が簡約 2 次無理数であるとする, 補題 5.5 より

$$\alpha_{i+1} = \frac{1}{\alpha_i - c_i} = \frac{0 \cdot \alpha_i + 1}{1 \cdot \alpha_i - c_i}$$

も 2 次無理数で, その共役元は

$$\alpha'_{i+1} = \frac{1}{\alpha'_i - c_i}$$

で与えられる。ただし  $c_i = \lfloor \alpha_i \rfloor$  は  $\alpha$  の  $i$  次部分商。ここで  $-1 < \alpha'_i < 0$  と  $c_i \geq 1$  より  $\alpha'_i - c_i < -1$  となるから,

$$-1 < \alpha'_{i+1} = \frac{1}{\alpha'_i - c_i} < 0.$$

従って, 命題 3.6 で示してある  $\alpha_{i+1} > 1$  と併せて,  $\alpha_{i+1}$  も簡約 2 次無理数となる。仮定より  $\alpha = \alpha_0$  は簡約 2 次無理数であるから, 数学的帰納法により主張を得る。□

### 5.3 循環連分数

無限単純連分数  $[c_0, c_1, c_2, \dots]$  が循環連分数であるとは, 次をみたすような  $l \geq 1$  と  $n \geq 0$  が存在することをいう:

$$c_{i+l} = c_i \quad (i \geq n)$$

( $c_n, c_{n+1}, \dots, c_{n+l-1}$  を循環節といい,  $l$  をその長さという)。なお,  $n = 0$  の場合には純循環であるという (そのときには  $c_0 \geq 1$  となっている)。

**注意 5.8**  $\alpha := [c_0, c_1, c_2, \dots]$  と置き, その  $i$  次全商を  $\alpha_i$  とするとき, 命題 4.1 の (2) より次の (a)–(c) は互いに同値であることがわかる:

$$(a) \quad c_{i+l} = c_i \quad (i \geq n).$$

$$(b) \quad \alpha_{i+l} = \alpha_i \quad (i \geq n).$$

$$(c) \quad \alpha_{n+l} = \alpha_n.$$

いま,  $\alpha = [c_0, c_1, c_2, \dots]$  を純循環な単純連分数 (で与えられた実数) とし, その循環節の長さを  $l$  とする:

$$c_{i+l} = c_i \quad (i \geq 0).$$

このとき, 上の注意で述べたように  $\alpha$  の  $l$  次全商は  $\alpha$  に一致するから, 命題 3.8 の (1) より

$$\alpha = \frac{p_{l-1}\alpha + p_{l-2}}{q_{l-1}\alpha + q_{l-2}}.$$

ただし  $p_i, q_i$  はそれぞれ  $\alpha$  の  $i$  次近似分子, 近似分母を表す. これより

$$q_{l-1}\alpha^2 - (p_{l-1} - q_{l-2})\alpha - p_{l-2} = 0$$

となり,  $\alpha$  は  $\mathbb{Z}$  係数の 2 次式

$$f(x) := q_{l-1}x^2 - (p_{l-1} - q_{l-2})x - p_{l-2}$$

の根になる ( $q_{l-1} \geq 1$  であることに注意). よって  $\alpha$  は 2 次無理数. また  $c_0, c_1, c_2, \dots \in \mathbb{Z}_+$  と  $l \geq 1$  より

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

となることが容易にわかるから,

$$f(0) = -p_{l-2} < 0, \quad f(-1) = (p_{l-1} - p_{l-2}) + (q_{l-1} - q_{l-2}) \geq 0.$$

これより  $\alpha$  の共役元  $\alpha'$  は不等式

$$-1 < \alpha' < 0$$

をみたすことがわかる.  $\alpha > c_0 \geq 1$  であつたから  $\alpha$  は簡約 2 次無理数となり, さらに

$$\alpha = \frac{p_{l-1} - q_{l-2} + \sqrt{(p_{l-1} - q_{l-2})^2 + 4p_{l-2}q_{l-1}}}{2q_{l-1}}$$

となる (解の公式において平方根の前の符号がプラスになる) こともわかる.

例 5.9  $a \in \mathbb{Z}_+$  に対し,  $\alpha := [a, a, a, \dots, a, \dots]$  と置くと,

$$\alpha = a + \frac{1}{\alpha} = \frac{a\alpha + 1}{\alpha}.$$

従って

$$\alpha^2 - a\alpha - 1 = 0$$

となり,

$$\alpha = \frac{a + \sqrt{a^2 + 4}}{2}.$$

問題 5.10  $\alpha := [a, b, a, b, \dots, a, b, \dots]$  ( $a, b \in \mathbb{Z}_+$ ) に対して上と同様の計算をせよ.

次に,  $\alpha = [c_0, c_1, c_2, \dots]$  を循環単純連分数 (で与えられた実数) とし,

$$c_{i+l} = c_i \quad (i \geq n)$$

とする. このとき  $\alpha$  の  $n$  次全商の単純連分数展開  $\alpha_n = [c_n, c_{n+1}, c_{n+2}, \dots]$  は純循環であるから  $\alpha_n$  は簡約 2 次無理数. 従って, 命題 3.8 の (1) と例 5.4 より  $\alpha$  は 2 次無理数である. 以上をまとめると:

命題 5.11 (1) 循環単純連分数で与えられる実数は 2 次無理数である.

(2) 純循環な単純連分数で与えられる実数は簡約 2 次無理数である.

## 5.4 2 次無理数の連分数展開

最後に命題 5.11 の逆を示す:

定理 5.12 (1) 2 次無理数は循環単純連分数に展開される.

(2) 簡約 2 次無理数は純循環な単純連分数に展開される.

[証明] (1)  $\alpha$  を 2 次無理数とすると, 問題 5.2 より

$$a\alpha^2 + b\alpha + c = 0$$

となるような  $a, b, c \in \mathbb{Z}$  ( $a \neq 0$ ) がとれる. 従って, 各  $i \geq 0$  に対し, 命題 3.8 の (1) で述べた

$$\alpha = \frac{p_{i-1}\alpha_i + p_{i-2}}{q_{i-1}\alpha_i + q_{i-2}}$$

より

$$a_i\alpha_i^2 + b_i\alpha_i + c_i = 0$$

が得られる. ここで  $a_i, b_i, c_i$  ( $a_i \neq 0$ ) は

$$\begin{aligned} a_i &:= ap_{i-1}^2 + bp_{i-1}q_{i-1} + cq_{i-1}^2, \\ b_i &:= 2ap_{i-1}p_{i-2} + b(p_{i-1}q_{i-2} + p_{i-2}q_{i-1}) + 2cq_{i-1}q_{i-2}, \\ c_i &:= ap_{i-2}^2 + bp_{i-2}q_{i-2} + cq_{i-2}^2, \end{aligned}$$

すなわち

$$\begin{pmatrix} a_i & b_i/2 \\ b_i/2 & c_i \end{pmatrix} = {}^t \begin{pmatrix} p_{i-1} & p_{i-2} \\ q_{i-1} & q_{i-2} \end{pmatrix} \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \begin{pmatrix} p_{i-1} & p_{i-2} \\ q_{i-1} & q_{i-2} \end{pmatrix}$$

により定まる有理整数である (cf. 例 5.4). さて,  $i \geq 1$  ならば

$$\begin{aligned} \frac{a_i}{q_{i-1}^2} &= a \left( \frac{p_{i-1}}{q_{i-1}} \right)^2 + b \frac{p_{i-1}}{q_{i-1}} + c - (a\alpha^2 + b\alpha + c) \\ &= 2a\alpha \left( \frac{p_{i-1}}{q_{i-1}} - \alpha \right) + a \left( \frac{p_{i-1}}{q_{i-1}} - \alpha \right)^2 + b \left( \frac{p_{i-1}}{q_{i-1}} - \alpha \right) \end{aligned}$$

となるから, 系 3.11 の (1) より,

$$\left| \frac{a_i}{q_{i-1}^2} \right| \leq 2|a\alpha| \frac{1}{q_{i-1}^2} + |a| \frac{1}{q_{i-1}^4} + |b| \frac{1}{q_{i-1}^2}.$$

よって任意の  $i \geq 1$  に対して

$$|a_i| \leq 2|a\alpha| + |a| + |b|$$

が成り立つ. 同様にして, 任意の  $i \geq 2$  に対して

$$|c_i| \leq 2|a\alpha| + |a| + |b|$$

が成り立つこともわかる. また

$$b_i^2 - 4a_i c_i = -4 \begin{vmatrix} a_i & b_i/2 \\ b_i/2 & c_i \end{vmatrix} = -4 \begin{vmatrix} a & b/2 \\ b/2 & c \end{vmatrix} = b^2 - 4ac$$

は  $i (\geq 0)$  によらずに一定であるから, 任意の  $i \geq 2$  に対して

$$b_i^2 = 4a_i c_i + b^2 - 4ac \leq 4(2|a\alpha| + |a| + |b|)^2 + b^2 - 4ac$$

が成り立つ. 以上より  ${}^t(a_0, b_0, c_0), {}^t(a_1, b_1, c_1), {}^t(a_2, b_2, c_2), \dots \in \mathbb{Z}^3$  は有界な点列となり,

$${}^t(a_{i_1}, b_{i_1}, c_{i_1}) = {}^t(a_{i_2}, b_{i_2}, c_{i_2}) = {}^t(a_{i_3}, b_{i_3}, c_{i_3}) = \dots \quad (0 \leq i_1 < i_2 < i_3 < \dots)$$

となるような  $i_1, i_2, i_3, \dots$  が存在することがわかる. このとき  $\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}$  は同一の 2 次式の根であるから, そのうち少なくとも 2 つは一致し, 主張が得られる.

(2)  $\alpha$  を簡約 2 次無理数とし, その  $i$  次全商, 部分商をそれぞれ  $\alpha_i, c_i$  とする. このとき (1) より  $\alpha_{n+l} = \alpha_n$  となるような  $n \geq 0$  と  $l \geq 1$  がとれる. いま  $n \geq 1$  であるとすると,

$$\alpha_{n-1} = c_{n-1} + \frac{1}{\alpha_n}, \quad \alpha_{n+l-1} = c_{n+l-1} + \frac{1}{\alpha_{n+l}}$$

より,

$$\alpha_{n-1} - \alpha_{n+l-1} = c_{n-1} - c_{n+l-1}.$$

従って補題 5.5 より

$$\alpha'_{n-1} - \alpha'_{n+l-1} = c_{n-1} - c_{n+l-1}$$

となることがわかる. ここで  $\alpha'_i$  は  $\alpha_i$  の共役元を表す. さて, 補題 5.7 で述べたように各  $\alpha_i$  は簡約 2 次無理数であるから不等式  $-1 < \alpha'_i < 0$  をみたす. これより

$$|c_{n-1} - c_{n+l-1}| = |\alpha'_{n-1} - \alpha'_{n+l-1}| < 1$$

という不等式が得られるが,  $c_i \in \mathbb{Z}$  であつたから  $c_{n+l-1} = c_{n-1}$  となり,  $\alpha_{n+l-1} = \alpha_{n-1}$  がわかる. 以上の操作を繰り返すことにより  $\alpha_l = \alpha_0 (= \alpha)$  となることがわかる.  $\square$

**例 5.13** 平方数ではない  $d \in \mathbb{Z}_+$  に対し,  $\lfloor \sqrt{d} \rfloor + \sqrt{d}$  は簡約 2 次無理数である (例 5.6) から,  $\lfloor \sqrt{d} \rfloor + \sqrt{d}$  は純循環な単純連分数に展開される:

$$\lfloor \sqrt{d} \rfloor + \sqrt{d} = [c'_0, c_1, \dots, c_{l-1}, c'_0, c_1, \dots, c_{l-1}, \dots] \quad (c'_0, c_1, \dots, c_{l-1} \in \mathbb{Z}_+).$$

いま  $c_0 := \lfloor \sqrt{d} \rfloor$  と置くと

$$c'_0 = \lfloor \lfloor \sqrt{d} \rfloor + \sqrt{d} \rfloor = 2c_0.$$

従って

$$c_0 + \sqrt{d} = [2c_0, c_1, \dots, c_{l-1}, 2c_0, c_1, \dots, c_{l-1}, \dots]$$

となり,  $\sqrt{d}$  の単純連分数展開は次のようになる:

$$\sqrt{d} = [c_0, c_1, \dots, c_{l-1}, 2c_0, c_1, \dots, c_{l-1}, 2c_0, \dots]$$

( $c_1, \dots, c_{l-1}, 2c_0$  が循環節).

**問題 5.14** 平方数ではない  $d \in \mathbb{Z}_+$  に対し,  $\sqrt{d}$  の  $i$  次全商, 部分商 ( $i \geq 0$ ) をそれぞれ  $\alpha_i, c_i$  とし,  $i$  次近似分子, 近似分母 ( $i \geq -2$ ) をそれぞれ  $p_i, q_i$  とする. また  $a_i, b_i \in \mathbb{Z}$  ( $i \geq 0$ ) を

$$\begin{pmatrix} a_i \\ b_i \end{pmatrix} := (-1)^i \begin{pmatrix} -p_{i-1}p_{i-2} + dq_{i-1}q_{i-2} \\ p_{i-1}^2 - dq_{i-1}^2 \end{pmatrix}$$

により定める. このとき次が成り立つことを示せ:

(1)  $i \geq 0$  に対し,

$$b_i \geq 1, \quad \alpha_i = \frac{a_i + \sqrt{d}}{b_i}.$$

(2)

$$\begin{aligned} a_0 &= 0, & b_0 &= 1; \\ a_{i+1} &= b_i c_i - a_i, & b_{i+1} &= \frac{d - a_{i+1}^2}{b_i} \quad (i \geq 0). \end{aligned}$$

(3)  $i \geq 0$  に対し,

$$c_i = \left\lfloor \frac{a_i + c_0}{b_i} \right\rfloor.$$

**注意 5.15** 例 5.13, 問題 5.14 と同じ記号の下で,

$$\alpha_l = c_0 + \sqrt{d} = \frac{a_l + \sqrt{d}}{b_l}.$$

これより

$$a_l = c_0, \quad b_l = 1$$

となることがわかる. 逆に,  $c_0 := \lfloor \sqrt{d} \rfloor$  とし,  $a_0, b_0, a_1, b_1, c_1, \dots$  を問題 5.14 の (2) と (3) によって定めると,  $a_l = c_0, b_l = 1$  となるような  $l \geq 1$  が存在する. また, このとき  $\sqrt{d}$  の単純連分数展開は

$$\sqrt{d} = [c_0, c_1, \dots, c_{l-1}, 2c_0, c_1, \dots, c_{l-1}, 2c_0, \dots]$$

で与えられる.

## 6 有理数による実数の近似

### 6.1 近似の可能性

命題 6.1  $\alpha \in \mathbb{R}$  とするとき, 任意の  $Q \in \mathbb{Z}_+$  に対して

$$|q\alpha - p| < \frac{1}{Q}, \quad q \leq Q$$

をみたすような  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  が存在する.

注意 6.2  $\alpha \in \mathbb{R}$  と  $Q \in \mathbb{Z}_+$  に対して上の命題のように  $p$  と  $q$  をとるとき,

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qQ} \leq \frac{1}{q^2}$$

となっている.

[命題 6.1 の証明]  $i = 0, 1, \dots, Q$  に対して  $a_i := [i\alpha]$  と置くと  $i\alpha - a_i \in [0, 1)$  となっている. 従って, 区間  $[0, 1)$  の分割

$$[0, 1) = \left[0, \frac{1}{Q}\right) \cup \left[\frac{1}{Q}, \frac{2}{Q}\right) \cup \dots \cup \left[\frac{Q-1}{Q}, 1\right)$$

を考えることにより

$$|(i_2\alpha - a_{i_2}) - (i_1\alpha - a_{i_1})| < \frac{1}{Q}$$

をみたす相異なる  $i_1, i_2$  の存在がわかる. ここで  $i_1 < i_2$  であるとしてよい. そのとき

$$p := a_{i_2} - a_{i_1}, \quad q := i_2 - i_1$$

と置くと, これらは求める条件をみたす. □

$\alpha$  の連分数展開を使うと, 上の命題の構成的な証明を与えることができる:

[命題 6.1 の別証明]  $\alpha$  の  $i$  次全商, 近似分子, 近似分母をそれぞれ  $\alpha_i, p_i, q_i$  とし,

$$j := \max\{i; i \geq 0, q_i \leq Q\}$$

と置く. このとき  $\alpha_j \in \mathbb{Z}$  ならば  $\alpha = \frac{p_j}{q_j}$ . また  $\alpha_j \notin \mathbb{Z}$  ならば  $q_j \leq Q < q_{j+1}$  であって, 系 3.11 の (1) より

$$\left| \alpha - \frac{p_j}{q_j} \right| \leq \frac{1}{q_j q_{j+1}}.$$

いずれの場合にも

$$\left| \alpha - \frac{p_j}{q_j} \right| < \frac{1}{q_j Q}$$

となり,  $p = p_j, q = q_j$  は命題の条件をみたす. □

## 6.2 近似分数による近似

**定理 6.3**  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ,  $i \geq 1$  とし,  $p_i, q_i$  をそれぞれ  $\alpha$  の  $i$  次近似分子, 近似分母とする. このとき任意の  $p \in \mathbb{Z}$  と  $q \leq q_i$  をみたす  $q \in \mathbb{Z}_+$  に対し,

$$\left| \alpha - \frac{p}{q} \right| \geq \left| \alpha - \frac{p_i}{q_i} \right|.$$

等号が成立するのは  $p = p_i$  かつ  $q = q_i$  のときに限る.

[証明]  $\alpha$  の  $j$  次全商, 近似分子, 近似分母をそれぞれ  $\alpha_j, p_j, q_j$  で表す. このとき命題 2.21 の (3) より

$$\begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} p_i & p_{i-1} \\ q_i & q_{i-1} \end{pmatrix} \begin{pmatrix} k \\ l \end{pmatrix}$$

となるような  $k, l \in \mathbb{Z}$  が (ただ 1 組) 存在することがわかる. ここで,  $k \leq 0$  ならば  $0 < q = q_i k + q_{i-1} l$  より  $l > 0$  でなければならない. また,  $k > 0$  ならば  $q = q_i k + q_{i-1} l \leq q_i$  より  $l \leq 0$  となることもわかる ( $i \geq 1$  としているから  $q_{i-1} \geq 1$ ).

いま  $k = 0$  であるとする.  $p = p_{i-1} l$ ,  $q = q_{i-1} l$  となるから, 系 3.11 の (2) より

$$\left| \alpha - \frac{p}{q} \right| = \left| \alpha - \frac{p_{i-1}}{q_{i-1}} \right| > \left| \alpha - \frac{p_i}{q_i} \right|$$

と求める不等式が得られる. そこで, 以下  $k \neq 0$  とする. このとき

$$q\alpha - p = (q_i k + q_{i-1} l)\alpha - (p_i k + p_{i-1} l) = k(q_i \alpha - p_i) \left( 1 - \frac{l}{k} \cdot \frac{q_{i-1} \alpha - p_{i-1}}{-q_i \alpha + p_i} \right)$$

は命題 3.8 の (1) より

$$k(q_i \alpha - p_i) \left( 1 - \frac{l}{k} \alpha_{i+1} \right)$$

に等しい. 従って,

$$|q\alpha - p| = |k| \cdot |q_i \alpha - p_i| \cdot \left| 1 - \frac{l}{k} \alpha_{i+1} \right| \geq |q_i \alpha - p_i| \cdot \left| 1 - \frac{l}{k} \alpha_{i+1} \right|.$$

さて, 上で述べたように  $\frac{l}{k} \leq 0$ . これと  $\alpha_{i+1} > 1$  より,

$$1 - \frac{l}{k} \alpha_{i+1} \geq 1.$$

よって  $|q\alpha - p| \geq |q_i \alpha - p_i|$  となり,  $0 < q \leq q_i$  も用いて

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{q_i}{q} \left| \alpha - \frac{p_i}{q_i} \right| \geq \left| \alpha - \frac{p_i}{q_i} \right|$$

と求める不等式が得られる. また,

$$\left| \alpha - \frac{p}{q} \right| = \left| \alpha - \frac{p_i}{q_i} \right| \iff |k| = 1 - \frac{l}{k} \alpha_{i+1} = \frac{q_i}{q} = 1 \iff p = p_i, q = q_i, k = 1, l = 0$$

が成り立つ. □

**注意 6.4** 定理 6.3 の主張は  $i = 0$  では成り立たない. 実際, 任意の  $a \in \mathbb{Z}$  と  $\frac{1}{2} < \theta < 1$  をみたす  $\theta \in \mathbb{R}$  に対して  $\alpha := a + \theta$  と置くと,  $\alpha$  の 0 次近似分子, 近似分母はそれぞれ  $p_0 = a$ ,  $q_0 = 1$  となるから

$$\left| \alpha - \frac{p_0}{q_0} \right| = \theta > \frac{1}{2}.$$

他方,  $p := a + 1$ ,  $q := 1$  とすると  $0 < q \leq q_0$  で

$$\left| \alpha - \frac{p}{q} \right| = 1 - \theta < \frac{1}{2}$$

となっている.

**問題 6.5** 定理 6.3 と同じ仮定の下で,  $\frac{p}{q} \neq \frac{p_i}{q_i}$  ならば  $|q\alpha - p| \geq |q_{i-1}\alpha - p_{i-1}|$  が成り立つことを示せ.

**定理 6.6**  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ ,  $i \geq 0$  とし,  $p_i, q_i$  ( $p_{i+1}, q_{i+1}$ ) を  $\alpha$  の  $i$  次 ( $i+1$  次) 近似分子, 近似分母とする. このとき次の 2 つの不等式のうち少なくとも一方が成り立つ:

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{2q_i^2}, \quad \left| \alpha - \frac{p_{i+1}}{q_{i+1}} \right| < \frac{1}{2q_{i+1}^2}.$$

[証明] いずれも成り立たないとすると,

$$\left| \alpha - \frac{p_i}{q_i} \right| \geq \frac{1}{2q_i^2}, \quad \left| \alpha - \frac{p_{i+1}}{q_{i+1}} \right| \geq \frac{1}{2q_{i+1}^2}.$$

さて, 系 3.11 の (3) より  $i$  の偶奇に応じて  $\frac{p_i}{q_i} < \alpha < \frac{p_{i+1}}{q_{i+1}}$  または  $\frac{p_i}{q_i} > \alpha > \frac{p_{i+1}}{q_{i+1}}$  となっているから,

$$\left| \frac{p_i}{q_i} - \frac{p_{i+1}}{q_{i+1}} \right| = \left| \alpha - \frac{p_i}{q_i} \right| + \left| \alpha - \frac{p_{i+1}}{q_{i+1}} \right| \geq \frac{1}{2} \left( \frac{1}{q_i^2} + \frac{1}{q_{i+1}^2} \right).$$

他方, 命題 2.21 の (3) で述べたように

$$\left| \frac{p_i}{q_i} - \frac{p_{i+1}}{q_{i+1}} \right| = \frac{1}{q_i q_{i+1}}$$

であるから,

$$\frac{1}{q_i q_{i+1}} \geq \frac{1}{2} \left( \frac{1}{q_i^2} + \frac{1}{q_{i+1}^2} \right).$$

これより  $(q_i - q_{i+1})^2 \leq 0$  となり,  $q_i = q_{i+1}$ . よって  $i = 0$  かつ  $q_0 = q_1 = 1$  でなければならないが, この場合には

$$\frac{p_0}{q_0} = [\alpha], \quad \frac{p_1}{q_1} = [\alpha] + 1$$

となっているから,

$$\left| \alpha - \frac{p_0}{q_0} \right| < \frac{1}{2q_0^2}, \quad \left| \alpha - \frac{p_1}{q_1} \right| < \frac{1}{2q_1^2}$$

のどちらかは成り立っている. これは矛盾. □

次の定理は定理 6.6 の逆を主張している:

**定理 6.7**  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$  とするとき,  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  が

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

をみたすならば,  $i \geq 0$  が存在して  $\frac{p}{q}$  は  $\alpha$  の  $i$  次近似分数に一致する.

[証明] 仮定より

$$\alpha = \frac{p}{q} - \frac{\varepsilon\theta}{q^2}, \quad 0 < \theta < \frac{1}{2}$$

となるような  $\varepsilon \in \{1, -1\}$  と  $\theta \in \mathbb{R}$  がとれる. いま  $\frac{p}{q}$  を

$$\frac{p}{q} = [c_0^*, c_1^*, \dots, c_i^*]$$

と単純連分数に展開する. ただし  $i \geq 0$  の偶奇は  $\varepsilon = (-1)^{i-1}$  が成り立つように選んでおく. 上の  $c_0^*, c_1^*, \dots, c_i^*$  から  $p_j^*, q_j^*$  ( $-2 \leq j \leq i$ ) を命題 2.21 と同様に定め,

$$\beta := \frac{q_{i-1}^* \alpha - p_{i-1}^*}{-q_i^* \alpha + p_i^*}$$

と置く. このとき,

$$\beta = \frac{q_{i-1}^* \left( \frac{p_i^*}{q_i^*} - \frac{\varepsilon\theta}{q^2} \right) - p_{i-1}^*}{-q_i^* \left( \frac{p_i^*}{q_i^*} - \frac{\varepsilon\theta}{q^2} \right) + p_i^*} = \left( \frac{q}{q_i^*} \right)^2 \frac{p_i^* q_{i-1}^* - p_{i-1}^* q_i^*}{\varepsilon\theta} - \frac{q_{i-1}^*}{q_i^*}.$$

ここで, 命題 2.21 の (3) と  $i$  の選び方より

$$p_i^* q_{i-1}^* - p_{i-1}^* q_i^* = (-1)^{i-1} = \varepsilon$$

であるから,

$$\beta = \left( \frac{q}{q_i^*} \right)^2 \frac{1}{\theta} - \frac{q_{i-1}^*}{q_i^*}.$$

従って,  $0 < q_i^* \leq q$ ,  $0 < \theta < \frac{1}{2}$  ならびに  $0 \leq q_{i-1}^* \leq q_i^*$  より  $\beta > 1$  がわかる. また,

$$\alpha = \frac{p_i^* \beta + p_{i-1}^*}{q_i^* \beta + q_{i-1}^*} = [c_0^*, c_i^*, \dots, c_i^*, \beta].$$

よって補題 4.2 より  $c_j^*$  ( $0 \leq j \leq i$ ) は  $\alpha$  の  $j$  次部分商となり,  $\frac{p}{q} = \frac{p_i^*}{q_i^*}$  は  $\alpha$  の  $i$  次近似分数に一致する. □

**系 6.8**  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$  とするとき,  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  が

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2}, \quad \gcd(p, q) = 1$$

をみたすならば,  $i \geq 0$  が存在して  $p, q$  はそれぞれ  $\alpha$  の  $i$  次近似分子, 近似分母に一致する.

### 6.3 近似の限界

$\alpha \in \mathbb{R} \setminus \mathbb{Q}$  に対し, 条件

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}, \quad \gcd(p, q) = 1$$

をみたすような  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  は無数に多く存在する. 実際, 任意の  $i \geq 0$  に対して  $\alpha$  の  $i$  次近似分子と近似分母は上の条件をみたす. 次の問題からわかるように, このような性質は  $\alpha$  が無理数であることの特徴付けになっている:

**問題 6.9**  $\alpha \in \mathbb{Q}$  とするとき, 任意の  $\varepsilon \in \mathbb{R}_+$  に対して

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{1+\varepsilon}}$$

をみたす  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  は有限個しか存在しないことを示せ.

以下,  $d$  次無理数 ( $d \geq 2$ ) に対する同様の結果を示す.

**定理 6.10**  $\alpha$  を  $d$  次無理数 ( $d \geq 2$ ) とするとき, 次の性質をもつ定数  $C \in \mathbb{R}_+$  が存在する: 任意の  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  に対し,

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{C}{q^d}.$$

[証明]  $\alpha$  の最小多項式の分母を払って  $\mathbb{Z}$  係数にしたものを

$$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

とし,

$$C' := \max\{|f'(\xi)|; \xi \in \mathbb{R}, \alpha - 1 \leq \xi \leq \alpha + 1\}, \quad C := \min\left\{\frac{1}{C'}, 1\right\}$$

と置く. このとき  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  に対し:

(1)  $\left| \alpha - \frac{p}{q} \right| \leq 1$  の場合には, 平均値の定理より

$$\frac{f(\alpha) - f\left(\frac{p}{q}\right)}{\alpha - \frac{p}{q}} = f'(\beta), \quad \alpha - 1 < \beta < \alpha + 1$$

となるような  $\beta \in \mathbb{R}$  が存在するが,  $f(\alpha) = 0$  であるから

$$\left| \frac{f\left(\frac{p}{q}\right)}{\alpha - \frac{p}{q}} \right| = |f'(\beta)| \leq C' \leq \frac{1}{C}.$$

さて,

$$q^d f\left(\frac{p}{q}\right) = a_d p^d + \cdots + a_1 p q^{d-1} + a_0 q^d$$

は有理整数であって,  $f(x)$  が  $\mathbb{Q}$  上既約である (問題 5.1 の (2)) ことより, この値は 0 ではない. 従って  $f\left(\frac{p}{q}\right) \geq \frac{1}{q^d}$  となり,

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{C}{q^d}.$$

(2)  $\left|\alpha - \frac{p}{q}\right| > 1$  の場合には, 明らかに

$$\left|\alpha - \frac{p}{q}\right| > 1 \geq \frac{1}{q^d} \geq \frac{C}{q^d}$$

が成り立つ. □

**系 6.11**  $\alpha$  を  $d$  次無理数 ( $d \geq 2$ ) とするとき, 任意の  $\varepsilon \in \mathbb{R}_+$  に対し,

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{d+\varepsilon}}$$

となるような  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  は有限個しか存在しない.

[証明] 定理の定数  $C \in \mathbb{R}_+$  をとる. このとき  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  が上の条件をみたすとする,

$$\frac{C}{q^d} \leq \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{d+\varepsilon}}$$

より  $q < C^{-1/\varepsilon}$  でなければならないが, そのような  $q \in \mathbb{Z}_+$  は有限個しか存在しない. また, 各  $q \in \mathbb{Z}_+$  に対して

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{d+\varepsilon}}$$

をみたす  $p \in \mathbb{Z}$  は有限個しか存在しない. □

**問題 6.12** 条件

$$\left|\sqrt{2} - \frac{p}{q}\right| < \frac{1}{q^3}$$

をみたす  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  を全て求めよ.

定理 6.10 を用いると, 超越数を具体的に構成することができる:

**命題 6.13**  $\alpha := \sum_{i=1}^{\infty} \frac{1}{10^{i!}}$  は超越数である.

[証明] 級数の収束性と  $\alpha \notin \mathbb{Q}$  であることは明らか. 各  $i \geq 1$  に対して

$$p_i := \sum_{j=1}^i 10^{i!-j!}, \quad q_i := 10^{i!}$$

と置くと  $p_i, q_i \in \mathbb{Z}_+$  で,

$$0 < \alpha - \frac{p_i}{q_i} = \sum_{j=i+1}^{\infty} \frac{1}{10^j!} < \frac{2}{10^{(i+1)!}} = \frac{2}{q_i^{i+1}}$$

が成り立つ. いま  $\alpha$  が  $d$  次無理数 ( $d \geq 2$ ) であると仮定し, 定理 6.10 の定数  $C \in \mathbb{R}_+$  をとると,

$$\frac{C}{q_i^d} \leq \left| \alpha - \frac{p_i}{q_i} \right| < \frac{2}{q_i^{i+1}}$$

となるから,

$$C < \frac{2}{q_i^{i+1-d}}.$$

右辺は  $i \rightarrow \infty$  としたとき 0 に収束するが, これは  $C > 0$  であることに反する. □

**命題 6.14**  $\alpha := [0, 10, 10^{2!}, \dots, 10^{i!}, \dots]$  は超越数である.

[証明]  $c_i, p_i, q_i$  ( $i \geq 0$ ) をそれぞれ  $\alpha$  の  $i$  次部分商, 近似分子, 近似分母とする. このとき

$$\begin{aligned} c_0 &= 0, & c_1 &= 10, & c_i &= c_{i-1}^i \quad (i \geq 2); \\ q_0 &= 1, & q_1 &= c_1, & q_i &= c_i q_{i-1} + q_{i-2} \quad (i \geq 2) \end{aligned}$$

より, 次が成り立つことが容易にわかる:

$$c_i \leq q_i < c_i^2 \quad (i \geq 1).$$

従って, 任意の  $i \geq 1$  に対して

$$q_{i+1} \geq c_{i+1} = c_i^{i+1} > q_i^{(i+1)/2}$$

となり, 系 3.11 の (1) より

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{q_i q_{i+1}} < \frac{1}{q_i^{(i+3)/2}}$$

が得られる. よって上の命題の証明と同様にして  $\alpha$  が超越数であることがわかる. □

## 7 Pell 方程式

平方数ではない  $d \in \mathbb{Z}_+$  に対し,  $x, y \in \mathbb{Z}$  を未知数とする方程式

$$(*) \quad x^2 - dy^2 = \pm 1$$

を **Pell 方程式** という (文献によっては, より一般の形の方程式を Pell 方程式と呼ぶこともある).  
明らかに

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \end{pmatrix}$$

は  $(*)$  の解で,  $xy = 0$  であるような解はこれらに限る. また,  ${}^t(x, y) = {}^t(p, q) \in \mathbb{Z}^2$  が  $(*)$  の解ならば

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p \\ -q \end{pmatrix}, \begin{pmatrix} -p \\ q \end{pmatrix}, \begin{pmatrix} -p \\ -q \end{pmatrix}$$

も  $(*)$  の解になる. よって  $x, y \in \mathbb{Z}_+$  であるような解 (**正の解**という) がわかれば, それから全ての解が得られることになる.

以下,  $(*)$  の解 (正の解) 全体のなす集合を  $S$  ( $S_+$ ) と書くことにする:

$$S := \{ {}^t(p, q) \in \mathbb{Z}^2 ; p^2 - dq^2 = \pm 1 \}, \quad S_+ := \{ {}^t(p, q) \in \mathbb{Z}_+^2 ; p^2 - dq^2 = \pm 1 \}.$$

### 7.1 Pell 方程式の解法

まずは Pell 方程式  $(*)$  の正の解のみを考える.

**補題 7.1**  ${}^t(p, q) \in S_+$  とするとき,  $i \geq 0$  が存在して  $p, q$  はそれぞれ  $\sqrt{d}$  の  $i$  次近似分子, 近似分母に一致する.

[証明] まず  $d \geq 2$  と  $q \geq 1$  より

$$p^2 = dq^2 \pm 1 \geq 2q^2 - 1 \geq q^2$$

となるから  $p \geq q$ , 従って

$$p + \sqrt{d}q \geq (1 + \sqrt{d})q > 2q.$$

また

$$(p - \sqrt{d}q)(p + \sqrt{d}q) = p^2 - dq^2 = \pm 1$$

より,

$$|p - \sqrt{d}q| = \frac{1}{p + \sqrt{d}q}.$$

よって,

$$\left| \sqrt{d} - \frac{p}{q} \right| = \frac{1}{(p + \sqrt{d}q)q} < \frac{1}{2q^2}.$$

容易にわかるように  $\gcd(p, q) = 1$  であるから, 系 6.8 より主張を得る.  $\square$

以下  $p_i, q_i$  ( $i \geq -2$ ) でそれぞれ  $\sqrt{d}$  の  $i$  次近似分子, 近似分母を表す. 上の補題より Pell 方程式 (\*) の正の解は適当な  $i \geq 0$  を用いて  ${}^t(x, y) = {}^t(p_i, q_i)$  と書けることがわかるが, 全ての  $i$  が解を与えるとは限らない.  ${}^t(p_i, q_i) \in S_+$  となるような  $i \geq 0$  を求めるために, 問題 5.14 と注意 5.15 を次の形に述べておく:

**命題 7.2**  $a_0, b_0, c_0, a_1, b_1, c_1, \dots$  を次により定める:

$$\begin{aligned} a_0 &:= 0, & b_0 &:= 1, & c_0 &:= \lfloor \sqrt{d} \rfloor; \\ a_{i+1} &:= b_i c_i - a_i, & b_{i+1} &:= \frac{d - a_{i+1}^2}{b_i}, & c_{i+1} &:= \left\lfloor \frac{a_{i+1} + c_0}{b_{i+1}} \right\rfloor \quad (i \geq 0). \end{aligned}$$

このとき:

(1)  $i \geq 0$  に対し,

$$a_i \in \mathbb{Z}, \quad b_i \in \mathbb{Z}_+, \quad p_{i-1}^2 - dq_{i-1}^2 = (-1)^i b_i.$$

(2)  $i \geq 0$  に対し,  $\sqrt{d}$  の  $i$  次全商, 部分商はそれぞれ

$$\alpha_i := \frac{a_i + \sqrt{d}}{b_i}, \quad c_i$$

で与えられる.

(3)  $a_l = c_0$  かつ  $b_l = 1$  となるような  $l \geq 1$  が存在する.

(4)  $a_l = c_0$  かつ  $b_l = 1$  となるような最小の  $l \geq 1$  をとるとき,  $i \geq 1$  に対して

$$a_i = c_0 \text{ かつ } b_i = 1 \iff l \mid i.$$

[証明] (1)–(3) は既に述べた.

(4) 例 5.13 で述べたように

$$\alpha_{i+l} = \alpha_i \quad (i \geq 1)$$

であるから,  $i, j \geq 1$  に対して

$$\alpha_i = \alpha_j \iff l \mid (i - j)$$

が成り立つことが  $l$  の最小性からわかる. 特に  $i \geq 1$  に対して

$$\alpha_i = \alpha_l \iff l \mid i.$$

これより主張を得る.  $\square$

注意 7.3 実は  $i \geq 1$  に対して

$$a_i = c_0 \quad \text{かつ} \quad b_i = 1 \quad \Longleftrightarrow \quad b_i = 1$$

が成り立つ. 実際,  $b_i = 1$  ( $i \geq 1$ ) とすると,  $\alpha_i = a_i + \sqrt{d}$  であるから, 補題 5.5, 例 5.6 ならびに補題 5.7 より,  $\alpha_i$  の共役元  $\alpha'_i$  は

$$-1 < \alpha'_i = a_i - \sqrt{d} < 0$$

をみたすことがわかる ( $\alpha_i$  は  $c_0 + \sqrt{d}$  の  $i$  次全商でもある). 従って

$$a_i < \sqrt{d} < a_i + 1$$

となり,  $a_i = \lfloor \sqrt{d} \rfloor = c_0$  が従う.

系 7.4 命題 7.2 と同じ記号の下で,  $b_l = 1$  となるような最小の  $l \geq 1$  をとるとき,  $i \geq 0$  に対し,

$$\begin{pmatrix} p_i \\ q_i \end{pmatrix} \in S_+ \quad \Longleftrightarrow \quad l \mid (i+1).$$

また, このとき

$$p_i^2 - dq_i^2 = (-1)^{i-1}$$

が成り立つ.

例 7.5 (1)  $d = 2$  の場合.

$$\begin{aligned} a_0 &= 0, & b_0 &= 1, & c_0 &= \lfloor \sqrt{2} \rfloor = 1; \\ a_1 &= 1 \cdot 1 - 0 = 1, & b_1 &= \frac{2 - 1^2}{1} = 1, & c_1 &= \left\lfloor \frac{1+1}{1} \right\rfloor = 2 \end{aligned}$$

より  $l = 1$  で,  $j = 1, 2, 3, 4$  に対する  $p_{j-1}, q_{j-1}$  は次のようになる:

$$\begin{aligned} \begin{pmatrix} p_0 \\ q_0 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix} & (1^2 - 2 \cdot 1^2 = -1); \\ \begin{pmatrix} p_1 \\ q_1 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 2 \end{pmatrix} & (3^2 - 2 \cdot 2^2 = 1); \\ \begin{pmatrix} p_2 \\ q_2 \end{pmatrix} &= \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 & 3 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 \\ 5 \end{pmatrix} & (7^2 - 2 \cdot 5^2 = -1); \\ \begin{pmatrix} p_3 \\ q_3 \end{pmatrix} &= \begin{pmatrix} 7 & 3 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 17 & 7 \\ 12 & 5 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 17 \\ 12 \end{pmatrix} & (17^2 - 2 \cdot 12^2 = 1). \end{aligned}$$

(2)  $d = 3$  の場合.

$$\begin{aligned} a_0 &= 0, & b_0 &= 1, & c_0 &= \lfloor \sqrt{3} \rfloor = 1; \\ a_1 &= 1 \cdot 1 - 0 = 1, & b_1 &= \frac{3 - 1^2}{1} = 2, & c_1 &= \left\lfloor \frac{1+1}{2} \right\rfloor = 1; \\ a_2 &= 2 \cdot 1 - 1 = 1, & b_2 &= \frac{3 - 1^2}{2} = 1, & c_2 &= \left\lfloor \frac{1+1}{1} \right\rfloor = 2 \end{aligned}$$

より  $l = 2$  で,  $j = 1, 2, 3$  に対する  $p_{2j-1}, q_{2j-1}$  は次のようになる:

$$\begin{aligned} \begin{pmatrix} p_1 \\ q_1 \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix} & (2^2 - 3 \cdot 1^2 = 1); \\ \begin{pmatrix} p_3 \\ q_3 \end{pmatrix} &= \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 & 5 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 \\ 4 \end{pmatrix} & (7^2 - 3 \cdot 4^2 = 1); \\ \begin{pmatrix} p_5 \\ q_5 \end{pmatrix} &= \begin{pmatrix} 7 & 5 \\ 4 & 3 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 26 & 19 \\ 15 & 11 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 26 \\ 15 \end{pmatrix} & (26^2 - 3 \cdot 15^2 = 1). \end{aligned}$$

## 7.2 Pell 方程式の解の構造

命題 7.1 と系 7.4 により Pell 方程式 (\*) の全ての解を原理的には得ることができる. 以下ではこれらの (無数に多くある) 解の間の関係を求めることを考える.

いま

$$p^2 - dq^2 = (p - \sqrt{d}q)(p + \sqrt{d}q)$$

という分解に注意し,

$$E := \left\{ p + \sqrt{d}q ; \begin{pmatrix} p \\ q \end{pmatrix} \in S \right\}$$

と置く. このとき,  $\sqrt{d} \notin \mathbb{Q}$  であることより, 写像

$$S \ni \begin{pmatrix} p \\ q \end{pmatrix} \mapsto p + \sqrt{d}q \in E$$

は全単射であることがわかる.

**補題 7.6**  $t(p, q) \in S_+$  とするとき:

(1)  $p^2 - dq^2 = 1$  ならば,

$$-p - \sqrt{d}q < -1 < -p + \sqrt{d}q < 0 < p - \sqrt{d}q < 1 < p + \sqrt{d}q.$$

(2)  $p^2 - dq^2 = -1$  ならば,

$$-p - \sqrt{d}q < -1 < p - \sqrt{d}q < 0 < -p + \sqrt{d}q < 1 < p + \sqrt{d}q.$$

[証明] まず

$$-p - \sqrt{d}q < -1, \quad 1 < p + \sqrt{d}q$$

となることは明らか. よって

$$(p - \sqrt{d}q)(p + \sqrt{d}q) = (-p + \sqrt{d}q)(-p - \sqrt{d}q) = p^2 - dq^2$$

より主張を得る. □

系 7.7  ${}^t(p, q) \in S$  に対し,

$$p + \sqrt{d}q > 1 \iff \begin{pmatrix} p \\ q \end{pmatrix} \in S_+$$

が成り立つ.

補題 7.8 (1) 集合  $E$  は除法について閉じている:

$$\varepsilon, \varepsilon' \in E \implies \frac{\varepsilon}{\varepsilon'} \in E.$$

(2) 系 7.4 と同じ記号の下で

$$\varepsilon_j := p_{jl-1} + \sqrt{d}q_{jl-1} \quad (j \geq 1)$$

と置くとき,

$$1 < \varepsilon_1 < \varepsilon_2 < \cdots < \varepsilon_j < \cdots.$$

[証明] (1)  $\varepsilon = p + \sqrt{d}q$ ,  $\varepsilon' = p' + \sqrt{d}q'$  ( ${}^t(p, q), {}^t(p', q') \in S$ ) とすると,  $(p')^2 - d(q')^2 = \pm 1$  より

$$\frac{1}{p' + \sqrt{d}q'} = \pm(p' - \sqrt{d}q')$$

となるから,

$$\frac{\varepsilon}{\varepsilon'} = \pm(p + \sqrt{d}q)(p' - \sqrt{d}q') = \pm((pp' - dq q') + \sqrt{d}(-pq' + p'q)).$$

ここで

$$(pp' - dq q')^2 - d(-pq' + p'q)^2 = (p^2 - dq^2)((p')^2 - d(q')^2) = \pm 1$$

であるから,

$$\begin{pmatrix} pp' - dq q' \\ -pq' + p'q \end{pmatrix} \in S.$$

これより主張を得る.

(2)  $c_0, c_1, c_2, \dots \in \mathbb{Z}_+$  より

$$1 \leq p_0 < p_1 < p_2 < \cdots, \quad 1 = q_0 \leq q_1 < q_2 < \cdots$$

となっていることによる. □

補題 7.9  $E_+ := E \cap \mathbb{R}_+$  と置き, 写像  $\lambda: E_+ \rightarrow \mathbb{R}$  を

$$\lambda: \varepsilon \mapsto \log \varepsilon$$

により定めるとき, 補題 7.8 と同じ記号の下で

$$\lambda(E_+) = (\log \varepsilon_1) \mathbb{Z}$$

が成り立つ.

[証明] 補題 7.8 の (1) より  $E_+$  も除法について閉じていることがわかるから,  $\lambda(E_+)$  は減法について閉じている. また, 補題 7.1, 系 7.4 ならびに系 7.7 より

$$\lambda(E_+) \cap \mathbb{R}_+ = \{\log \varepsilon_j; j \geq 1\}$$

となることがわかるから, 補題 7.8 の (2) より,

$$\min(\lambda(E_+) \cap \mathbb{R}_+) = \log \varepsilon_1.$$

よって定理 1.4 の証明と同様にして主張を得る (cf. 問題 1.5). □

系 7.10 (1)

$$E_+ = \{\varepsilon_1^j; j \in \mathbb{Z}\}, \quad E = \{\pm \varepsilon_1^j; j \in \mathbb{Z}\}.$$

(2)  $j \geq 1$  に対し,

$$\varepsilon_j = \varepsilon_1^j, \quad p_{jl-1} + \sqrt{d}q_{jl-1} = (p_{l-1} + \sqrt{d}q_{l-1})^j$$

が成り立つ.

以上をまとめると:

定理 7.11 Pell 方程式 (\*) の全ての解  ${}^t(x, y) = {}^t(p, q)$  は

$$p + \sqrt{d}q = \pm(p_{l-1} + \sqrt{d}q_{l-1})^j \quad (j \in \mathbb{Z})$$

により与えられる. ここで,  $l$  は  $\sqrt{d}$  の連分数展開の循環節の長さ (最小にとる) で,  $p_{l-1}, q_{l-1}$  はそれぞれ  $\sqrt{d}$  の  $l-1$  次近似分子, 近似分母を表す ( ${}^t(x, y) = {}^t(p_{l-1}, q_{l-1})$  を (\*) の正の最小解という).

例 7.12 例 7.5 より:

(1)  $d = 2$  の場合. 正の最小解は  ${}^t(x, y) = (1, 1)$  で,

$$\begin{aligned}(1 + \sqrt{2})^2 &= 3 + 2\sqrt{2} = p_1 + \sqrt{2}q_1, \\(1 + \sqrt{2})^3 &= 7 + 5\sqrt{2} = p_2 + \sqrt{2}q_2, \\(1 + \sqrt{2})^4 &= 17 + 12\sqrt{2} = p_3 + \sqrt{2}q_3.\end{aligned}$$

(2)  $d = 3$  の場合. 正の最小解は  ${}^t(x, y) = (2, 1)$  で,

$$\begin{aligned}(2 + \sqrt{3})^2 &= 7 + 4\sqrt{3} = p_3 + \sqrt{3}q_3, \\(2 + \sqrt{3})^3 &= 26 + 15\sqrt{3} = p_5 + \sqrt{3}q_5.\end{aligned}$$

問題 7.13 次の Pell 方程式の正の最小解を求めよ:

(1)  $x^2 - 7y^2 = \pm 1$ .

(2)  $x^2 - 13y^2 = \pm 1$ .

## 参考文献

- [1] 河田敬義, 数論 — 古典数論から類体論へ —, 岩波書店, 1992.
- [2] 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.
- [3] 塩川宇賢, 無理数と超越数, 森北出版, 1999.
- [4] 高木貞治, 初等整数論講義 (第 2 版), 共立出版, 1971.
- [5] G.H. ハーディー・E.M. ライト (示野信一・矢神毅 訳), 数論入門 I・II, シュプリンガー数学クラシックス, シュプリンガー・フェアラーク東京, 2001.

## 問題略解

問題 1.3 (1)  $A \neq \emptyset$  より,  $\alpha \in A$  を任意にとると,  $0 = \alpha - \alpha$  は  $A$  に属する.

(2)  $\alpha \in A$  とすると, (1) より  $0 \in A$  であるから,  $-\alpha = 0 - \alpha$  は  $A$  に属する.

(3)  $\alpha, \alpha' \in A$  とすると, (2) より  $-\alpha' \in A$  であるから,  $\alpha + \alpha' = \alpha - (-\alpha')$  は  $A$  に属する.

問題 1.5 定理 1.4 の証明と同様に,  $A \neq \{0\}$  の場合を考えればよい. このとき  $A_+ := A \cap \mathbb{R}_+$  は空ではない. そこで

$$\alpha := \inf A_+$$

と置くと:

(1)  $\alpha > 0$  の場合. このときには  $\alpha \in A$ , すなわち  $\alpha = \min A_+$  となる. 実際, 仮に  $\alpha \notin A$  とすると, 下限の定義より  $\alpha < \alpha'' < \alpha' < 2\alpha$  をみたす  $\alpha', \alpha'' \in A$  の存在がわかるが, これより  $\alpha' - \alpha'' \in A$  と  $0 < \alpha' - \alpha'' < \alpha$  が従い,  $\alpha$  の定義に反する. よって, 定理 1.4 の証明と同様にして  $A = \alpha\mathbb{Z}$  が示せる. なお,  $\alpha$  の一意性については命題 1.1 の証明と同様.

(2)  $\alpha = 0$  の場合. このときには, 任意の  $\beta, \gamma \in \mathbb{R}$  ( $\beta < \gamma$ ) に対し,  $0 < \alpha' < \gamma - \beta$  となる  $\alpha' \in A$  が存在し,  $\alpha'' := \alpha'(\lfloor \frac{\beta}{\alpha'} \rfloor + 1)$  は  $\alpha'' \in A$  と  $\beta < \alpha'' < \gamma$  をみたす.

問題 1.9 (1)  $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$  が  $1 \in a\mathbb{Z} + b\mathbb{Z}$  と同値であることによる.

(2)  $ak + bl = 1$  となるような  $k, l \in \mathbb{Z}$  をとると,  $ab' = a'b$  より,

$$b' = b'(ak + bl) = b(a'k + b'l) \in b\mathbb{Z}.$$

同様にして  $b \in b'\mathbb{Z}$  もわかるから,  $b = b'$ . これより  $a = a'$  もわかる.

問題 1.12 (1)  $(a\mathbb{Z} + b\mathbb{Z}) + c\mathbb{Z} = a\mathbb{Z} + (b\mathbb{Z} + c\mathbb{Z}) = a\mathbb{Z} + b\mathbb{Z} + c\mathbb{Z}$  であることによる.

(2)  $(a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z} = a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z}) = a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z}$  であることによる.

(3)  $ab\mathbb{Z} + ac\mathbb{Z} = a(b\mathbb{Z} + c\mathbb{Z}) = |a|(b\mathbb{Z} + c\mathbb{Z})$  であることによる.

(4)  $ab\mathbb{Z} \cap ac\mathbb{Z} = a(b\mathbb{Z} \cap c\mathbb{Z}) = |a|(b\mathbb{Z} \cap c\mathbb{Z})$  であることによる.

問題 1.19  $e > f$  であるとして一般性を失わない. このとき,

$$\begin{aligned} a^{2^e} - 1 &= (a^{2^{e-1}} - 1)(a^{2^{e-1}} + 1) \\ &= (a^{2^{e-2}} - 1)(a^{2^{e-2}} + 1)(a^{2^{e-1}} + 1) \\ &= (a^{2^{e-3}} - 1)(a^{2^{e-3}} + 1)(a^{2^{e-2}} + 1)(a^{2^{e-1}} + 1) \\ &= \dots \end{aligned}$$

より  $a^{2^e} - 1 = (a^{2^e} + 1) - 2$  は  $a^{2^f} + 1$  で割り切れることがわかるから,

$$\gcd(a^{2^e} + 1, a^{2^f} + 1) = \gcd(2, a^{2^f} + 1) = \begin{cases} 1 & (2 \nmid (a^{2^f} + 1) \text{ の場合}) \\ 2 & (2 \mid (a^{2^f} + 1) \text{ の場合}) \end{cases}.$$

よって

$$2 \mid (a^{2^f} + 1) \iff a \text{ は奇数}$$

より主張を得る.

**問題 2.10** 容易.

**問題 2.11** 命題 2.4 より明らか.

**問題 2.12** 命題 2.6 の等式において, 両辺の転置をとればよい.

**問題 2.13** まず,

$$\begin{vmatrix} x_0 \end{vmatrix} = x_0, \quad \begin{vmatrix} x_0 & 1 \\ -1 & x_1 \end{vmatrix} = x_0 x_1 + 1.$$

また,

$$\begin{aligned} \begin{vmatrix} x_0 & 1 & & & 0 \\ -1 & \ddots & \ddots & & \\ & \ddots & \ddots & 1 & \\ 0 & & -1 & x_{i-2} & 1 \\ \hline 0 & \dots & \dots & 0 & -1 & x_i \end{vmatrix} &= x_i \begin{vmatrix} x_0 & 1 & & & 0 \\ -1 & \ddots & \ddots & & \\ & \ddots & \ddots & 1 & \\ 0 & & -1 & x_{i-2} & 1 \end{vmatrix} + \begin{vmatrix} x_0 & 1 & & 0 \\ -1 & \ddots & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & x_{i-2} \end{vmatrix} \begin{vmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{vmatrix} \\ &= x_i \begin{vmatrix} x_0 & 1 & & & 0 \\ -1 & \ddots & \ddots & & \\ & \ddots & \ddots & 1 & \\ 0 & & -1 & x_{i-2} & 1 \end{vmatrix} + \begin{vmatrix} x_0 & 1 & & 0 \\ -1 & \ddots & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & x_{i-2} \end{vmatrix}. \end{aligned}$$

従って, 命題 2.8 より求める等式を得る.

**問題 2.22**  $i = -2, -1$  に対しては明らか.  $i \geq 0$  に対しては  $p_i q_{i-1} - p_{i-1} q_i = \pm 1$  による.

**問題 2.23**  $k_0 = 1 = q_{-2}$  と  $l_0 = 0 = -p_{-2}$  は明らか. また, 系 2.7 より,  $i \geq 0$  に対して

$$(-1)^{i-1} \begin{pmatrix} q_{i-1} & -p_{i-1} \\ -q_i & p_i \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -c_i \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -c_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -c_0 \end{pmatrix}$$

が成り立つことがわかるから,

$$a_{i+1} = a(-1)^{i-1} q_{i-1} + b(-1)^i p_{i-1}.$$

これより

$$k_{i+1} = (-1)^{i-1} q_{i-1}, \quad l_{i+1} = (-1)^i p_{i-1} \quad (i \geq 0)$$

を得る.

**問題 3.10**  $\eta = \frac{\alpha\xi + \beta}{\gamma\xi + \delta}$  より,

$$-\gamma\eta + \alpha = \frac{\alpha\delta - \beta\gamma}{\gamma\xi + \delta}, \quad (-\gamma\eta + \alpha)\xi = \delta\eta - \beta.$$

これより主張を得る.

**問題 3.13** 命題 3.8 の (2) より

$$\left| \alpha - \frac{p_i}{q_i} \right| = \frac{1}{(q_i \alpha_{i+1} + q_{i-1}) q_i}$$

であつて,  $\alpha_{i+1} < c_{i+1} + 1$  と  $c_{i+2} \geq 1$  より

$$q_i \alpha_{i+1} + q_{i-1} < q_i (c_{i+1} + 1) + q_{i-1} = q_{i+1} + q_i \leq q_{i+1} c_{i+2} + q_i = q_{i+2}.$$

これより求める不等式を得る.

**問題 3.16** (1)  $\alpha = \sqrt{3}$  とするとき,

$$\begin{aligned} \alpha_0 &= \sqrt{3}, & c_0 &= \lfloor \sqrt{3} \rfloor = 1; \\ \alpha_1 &= \frac{1}{\sqrt{3}-1} = \frac{1+\sqrt{3}}{2}, & c_1 &= \left\lfloor \frac{1+\sqrt{3}}{2} \right\rfloor = 1; \\ \alpha_2 &= \frac{1}{\frac{1+\sqrt{3}}{2}-1} = 1+\sqrt{3}, & c_2 &= \lfloor 1+\sqrt{3} \rfloor = 2; \\ \alpha_3 &= \frac{1}{(1+\sqrt{3})-2} = \frac{1+\sqrt{3}}{2}, & c_3 &= \left\lfloor \frac{1+\sqrt{3}}{2} \right\rfloor = 1. \end{aligned}$$

以下同様であるから,

$$\sqrt{3} = [1, 1, 2, 1, 2, \dots, 1, 2, \dots].$$

(2)  $\alpha = \sqrt{5}$  とするとき,

$$\begin{aligned} \alpha_0 &= \sqrt{5}, & c_0 &= \lfloor \sqrt{5} \rfloor = 2; \\ \alpha_1 &= \frac{1}{\sqrt{5}-2} = 2+\sqrt{5}, & c_1 &= \lfloor 2+\sqrt{5} \rfloor = 4; \\ \alpha_2 &= \frac{1}{(2+\sqrt{5})-4} = 2+\sqrt{5}, & c_2 &= \lfloor 2+\sqrt{5} \rfloor = 4. \end{aligned}$$

以下同様であるから,

$$\sqrt{5} = [2, 4, 4, \dots, 4, \dots].$$

(3)  $\alpha = \sqrt{7}$  とするとき,

$$\begin{aligned} \alpha_0 &= \sqrt{7}, & c_0 &= \lfloor \sqrt{7} \rfloor = 2; \\ \alpha_1 &= \frac{1}{\sqrt{7}-2} = \frac{2+\sqrt{7}}{3}, & c_1 &= \left\lfloor \frac{2+\sqrt{7}}{3} \right\rfloor = 1; \\ \alpha_2 &= \frac{1}{\frac{2+\sqrt{7}}{3}-1} = \frac{1+\sqrt{7}}{2}, & c_2 &= \left\lfloor \frac{1+\sqrt{7}}{2} \right\rfloor = 1; \\ \alpha_3 &= \frac{1}{\frac{1+\sqrt{7}}{2}-1} = \frac{1+\sqrt{7}}{3}, & c_3 &= \left\lfloor \frac{1+\sqrt{7}}{3} \right\rfloor = 1; \\ \alpha_4 &= \frac{1}{\frac{1+\sqrt{7}}{3}-1} = 2+\sqrt{7}, & c_4 &= \lfloor 2+\sqrt{7} \rfloor = 4; \\ \alpha_5 &= \frac{1}{(2+\sqrt{7})-4} = \frac{2+\sqrt{7}}{3}, & c_5 &= \left\lfloor \frac{2+\sqrt{7}}{3} \right\rfloor = 1. \end{aligned}$$

以下同様であるから,

$$\sqrt{7} = [2, 1, 1, 1, 4, 1, 1, 1, 4, \dots, 1, 1, 1, 4, \dots].$$

**問題 4.7**  $e = 2.7182818\dots$  より

$$2.7182818 \leq e \leq 2.7182819$$

で,

$$2.7182818 = \left[ 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, \frac{4776}{409} \right], \quad 2.7182819 = \left[ 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, \frac{9016}{1819} \right].$$

これより,  $e$  の連分数展開は次のようになることがわかる:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, \dots].$$

なお,

$$\left\lfloor \frac{4776}{409} \right\rfloor = 11, \quad \left\lfloor \frac{9016}{1819} \right\rfloor = 4$$

であるから,  $e$  の近似値 2.7182818 からは, この先の部分商を求めることはできない.

問題 5.1 (1)  $\alpha$  を  $d$  次の代数的数とし,

$$\alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = \alpha^d + a'_{d-1}\alpha^{d-1} + \cdots + a'_1\alpha + a'_0 = 0$$

$(a_i, a'_i \in \mathbb{Q})$  とすると,

$$(a_{d-1} - a'_{d-1})\alpha^{d-1} + \cdots + (a_1 - a'_1)\alpha + (a_0 - a'_0) = 0$$

となる. 従って, 次数の最小性より  $a_{d-1} - a'_{d-1} = \cdots = a_1 - a'_1 = a_0 - a'_0 = 0$  がわかる.

(2) 代数的数  $\alpha$  の最小多項式  $f(x)$  が  $\mathbb{Q}$  上  $f(x) = g(x)h(x)$  と分解したとすると,  $g(\alpha)h(\alpha) = f(\alpha) = 0$  より  $g(\alpha) = 0$  または  $h(\alpha) = 0$  となるから,  $\deg g(x) = \deg f(x)$  または  $\deg h(x) = \deg f(x)$ , 従って  $h(x) \in \mathbb{Q}$  または  $g(x) \in \mathbb{Q}$  でなければならない.

問題 5.2 (a) から (b) が従うことは明らか.

(b) を仮定し,  $ax^2 + bx + c = a(x - \alpha)(x - \alpha')$  により  $\alpha'$  を定めると,  $\alpha' \in \mathbb{R}$  で

$$\alpha + \alpha' = -\frac{b}{a}, \quad \alpha\alpha' = \frac{c}{a}$$

は  $\mathbb{Q}$  に属する. すなわち (c) が成り立つ.

(c) を仮定し,  $b^* := -(\alpha + \alpha')$ ,  $c^* := \alpha\alpha'$  と置けば,  $\alpha^2 + b^*\alpha + c^* = 0$  となる. すなわち (a) が成り立つ. また, 仮に  $\alpha = \alpha'$  とすると,  $2\alpha = \alpha + \alpha' \in \mathbb{Q}$  より  $\alpha \in \mathbb{Q}$  となって矛盾. なお, 最小多項式については明らか.

問題 5.10

$$\alpha = a + \frac{1}{b + \frac{1}{\alpha}} = \frac{(ab + 1)\alpha + a}{b\alpha + 1}$$

より  $b\alpha^2 - ab\alpha - a = 0$  となるから,

$$\alpha = \frac{ab + \sqrt{a^2b^2 + 4ab}}{2b}.$$

問題 5.14 (1)  $i \geq 0$  に対し,  $(-1)^i(\sqrt{d} - \frac{p_i}{q_i}) > 0$  と  $\frac{p_i}{q_i} > 0$  より  $(-1)^i(p_i^2 - dq_i^2) < 0$  がわかるから,  $b_i > 0$  ( $i \geq 1$ ). 従って,  $b_0 = 1^2 - d \cdot 0^2 = 1$  より,  $b_i \geq 1$  ( $i \geq 0$ ) を得る. また,

$$\alpha_i = \frac{q_{i-2}\sqrt{d} - p_{i-2}}{-q_{i-1}\sqrt{d} + p_{i-1}} = \frac{-p_{i-1}p_{i-2} + dq_{i-1}q_{i-2} + (p_{i-1}q_{i-2} - p_{i-2}q_{i-1})\sqrt{d}}{p_{i-1}^2 - dq_{i-1}^2} = \frac{a_i + \sqrt{d}}{b_i}.$$

(2)  $a_0 = -1 \cdot 0 + d \cdot 0 \cdot 1 = 0$  で,

$$\begin{aligned} (-1)^i(a_{i+1} + a_i) &= p_i p_{i-1} - dq_i q_{i-1} - p_{i-1} p_{i-2} + dq_{i-1} q_{i-2} \\ &= (c_i p_{i-1} + p_{i-2}) p_{i-1} - d(c_i q_{i-1} + q_{i-2}) q_{i-1} - p_{i-1} p_{i-2} + dq_{i-1} q_{i-2} \\ &= c_i(p_{i-1}^2 - dq_{i-1}^2) \\ &= (-1)^i b_i c_i \end{aligned}$$

より  $a_{i+1} = b_i c_i - a_i$  がわかる. また, 既にししたように  $b_0 = 1$  で,

$$\begin{aligned} -b_i b_{i+1} &= (p_{i-2}^2 - dq_{i-2}^2)(p_{i-1}^2 - dq_{i-1}^2) \\ &= p_{i-1}^2 p_{i-2}^2 - dp_{i-1}^2 q_{i-2}^2 - dp_{i-2}^2 q_{i-1}^2 + d^2 q_{i-1}^2 q_{i-2}^2 \\ &= (-p_{i-1} p_{i-2} + dq_{i-1} q_{i-2})^2 - d(p_{i-1} q_{i-2} - p_{i-2} q_{i-1})^2 \\ &= a_{i+1}^2 - d \end{aligned}$$

より  $b_{i+1} = \frac{d - a_{i+1}^2}{b_i}$  がわかる.

(3) 一般に,  $\xi \in \mathbb{R}$  と  $m \in \mathbb{Z}_+$  に対し,  $\left\lfloor \frac{\xi}{m} \right\rfloor = \left\lfloor \frac{\lfloor \xi \rfloor}{m} \right\rfloor$  が成り立つ. 実際,  $k := \lfloor \xi \rfloor$ ,  $l := \left\lfloor \frac{k}{m} \right\rfloor$  と置くと,  $lm \leq k \leq (l+1)m - 1$  より  $lm \leq \xi < (l+1)m$ , すなわち  $l \leq \frac{\xi}{m} < l+1$  がわかるから,  $\left\lfloor \frac{\xi}{m} \right\rfloor = l$ . 従って, (1) と  $\lfloor a_i + \sqrt{d} \rfloor = a_i + \lfloor \sqrt{d} \rfloor = a_i + c_0$  より

$$c_i = \lfloor \alpha_i \rfloor = \left\lfloor \frac{a_i + \sqrt{d}}{b_i} \right\rfloor = \left\lfloor \frac{a_i + c_0}{b_i} \right\rfloor$$

を得る.

**問題 6.5** 定理 6.3 の証明において  $l = 0$  であるとする,  $p = p_i k$ ,  $q = q_i k$  となつて  $\frac{p}{q} \neq \frac{p_i}{q_i}$  に反するから,  $l \neq 0$ . このとき

$$q\alpha - p = l(q_{i-1}\alpha - p_{i-1}) \left(1 - \frac{k}{l} \cdot \frac{-q_i\alpha + p_i}{q_{i-1}\alpha - p_{i-1}}\right) = l(q_{i-1}\alpha - p_{i-1}) \left(1 - \frac{k}{l} \cdot \frac{1}{\alpha_{i+1}}\right)$$

より

$$|q\alpha - p| = |l| \cdot |q_{i-1}\alpha - p_{i-1}| \cdot \left|1 - \frac{k}{l} \cdot \frac{1}{\alpha_{i+1}}\right| \geq |q_{i-1}\alpha - p_{i-1}| \cdot \left|1 - \frac{k}{l} \cdot \frac{1}{\alpha_{i+1}}\right|$$

となる. 従って,  $\frac{k}{l} \leq 0$  と  $\alpha_{i+1} > 1$  より  $|q\alpha - p| \geq |q_{i-1}\alpha - p_{i-1}|$  を得る.

**問題 6.9**  $\alpha = \frac{m}{n}$  ( $m \in \mathbb{Z}$ ,  $n \in \mathbb{Z}_+$ ) とすると  $\alpha - \frac{p}{q} = \frac{mq - np}{nq}$ . 従って

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{1+\varepsilon}}$$

とすると,

$$\frac{1}{nq} \leq \frac{|mq - np|}{nq} < \frac{1}{q^{1+\varepsilon}}$$

より  $q < n^{1/\varepsilon}$  でなければならないが, そのような  $q \in \mathbb{Z}_+$  は有限個しか存在しない. また, 各  $q \in \mathbb{Z}_+$  に対して

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{1+\varepsilon}}$$

をみたす  $p \in \mathbb{Z}$  は有限個しか存在しない.

問題 6.12  $\alpha = \sqrt{2}$  に対して定理 6.10 の証明と同様に  $f(x)$ ,  $C'$ ,  $C$  を定めると,

$$f(x) = x^2 - 2, \quad C' = 2(\sqrt{2} + 1), \quad C = \frac{1}{2(\sqrt{2} + 1)}.$$

従って,  $p \in \mathbb{Z}$  と  $q \in \mathbb{Z}_+$  が条件をみたすとする,

$$\frac{1}{2(\sqrt{2} + 1)} \cdot \frac{1}{q^2} \leq \left| \sqrt{2} - \frac{p}{q} \right| < \frac{1}{q^3}$$

より  $q < 2(\sqrt{2} + 1)$  でなければならない. よって  $q \in \{1, 2, 3, 4\}$ . ここで

$$\left| \sqrt{2} - \frac{p}{q} \right| < \frac{1}{q^3} \iff q\sqrt{2} - \frac{1}{q^2} < p < q\sqrt{2} + \frac{1}{q^2}$$

であるから:

- (1)  $q = 1$  の場合, 条件をみたす  $p$  は  $p = 1, 2$ .
- (2)  $q = 2$  の場合, 条件をみたす  $p$  は  $p = 3$ .
- (3)  $q = 3$  の場合, 条件をみたす  $p$  は存在しない.
- (4)  $q = 4$  の場合, 条件をみたす  $p$  は存在しない.

問題 7.13 (1)  $d = 7$  のとき,

$$\begin{aligned} a_0 &= 0, & b_0 &= 1, & c_0 &= \lfloor \sqrt{7} \rfloor = 2; \\ a_1 &= 1 \cdot 2 - 0 = 2, & b_1 &= \frac{7 - 2^2}{1} = 3, & c_1 &= \left\lfloor \frac{2 + 2}{3} \right\rfloor = 1; \\ a_2 &= 3 \cdot 1 - 2 = 1, & b_2 &= \frac{7 - 1^2}{3} = 2, & c_2 &= \left\lfloor \frac{1 + 2}{2} \right\rfloor = 1; \\ a_3 &= 2 \cdot 1 - 1 = 1, & b_3 &= \frac{7 - 1^2}{2} = 3, & c_3 &= \left\lfloor \frac{1 + 2}{3} \right\rfloor = 1; \\ a_4 &= 3 \cdot 1 - 1 = 2, & b_4 &= \frac{7 - 2^2}{3} = 1 \end{aligned}$$

より  $l = 4$ . また,

$$\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 8 \\ 3 \end{pmatrix}$$

より, 正の最小解は  ${}^t(x, y) = {}^t(8, 3)$ .

(2)  $d = 13$  のとき,

$$\begin{aligned}
a_0 &= 0, & b_0 &= 1, & c_0 &= \lfloor \sqrt{13} \rfloor = 3; \\
a_1 &= 1 \cdot 3 - 0 = 3, & b_1 &= \frac{13 - 3^2}{1} = 4, & c_1 &= \left\lfloor \frac{3 + 3}{4} \right\rfloor = 1; \\
a_2 &= 4 \cdot 1 - 3 = 1, & b_2 &= \frac{13 - 1^2}{4} = 3, & c_2 &= \left\lfloor \frac{1 + 3}{3} \right\rfloor = 1; \\
a_3 &= 3 \cdot 1 - 1 = 2, & b_3 &= \frac{13 - 2^2}{3} = 3, & c_3 &= \left\lfloor \frac{2 + 3}{3} \right\rfloor = 1; \\
a_4 &= 3 \cdot 1 - 2 = 1, & b_4 &= \frac{13 - 1^2}{3} = 4, & c_4 &= \left\lfloor \frac{1 + 3}{4} \right\rfloor = 1; \\
a_5 &= 4 \cdot 1 - 1 = 3, & b_5 &= \frac{13 - 3^2}{4} = 1
\end{aligned}$$

より  $l = 5$ . また,

$$\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 18 \\ 5 \end{pmatrix}$$

より, 正の最小解は  ${}^t(x, y) = {}^t(18, 5)$ .