01 群の定義

ゼロから始める群論 2020

定義 (群)

集合 G $(\neq \emptyset)$ に対し，2 項演算「 $\cdot$ 」

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a \cdot b = c \end{array}$$

が与えられていて*, 次の 3 条件 (G1) – (G3) を満たすとき，G を**群**という．

(G1) $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (結合法則)

(G2) $\exists e \in G, \forall a \in G, e \cdot a = a \cdot e = a$ (単位元の存在)

(G3) $\forall a \in G, \exists x \in G, a \cdot x = x \cdot a = e$ (逆元の存在：なお，このような x が存在するとき，この x を a の逆元といい，a^{-1} と表す†)

2 項演算が与えられている集合 G が, 上記 (G1), (G2), (G3) を満たし，さらに次の (G4) も満たすときは G は**可換群** (または**アーベル群**) という．

(G4) $\forall a, b \in G, a \cdot b = b \cdot a$ (交換法則)

(例) (1) 演算として加法を考える．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 (0 が単位元の) 群である．正の整数 (自然数) 全体の集合 $\mathbb{N}$ は単位元をもたないから群にはならない．また，0 以上の整数全体の集合 $\mathbb{N}_{\geqq 0}$ は単位元をもつが，$a \neq 0$ に対する逆元が $\mathbb{N}_{\geqq 0}$ に存在しないので群にはならない． □

*演算子記号「$\cdot$」を省略して ab のようにかくこともある．また，2 項演算は単に演算ともいう．「集合 S に演算が与えられている」とは，どんな 2 元 $a, b \in S$ に対してもその演算結果 $a \cdot b$ が S の元としてただ一つ定まることを意味する．「集合 S に演算が与えられている」は「演算が集合 S で閉じている」ともいう．

†後に示すように，各元 $a \in G$ に対し逆元はただ一つ (つまり一意的に) 存在する．そこでこの一意的に定まる元を a^{-1} とかくのである．

(2) 演算として乗法を考える．$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ は 0 に対する逆元が存在しないため，群にはならない．$\mathbb{Q}$ から 0 を除いた集合 $\mathbb{Q}^{\times}$ および $\mathbb{R}$ から 0 を除いた集合 $\mathbb{R}^{\times}$ は，1 が単位元であり，またすべての元 a に対してその逆数 $\frac{1}{a}$ が逆元となるため群となる．$\mathbb{Z}$ から 0 を除いた集合 $\mathbb{Z} \backslash \{0\}$ は 1 以外の元に対する逆元が $\mathbb{Z} \backslash \{0\}$ に存在しないため群とはならない． □

どの演算に関して群であるかを明示するために，群 G と演算の記号を用いて $(G, \ \cdot\ )$ のような表現をすることがある．例えば加法群 $\mathbb{Q}$ は $(\mathbb{Q}, +)$，乗法群 $\mathbb{Q}^{\times}$ は $(\mathbb{Q}^{\times}, \times)$ のように表すことがある．

G が有限集合のとき，$G = \{a_1, \cdots, a_n\}$ と表し，元の間の演算結果を次のような表にすると便利なことがある．この表で x は $x = a_i \cdot a_j$ で定める．

$\cdot$	a_1	$\cdots$	a_j	$\cdots$	a_n
$\vdots$			$\vdots$		
a_i		$\cdots$	x		
$\vdots$					
a_n					

(例)(3) 集合 $\mathbb{Z}_n := \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \cdots \overline{n-1}\}$ に対し，演算 $+$ を

$\overline{i} + \overline{j} = \overline{(i + j \text{ を } n \text{ でわったときのあまり})}$

と定義する．$\mathbb{Z}_4$ に対しての結果は次のとおり．

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

$\mathbb{Z}_4$ は演算 $+$ に関して群となる (一般に，$\mathbb{Z}_n$ は演算 $+$ に関して群となる).

(例) (4) 集合 $\{1, 2, 3\}$ に対し，演算 $\times$ を

$i \times j = (ij \text{ を } 4 \text{ でわったときのあまり})$

と定義する．演算結果は次のとおりにまとめられる．

$\times$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

この集合は演算 $\times$ に関して群とはならない (演算「$\times$ 」に関して閉じていない).

定理 01

(1) 群 G に対し，その単位元 e は一意的に存在する.
(2) 群 G の任意の元 a に対し，その逆元 a^{-1} は一意的に存在する.

(証明のポイント) 単位元 e が「一意的に存在する」ことをいうためには，存在が保証されている e と，(e と別のものかもしれない)e と同じ性質を満たすような e' を用意したとき，$e = e'$ となることを示せばよい．逆元についても同様.
なお，証明の中で，演算記号「$\cdot$」は省略し，演算 $a \cdot b$ は単に ab とかくことにする.

(証明)(1) 単位元 e は次の性質をもっている.
$\forall x \in G, ex = xe = x \cdots$①
この性質を満たす (e と異なるかもしれない) ような e' が存在したとする；
$\forall x \in G, e'x = xe' = x \cdots$②
①，②は任意の元について成立するので，特に①で $x = e'$，②で $x = e$ として
$ee' = e'e = e' \cdots$①$'$
$e'e = ee' = e \cdots$②$'$
となる．①$'$ と②$'$ により $e' = e'e = e$ を得る.

(2) a の逆元 a^{-1} は次の性質をもっている.
$aa^{-1} = a^{-1}a = e \cdots$③
この性質を満たす (a^{-1} と異なるかもしれない) ような y が存在したとする；
$ay = ya = e \cdots$④
④の $ay = e$ に対して左から a^{-1} をかけて
$a^{-1}(ay) = a^{-1}e \cdots$④$'$
④$'$ 左辺は結合法則，a^{-1} の性質③，単位元の性質により
$a^-1(ay) = (a^{-1}a)y = ey = y$
となる．一方④$'$ 右辺は単位元の性質により $a^{-1}y = a^{-1}$ となる．すなわち，$y = a^{-1}$ を得る. □

～演習問題～

01-1 整数全体の集合 $\mathbb{Z}$ に次のように演算 $*$ を定める．この演算に関して $\mathbb{Z}$ は群となるか.
(1) $a * b = ab + 1$
(2) $a * b = 2ab$

01-2 集合 $G = \{1, 2, 3, 4\}$ に対し，演算 $a * b$ を
$a * b = \min\{a, b\}$
で定める．G は $*$ に関して群になるか*.

01-3 群 G の元 a, b に対し，次を示せ.
(1) $(ab)^{-1} = b^{-1}a^{-1}$
(2) $(a^{-1})^{-1} = a$

01-4 (飛ばしてもよい) 群の定義の (G2)，(G3) は次の (G2)$'$，(G3)$'$ に置き換えてもよいことを示せ．すなわち，結合法則 (G1) が成り立つ演算が与えられた集合 G が，次の (G2)$'$, (G3)$'$ を満たせば G は群になることを示せ.
(G2)$'$ $\exists e' \in G, \forall a \in G, a \cdot e' = a$
(右単位元の存在)
(G3)$'$ $\forall a \in G, \exists a' \in G, a \cdot a' = e'$
(右逆元の存在)

*$\min\{a, b\}$ は a, b のうち大きくない方を意味する.
(01-1)(1) 群にならない ((G1) が満たされない) (2) 群にはならない ((G2) が満たされない) (01-2) 群にならない ((G3) が満たされない) (01-3) (1) $(ab)(b^{-1}a^{-1})$ および $(b^{-1}a^{-1})(ab)$ を計算して e となることを示せばよい. (2) a^{-1} の定義から $aa^{-1} = a^{-1}a = e$ である．これと $(a^{-1})^{-1}$ の定義および逆元の一意性から $(a^{-1})^{-1} = a$ となる． (01-4) YouTube 上で公開されている「群の定義をそぎ落とす！」を参照