# 補 講1　諸定理の証明

## 1.0　はじめに

この補講では，本文で証明しなかった，ちょっと高度と思えるものの証明を与えておきます。それは以下の定理です。

- 除法の原理
- 素数が無数に存在すること
- 素因数分解の可能性および一意性

より体系的な証明を求める読者は，たとえば「さらに勉強するために」で紹介しているような 松坂著「代数系入門」のような本を参照してください。

## 1.1　除法の原理の証明

本節では「除法の原理」の証明を与えます。

もっとも，きちんと証明をしようと思えば，自然数の公理である **ペアノの公理**　**ペアノの公理** からはじめなければなりませんので，かなり長くなってしまいます。

そこで，自然数の集合の一つの性質である「最小元の存在」定理から出発し，数学的帰納法について少し復習し，それを用いて「除法の原理」を証明して見せることにします。

なお「ペアノの公理」に興味のある人は，たとえば 松坂和夫著,「代数系入門」(岩波書店) の付録を読んでみてください[1]。

### 1.1.1　自然数の集合の性質と数学的帰納法

まず自然数の集合のもつ次の性質を紹介しておきます。この性質は証明するまでもなく当り前のように思えるかもしれません。そういった方には証明は不要と感じられることでしょう[2]。

[1] 上記の松坂先生の本は，本シリーズと同じように「整数」から話をはじめ，より一般的，抽象的に代数に関する理論の初歩をていねいに解説しています。
(本シリーズで勉強し，少し経験を積んだ後で!) 読んでみることをお勧めします。

[2] しかし，数学者はそれでは満足せず，この定理にも証明を与えています。そのような試みが「自然数とは何か」というより根本的な問いに答えることになるわけです。

ひとまずここでは，この定理を正しいとして受け入れ，数学的帰納法が正しいことの証明に応用してみせます。

**定理 (最小元の存在)**　自然数全体の集合 $\mathbb{N}$ の空でない部分集合 $A$ は最小元を持つ。
つまり $a_0 \in A$ で任意の $a \in A$ に対して $a_0 \leqq a$ となるものが存在する。

さて，この定理を用いると，次の定理が証明できます。

**定理 (数学的帰納法の原理　その 1)**　自然数の集合 $A$ が次の二つの性質をもつとする。 **数学的帰納法の原理**
(I) $A$ は 1 を含む。
(II) 自然数 $n$ が $A$ に含まれるなら，$n+1$ も $A$ に含まれる。
このとき，$A$ は自然数全体の集合 $\mathbb{N}$ と一致する。

**証明**　$A$ に含まれない自然数全体の集合を $A'$ とする。$A'$ が空集合であることを証明する。
もし $A'$ が空集合でなければ,「最小元の存在」定理から $A'$ は最小元 $n_0$ をもつ。仮定 (I) から $n_0 > 1$。よって $n_0 - 1 \geqq 1$ だが，$n_0$ は $A$ に含まれない最小の自然数なので，$n_0 - 1$ は $A$ の要素である。よって仮定 (II) から

$$n_0 = (n_0 - 1) + 1 \in A$$

これは矛盾。 **(証明終)**

この定理から,「数学的帰納法」が正しい証明方法であることが示せます。

**定理 (数学的帰納法　その 1)**　自然数 $n$ に関する命題 $P(n)$ があり， **数学的帰納法**

(1) $n = 1$ のとき成り立つ。つまり $P(1)$ が真。
(2) $n = k$ のとき，命題が成り立つと仮定すると，$n = k+1$ のときも命題が成り立つ。つまり，$P(k)$ が真であると仮定すると，$P(k+1)$ も真。

が成り立つとき，命題 $P(n)$ はすべての自然数 $n$ について成り立つ。

**証明**　$P(n)$ が真となる自然数 $n$ の全体の集合を $A$ とすれば,「数学的帰納法の原理その 1」の仮定 (I), (II) を満たす。よって $A$ は $\mathbb{N}$ と一致する。
ゆえに $P(n)$ はすべての自然数に対して成り立つ。 **(証明終)**

高校の数学で学習する「数学的帰納法」という証明方法は，上のようなものですが，これは次の形でもよく用いられます。「除法の原理」の証明では，この形の帰納法が使われます。

**定理 (数学的帰納法　その 2)**　自然数 $n$ に関する命題 $P(n)$ があり，

(1) $n=1$ のときなりたつ。
(2) $n>1$ とする。$0 \leqq k < n$ なるすべての自然数 $k$ に対して $P(k)$ が成り立つと仮定すると，$P(n)$ も成り立つ。

が成り立つとき，命題 $P(n)$ はすべての自然数 $n$ について成り立つ。

また，ここでは (1) として $n=1$ としましたが，$n=0$ としても構いません。

この第二番目の「数学的帰納法」が正しいことは，次の定理から示せます。

**定理 (数学的帰納法の原理　その 2)**　自然数の集合 $A$ が次の二つの性質をもつとする。
(I) $A$ は 1 を含む。
(II) 自然数 $n$ が 1 より大きく，$1 \leqq k < n$ であるすべての整数 $k$ が $A$ に含まれるなら，$n$ も $A$ に含まれる。
このとき，$A$ は自然数全体の集合 $\mathbb{N}$ と一致する。

証明は先のものと同様ですから，書き下してみてください。

### 1.1.2　除法の原理の証明

それでは「除法の原理」を証明しましょう。

**定理 (除法の原理)**　$a,\ b$ を整数とする。このとき，　**除法の原理**

$$a = bq + r, \quad 0 \leqq r < b \quad \cdots\cdots (*)$$

を満たす整数 $q,\ r$ がただ一組だけ存在する。

**証明**　はじめに $(*)$ を満たす $q,\ r$ が存在することを示す。そのために $a$ に関する数学的帰納法を用いる。
(I)　$a=0$ なら，$q=0,\ r=0$ とすればよい。
(II)　$a$ より小さい自然数について $(*)$ を満たす $q,\ r$ が存在すると仮定する。
このとき $a<b$ なら $q=0,\ r=a$ とおけばよい。
$a \geqq b$ なら，$0 \leqq a-b < a$ なので，帰納法の仮定から

$$a - b = bq' + r', \quad 0 \leqq r' < b$$

を満たす整数 $q',\ r'$ が存在する。この式を書き直せば，

$$a = b(q'+1) + r', \quad 0 \leqq r' < b$$

よって $q = q'+1,\ r = r'$ とおけば $(*)$ が成り立つ。

(I), (II) からどんな整数 $a,\ b$ についても

$$a = bq + r, \quad 0 \leqq r < b \ \cdots\cdots (*)$$

を満たす整数 $q,\ r$ が存在する。

次に $(*)$ を満たす $q,\ r$ がもう一組あったとし，それを $q_1,\ r_1$ とする。つまり

$$\begin{aligned} a &= bq + r, & 0 \leqq r < b \\ a &= bq_1 + r_1, & 0 \leqq r_1 < b \end{aligned}$$

とする。このとき

$$bq + r = bq_1 + r_1 \quad \cdots\cdots (**)$$

$q \neq q_1$ とする。もし $q_1 > q$ ならば，$r_1$ と $bq$ を移項して整理すれば，

$$b(q_1 - q) = r - r_1$$

ここで $q_1 - q \geqq 1$ なので $b(q_1 - q) \geqq b$。一方 $r - r_1 < b$。これは矛盾。

$q_1 < q$ のときも同様。よって $q = q_1$。

これを $(**)$ に代入すれば $r = r_1$ を得る。

よって $(*)$ を満たす $q,\ r$ はただ一組である。 **(証明終)**

## 1.2 素数が無限個存在すること

8 ページで次の定理を紹介しました。本節では，この定理の証明を与えておきます。

**定理 (素数の個数)** 素数は無数に存在する。

**証明** 背理法を用いる。

素数が有限個しかないとし，そのうちの最大のものを $p$ とする。そして，$p$ 以下のすべての素数の積に 1 を加えたものを $N$ とする。つまり

$$N = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot p + 1$$

とおく。

$N > p$ なので，これは合成数。つまり素数で割り切れるはず。しかし，2 から $p$ までのどの素数で割っても，1 余る。これは矛盾。 **(証明終)**

## 1.3　素因数分解の可能性，一意性

やはり 9 ページで次の定理を紹介しました。証明を与えておきます。

**定理 (素因数分解の可能性)**　**素因数分解の可能性**

どんな整数も素数の積として表すことができる。

**証明**　与えられた数が素数なら，議論する必要はない。その数自身を用いて素因数分解ができている。

与えられた数 $n$ が合成数だとする。$n$ は $n$ より小さい少なくとも一つの素数 $p_1$ を約数にもつ。つまり

$$n = p_1 \times n_1$$

と表すことができる。ここで $n_1$ が素数なら，$n$ は二つの素数 $p,\ n_1$ の積で表されたことになり，証明が終わる。

もし $n_1$ が合成数なら，同様にして $n_1$ より小さい素数 $p_2$ を用いて

$$n_1 = p_2 \times n_2 = p_1 \times p_2 \times n_2$$

と表される。この手続きを繰り返すと，

$$n > n_1 > n_2 > \cdots \geqq 1$$

という列が得られるが，これはどこかで必ず終わる。

よってどんな整数も素数の積として表すことができる。　**(証明終)**

次の定理も証明を与えておきます。

**定理 (素因数分解の一意性)**　**素因数分解の一意性**

素因数分解の結果は，分解していく順序によらない。

**証明**　$p_1,\ \cdots,\ p_r,\ q_1,\ \cdots,\ q_s$ を素数として，

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

と表されたとする。$q_1 q_2 \cdots q_s$ は $p_1$ で割り切れるので，$q_1,\ \cdots,\ q_s$ の中に $p_1$ で割り切れるもの $q_i$ がある。番号をつけ換えておいて，$q_1$ が $p_1$ で割り切れるとしてよい。しかし $q_1$ は素数であるから，$p_1 = q_1$。そこで

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

の両辺を $p_1 = q_1$ で割れば，

$$p_2 \cdots p_r = q_2 \cdots q_s$$

同様にして $q_2, \cdots, q_s$ の中に $p_2$ に等しいものがあり，$p_3 \cdots p_r = q_3 \cdots q_s$ を得る。

以下これを繰り返せば，$r \leqq s$ であり，(適当に番号をつけ換えておくことによって) $p_1 = q_1, \cdots, p_r = q_r$ となる。

次に $p_i$ と $q_j$ の役割を入れ換えて上と同じ議論をすれば $s \leqq r$。よって $r = s$。

以上で素因数分解の一意性が示せた。 **(証明終)**