イデアル

有理整数環 $\mathbb{Z}$ において，a の倍数全体の集合は，

$$\mathbb{Z}a = \{ra | r \in \mathbb{Z}\}$$

と表される．$\mathbb{Z}$ の部分集合 $\mathbb{Z}a$ を I と書くと，I は次の性質を満たす．

$$b, c \in I \Longrightarrow b + c \in I$$
$$m \in \mathbb{Z}, b \in I \Longrightarrow mb \in I$$

定義 1　整数環 $\mathbb{Z}$ の部分集合 I が以下の条件を満たすとき，I を $\mathbb{Z}$ の**イデアル**という．

1. $m, n \in I$ であれば $m + n \in I$
2. $m \in I$ と任意の整数 a に対して $am \in I$

整数 $m_1, m_2, m_3, \cdots, m_i$ が与えられたとき，$\mathbb{Z}$ の部分集合 $(m_1, m_2, m_3, \cdots, m_i)$ を

$$(m_1, m_2, m_3, \cdots, m_i) = \left\{ \sum_{j=1}^{l} a_j m_j \;\middle|\; a_j \in \mathbb{Z} (j = 1, 2, 3, \cdots, l) \right\}$$

と定めると，これは $\mathbb{Z}$ のイデアルであることが分かる．これを $m_1, m_2, m_3, \cdots, m_i$ から生成されるイデアルと呼ぶ．ただ 1 つの整数 m から生成されるイデアル (m) を特に**単項イデアル**という．

定理 1 整数環 $\mathbb{Z}$ のイデアル I は全て単項イデアルである

［証明］$I = \{0\}$ のときは $I = (0)$ である．

I が 0 と異なる元 m を含む場合，もし $m < 0$ ならばイデアルの定義より $-m \in I$ だから，I は必ず自然数を含む．その自然数の中で最小のものを a とする．a は I の元だから

$$(a) = \mathbb{Z}a \subset I$$

逆に I の任煮の元を n とすると，

$$n = aq + r (0 \leq r < a)$$

を満たす整数 q, r が存在する．$a \in I$ より，$aq \in I$．また $n \in I$ であるから $r = n - aq \in I$．I の元で，最小の自然数は a であるので，$0 < r < a$ となることは無い．よって $r = 0$.

$$\therefore n = aq \in (a)$$
$$\therefore I \subset (a)$$
$$\therefore I = (a)$$

［証明おわり］

定理 2 整数 $m_1, m_2, m_3, \cdots, m_i$ から生成されるイデアル $(m_1, m_2, m_3, \cdots, m_i)$ に対して，$m_1, m_2, m_3, \cdots, m_i$ の最大公約数[*1]を d とすると，

$$(m_1, m_2, m_3, \cdots, m_i) = (d)$$

[*1] この場合，m の中に 0 を含んでもかまわない．その場合最大公約数は $(0, m) = m$ と定義する．

が成り立つ.

［証明］前定理よりイデアルは全て単項イデアルであることがわかった．よってその単項イデアルがどのようなものであるか調べればよい.

$$(m_1, m_2, m_3, \cdots, m_l) = (d_1)$$

とすると，$(-d_1) = (d_1)$ であるので，$d_1 > 0$ と仮定してよい.

$$d_1 = a_1 m_1 + a_2 m_2 + a_3 m_3 + \cdots a_l m_l$$

と書ける．右辺の各項は d で割り切れるので，d_1 も d で割り切れる．また,

$$m_j = b_j d_1 + c_j (0 \leq c_j < d_1)$$

とおくと，$b_j d_1 \in I, m_j \in I$ より

$$c_j = m_j - b_j d_1 \in I$$

c_1 は d_1 より小さい自然数とはなりえないので，$c_j = 0$ つまり d_1 は $m_1, m_2, m_3, \cdots, m_l$ の公約数である．d の倍数でもあるので,

$$d = d_1$$

［証明おわり］

参考文献

[1] 上野健爾『代数入門 1』（岩波講座 現代数学への入門，1995 年）

[2] 山本芳彦『数論入門 1』（岩波講座 現代数学への入門，1996 年）