

3 第3回

3.1 部分群

ある群 G の部分集合 H が群をなすとき、 H を部分群という。 H が群の部分群であることを証明するには、 H が群の性質 $G1$ と $G2$ を満足することのみを示せば良い。

(例) e を G の単位元とすると、 $H = \{e\}$ は G の部分群である。明らかに、 $e \circ e = e$ から $G1$ と $G4$ を満足する。

3.2 巡回群

有限群 G の要素 h に対して

$$h, h \circ h = h^2, h \circ h \circ h = h^3, \dots$$

を作ると、必ず $h^n = e$ を満たす整数 n が存在する。なぜならば G は有限群だから必ず

$$h^j = h^i$$

となる i と $j (j > i)$ が存在する。このとき、右から $(h^{-1})^i$ を乗じると

$$\underbrace{h \circ \dots \circ h}_{j \text{ 個}} \circ \underbrace{h^{-1} \circ \dots \circ h^{-1}}_{i \text{ 個}} = \underbrace{h \circ \dots \circ h}_{i \text{ 個}} \circ \underbrace{h^{-1} \circ \dots \circ h^{-1}}_{i \text{ 個}}$$

すなわち

$$h^{j-i} = e$$

が得られるからである。

特に、 $h^n = e$ をみたす最小の n を h の位数 (order) と呼ぶ。また

$$H = \{h, h^2, h^3, \dots, h^n = e\}$$

は G の部分群であり、 h によって生成される巡回群 (cyclic group) と呼ぶ。

H が群をなすことは、次のようにして分かる。

$$\begin{aligned} G1 \quad h^i \circ h^j &= h^{i+j} \\ &= \begin{cases} h^{i+j} \in H & (i+j \leq n) \\ h^{i+j-n} \in H & (i+j > n) \end{cases} \end{aligned}$$

$$G3 \quad h^n = e \in H$$

$$G4 \quad h^i \text{ の逆元は } h^{n-i} \text{ である。なぜなら}$$

$$h^i \circ h^{n-i} = h^n = e$$

(例) $G = \{1, 2, 3, 4, 5, 6\}$

演算 : $x \circ y = xy \pmod{7}$ で定める。

- $h = 2$ とすると

$$h^2 = 2 \times 2 = 4$$

$$h^3 = 2 \times 2 \times 2 = 8 = 1 \pmod{7}$$

従って、 $h = 2$ によって生成される巡回群 $H = \{2, 4, 1\}$

- $h = 4$ とすると

$$h^2 = 4 \times 4 = 2$$

$$h^3 = 4 \times 2 = 1 \pmod{7}$$

$h = 4$ によって生成される巡回群 $H = \{4, 2, 1\}$

- $h = 6$ とすると

$$h^2 = 6 \times 6 = 1 \pmod{7}$$

$h = 6$ によって生成される巡回群 $H = \{6, 1\}$

- $h = 3$ とすると

$$h^2 = 3 \times 3 = 2 \pmod{7}$$

$$h^3 = 2 \times 3 = 6$$

$$h^4 = 6 \times 3 = 4 \pmod{7}$$

$$h^5 = 4 \times 3 = 5 \pmod{7}$$

$$h^6 = 5 \times 3 = 1 \pmod{7}$$

$h = 3$ によって生成される巡回群 $H = \{3, 2, 6, 4, 5, 1\} = G$

3.3 部分群による類別

G : 群

$H = \{h_1 = e, h_2, h_3, \dots, h_n\} : G$ の部分群

$\forall x \in G$ に対し

$$xH = \{x \circ h_1, x \circ h_2, x \circ h_3, \dots, x \circ h_n\}$$

とする。このとき、次の性質が成り立つ。

1. xH の要素は全て異なる。

もしそうでないとすると、ある $i \neq j$ について

$$x \circ h_i = x \circ h_j$$

左から x^{-1} を乗じると

$$h_i = h_j$$

となり、これは仮定 $h_i \neq h_j (i \neq j)$ に矛盾する。

2. $y \notin xH$ ならば $yH \cap xH = \emptyset$

yH と xH は共通元をもたない。

もしそうでないとすると、ある i, j について

$$\begin{array}{ccc} y \circ h_i & = & x \circ h_j \\ \cap & & \cap \\ yH & & xH \end{array}$$

が成り立つ。右から h_i^{-1} を乗じると $(y \circ h_i) \circ h_i^{-1} = (x \circ h_j) \circ h_i^{-1}$

$$y = x \circ (h_j \circ h_i^{-1})$$

ここで、 H は部分群なので、ある $h_h \in H$ が存在して

$$h_h = h_j \circ h_i^{-1}$$

が成り立つ。従って、 $y = x \circ h_h \in xH$ となり、これは $y \notin xH$ に矛盾する。

さて、以上の結果のもとに次のような群 G の類別を考えよう。

H	コセットリーダー $h_1 = e$	h_2	h_3	$\cdots$	h_n	
g_2H	$g_2 \circ h_1 = g_2$	$g_2 \circ h_2$	$g_2 \circ h_3$	$\cdots$	$g_2 \circ h_n$	
g_3H	$g_3 \circ h_1 = g_3$	$g_3 \circ h_2$	$g_3 \circ h_3$	$\cdots$	$g_3 \circ h_n$	コセット
$\vdots$						
g_mH	$g_m \circ h_1 = g_m$	$g_m \circ h_2$	$g_m \circ h_3$	$\cdots$	$g_m \circ h_n$	

(a) 全ての G の元は、この表に出現する。(もし、そうでないならば、出現していない g を g_{m+1} としてこの操作を繰り返せば良い)

(b) この表に G の元は唯一回ずつ出現する。

これらのことは性質 (1) と (2) から容易に導かれる。

このような類別を H による (左) 類別とよび、各類 g_iH のことを (左) コセットあるいは (左) 剰余類と呼ぶ。また、一番左側の要素 g_i のことをコセットリーダーと呼ぶ。

(例) 先ほどの群 $G = \{1, 2, \dots, 6\}$ を再び考えよう。

$H = \{2, 4, 1\}$ とするとき、 H による左類別は、たとえば

H	1	2	4
$3H$	3	6	5

となる。この場合、コセットリーダーは 1 と 3 である。 $H = \{1, 6\}$ とするとき、 H による左類別は

H	1	6
$2H$	2	5
$3H$	3	4

となる。

このとき次の定理は明らかである。

定理 4 H が有限群 G の部分群であるならば、 H の位数は G の位数を割り切る。

(証明) 上の類別が m 行 n 列の表になることから明らか。 □

注意： G の位数の任意の約数の位数を持つ部分群が存在するか否かは G によって異なる。(群論の難しさ！)

3.4 環 (ring)

環 R は、次の 4 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。

$R1$ R は加法 $+$ に対して可換群である。

$R2$ $\forall a, b \in R$ ならば、 $a \cdot b \in R$ (閉包)

$R3$ $\forall a, b, c \in R$ ならば、
 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (結合則)

$R4$ $\forall a, b, c \in R$ ならば
 $a \cdot (b + c) = a \cdot b + a \cdot c$
 $(b + c) \cdot a = b \cdot a + c \cdot a$ (分配則)

特に、 $\forall a, b \in R$ に対し、 $a \cdot b = b \cdot a$ (可換則) が成り立つとき、可換環 (commutative ring) という。

定理 5 R の加法 $+$ に対する単位元を 0 で表し、 A の逆元を $-a$ によって表す。このとき、任意の $a, b \in R$ に対して

$$(1) \quad a \cdot 0 = 0 \cdot a = 0$$

$$(2) \quad a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$$

が成り立つ。

(証明)

$$(1) \quad a \cdot 0 \stackrel{R1}{=} a \cdot (0 + 0) \stackrel{R4}{=} a \cdot 0 + a \cdot 0$$

両端の式に $-(a \cdot 0)$ を加えると $0 = a \cdot 0$ を得る。 $0 = 0 \cdot a$ も同様。

$$(2) \quad 0 \stackrel{R1}{=} a \cdot 0 \stackrel{R1}{=} a \cdot (b + (-b)) \stackrel{R4}{=} a \cdot b + a \cdot (-b)$$

両端の式に $-(a \cdot b)$ を加えると $-(a \cdot b) = a \cdot (-b)$ を得る。 $(-a) \cdot b = -(a \cdot b)$ も同様。 □