§1. 除法の原理

「除法の原理」は、小学校以来よく計算してきた、整数を 0 でない別の整数で割って商と余りを求める操作を裏付ける原理である。ここでは、この原理の証明方法と最大公約数について深く学ぶ。

● 1 - 1 : 除法の原理

除法の原理が成り立つ背景には、自然数の整列性が隠されている。自然数の整列性については後の補足を参照のこと。

定理 1 - 1 - 1 (除法の原理)
任意の $a, b \in \mathbb{Z},\ b > 0$ に対して、次の条件を満たす整数 $q, r \in \mathbb{Z}$ が一意的に存在する。

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

(**証明**)

I. q, r の存在：集合

$$M = \{\ a - nb \mid n \in \mathbb{Z},\ a - nb \geq 0\ \}$$

を考える。$a - (-|a|)b \geq 0$ より、$M \neq \varnothing$ がわかる。よって、M に最小元 r が存在する (自然数の整列性)。$r = a - qb\ (q \in \mathbb{Z})$ と書く。この q と r が定理の条件を満たす 2 つの整数となる。実際にそうなっていることを示すには、$0 \leq r < b$ が満たされていることを確かめればよい。

$r \in M$ なので、$0 \leq r$ は満たされている。$r < b$ となることを証明する。背理法で示す。$r \geq b$ であると仮定する。すると、$0 \leq r - b = a - (q+1)b$ となる。これは M が r より真に小さい元 $r - b$ を含むことを意味し、r が M の最小元であることに反する。よって、$r < b$ でなければならない。

II. q, r の一意性：a が次のように 2 通りに表わされたとする。

$$a = qb + r = q'b + r', \qquad 0 \leq r, r' < b.$$

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

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

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、$|r' - r| = |q - q'|b \geq b$ を得る。一方、$0 \leq r, r' < b$ であるから、$|r - r'| < b$ 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。 □

● 1 - 2 : 約数と倍数

2 つの整数 $a\ (\neq 0),\ b$ に対して、$b = qa$ となる $q \in \mathbb{Z}$ が存在するとき、b は a の**倍数** (multiple) である、あるいは、a は b の**約数** (divisor) であると呼ばれる。このことを記号 $a|b$ で表わす。$a|b$ でないことを $a \nmid b$ で表わす。例えば、$2|4$ であり、$3 \nmid 4$ である。また、1 は任意の整数の約数であり、0 は任意の整数の倍数である。

整数 $a\ (\neq 0), b\ (\neq 0), c, d, m, n$ に対して次が成り立つ。

(i) $a|b,\ b|c\ \Rightarrow\ a|c.$

(ii) $a|b,\ b|a\ \Rightarrow\ a = \pm b.$

(iii) $a|c,\ b|d\ \Rightarrow\ ab|cd.$

(iv) $a|c,\ a|d\ \Rightarrow\ a|(mc + nd).$

自然数の整列性により、0 でない整数 b に対して、その約数は有限個しかない。

● 1 - 3 : 最大公約数

2 つの整数 $a\ (\neq 0),\ b$ に対して、$d|a,\ d|b$ を満たす整数 d を a, b の**公約数** (common divisor) という。a, b の正の公約数の中で最大のものを a, b の**最大公約数** (greatest common divisor) という。a, b の最大公約数を $\gcd(a, b)$ または単に、(a, b) で表わす。

定理 1 - 3 - 1
整数 $a, b\ \ (a \neq 0)$ の最大公約数は、$\mathbb{Z}$ の部分集合 $\{\ xa + yb \mid x, y \in \mathbb{Z}\ \}$ に属する正の整数の中の最小元として特徴づけられる。

(**証明**)

$I := \{\ xa + yb \mid x, y \in \mathbb{Z}\ \}$ とおく。$0 \neq \pm a \in I$ であるから、I は 0 でない正の整数を含む。したがって、I に属する最小の正の整数 d_0 が存在する（自然数の整列性)。この d_0 が a, b の最大公約数に一致することを示す。a, b の最大公約数を d とおくとき、$d \geq d_0$ かつ $d_0 \geq d$ となることを示せばよい。

(i) $d_0 \geq d$ の証明：$d|a,\ d|b$ より、任意の $x, y \in \mathbb{Z}$ に対して、$d|(xa + yb)$, すなわち、任意の $h \in I$ に対して $d|h$ となる。$d_0 \in I$ なので、特に、$d|d_0$ が成り立つ。これより、$d_0 \geq d$ を得る。

(ii) $d \geq d_0$ の証明：これを示すには、$d_0|a$ かつ $d_0|b$ であることを示せばよい。

$a = qd_0 + r\ (q, r \in \mathbb{Z},\ 0 \leq r < d_0)$ と書き表わすと、$d_0 \in I$ ゆえ、$d_0 = xa + yb\ (x, y \in \mathbb{Z})$ と表わされる。すると、

$$r = a - qd_0 = (1 - qx)a + (-qy)b\ \in\ I$$

となるので、d_0 の選び方から $r = 0$ とわかる。よって、$d_0|a$ である。同様にして、$d_0|b$ が示される。 □

演習 1-1　整数 $a, b\ (a \neq 0)$ の最大公約数は a, b の任意の公約数で割り切れることを示せ。

例 1 - 3 - 2　$3x + 5y\ (x, y \in \mathbb{Z})$ の形で表わされる整数全体からなる集合 $I = \{\ 3x + 5y \mid x, y \in \mathbb{Z}\ \}$ は、[定理 1 - 3 - 1] により $\gcd(3, 5) = 1$ の倍数全体からなる集合に等しい。したがって、$I = \{1 \cdot m \mid m \in \mathbb{Z}\ \} = \mathbb{Z}$ となる。

0 でない整数 a, b の最大公約数が 1 のとき、a, b は**互いに素** (relatively prime) であると呼ばれる。[定理 1 - 3 - 1] の系として直ちに次が得られる。

系 1 - 3 - 3
整数 $a, b\ \ (a \neq 0)$ の最大公約数を d とするとき、$ax + by = d$ を満たす $x, y \in \mathbb{Z}$ が存在する。特に、a, b が互いに素ならば、$ax + by = 1$ を満たす $x, y \in \mathbb{Z}$ が存在する。

上の系の応用として、次が得られる。

系 1 - 3 - 4
整数 $a, b, s, t\ (a \neq 0,\ b \neq 0)$ について、次が成り立つ。
(1) $a|st,\ \gcd(a, s) = 1 \quad \Rightarrow \quad a|t.$
(2) $a|s,\ b|s,\ \gcd(a, b) = 1 \quad \Rightarrow \quad ab|s.$

(**証明**)

(1) [系 1 - 3 - 2] により、$ax + sy = 1$ を満たす整数 x, y が存在する。この両辺に t を掛けて、$tax + tsy = t$ となる。仮定 $a|st$ により、$a|(tax + tsy)$ となるから、$a|t$ が示された。

(2) $a|s$ より、$s = aa'$ $(a' \in \mathbb{Z})$ と書くことができる。$b|a'$ を示せばよい。$\gcd(a, b) = 1$ なので、$ua + vb = 1$ となる $u, v \in \mathbb{Z}$ が存在する ([系 1 - 3 - 2])。この両辺に a' を掛けると、$us + va'b = uaa' + vba' = a'$ となる。$b|s$ であるから、$b|(us + va'b)$ である。よって、$b|a'$ が示された。 □

演習 1-2 各 $a \in \mathbb{Z}$ に対して、a の倍数全体からなる集合を $a\mathbb{Z}$ で表わす：$a\mathbb{Z} = \{\, xa \mid x \in \mathbb{Z} \,\}$. $\mathbb{Z}$ の部分集合 I, J に対して $I + J$ を

$$I + J = \{\, i + j \mid i \in I,\ j \in J \,\}$$

によって定義する。すると、2 つの整数 a $(\neq 0)$, b の最大公約数とは、[定理 1 - 3 - 1](の証明) より、$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ となる正の整数 d のことであるといえる。では、$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ となる正の整数 m は何を表わしているか？

● 1 - 4 : 補足. 自然数の整列性と数学的帰納法

最初に、自然数の整列性について説明する。A を $\mathbb{R}$ の空でない部分集合とする。「すべての $a \in A$ に対して $a \geq m$」を満たす A に属する実数 m を A の**最小元** (minimal element) という。$\mathbb{R}$ の空でない部分集合に最小元がいつでも存在するわけではない。

例 1 - 4 - 1 (1) $\{-1, \sqrt{2}, 3\}$ や $\{0\} \cup \{\, x \in \mathbb{R} \mid x > 3 \,\}$ には最小元が存在する。これらの集合は、それぞれ、-1, 0 を最小元に持つ。

(2) $\{x \in \mathbb{R} \mid 2 < x \leq 4\}$ には最小元が存在しない。なぜならば、$2 < a \leq 4$ を満たすどのような実数 a に対しても、$a' := \frac{2+a}{2}$ を考えると、$2 < a' < a \leq 4$ が満たされるからである。 □

ところが、$\mathbb{N}$ の部分集合に限定すると次が成り立つ。

自然数の整列性

$\mathbb{N}$ の中の空でない任意の部分集合には最小元が存在する。すなわち、次が成り立つ。

$$\varnothing \neq M \subset \mathbb{N} \implies \exists\, m_0 \in M \ \text{ s.t. } \forall\, m \in M,\ m \geq m_0.$$

上と同様のことは $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ の部分集合については成り立たないので、整列性は $\mathbb{N}$ の持つ著しい特徴であるといえる。

演習 1-3 * $\mathbb{Z}$ の空でない部分集合であって、最小元をもたないものの例を 2 つ挙げよ。

数学的帰納法 (mathematical induction) の原理は $\mathbb{N}$ の持つ重要な性質の 1 つである。数学的帰納法の「偉大な」ところは、$P(1), P(2), P(3), \cdots\cdots$ のような無限個の命題が真であることを、わずか 2 ステップで証明できてしまうことにある。ここでは、$\mathbb{N}$ を

- 整列性を持つ ($\mathbb{R}$ の部分) 集合であって、
- 1 を最小元として持ち、
- 「$n \in \mathbb{N}$ ならば $n + 1 \in \mathbb{N}$」を満たすもの

と捉えて、帰納法の原理を導く。

定理 1 - 4 - 2 (**帰納法の原理**)
$\mathbb{N}$ 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「$\forall n \in \mathbb{N},\ P(n)$」は真である、すなわち、命題 $P(1), P(2), P(3), \cdots\cdots$ 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、$P(k)$ が成り立つと仮定すると、$P(k+1)$ も成り立つ。

(**証明**)

背理法で証明する。

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

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、$m-1 \notin M$ である。よって、$P(m-1)$ が成り立ち、したがって 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。 □

注意 1：定理の I, II をそれぞれ帰納法の第 1 段、第 2 段と呼ぶ。II における「$k \in \mathbb{N}$ について、$P(k)$ が成り立つと仮定する」の部分を**帰納法の仮定** (induction hypothesis) と呼ぶ。

注意 2：定理の証明は分かりにくかったかもしれないが、それが成り立つ理由はとても単純である。まず、I により $P(1)$ が成り立ち、次に、II において $k = 1$ の場合を考えると ($P(1)$ が成り立っているので) $P(2)$ が成り立つことがわかり、さらに II において $k = 2$ の場合を考えると ($P(2)$ が成り立っているので) $P(3)$ が成り立つことがわかり $\cdots\cdots$ というように、次々と「成り立つ」ことが連鎖していくわけである。

大学で学ぶ数学では、[定理 1 - 4 - 2] の基本型だけでなく、様々な形の帰納法が使われる。ここで紹介する累積的帰納法はそのうちの 1 つである。基本型の帰納法では、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 “力を借りた”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、$P(1), \cdots, P(n-1)$ のすべての力を借りて、$P(n)$ が成り立つこと示す、というのが累積的帰納法である。

定理 1 - 4 - 3 (**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「$\forall n \in \mathbb{N},\ P(n)$」は真である、すなわち、命題 $P(1), P(2), P(3), \cdots\cdots$ 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。

上の定理は [定理 1 - 4 - 2] を用いて証明することができる（「$i \leq n$ を満たすすべての自然数 i について $P(i)$ である」という条件を $Q(n)$ とおき、それがすべての $n \in \mathbb{N}$ について真であることを示す)。累積的帰納法も数学的帰納法と呼ばれる。