§4. 累積的帰納法

高校で学ぶ数学的帰納法（前回学んだ帰納法）では、n 番目の命題 $P(n)$ が成り立つことを示すために、1 つ手前の $P(n-1)$ の “力を借りる”が、$P(n-1)$ だけでは “力が足りない”場合がしばしば起こる。このような場合に、$P(1), \dots, P(n-1)$ のすべての力を借りて、$P(n)$ が成り立つこと示す、というのがこの節で学ぶ累積的帰納法である。

● 4-1：累積的帰納法（原型）

累積的帰納法 (次の定理) は前節で説明されてている普通の数学的帰納法から証明することができる。

定理 4-1-1 (累積的帰納法)
$\mathbb{N}$ を定義域とする命題関数 $P(n)$ が与えられているとする。もし、次の I, II が示されたとすると、全称命題「すべての $n \in \mathbb{N}$ に対して $P(n)$」は真である、すなわち、命題 $P(1), P(2), P(3), \dots\dots$ はすべて成り立つ。

I. $P(1)$ は成り立つ。

II. $k \in \mathbb{N}$ について、$i \leq k$ を満たすすべての自然数 i に対して $P(i)$ が成り立つと仮定すると、$P(k+1)$ も成り立つ。

(**証明**)

[定理 3-2-2] の証明と同様に背理法で証明することができる。

$$M := \{\, n \in \mathbb{N} \mid P(n) \text{ は成り立たない} \,\}$$

とおき、$M \neq \varnothing$ であると仮定する。このとき、自然数の整列性から、M の中に最小の自然数 m が存在する。I により、$m > 1$ である。すると、$m-1 \in \mathbb{N}$ であるが、m の最小性から、$i \leq m-1$ なるすべての自然数 i に対して $i \notin M$ である。よって、$i \leq m-1$ なるすべての自然数 i に対して $P(i)$ は成り立つ。II により、$P(m) = P((m-1)+1)$ が成り立つ。これは $m \notin M$ を意味しており、$m \in M$ に矛盾する。よって、$M = \varnothing$ でなければならない。つまり、すべての $n \in \mathbb{N}$ に対して $P(n)$ が成り立つ。 □

累積的帰納法も数学的帰納法と呼ばれる。

例 4-1-2 (除法の原理) 任意の自然数 m, n に対して、

$$n = qm + r, \qquad 0 \leq r < m \tag{4-1 a}$$

を満たす整数 q, r が一意的に存在する。

(**証明**)

[$\boldsymbol{q, r}$ **の存在の証明**] n に関する命題関数 $P(n)$ を次のように定める：

$P(n)$: 任意の $m \in \mathbb{N}$ に対して、$n = qm + r,\ 0 \leq r < m$ を満たす整数 q, r が存在する。

すべての自然数 n に対して $P(n)$ が真であることを累積的帰納法で証明する。

I. $P(1)$ が成立すること：$m = 1$ のときには $q = 1,\ r = 0$ にとり、$m \geq 2$ のときには $q = 0,\ r = 1$ にとると、q, r は整数であり、$1 = qm + r,\ 0 \leq r < m$ が満たされる。よって、$P(1)$ は成立する。

II. n を自然数とし、n よりも小さい任意の自然数 k については、$P(k)$ は成り立つと仮定する。$m \in \mathbb{N}$ を任意にとる。

• $n < m$ の場合：$q = 0,\ r = n$ とおくと q, r は整数であり、$n = qm + r,\ 0 \leq r < m$ が満たされる。

• $n = m$ の場合：$q = 1,\ r = 0$ とおくと q, r は整数であり、$n = qm + r,\ 0 \leq r < m$ が満たされる。

• $n > m$ の場合：$k := n - m$ とおく。$1 \leq k < n$ であるから、帰納法の仮定より $P(k)$ は成立する。よって、$k = q'm + r',\ 0 \leq r' < m$ を満たす整数 q', r' が存在する。このとき、$q = q' + 1,\ r = r'$ とおくと、q, r は整数であり、$n = qm + r,\ 0 \leq r < m$ が満たされる。

いずれの場合も $n = qm + r,\ 0 \leq r < m$ を満たす整数 q, r が存在することが示されたので、$P(n)$ は成り立つ。累積的帰納法より、q, r の存在は証明された。

[**q, r の一意性の証明**] これは帰納法を用いずに示される。

n が次のように 2 通りに表わされたとする。

$$n = qm + r = q'm + r', \qquad 0 \leq r, r' < m.$$

$q = q'$ かつ $r = r'$ となることを証明すればよい。式変形して、

$$(*) \qquad (q - q')m = r' - r$$

を得る。ここで、$q - q' \neq 0$ であると仮定すると、等式 $(*)$ の両辺の絶対値をとって $|r' - r| = |q - q'|m \geq m$ を得る。一方、$0 \leq r, r' < m$ であるから、$|r - r'| < m$ である。ここに矛盾が生じた。よって、$q = q'$ であり、したがってまた、等式 $(*)$ より、$r = r'$ である。 □

● 4 - 2 ： 素因数分解の可能性と一意性—累積的帰納法の適用例として—

1 と自分自身以外に正の約数を持たない、1 でない自然数を**素数**といい、1 でも素数でもない自然数を**合成数**という。例えば、$2, 3, 5, 7, 11$ は素数、$4, 6, 8, 9, 10$ は合成数である。合成数とは ab $(a, b \in \mathbb{N},\ a, b > 1)$ のように、2 つの 2 以上の自然数の積に分解できる数のことに他ならない。

自然数は素数の積に表わすことができ、そのときに現れる素数は順番を無視すると一意的に決まることは知っているであろう。実は、これらの事実は累積的帰納法を使って証明される。ツェルメロ（Zermelo, 1871–1953）による巧妙な証明を紹介しよう。

定理 4 - 2 - 1 (素因数分解の可能性と一意性)

1 以外の任意の自然数 n は、有限個の素数の積に表わすことができる：

(4 - 2 a) $$n = p_1 p_2 \cdots p_r \qquad (r \geq 1,\ p_1, p_2, \ldots, p_r \text{ は素数}).$$

さらに、この表わし方は、$p_1, p_2, \ldots, p_r$ の並べ方の順番を除いて一意的である。(4 - 2 a) の表示を n の**素因数分解** (prime decomposition) といい、各 p_i $(i = 1, \ldots, r)$ を n の**素因数** (prime factor) という。

注意：上の定理の中に「並べ方の順番を除いて一意的である」という表現がある。この言い方するときには、「本質的には一意的である」、もう少し砕けた言い方をすれば、「あまり重要とは思われない違いを無視すれば一通りしかない」という気持ちが込められている。

(**定理 4 - 2 - 1 の証明**)

(1) 素因数分解の可能性：証明は演習問題とする。

(2) 書き表わし方の一意性：数学的帰納法で証明する。自然数 $n \geq 2$ に対して定義される命題関数 $P(n)$ を次のように定める：

$P(n)$ ： n を素数の積に書き表わすときの表わし方は順番を無視すれば一意的である。

I. $P(2)$ が成立すること：2 は素数であるから、これを 2 個以上の素数の積として表わすことはできない。よって、2 を素数の積に書き表わす仕方は一意的である。

Ⅱ. n を $n > 2$ なる自然数とし、n よりも小さい 2 以上の任意の自然数 k については、$P(k)$ は成り立つと仮定する。

• n が素数の場合：第 1 段と同様の理由で、n を素数の積に書き表わす仕方は一意的である。

• n が合成数の場合：n が素数の積に次のように 2 通りの仕方で書き表わされたと仮定する (n は合成数なので、下記の表示で、$r, s \geq 2$ に注意)。

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \qquad (p_1, \ldots, p_r, q_1, \ldots, q_s \text{ は素数}).$$

このとき、もし、q_1 が $p_1,\ p_2, \ldots, p_r$ のどれかと一致することが示されれば、$\frac{n}{q_1} \in \mathbb{N}$ に帰納法の仮定を用いて、$r = s$ であって、かつ、順番を適当に並べ変えると $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$ となることがわかる。

背理法で q_1 が $p_1,\ p_2, \ldots, p_r$ のどれかと一致することを示す。そのために、q_1 が $p_1,\ p_2, \ldots, p_r$ のどれとも一致しないと仮定する。すると、$q_1 \neq p_1$ である。

$q_1 < p_1$ のとき、$m := (p_1 - q_1)p_2 \cdots p_r$ は $1 < m < n$ を満たす自然数であるから、帰納法の仮定により、m を素数の積に分解する仕方は順番を無視すれば一意的である。この事実と、上式の右辺が

$$(p_1 - q_1)p_2 \cdots p_r = q_1(q_2 \cdots q_s - p_2 \cdots p_r)$$

と表せることから、q_1 は、$p_1 - q_1$ の素因数か、または、$p_2, \cdots, p_r$ のどれかに一致しなければならない。仮定から、q_1 は $p_2, \cdots, p_r$ とは一致しないので、q_1 は、$p_1 - q_1$ の素因数、つまり、q_1 は $p_1 - q_1$ を割り切ることがわかる。これより、q_1 は p_1 を割り切ることになるが、p_1, q_1 はともに素数であるから、$p_1 = q_1$ でなければならない。これは、$q_1 \neq p_1$ に矛盾する。

$q_1 > p_1$ のときは、m のかわりに、$(q_1 - p_1)p_2 \cdots p_r$ について上と同様の議論を行って、矛盾が出る。

こうして、すべての $k < n$ に対して $P(k)$ が成り立つとき、n が素数であっても合成数であっても $P(n)$ は成り立つことが示された。

これで、帰納法が完成し、一意性の証明が終わった。 □

(4 - 2 a) の右辺に現れる素数のうち同じものを冪の形にまとめて、次が得られる。

系 4 - 2 - 2 (**素因数分解の標準形**)

1 以外の任意の自然数 n は、素数の冪の積として次のように一意的に表わすことができる：

(4 - 2 b) $$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

ここで、$k \geq 1$ であり、$p_1 < p_2 < \cdots < p_k$ は素数、$e_1, e_2, \ldots, e_k$ は自然数である。

(4 - 2 b) の表示を n の**素因数分解 (の標準形)** という。

例 4 - 2 - 3

$$\begin{aligned} 4 &= 2^2, & 6 &= 2 \cdot 3, & 8 &= 2^3, & 9 &= 3^2, \\ 10 &= 2 \cdot 5, & 12 &= 2^2 \cdot 3, & 14 &= 2 \cdot 7, & 15 &= 3 \cdot 5, \\ 16 &= 2^4, & 18 &= 2 \cdot 3^2, & 20 &= 2^2 \cdot 5, & 21 &= 3 \cdot 7 \end{aligned}$$

● 4 - 3 : 累積的帰納法（第 1 段が複数の命題からなる場合）

累積的帰納法の変形版として、次もしばしば使われる。

定理 4 - 3 - 1 (累積的帰納法)

$n_0 \leq n_1$ を満たす $n_0, n_1 \in \mathbb{Z}$ と、$N := \{\, n \in \mathbb{Z} \mid n \geq n_0 \,\}$ を定義域とする命題関数 $P(n)$ が与えられているとする。もし、次の I, II が示されたとすると、全称命題「$\forall\, n \in N,\ P(n)$」は真である、すなわち、命題 $P(n_0), P(n_0+1), P(n_0+2), \ldots\ldots$ はすべて成り立つ。

I. $P(n_0), P(n_0+1), \ldots, P(n_1)$ は成り立つ。

II. $k \geq n_1$ を満たす $k \in \mathbb{Z}$ について、$n_0 \leq i \leq k$ を満たすすべての自然数 i に対して $P(i)$ が成り立つと仮定すると、$P(k+1)$ も成り立つ。

(**証明**)

$n \in \mathbb{N}$ に対して $P'(n) = P(n + n_0 - 1)$ とおく。すべての $n \in \mathbb{N}$ に対して $P'(n)$ が真であることを [定理 4 - 1 - 1] を用いて証明する。

I. 仮定により $P'(1) = P(n_0)$ は成立する。

II. $k \in \mathbb{N}$ とし、$i \leq k$ を満たすすべての自然数 i に対して $P'(i)$ が成り立つと仮定する。

$k \leq n_1 - n_0$ ならば、$P'(k+1) = P(k+n_0)$ は I により成り立つ。

$k > n_1 - n_0$ ならば、$k + n_0 - 1 \geq n_1$ である。$n_0 \leq j \leq k + n_0 - 1$ を満たすすべての自然数 j に対して、$j - n_0 + 1 \leq k$ であるから仮定により $P'(j - n_0 + 1) = P(j)$ が成り立つ。したがって、II により、$P(k+n_0) = P'(k+1)$ が成り立つ。

I, II により、すべての $n \in \mathbb{N}$ に対して $P'(n)$ が真であることが示された。 □

例 4 - 3 - 2 $a_1 = 1,\ a_2 = 3$ および漸化式

$$a_n = 3a_{n-1} - 2a_{n-2} \quad (n = 3, 4, 5, \ldots)$$

により定まる実数列 $\{a_n\}_{n=1}^{\infty}$ を考える。この実数列の一般項は

$$a_n = 2^n - 1 \quad (n \in \mathbb{N})$$

により与えられる。

(**証明**)

$P(n)$ を

$$P(n): \quad a_n = 2^n - 1$$

と定める。すべての $n \in \mathbb{N}$ に対して $P(n)$ が真であることを数学的帰納法 (累積的帰納法) で証明する。

I. $P(1), P(2)$ は初期条件 $a_1 = 1,\ a_2 = 3$ により成立している。

II. $k \geq 2$ とし、$1 \leq i \leq k$ を満たすすべての $i \in \mathbb{N}$ に対して $P(i)$ は真であると仮定する。このとき、

$$\begin{aligned} a_{k+1} &= 3a_k - 2a_{k-1} \\ &= 3(2^k - 1) - 2(2^{k-1} - 1) \qquad \text{(帰納法の仮定)} \\ &= 3 \cdot 2^k - 2^k - 1 \\ &= 2^{k+1} - 1 \end{aligned}$$

となる。したがって、$P(k+1)$ も真である。

I, II により、すべての $n \in \mathbb{N}$ に対して $a_n = 2^n - 1$ である。 □