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,【割り算の定理】(定理 2.1) の証明の根拠でもあった，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．

実際，$\boldsymbol{N}$ の空でない部分集合 S がひとつ与えられたとする．$S \neq \phi$ なので，ある n_0 が S に属する．そこで，まず $1 \in S$ かどうかをチェックし，そうでないときは，次に $2 \in S$ かどうかをチェックし，またもそうでないときには $3 \in S$ をチェックする．一方 $n_0 \in S$ であったから，この操作を順に繰り返せば，n_0 回以下の操作で，初めて $m \in S$ となる自然数 $m \leq n_0$ が見つかるはずである．この m が S の最小値となることは明らかであろう．

上の議論で重要なことは，$n_0 \in S$ の存在によって操作が無限に続かないことが保証されている点にある．それでもなお，証明としては少し曖昧なところがある（ような気がする）．たとえば，n_0 が 5 とか 623 とかいう定数ではなく，ただ存在がわかっているだけの数なのに，'n_0 回以下の操作' なんて言っちゃっていいの？

そこで，ここでは，**数学的帰納法**を用いて厳密な証明を与えよう．数学的帰納法とは 知ってるとは思うけど…，自然数 n に関する命題 (性質・条件) $P(n)$ が与えられたとき，すべての n に対して $P(n)$ が正しい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」を証明してみよう．

【数学的帰納法の原理】$\Longrightarrow$【最小値原理】　S を自然数からなる空でない集合とする．$\underline{S}$

2015 年度「代数入門」講義資料（2015 年 10 月）ver.1002

が最小値をもたないと仮定して矛盾を導く．まず，

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

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…と疑心暗鬼のあなたに言いたい．それは可能なのだ！

【最小値原理】$\Longrightarrow$【数学的帰納法の原理】　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．このとき，

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

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;

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

$a\boldsymbol{Z} = (-a)\boldsymbol{Z}$ 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ことに注意する．また，別の整数 b に対して，$a|b$ が $b \in a\boldsymbol{Z}$ と同値であることにも注意せよ．

まず，$\boldsymbol{Z}$ の部分集合に関する次の一般的命題から始めよう．

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．このとき，$-m = 0 - m \in I$ であり，$2m = m - (-m) \in I$，$3m = 2m - (-m) \in I, \cdots$ 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．逆の包含関係 $I \subset m\boldsymbol{Z}$ 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，$a, mq \in I$ 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 $I \subset m\boldsymbol{Z}$.
(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． □

さて，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，すなわち上の命題の (i) が成り立つことが容易にわかる． よって，(ii) が成り立ち，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．

まず，$a, b \in I = d\boldsymbol{Z}$ より $d|a$ かつ $d|b$ となるから d は a, b の公約数である． 次に，$c \in \boldsymbol{N}$ 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とになる． これを定理としてまとめておく．

定理 3.2 (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) も全く同様にして示すことができる． あ，いけね，一般に $a_1, \cdots, a_n \in \boldsymbol{Z}$ の最大公約数 $\gcd(a_1, \cdots, a_n)$ を定義すんの忘れてたけど，いいよね，わかるよね． というか，少し強引だが，この定理によって最大公約数を "定義" してしまえばいいのだ！ 今後はこの定理を自由に使っていこう． これでいいのだ！ とは言っても，バカボンのパパではない私はちょっと不安なので，あらためて定義を書いておこうっと．

定義 3.3 $a_1, \cdots, a_n \in \boldsymbol{Z}$ の最大公約数とは，次の (1), (2) をみたす整数 $d \geq 0$ のことである． (1) $d|a_i$ $(i = 1, \cdots, n)$, (2) $c|a_i$ $(i = 1, \cdots, n)$ ならば $c|d$.

最後に，上の定理に関連して，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 3.4 $a_1, \cdots, a_n \in \boldsymbol{Z}$ 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． □