第3章　最小値原理と数学的帰納法

3.1　最小値原理

自然数は「ものを数えるための言葉」であり，‘個数’を表す一方で‘順序’を表すとも考えられる．‘順序’としての自然数がもつ重要な性質として，次の原理がある．

最小値原理　自然数からなる空でない集合は最小値をもつ．

この原理は【割り算の定理】(定理 2.1) の証明の根拠にもなっている（このことを確かめよ）．

さて，この**最小値原理**は成り立つのが当たり前で，あえて証明する必要はないように見える．しかし，ここでは**数学的帰納法**を用いて厳密な証明を与えてみよう．数学的帰納法とは，自然数 n に関する命題 (性質・条件) $P(n)$ が与えられたとき，

$$\text{すべての } n \text{ に対して } P(n) \text{ が成り立つ}$$

ことを証明するための論法のひとつであり，以下のように定式化される．

数学的帰納法の原理　自然数 n に関する命題 $P(n)$ に対して，次の (1), (2) が成り立つならば，すべての自然数 n について $P(n)$ が成り立つ．
(1)　$P(1)$ が成り立つ．
(2)　任意の n に対して，もし $P(n)$ が成り立つならば $P(n+1)$ が成り立つ．

これを用いて「最小値原理」を証明する．

「【数学的帰納法の原理】⇒【最小値原理】」の証明　S を自然数からなる空でない集合とする．S が最小値をもたないと仮定して矛盾を導く．まず，

$$P(n) : 『\ n \text{ より小さい任意の自然数 } m \text{ について } m \notin S \text{ である}』$$

によって命題 $P(n)$ を定める．
(1)　1 より小さい自然数は存在しないから，明らかに $P(1)$ が成り立つ．
(2)　n を任意にとり，$P(n)$ が成り立つとする．すなわち，$1, 2, \cdots, n-1 \notin S$ である．このとき，もし $n \in S$ ならば，n が S の最小値ということになって，S が最小値をもたないという仮定に反する．したがって $n \notin S$ であり，$P(n+1)$ が成り立つ．
よって，「数学的帰納法の原理」より $P(n)$ がすべての $n \in \boldsymbol{N}$ に対して成り立つ．ところで，$S \neq \phi$ であったから，ある $n_0 \in S$ が存在するが，これは $P(n_0+1)$ が成り立たないことを意味し矛盾である．　□

ええっと，いま,「最小値原理」を「数学的帰納法の原理」から導いたわけであるが，なんとなく違和感を覚えないだろうか？　つまり,「最小値原理」の方が 1 行で書けてカンタンだし，そもそも「数学的帰納法の原理」より当たり前っぽい感じがする (オレだけ？)．

そこで，発想を転換して,「最小値原理」を “基本原理” として捉えることにしよう．この立場をとるならば,「数学的帰納法の原理」を「最小値原理」から導かなくてはならない…が，そんなことできんのかよぉ…と疑心暗鬼のキミに静かに告げたい，……それは可能なのだよ…… と．

「【最小値原理】⇒【数学的帰納法の原理】」の証明　命題 $P(n)$ について，(1), (2) が成り立っているとする．このとき，すべての $n \in \boldsymbol{N}$ について $P(n)$ が成り立つことを示したい．そこで，$P(n)$ が成り立たないような n が存在すると仮定して矛盾を導く．集合 S をそのような自然数 n 全体の集合，すなわち

$$S = \left\{ n \in \boldsymbol{N} \,\middle|\, P(n) \text{ が成り立たない} \right\}$$

とする．仮定より $S \neq \phi$ だから,「最小値原理」より S は最小値 m をもつ．(1) より $1 \notin S$ なので $m > 1$，したがって，ある $l \in \boldsymbol{N}$ によって $m = l + 1$ と表すことができるが，$l < m$ なので m の最小性より $l \notin S$．これは $P(l)$ が成り立つことを意味するので，(2) を用いれば，$P(l+1)$ すなわち $P(m)$ が成り立つことになって $m \in S$ に矛盾する．□

以上の議論により,「最小値原理」は「数学的帰納法の原理」と同等であり，一方がもう一方よりもエライということはない．片方を用いて証明できる命題はもう片方を使っても証明できるはずであり，どっちかじゃないと証明できない命題は（原理的には）ないはずである．たとえば,【割り算の定理】(定理 2.1) は「最小値原理」を使って証明されているが,「数学的帰納法」によっても証明できるはずである．このことを実際に確かめてみよう．

定理 2.1 の別証明　a, b ともに正の場合のみを扱い（他の場合も容易にこの場合に帰着される），q, r の存在を a に関する数学的帰納法によって示そう（一意性については元の証明と同じ）．$a = 1$ のときは，$b = 1$ かそうでないかに応じて $(q, r) = (1, 0), (0, 1)$ とおけばよい．次に，a に対して

$$a = bq + r, \quad 0 \leq r < b$$

をみたす整数の組 (q, r) が存在したと仮定する（帰納法の仮定）．このとき，$r + 1 \leq b$ であるが,

$$a + 1 = \begin{cases} qb + (r+1), & (r + 1 < b \text{ のとき}) \\ (q+1)b + 0, & (r + 1 = b \text{ のとき}) \end{cases}$$

を考えれば，$r + 1 < b$ であるか $b = r + 1$ であるかに応じて $(q, r + 1)$ または $(q + 1, 0)$ が $a + 1$ に対応する整数の組としてとれることがわかる．□

3.2 最大公約数再論

前章で最大公約数を定義し，それを計算するためのひとつの方法として，ユークリッドの互除法を提示した． このことは，2 つの整数に対して最大公約数が確かに存在することを示している． この節では，最大公約数への別の方向からのアプローチを試み，さらに，整数係数 1 次方程式の整数解との関連を見る．

整数 a の倍数全体の集合を $a\boldsymbol{Z}$ で表す;

$$a\boldsymbol{Z} = \left\{ ax \,\middle|\, x \in \boldsymbol{Z} \right\}.$$

ここで，$a\boldsymbol{Z} = (-a)\boldsymbol{Z}$ なので，必要ならばいつでも $a \geq 0$ ととり直すことができる．

さて，$\boldsymbol{Z}$ の部分集合に関する次の一般的命題から始める． 最小値原理が証明のキーポイントとなっていることに注意しよう．

命題 3.1 $\boldsymbol{Z}$ の空でない部分集合 I について，次の (i), (ii) は同値である．

(i) $a, b \in I$ ならば $a - b \in I$，すなわち I は差について閉じている．

(ii) $I = m\boldsymbol{Z}$ をみたす $m \in \boldsymbol{Z}$ が存在する．

証明 (i)⇒(ii): $I \neq \phi$ より，少なくともひとつの元 $x \in I$ が存在する． よって，$0 = x - x \in I$ である． $I = \{0\}$ ならば $m = 0$ とおけばよいので，以下，$\{0\} \subsetneq I$ とする． $a \in I$ が負だったら $-a = 0 - a \in I$ を考えることにより，$I \cap \boldsymbol{N} \neq \phi$ がわかる． そこで，最小値原理より $I \cap \boldsymbol{N}$ の最小値 m がとれる． この m について，$m\boldsymbol{Z} \subset I$ および $I \subset m\boldsymbol{Z}$ を順に示す． まず，$-m = 0 - m \in I$ であり，したがって $2m = m - (-m) \in I,\ 3m = 2m - (-m) \in I, \cdots$ のようにして（厳密には数学的帰納法により），任意の $n \in \boldsymbol{N}$ に対して $nm \in I$ が確かめられ，さらに $(-n)m = 0 - nm \in I$ でもあるから，$m\boldsymbol{Z} \subset I$ が示される． 次に，$I \subset m\boldsymbol{Z}$ を示すために，$a \in I$ を任意にとる． 割り算の定理から $a = mq + r$，$0 \leq r < m$ をみたす $q, r \in \boldsymbol{Z}$ がとれるが，$a \in I$ および $mq \in m\boldsymbol{Z} \subset I$ より $r = a - mq \in I$ となるから，もし $r > 0$ ならば m の最小性に矛盾する． よって $r = 0$ すなわち $a = mq \in m\boldsymbol{Z}$ となるから $I \subset m\boldsymbol{Z}$ が得られた．

(ii)⇒(i): $a, b \in I = m\boldsymbol{Z}$ とすると，$a = ma_0,\ b = mb_0$ $(a_0, b_0 \in \boldsymbol{Z})$ と表されるから，$a - b = m(a_0 - b_0) \in m\boldsymbol{Z} = I$ を得る． □

次の補題は，$a\boldsymbol{Z}$ の定義から直ちに確かめられる．

補題 3.2 整数 a, b に対して，

$$a|b, \qquad b \in a\boldsymbol{Z}, \qquad b\boldsymbol{Z} \subset a\boldsymbol{Z}$$

は，どのふたつも互いに同値である．

いま $a, b \in \boldsymbol{Z}$ に対して

$$I = \left\{ ax + by \,\middle|\, x, y \in \boldsymbol{Z} \right\}$$

とおくと，I は差について閉じている，すなわち上の命題 3.1 の (i) が成り立つことが容易にわかる． よって，(ii) も成り立ち，ある $d \in \boldsymbol{Z}$ が存在して $I = d\boldsymbol{Z}$ と表される． こ

こで，$d \geq 0$ であるとしてよい． この d は a, b の最大公約数であることが次のようにして確かめられる（補題 3.2 を何度か援用する）． まず，$a = a \cdot 1 + b \cdot 0 \in I = d\boldsymbol{Z}$ より $d|a$，同様に $d|b$ となるから d は a, b の公約数である． 次に，c を a, b の公約数とする．$d \in I$ と I の定義より，$d = ax + by$ $(x, y \in \boldsymbol{Z})$ と書けていることに注意すれば，命題 2.2 (2) から $c|d$ が導かれる． よって $d = \gcd(a, b)$ が示された．

以上により，与えられた整数 a, b に対して，それらの最大公約数 d の存在が（ユークリッドの互除法によらずに）厳密に証明できた． これを定理としてまとめておく．

定理 3.3 (1) 任意の $a, b \in \boldsymbol{Z}$ に対して

$$\left\{ ax + by \,\middle|\, x, y \in \boldsymbol{Z} \right\} = d\boldsymbol{Z}, \quad d \geq 0$$

をみたす $d \in \boldsymbol{Z}$ が存在し，$d = \gcd(a, b)$ が成り立つ．
(2) 任意の $a_1, \cdots, a_n \in \boldsymbol{Z}$ に対して

$$\left\{ a_1x_1 + \cdots + a_nx_n \,\middle|\, x_1, \cdots, x_n \in \boldsymbol{Z} \right\} = d\boldsymbol{Z}, \quad d \geq 0$$

をみたす $d \in \boldsymbol{Z}$ が存在し，$d = \gcd(a_1, \cdots, a_n)$ が成り立つ．

(1) は上で示したが，(2) も同様に示すことができる． あ，いけね，一般に n が 2 より大きい場合も含めて $a_1, \cdots, a_n \in \boldsymbol{Z}$ の最大公約数 $\gcd(a_1, \cdots, a_n)$ を定義すんの忘れてた． あらためて定義を書いておこうっと（ついでに最小公倍数もね）．

定義 3.4 $a_1, \cdots, a_n \in \boldsymbol{Z}$ とする．
(1) $d|a_i$ $(i = 1, \cdots, n)$, (2) $c|a_i$ $(i = 1, \cdots, n)$ ならば $c|d$
をみたす整数 $d \geq 0$ を $a_1, \cdots, a_n$ の最大公約数といい，$\gcd(a_1, \cdots, a_n)$ で表す． また，
(3) $a_i|m$ $(i = 1, \cdots, n)$, (4) $a_i|l$ $(i = 1, \cdots, n)$ ならば $m|l$
をみたす整数 $m \geq 0$ を $a_1, \cdots, a_n$ の最小公倍数といい，$\mathrm{lcm}(a_1, \cdots, a_n)$ で表す．

最後に，定理 3.3 に関連して，整数係数 1 次方程式の整数解に関する定理を述べる．

定理 3.5 $a_1, \cdots, a_n \in \boldsymbol{Z}$ の最大公約数を d とする． $b \in \boldsymbol{Z}$ に対して，未知数 $x_1, \cdots, x_n$ に関する方程式

$$a_1x_1 + \cdots + a_nx_n = b$$

の整数解が存在するための必要十分条件は，$d|b$ である．

証明 前定理より

$$\left\{ a_1x_1 + \cdots + a_nx_n \,\middle|\, x_1, \cdots, x_n \in \boldsymbol{Z} \right\} = d\boldsymbol{Z}$$

が成り立っている． よって，与えられた方程式が整数解をもつことと，$b \in d\boldsymbol{Z}$ は同値である． 一方，$b \in d\boldsymbol{Z}$ は $d|b$ と同値なので，定理の主張を得る． □