02 部分群

ゼロから始める群論 2020

定義 (部分群)

群 G の部分集合 $H(\neq \varnothing)$ が G の演算によって群になるとき，H を G の**部分群**という*.

(例) (1) 整数全体の集合 $\mathbb{Z}$，有理数全体の集合 $\mathbb{Q}$，実数全体の集合 $\mathbb{R}$ は集合の包含関係

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$$

が成り立つ．演算として加法を考えているとき，上に登場する集合はすべて群になるが，小さい方の群は大きい方の群の部分群である．□

(2) 乗法群 $\mathbb{Q}^\times$ は乗法群 $\mathbb{R}^\times$ の部分群である．一方，乗法群 $\mathbb{Q}^\times$ は加法群 $\mathbb{Q}$ の部分群ではない (両者の二項演算が異なるため)．□

(3) 群 G について，群 G 自身，および単位元のみからなる集合 $\{e\}$ は G の部分群である．これらを G の自明な部分群という．□

(4) 2 元からなる集合 $\{1, -1\}$ は乗法群 $\mathbb{Q}^\times$ の部分群である．□

(5) 2 べきの集合 $\{2^n | n \in \mathbb{Z}\}$ は乗法群 $\mathbb{Q}^\times$ の部分群である．□

(6) 群 $\mathbb{Z}_4$ の演算表を再掲する．

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

この演算表からも分かるように，$\{\overline{0}, \overline{2}\}$ は $\mathbb{Z}_4$ の部分群である．□

定理 02

G を群，H をその部分群とする．

(1) H の単位元は G の単位元 e と一致する．

(2) $a \in H$ の H での逆元は，a の G での逆元 a^{-1} と一致する．

(証明のポイント) 前回の定理 01 と同様に，H の単位元 e' を用意し，その性質を考えて $e' = e$ を証明する．(2) も同様．

(証明)(1) H の単位元 e' の性質は

$$\forall a \in H, e'a = ae' = a \cdots ①$$

である．①で $a = e'$ として

$$e'e' = e' \cdots ①'$$

を得る．ここで e' の G での逆元 x，すなわち

$$e'x = xe' = e \cdots ②$$

を満たすような x を用意する．①′ に対して，左から x をかけると

$$x(e'e') = xe' \cdots ①''$$

となる．①″ の左辺は結合法則，x の性質②, 単位元 e の性質により

$$x(e'e') = (xe')e' = ee' = e'$$

一方①″ の右辺は x の性質①′ により $xe' = e$．ゆえに $e' = e$ が示せた．

(2) a の H での逆元を a' とすると，

$$aa' = a'a = e \cdots ③$$

③の $aa' = e$ の両辺に左から a の G での逆元 a^{-1} をかけて

$$a^{-1}(aa') = a^{-1}e \cdots ③'$$

③′ の左辺は結合法則および単位元 e の性質により

$$a^{-1}(aa') = (a^{-1}a)a' = ea' = a'$$

となり，③′ の右辺は単位元 e の性質により a^{-1} となる．ゆえに $a' = a^{-1}$ が示せた．□

群 G の元 a と自然数 n に対し，

$$a^n = \overbrace{a \cdot a \cdots \cdot a}^{n}, \quad a^{-n} = (a^{-1})^n, \quad a^0 = e$$

と定義する．このように定義すると，任意の整数 m, n に対し，

$$a^m a^n = a^{m+n}, (a^m)^n = a^{mn}, (a^n)^{-1} = (a^{-1})^n$$

が成立する (指数法則)．

群 G に属する元の個数を G の位数といい，$|G|$ で表す*．群 G の元 a に対し，

$$H = \{a^n | n \in \mathbb{Z}\}$$

は G の部分群になる．この H を a から生成される群といい，$H = <a>$ とかく．H の位数を

---

*H が G の部分群であることを記号で $H \leq G$ と表すことがある．

*集合の元の個数と同様の表記である．なお，G が無限に元をもつときは，$|G| = \infty$ とする．

a の位数といい，$\mathrm{ord}\, a$ とかく．$\mathrm{ord}\, a$ が有限のとき，位数は $a^n = e$ となるような最小の自然数 n のことを表す．G が 1 つの元 a で生成されるとき，すなわち $G =< a >$ となるとき，G を巡回群といい，a を G の生成元という．

(例)(7) 加法群 $\mathbb{Z}$ は 1 または -1 から生成される．すなわち，$\mathbb{Z} =< 1 >=< -1 >$．このように，一般に生成元は一意的でない． □

(8) 群 $\mathbb{Z}_6$ の各元 $\overline{0}, \overline{1}, \cdots, \overline{5}$ において，

$\overline{0}$ の位数は 1

$\overline{1}, \overline{5}$ の位数は 6

$\overline{2}, \overline{4}$ の位数は 3

$\overline{3}$ の位数は 2

である．特に，$\overline{1}, \overline{5}$ は $\mathbb{Z}_6$ の生成元である． □

〜演習問題〜

02-1 前回の演習 01-3 で証明した，

$(ab)^{-1} = b^{-1}a^{-1}$ および $(a^{-1})^{-1} = a$

を利用して，$(a^{-2})^{-3} = a^6$ を示せ．

02-2 次の問いに答えよ．

(1) 巡回群 $G =< a >$ の部分群 $H \neq \{e\}$ について，

$a^k \notin H (k = 1, 2, 3)$ かつ $a^4 \in H$

ならば a^5, a^{10}, a^{15} はいずれも H に属さないことを示せ．

(2) 巡回群 G の部分群 H は巡回群であることを示せ．

(02-1) $(a^{-2})^{-1} = (a^{-1} \cdot a^{-1})^{-1} = (a^{-1})^{-1} \cdot (a^{-1})^{-1} = a \cdot a = a^2$ により $(a^{-2})^{-3} = \{(a^{-2})^{-1}\}^3 = (a^2)^3 = a^6$

(02-2) (1) $a^5 \in H$ と仮定する．$a^4 \in H$ であるから $(a^4)^{-1} \in H$ であり，$a = (a^4)^{-1}a^5 \in H$ となり $a \notin H$ に反する．$a^{10} \in H$ と仮定すると $a^2 = (a^4)^{-2}a^{10} \in H$ から矛盾，また $a^{15} \in H$ を仮定すると $a^3 = (a^4)^{-3}a^{15} \in H$ から矛盾．(2) $G =< a >$ とする．$H = \{e\}$ なら $H =< e >$ で H は巡回群となる．そこで $H \neq \{e\}$ とする．H は巡回群 $G =< a >$ の部分群であるから，ある 0 でない整数 k が存在し，$a^k \in H$ となる．もし k が負であっても H は群であるから a^k の逆元が H に存在し $a^{-k} = (a^k)^{-1} \in H$ となる．すなわち $n := \min\{k | a^k \in H, k \in \mathbb{N}\}$ となる自然数 (正の整数)n が定まる．以下，$H =< a^n >$ を示す．H から任意の元 $a^m \in H$ をとる．m を n で割れば $m = nq + r, 0 \leqq r < n$ となる整数 q, r が存在する．$a^m = a^{nq}a^r$ を変形して $a^r = (a^n)^{-q}a^m$． $a^n, a^m \in H$ であるから $a^r \in H$ となる．ここで n の最小性から $r = 0$ となる．すなわち $a^m = (a^n)^q \in < a^n >$ を得る．a^m は H の任意の元であったから $H \subset < a^n >$ が示せたことになる．一方 $a^n \in H$ だから明らかに $H \supset < a^n >$．以上により $H =< a^n >$，すなわち H は巡回群である．