

5 第5回

5.1 最大公約数

整数 a と b の両方を割り切る最大の整数を最大公約数と呼び、 (a, b) と書く。特に、 $(a, b) = 1$ のとき、 a と b を互いに素という。

5.2 ユークリッドの互除法

定理 10 2つの整数 $\forall a > 0, b > 0 (a \geq b)$ が与えられたとき、 $a_0 = a, a_1 = b$ とおき、 $n = 1, 2, \dots$ に対して $a_n > 0$ である限り

$$a_{n-1} = a_n q_n + a_{n+1}, \quad 0 \leq a_{n+1} < a_n$$

によって a_{n+1} を再帰的に定める。このとき、ある自然数 $N (\geq 1)$ が存在し、 $a_{N+1} = 0$ かつ $a_N = (a, b)$ である。

(例) $a = 14, b = 6$ とすると

$$\begin{aligned} a_0 &= 14, a_1 = 6 \\ 14 &= 2 \times 6 + 2 \quad \therefore a_2 = 2 \\ 6 &= 3 \times 2 + 0 \quad \therefore a_3 = 0 \\ \therefore (a, b) &= a_2 = 2 \end{aligned}$$

系 1 任意の整数 a, b に対し

$$(a, b) = xa + yb$$

となる整数 x, y の組が存在する。

(例) 33019 と 10947 の最大公約数

$$\begin{array}{r} 3 \\ 10947 \overline{) 33019} \\ \underline{32841} \\ 178 \end{array} \quad \begin{array}{r} 61 \\ 178 \overline{) 10947} \\ \underline{10680} \\ 267 \\ \underline{178} \\ 89 \end{array} \quad \begin{array}{r} 2 \\ 89 \overline{) 178} \\ \underline{178} \\ 0 \end{array}$$

$$\therefore (33019, 10947) = 89$$

またこのプロセスを行列で表すと

$$\begin{aligned} \begin{bmatrix} 10947 \\ 178 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix} \begin{bmatrix} 33019 \\ 10947 \end{bmatrix} \\ &\quad \uparrow \text{商} \\ \begin{bmatrix} 178 \\ 89 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & -61 \end{bmatrix} \begin{bmatrix} 10947 \\ 178 \end{bmatrix} \\ \begin{bmatrix} 89 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 178 \\ 89 \end{bmatrix} \end{aligned}$$

従って

$$\begin{aligned} \begin{bmatrix} 89 \\ 0 \end{bmatrix} &= \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 178 \\ 89 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -61 \end{bmatrix} \begin{bmatrix} 10947 \\ 178 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -61 \\ -2 & 123 \end{bmatrix} \begin{bmatrix} 10947 \\ 178 \end{bmatrix} \\ &= \begin{bmatrix} 1 & -61 \\ -2 & 123 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -3 \end{bmatrix} \begin{bmatrix} 33019 \\ 10947 \end{bmatrix} \\ &= \begin{bmatrix} -61 & 184 \\ 123 & -371 \end{bmatrix} \begin{bmatrix} 33019 \\ 10947 \end{bmatrix} \end{aligned}$$

となり、1行目から

$$89 = (-61) \times 33019 + 184 \times 10947$$

が分かる。

5.3 体 (Field)

[定義] 体 F は、次の3つの性質を満足する2つの2項演算、加法 $+$ および乗法 $\cdot$ をもつ集合である。

$F1$: F は加法に対して可換群である。

$F2$: $\forall a, b \in F$ ならば、 $a \cdot b = c \in F$ (閉包) また非零元は乗法のもとに可換群をなす。

$F3$: $\forall a, b, c \in F$ ならば

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

$$(b + c) \cdot a = b \cdot a + c \cdot a \text{ (分配則)}$$

換言すると、乗法に関して単位元 1 もち、すべての非零元が乗法に関し逆元をもつ可換環が体である。

(例 1) すべての実数 (あるいは有理数、複素数) の集合 R (あるいは Q, C) は通常の加法、乗法に関して体をなす。

(例 2) 整数の集合 Z は、 ± 1 以外の元が乗法に関する逆元をもたないので、通常の加法、乗法に関して 体でない。

[定義] 有限の q 個からなる体をガロア体、あるいは有限体といい、 $GF(q)$ あるいは F_q と書く。

ガロア体の位数 (元の数) q は必ず $q = p^m$ (p は素数、 $m = 1, 2, \dots$) でなければならない。(証明は後述)

(例 1) $\{0, 1\}$ 下記の演算について $GF(2)$ となる。

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

(例 2) $\{0, 1, 2\}$ は下記の演算について $GF(3)$ となる。

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

(例 3) $\{0, 1, 2, 3\}$ は下記の演算について $GF(2^2) = GF(4)$ となる。

+	0	1	2	3	·0	1	2	3
0	0	1	2	3	0	0	0	0
1	1	0	3	2	1	0	1	2
2	2	3	0	1	2	0	2	3
3	3	2	1	0	3	0	3	1

注意：単純に $\text{mod } 4$ をとった

+	0	1	2	3	·0	1	2	3
0	0	1	2	3	0	0	0	0
1	1	2	3	0	1	0	1	2
2	2	3	0	1	2	0	2	0
3	3	0	1	2	3	0	3	2

では 体 とならない。

[定義](部分体と拡大体) 体 F の部分集合 $S(\subset F)$ が体 F と同一演算のもとで体をなすとき、 S を F の部分体という。逆に F は S の拡大体という。

(例 4) $GF(2)$ は $GF(4)$ の部分体であるが、 $GF(3)$ の部分体ではない。また逆に $GF(4)$ は $GF(2)$ の拡大体である。

[定義](剰余類環 (residual class ring) あるいは商環 (quotient)) a を自然数とし、 $Z_a = \{0, 1, \dots, a-1\}$ に対し、加法と乗法を

$$b + c = R_a[b \oplus c] \quad \forall a, b \in Z_a$$

$$b \cdot c = R_a[b \odot c] \quad \forall a, b \in Z_a$$

で定義するとき、 Z_a を剰余類環あるいは商環という。(ただし $\oplus, \odot$ は通常の加法と乗法である)

定理 11 p が素数のとき、またそのときに限って剰余類環 Z_p は体である。

(証明) p を素数とする。 $b \in Z_p$ かつ $b \neq 0$ とするとき、 Z_p は可換環なので、 Z_p が体になるためには、 b の逆元の存在を示せば良い。

p は素数なので、 $(p, b) = 1$ であり、ユークリッド互除法から

$$1 = xa + yb$$

をみたす、ある整数の組 (x, y) が存在する。従って

$$\begin{aligned} 1 &= R_p[1] \\ &= R_p[xa + yb] \\ &= R_p[R_p[xp] + R_p[yb]] \\ &= R_p[yb] \\ &= R_p[R_p[y]R_p[b]] \\ &= R_p[R_p[y]b] \end{aligned}$$

が得られる。従って、 $R_p[y]$ は Z_p における乗法について、 b の逆元である。ゆえに、 Z_p に属する非零元が逆元を有するので、 Z_p は体をなす。

他方、 p が合成数で $p = m \cdot b$ と書けるとする。もし、 Z_p が体であるとすれば、 m は逆元 m^{-1} をもつ。従って

$$b = R_p[b] = R_p[m^{-1} \cdot m \cdot b] = R_p[m^{-1}] = 0$$

となり、これは b が R で割り切れることを意味する。ここで、 $b \in \{0, 1, \dots, p-1\}$ なので、 $b = 0$ となり、これは仮定 $p > 0$ に矛盾する。従って、背理法により、 Z_p は体でないことが分かる。

(例) $Z_5 = \{0, 1, 2, 3, 4\}$ は

演算 $b + c = R_5[b + c] \quad \forall b, c \in Z_5$

$$b \cdot c = R_5[b \cdot c] \quad \forall b, c \in Z_5$$

のもとで $GF(5)$ となる。