

8 「重要な補題」の証明

- [I] 良く知られているように、自然数全体の集合と自然数のペア全体の集合は同じ濃度を持つ。実際、関数

$$g(t) = \frac{t(t+1)}{2}$$

を用いて

$$J(x, y) = x + g(x + y)$$

と定義すると、以下で確かめられるように、写像

$$J : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}, \quad \text{ただし } \mathbb{N} = \{0, 1, 2, 3, \dots\}$$

は全単射である。ここで、関数 $g(t)$ は

$$(\spadesuit) \quad g(t+1) - g(t) = t+1$$

をみたし、したがって

$$(\clubsuit) \quad 0 = g(0) < g(1) < g(2) < \dots < g(t) < \dots \rightarrow \infty \quad (t \rightarrow \infty)$$

が成り立つことを注意しておく。

- [II] 単射であること：

[証明] 4つの自然数 x, y, x', y' が $J(x, y) = J(x', y')$ をみたすと仮定する。このとき、 $z = x + y$, $z' = x' + y'$ とおけば

$$(\heartsuit) \quad x + g(z) = x' + g(z')$$

が成り立つ。いま、もし $z < z'$ ならば、 $(\spadesuit)$ と $(\clubsuit)$ を用いて

$$x - x' = g(z') - g(z) \geq g(z+1) - g(z) = z+1 = x+y+1 > x$$

から $-x' > 0$ となって矛盾する。よって $z \geq z'$ であるが、同様に逆の不等号も得られるから、結局 $z = z'$ が成り立つ。したがって $(\heartsuit)$ から $x = x'$ 、よって

$$y = z - x = z' - x' = y'$$

も得られ、 J の単射性が示された。

(証明終)

[III] 全射であること：

[証明] 任意の $w \in \mathbb{N}$ に対して、 $J(x, y) = w$ をみたす $x, y \in \mathbb{N}$ が存在することをいえばよい。まず、 $g(t)$ の性質 (♣) により、 w に対して

$$g(t) \leq w < g(t+1)$$

をみたす自然数 t がとれる。そこで、

$$x = w - g(t), \quad y = g(t+1) - w - 1$$

と定めると、明らかに $x, y \geq 0$ すなわち $x, y \in \mathbb{N}$ であり、

$$x + y = g(t+1) - g(t) - 1 = t,$$

$$\therefore w = x + g(t) = J(x, y)$$

となって、 J が全射であることが確かめられた。 (証明終)

[IV] 2変数関数 $J : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ は全単射であることから、その逆関数

$$\mathbb{N} \rightarrow \mathbb{N} \times \mathbb{N}, \quad w \mapsto (K(w), L(w))$$

が考えられる。すなわち、

$$K(J(x, y)) = x, \quad L(J(x, y)) = y \quad \text{および} \quad J(K(w), L(w)) = w$$

をみたす二つの1変数関数 K, L が存在する。

[V] 命題 J, K, L は $\mathcal{M}_B$ に属する。

[証明] $g(t) = \frac{t(t+1)}{2}$ は $\mathcal{M}_B$ に属し、

$$J(x, y) = x + g(x + y)$$

となっているから、 J は $\mathcal{M}_B$ に属する。さらに、 J の全射性の証明から、 w に対して

$$g(t_0) \leq w < g(t_0 + 1)$$

をみたす t_0 がとれて

$$K(w) = w - g(t_0), \quad L(w) = g(t_0 + 1) - w - 1$$

とかけることがわかる。ここで、 $t_0 \leq g(t_0) \leq w$ となっているから、

$$t_0 = \mu_{t \leq w}[w < g(t+1)]$$

が成り立っている。以上より、 K, L は

$$\begin{cases} K(w) = w \smile g(\mu_{t \leq w}[w < g(t+1)]) \\ L(w) = g(\mu_{t \leq w}[w < g(t+1)] + 1) \smile (w+1) \end{cases}$$

と表され $\mathcal{M}_B$ に属することがわかった。 (証明終)

注意 K, L は

$$K(w) = \mu_{x \leq w} [\mu_{y \leq w} [J(x, y) = w] \leq w]$$

$$L(w) = \mu_{y \leq w} [\mu_{x \leq w} [J(x, y) = w] \leq w]$$

とかけることも確かめられ、これを根拠にしても $\mathcal{M}_B$ に属することがいえる。

[VI] **中国の剰余定理** $m_1, \dots, m_n$ をどの二つも互いに素な整数とすると、任意の整数の組 $a_1, \dots, a_n$ に対して

$$a \equiv a_i \pmod{m_i} \quad (1 \leq i \leq n)$$

をみたす整数 a が存在する。さらに、このような a は $m_1 \cdots m_n$ を法として一意的に定まる。

[VII] **大切な補題** 次の (b) をみたす $\mathcal{M}_B$ に属する 2 変数関数 $M(i, x)$ が存在する；

$$(b) \quad \begin{cases} \text{任意の } n > 0 \text{ および } A \geq 0 \text{ に対して、} \\ \begin{cases} M(i, x_0) \text{ と } M(j, x_0) \text{ は互いに素} & (0 \leq i < j \leq n) \\ A < M(i, x_0) & (0 \leq i \leq n) \end{cases} \\ \text{をみたす自然数 } x_0 \text{ が存在する。} \end{cases}$$

[証明] $M(i, x) = 1 + (i+1)x$ とおけばよいことを以下で示す。いま、 n, A に対して、自然数 x_0 を $n!$ の倍数で $A-1 < x_0$ をみたすようにとる。このとき、 $A < 1 + (i+1)x_0$ ($i = 0, \dots, n$) となることは明らかである。さらに、ある $0 \leq i < j \leq n$ について $1 + (i+1)x_0, 1 + (j+1)x_0$ が互いに素でないとすると、素数 p が存在して

$$1 + (i+1)x_0 \equiv 1 + (j+1)x_0 \equiv 0 \pmod{p}$$

となる。このとき $(j-i)x_0 \equiv 0 \pmod{p}$ であるが、 $0 < j-i \leq n$ より $j-i$ は $n!$ の、したがって x_0 の約数となるから、結局 $x_0 \equiv 0 \pmod{p}$ が導かれ、

$$1 \equiv 1 + (i+1)x_0 \equiv 0 \pmod{p}$$

となって矛盾する。よって、 $1 + (i+1)x_0, 1 + (j+1)x_0$ は互いに素である。
(証明終)

[VIII] **重要な補題** (再記) 次の (*) をみたす $\mathcal{M}_B$ に属する 2 変数関数 $T(i, w)$ が存在する；

$$(*) \quad \begin{cases} \text{任意の自然数の有限列 } a_0, a_1, \dots, a_n \text{ に対して、} \\ a_i = T(i, w_0) \quad (i = 0, 1, \dots, n) \\ \text{をみたす自然数 } w_0 \text{ が存在する。} \end{cases}$$

[証明] まず、**大切な補題**の $M(i, x)$ を用いて、3 変数関数

$$U(i, x, y) = \mu_{t < M(i, x)} [y \equiv t \pmod{M(i, x)}]$$

を定義すれば、これは $\mathcal{M}_B$ に属する。いま、自然数の有限列 $a_0, \dots, a_n$ に対して、 $A = \max\{a_0, \dots, a_n\}$ とおき、**大切な補題**の条件 (b) をみたすように x_0 をとる。さらに、**中国の剰余定理**を用いれば、

$$y_0 \equiv a_i \pmod{M(i, x_0)} \quad (0 \leq i \leq n)$$

となるように y_0 を選ぶことができる。このとき、 $U(i, x, y)$ および A の定義から、各 $i = 0, \dots, n$ に対し

$$\begin{cases} 0 \leq U(i, x_0, y_0) \leq a_i \leq A < M(i, x_0) \\ U(i, x_0, y_0) \equiv a_i \pmod{M(i, x_0)} \end{cases}$$

であり、したがって $U(i, x_0, y_0) = a_i$ でなければならない。以上より、 $U(i, x, y)$ は次をみたすことが示された；

$$\begin{cases} \text{任意の自然数の有限列 } a_0, a_1, \dots, a_n \text{ に対して、} \\ a_i = U(i, x_0, y_0) \quad (i = 0, 1, \dots, n) \\ \text{をみたす自然数 } x_0, y_0 \text{ が存在する。} \end{cases}$$

そこで、 $\mathcal{M}_B$ に属する関数 K, L を用いて

$$T(i, w) = U(i, K(w), L(w))$$

とおけば、 T は $\mathcal{M}_B$ に属し、**重要な補題**の (*) をみたすことがわかる。

(証明終)