

# 代数学

## 1 整数の性質

### 1.1 基礎

整数全体の集合  $\mathbb{Z}$  には加法、乗法という演算が定義されている。 $\mathbb{Z}$  上の加法と乗法は以下の性質を満たす。

- 任意の  $a, b, c \in \mathbb{Z}$  に対して

$$(a + b) + c = a + (b + c)$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

が成立する

- 任意の  $a, b \in \mathbb{Z}$  に対して

$$a + b = b + a$$

$$a \cdot b = b \cdot a$$

が成立する

- 任意の  $a, b, c \in \mathbb{Z}$  に対して

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

が成立する

- 加法と乗法にはそれぞれ単位元  $0 \in \mathbb{Z}$  と  $1 \in \mathbb{Z}$  が存在する
- 任意の  $x \in \mathbb{Z}$  に対して加法に関する逆元  $-x \in \mathbb{Z}$  が存在する

このような構造を代数的構造 ( $\mathbb{Z}$  は環という構造) という。

さらに  $\mathbb{Z}$  は以下のような性質を満たす。

- 任意の  $a, b \in \mathbb{Z}$  に対して以下の 3 つのうちいずれか 1 つのみが成立する
  - $a > b$

- $a < b$
- $a = b$
- 任意の  $a, b, c \in \mathbb{Z}$  に対して  $a < b$  かつ  $b < c$  ならば  $a < c$  である
- 任意の  $a, b, c \in \mathbb{Z}$  に対して  $a < b$  ならば  $a + c < b + c$  である

このような構造を順序構造という。

**命題 1**  $a, b, c \in \mathbb{Z}$  のとき、 $ac = bc$  かつ  $c \neq 0$  ならば  $a = b$  である

**証明 1** まず  $ac = bc$  の両辺に  $bc$  の加法逆元  $-bc$  を加える。すると

$$\begin{aligned} ac - bc &= bc - bc \\ \Rightarrow ac - bc &= 0 \end{aligned}$$

となり、分配法則から

$$ac - bc = (a - b)c$$

であるため

$$\begin{aligned} ac - bc &= 0 \\ \Rightarrow (a - b)c &= 0 \end{aligned} \tag{1.1}$$

となる。式 (1.1) より  $a - b = 0$  もしくは  $c = 0$  のどちらか一方が成立する。しかし、仮定より  $c \neq 0$  であるため

$$a - b = 0$$

が成立する。両辺に  $b$  を加えると

$$\begin{aligned} a - b + b &= 0 + b \\ \Rightarrow a + b - b &= b \\ \Rightarrow a + 0 &= b \\ \Rightarrow a &= b \end{aligned}$$

となり、示された。

**命題 2**  $a \in \mathbb{Z}$  のとき  $0 \cdot a = 0$  である。

**証明 2** 零元の性質から  $0 = 0 + 0$  であるため

$$0 \cdot a = (0 + 0) \cdot a$$

であり、分配法則より

$$\begin{aligned} 0 \cdot a &= (0 + 0) \cdot a \\ &= 0 \cdot a + 0 \cdot a \end{aligned}$$

となる。ここで両辺に  $0 \cdot a$  の加法逆元  $-(0 \cdot a)$  を加えると、

$$\begin{aligned} 0 \cdot a &= 0 \cdot a + 0 \cdot a \\ 0 \cdot a - (0 \cdot a) &= 0 \cdot a + 0 \cdot a - (0 \cdot a) \\ 0 &= 0 \cdot a + 0 \end{aligned}$$

となり示された。

このように様々な命題は代数的構造の定義から証明できる。しかし、手間がかかるため以降簡単なものは認めて議論を行う。

**定理 1** 除法の定理

$a \in \mathbb{Z}, a \geq 0, b \in \mathbb{N}$  とする。このとき次を満たす  $q, r \in \mathbb{Z}$  の組が唯一つ定まる。

$$a = b \cdot q + r \quad (a \leq r < b)$$

このとき  $q$  のことを  $a$  を  $b$  で割った商、 $r$  のことを剰余と言う。

この定理は整数をグループ分けしているとも言える。

この定理は  $(q, r) \in \mathbb{Z}^2$  存在性と一意性の 2 つを主張している。除法の定理の証明には数学的帰納法を用いる。

自然数の性質 (数学的帰納法の原理)

**第 1 形式**  $S \subset \mathbb{N}$  のとき、 $1 \in S$  であり任意の  $a \in S$  に対して  $a \in S \Rightarrow a + 1 \in S$  が成立するならば  $S = \mathbb{N}$  である

**第 2 形式**  $S \subset \mathbb{N}$  のとき、 $1 \in S$  でありある  $a \in S$  に対して  $1, 2, \dots, a \in S \Rightarrow a + 1 \in S$  が成立するならば  $S = \mathbb{N}$  である

この自然数の性質を用いて数学的帰納法の正当性を示す。

定理 2 各自然数ごとの命題  $P(n)$  について

1.  $P(1)$  が真である
2. ある  $a \in \mathbb{N}$  に対して、 $P(a)$  が真ならば  $P(a+1)$  も真である

の双方が真であるならば、任意の  $m \in \mathbb{N}$  に対して  $P(m)$  が真である。

証明 3  $S := \{n \in \mathbb{N} \mid P(n)\}$  とし、item 1, item 2 とともに成立するとする。ここで item 1 から  $1 \in S$  であり、item 2 から任意の  $a \in \mathbb{N}$  に対して  $a \in S$  ならば  $a+1 \in S$  である。したがって自然数の性質より

$$S = \mathbb{N} \text{ であり}$$

$S$  の定義から任意の  $n \in S$  に対して  $P(n)$  が真となるため、任意の  $n \in \mathbb{N}$  に対しても  $P(n)$  が真となる。

定理 1 を数学的帰納法を用いて証明する。

証明 4 まず存在証明を行う。

1.  $0 \leq a < b$  のとき  $= 0, r = a$  とすれば

$$a = b \cdot q + r \Rightarrow a = r$$

となり、存在することが示された。

2.  $a \geq b$  とし、 $0 \leq k \leq a-1$  に対して  $q, r$  が存在すると仮定する。このとき  $a \geq b, b > 0$  であることから

$$0 \leq a - b \leq a - 1$$

が成立する。よって仮定より

$$a - b = b \cdot q' + r'$$

を満たす  $q', r'$  が存在する。この式を変形すると

$$\begin{aligned} a - b &= b \cdot q' + r' \\ \Rightarrow a &= b \cdot q' + b + r' \\ \Rightarrow a &= b \cdot (q' + 1) + r' \end{aligned}$$

となり、 $q = q' + 1, r = r'$  としたときに

$$a = b \cdot q + r$$

が成立する。このとき  $q, r$  ともに自然数であるため、存在することが示された。

以上より、定理 2 から任意の  $a \in \{x \in \mathbb{Z} \mid 0 \leq x\}, b \in \mathbb{N}$  に対して

$$a = b \cdot q + r \quad (a \leq r < b)$$

を満たす  $q, r$  が存在する。

次に  $q, r$  の一意性を示す。ある  $a, q_1, q_2 \in \{x \in \mathbb{Z} \mid 0 \leq x\}, b \in \mathbb{N}, r_1, r_2 \in \{x \in \mathbb{Z} \mid 0 \leq x < b\}$  に対して

$$a = b \cdot q_1 + r_1, \quad a = b \cdot q_2 + r_2$$

が成立するとする。ここで  $q_1 \geq q_2 + 1$  とすると

$$\begin{aligned} b \cdot q_1 + r_1 &\geq b \cdot q_1 \geq b \cdot (q_2 + 1) \\ &\Rightarrow b \cdot q_1 + r_1 \geq b \cdot q_1 \geq b \cdot q_2 + b \\ &\Rightarrow b \cdot q_1 + r_1 \geq b \cdot q_2 + b \end{aligned}$$

となり

$$b \cdot q_2 + b > b \cdot q_2 + r_2$$

であるため

$$\begin{aligned} b \cdot q_1 + r_1 &\geq b \cdot q_2 + b > b \cdot q_2 + r_2 \\ &\Rightarrow b \cdot q_1 + r_1 > b \cdot q_2 + r_2 \end{aligned}$$

が成立する。仮定より

$$b \cdot q_1 + r_1 > b \cdot q_2 + r_2 \Rightarrow a > a$$

であり矛盾するため  $q_1 < q_2 + 1$  である。  $q_1 + 1 > q_2$  とすると

$$\begin{aligned} b \cdot q_1 + r_1 &< b \cdot q_1 + b \\ &\Rightarrow b \cdot q_1 + r_1 < b \cdot (q_1 + 1) \end{aligned}$$

となり

$$b \cdot (q_1 + 1) \leq b \cdot q_2 \leq b \cdot q_2 + r_2$$

であるため

$$\begin{aligned} b \cdot q_1 + r_1 &< b \cdot (q_1 + 1) \leq b \cdot q_2 \leq b \cdot q_2 + r_2 \\ &\Rightarrow b \cdot q_1 + r_1 < b \cdot q_2 + r_2 \end{aligned}$$

が成立する。仮定より

$$b \cdot q_1 + r_1 < b \cdot q_2 + r_2 \Rightarrow a < a$$

であり矛盾するため  $q_1 + 1 > q_2$  である。

以上より  $q_1, q_2$  に対して

$$q_1 < q_2 + 1, \quad q_1 + 1 > q_2$$

が成立しなければならないため  $q_1 = q_2$  となる。さらに  $r_1 = a - b \cdot q_1, r_2 = a - b \cdot q_2$  なので  $r_1 = r_2$  となり一意性が示された。

よって定理 1 が正しいことが示された。

**定理 3** 除法の定理の拡張

$a \in \mathbb{Z}, a \geq 0, b \in \mathbb{Z} - \{0\}$  とする。このとき

$$a = b \cdot q + r \quad (a \leq r < |b|)$$

を満たす  $q, r \in \mathbb{Z}$  の組が唯一つ定まる。

定理 3 を示す。

**証明 5**  $b$  が 0 より大きい場合については定理 1 によって示されているため、 $b < 0$  の場合について示せばよい。

$b < 0$  の場合も定理 1 と同様に数学的帰納法によって示すことができる。

## 1.2 約数

**定義 1**  $a, b \in \mathbb{Z}$  とする。このとき

$$a \text{ は } b \text{ で割り切れる} :\Leftrightarrow \exists q \in \mathbb{Z} . t . a = bq$$

と定義する。そして  $a$  が  $b$  で割り切れることを  $b \mid a$  と書く。

**命題 3**  $a, b, c \in \mathbb{Z}$  としたとき以下の 3 つが成立する。

1.  $b \mid a \wedge b \mid c$  ならば  $b \mid (a + c)$
2.  $b \mid a$  ならば  $\forall x \in \mathbb{Z} . t . b \mid ax$
3.  $c \mid b \wedge b \mid a$  ならば  $c \mid a$