群（有限群）

Ver. 0.10

Chap. 1 群

§1 群の定義

<u>群</u>

集合Gが次をみたすときGを群という.

- 演算が定義されている

$$\begin{aligned} G \times G &\longrightarrow G \\ (x, y) &\longmapsto xy \end{aligned}$$

- この演算が次をみたす.

結合則

$$^\forall x, y, z \in G \quad (xy)z = x(yz)$$

単位元 (eと書く) がある.

$$^\forall x \in G \quad xe = ex = x$$

任意の元にその逆元 (xに対しx^{-1}と書く) がある.

$$^\forall x \in G \quad ^\exists x^{-1} \in G$$

$$xx^{-1} = x^{-1}x = e$$

演算はしばしば積とよばれる.

対称群 S_n

$X = \{1, 2, \cdots, n\}$ のいれかえを考える.

たとえば $n = 3$ として

$$\begin{matrix} 1, & 2, & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{matrix}$$

これを $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ と書く.

これらのすべてを集めたものを S_n と書く.

$n = 3$ の場合

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

S_3 には積がある.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

結合則をみたす.

$$\left(\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right)\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\left(\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right)$$

$$=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

同じ

単位元がある $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

逆元がある

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\rightsquigarrow\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}\rightsquigarrow\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

$$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

S_n は群.

これを対称群(n次対称群)という.

一般に群の演算は可換ではない.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

違う

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

演算がすべて可換な群を可換群

とかアーベル群という.

$\mathbb{Z}$ は $+$ に関してアーベル群

$x, y \in \mathbb{Z} \rightsquigarrow xy = x + y$

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto x + y \end{aligned}$$

xy

結合則 OK.

単位元 0

逆元 $x \rightsquigarrow -x$

アーベル群では演算の記号に $+$ を使うことが多い

群の位数

群Gの濃度をGの位数といい$\#G$と書く.

有限群のときは個数

$$\#S_3 = 6$$

$$\#S_n = n!$$

§2 部分群

部分群

Gの部分集合Hが e を含み Gの演算で群となるとき HをGの部分群という.

これは Hが次をみたすとき. ということもできる.

$$^{\forall}x, y \in H \Rightarrow xy \in H$$

$$^{\forall}x \in H \Rightarrow x^{-1} \in H$$

このとき $e \in H$ は

$x, x^{-1} \in H$ $xx^{-1} \in H$ から いえる.

例)

$$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \subset S_3$$

Prop.

$H \subset G$ が G の部分群

$\Leftrightarrow$ 「$x, y \in H \Rightarrow xy^{-1} \in H$」

(証)

$\Rightarrow$ は明らか

$\Leftarrow$

$x \in H$ に対して $xx^{-1} \in H$ だから $e \in H$

$^\forall y \in H$ に対して $e \in H$ だから $ey^{-1} = y^{-1} \in H$

$^\forall x, y \in H$ に対して $y^{-1} \in H$ だから

$$xy = x(y^{-1})^{-1} \in H$$

$\langle S \rangle$

群 G の元を任意に選んでそのすべてを S とする.

$$x = x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n} \in G$$

$$x_1, \ldots, x_n \in S$$

そのもの

$$m_1 \ldots m_n = 1, -1$$

逆元

となる x たちのすべてを集めると G の部分群になる.

これを $\langle S \rangle$ と書く.

生成元

$G = \langle S \rangle$ のとき G は S で生成される,

S は G の生成系などといい

S の元を G の生成元という.

例

$\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$ は S_n の生成系

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

他の選び方もある。 また、ムダがあってもよい。

巡回群

唯一つの元で生成される群. すなわち

$G = \langle g \rangle$ となる群を巡回群という.

$\langle \{g\} \rangle$

$$A_3 = \left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \right\}$$

交代群

A_3 は S_3 の部分群で巡回群

$$A_3 = \left\langle \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \right\rangle = \left\langle \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \right\rangle$$

$\left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \right\} \subset S_3$ も巡回群

元の位数

$x \in G$ $\quad x^n = e$ となるとき

n を x の位数という.

このような n がないとき x の位数は無限という.

§3 準同型写像

§4 剩余群