

2012年6月26日

体の定義

集合 A に2つの演算 $+$ (加法) と \times (乗法) が定義されていて、下記の性質が成り立つとき、 A は環であるという。

- (1) $\forall a, b, c \in A, (a + b) + c = a + (b + c)$ (結合法則)
- (2) $\forall a, b \in A, a + b = b + a$ (交換法則)
- (3) $\exists 0 \in A, \forall a \in A, a + 0 = a$ (零元の存在)
- (4) $\forall a \in A, \exists b \in A, a + b = 0$ (加法に関する逆元の存在)
- (5) $\forall a, b, c \in A, (a \times b) \times c = a \times (b \times c)$ (結合法則)
- (6) $\exists 1 \in A, \forall a \in A, a \times 1 = 1 \times a = a$ (単位元の存在)
- (7) $\forall a, b, c \in A, a \times (b + c) = (a \times b) + (a \times c), (b + c) \times a = (b \times a) + (c \times a)$ (分配法則)

さらに、環 A が次の条件を満たすとき、体という。

- (1) $\forall a, b \in A, a \times b = b \times a$ (乗法に関する交換法則)
- (2) $\forall a \in A - \{0\}, \exists b \in A, a \times b = 1$ (乗法に関する逆元の存在)

例えば、 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ は体である。 \mathbb{Z} は体ではない。 p を素数とすると、 $\mathbb{Z}/p\mathbb{Z}$ は体であることがわかる。そのためには次に述べるユークリッドの互除法が必要である。

K を体、 $K[x]$ を多項式環という。定数ではない多項式 $f(x) \in K[x]$ が既約とは、 $f(x)$ が定数でない多項式2つの積として表せないときをいう。特に、1次式は既約である。

ユークリッドの互除法

以下 $A = \mathbb{Z}$ または $A = K[x]$ (ただし K は体) とする。

- $A = \mathbb{Z}$ のとき、 $a \in A, b \in A, b > 0$ とすると、 a を b で割った商と余りを求めることができる。すなわち、 $a = bq + r, 0 \leq r < b$ となる $q, r \in A$ がただひとつ定まる。
- $A = K[x]$ のとき、 $a(x) \in A, b(x) \in A, b(x) \neq 0$ とすると、 $a(x)$ を $b(x)$ で割った商と余りを求めることができる。すなわち、 $a(x) = b(x)q(x) + r(x), 0 \leq \deg r(x) < \deg b(x)$ または $r(x) = 0$ となる $q(x), r(x) \in A$ がただひとつ定まる。

以後、 $a(x), b(x)$ の代わりに、 a, b と書く。 $A = \mathbb{Z}, A = K[x]$ いずれの場合にも、 $r = 0$ となるとき、 $b|a$ と書き、 a は b で割り切れる、という。

$a, b \in A$ とし、 a と b の少なくとも一方は 0 でないとする。 a と b の最大公約数 (最大公約元) d とは、以下の条件を満たすものである。

(1) $d > 0$ ($A = \mathbb{Z}$ の場合), d は最高次の係数が 1 ($A = K[x]$ の場合)

(2) $(d|a) \wedge (d|b)$

(3) $\forall e \in A, ((e|a) \wedge (e|b)) \implies e|d$

a と b の最大公約元を $\gcd(a, b)$ と書く。

$a, b \in A$ とし、 a と b の少なくとも一方は 0 でないとする。今、 0 でない方を b として一般性を失わない。 $A = \mathbb{Z}$ の場合は $b' = |b|$, $A = K[x]$ のときは $b' = b$ とおく。 $r_0 = a, r_1 = b'$ とおき、 $k = 0, 1, \dots$ に対して、 r_k を r_{k+1} で割った商を q_{k+2} , 余りを r_{k+2} とおく。このとき

$$\begin{aligned} r_k > r_{k+1} & \quad (A = \mathbb{Z}) \\ \deg r_k > \deg r_{k+1} & \quad (A = K[x]) \end{aligned}$$

なので、 $\exists n, r_n \neq 0, r_{n+1} = 0$ となる。すると r_{n+2} 以降は定義できない。

このとき、

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}q_n \\ &= r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n \\ &= -r_{n-3}q_n + r_{n-2}(1 + q_{n-1}q_n) \\ &= \dots \\ &= m_0r_0 + m_1r_1 \\ &= m_0a + m_1b' \\ &= m_0a \pm m_1b. \end{aligned}$$

これより、

$$\gcd(a, b) = \begin{cases} r_n & (A = \mathbb{Z}), \\ r_n \text{ をその最高次の係数で割ったもの} & (A = K[x]) \end{cases}$$

であり、しかも $\exists s, t \in A, sa + tb = \gcd(a, b)$ となる。

特に、 $b = p$ を素数とし、 a を p の倍数ではない整数とすると、 $\mathbb{Z}/p\mathbb{Z}$ において $[a] \neq [0]$ である。上より $sa + tp = 1$ となる $s, t \in \mathbb{Z}$ が存在するが、これは $[s][a] = [1]$ を意味している。よって $\mathbb{Z}/p\mathbb{Z}$ は体である。