数学科リレー講座

3 日目 いろいろな群

目次

1 前回の復習

1.1 群とは・・・

集合 G が次の条件を満たすとき, G は**群**であるという.

(G1) G の任意の 2 つの元 a, b に対して, 演算 $\circ$ が定義されていて, $a \circ b$ もまた G の元となる.

(G2) **単位元**と呼ばれる元 e があり, すべての $a \in G$ に対して $a \circ e = e \circ a = a$ を満たす.

(G3) すべての $a \in G$ に対して $a \circ a' = a' \circ a = e$ となるような $a' \in G$ が存在する. この a' を x の**逆元**という.

(G4) (結合法則) すべての $a, b, c \in G$ に対し, $(a \circ b) \circ c = a \circ (b \circ c)$ が成り立つ.

群 G がさらに

(G5) すべての $a, b \in G$ に対して, 交換法則 $a \circ b = b \circ a$ を満たす.

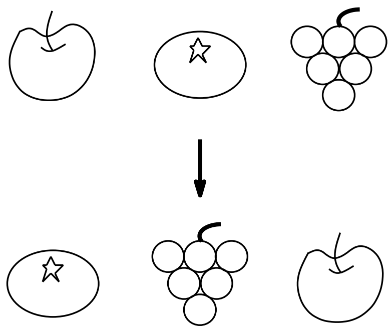
とき, G を**可換群** (または**アーベル群**) という.

群 G の元の個数 $|G|$ を G の**位数**という. 位数が有限な群のことを**有限群**, 位数が有限でない群のことを**無限群**という.

2　置換と対称群

2.1　置換

下図のように, 3 つ並んだ果物を置き換えることを考えてみよう.



問1　3 つの果物はそれぞれ何でしょう.

上図のような置き換えを

$$\begin{pmatrix} リ & ミ & ブ \\ ミ & ブ & リ \end{pmatrix}$$

と表すことにする. 上の行の横並びが初めの状態を表しており, 下の行の横並びが置き換えた後の状態を表している.

このような置き換えを**置換**という. 置換 $\begin{pmatrix} リ & ミ & ブ \\ ミ & ブ & リ \end{pmatrix}$ は, リンゴがあったところにミカンを置き, ミカンがあったところにブドウを置き, ブドウがあったところにリンゴを置くということを表している. 初めの状態を表す順序は関係がなく, 以下の 6 つの置換はすべて同じことを表している.

$$\begin{pmatrix} リ & ミ & ブ \\ ミ & ブ & リ \end{pmatrix}, \quad \begin{pmatrix} ミ & リ & ブ \\ ブ & ミ & リ \end{pmatrix}, \quad \begin{pmatrix} ブ & ミ & リ \\ リ & ブ & ミ \end{pmatrix}$$

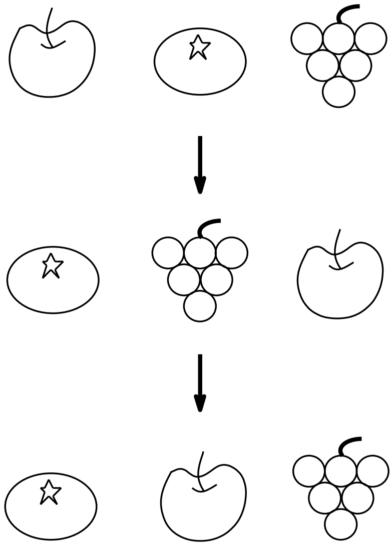
$$\begin{pmatrix} リ & ブ & ミ \\ ミ & リ & ブ \end{pmatrix}, \quad \begin{pmatrix} ミ & ブ & リ \\ ブ & リ & ミ \end{pmatrix}, \quad \begin{pmatrix} ブ & リ & ミ \\ リ & ミ & ブ \end{pmatrix}$$

問2 前のページの置換で異なるものは全部で何通りあるだろうか. すべて書き出してみよう.

リンゴ, ミカン, ブドウの置換全体からなる集合を S_3 と置く.

2.2 置換の積

今度は次のような置き換えを考えよう.



上図では, 1 回目の置換は $\begin{pmatrix} \text{リ} & \text{ミ} & \text{ブ} \\ \text{ミ} & \text{ブ} & \text{リ} \end{pmatrix}$ で, 2 回目の置換は $\begin{pmatrix} \text{ミ} & \text{ブ} & \text{リ} \\ \text{ミ} & \text{リ} & \text{ブ} \end{pmatrix}$ であり, 初めと 2 回置き換えた後に注目すると, 置換は $\begin{pmatrix} \text{リ} & \text{ミ} & \text{ブ} \\ \text{ミ} & \text{リ} & \text{ブ} \end{pmatrix}$ となっている. このとき, 置換 $\begin{pmatrix} \text{リ} & \text{ミ} & \text{ブ} \\ \text{ミ} & \text{リ} & \text{ブ} \end{pmatrix}$ を 1 回目の置換と 2 回目の置換の**積**といい,

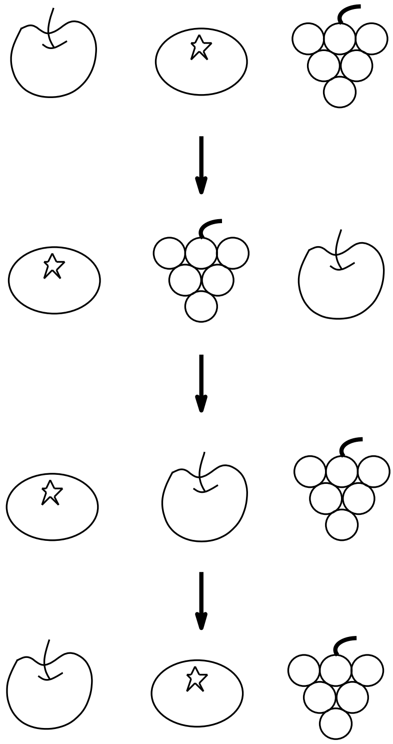
$$\begin{pmatrix} \text{ミ} & \text{ブ} & \text{リ} \\ \text{ミ} & \text{リ} & \text{ブ} \end{pmatrix} \circ \begin{pmatrix} \text{リ} & \text{ミ} & \text{ブ} \\ \text{ミ} & \text{ブ} & \text{リ} \end{pmatrix} = \begin{pmatrix} \text{リ} & \text{ミ} & \text{ブ} \\ \text{ミ} & \text{リ} & \text{ブ} \end{pmatrix} \qquad (\star)$$

と表す. ここで注意して欲しいのは, 普通の数の掛け算とは違い, 1 回目の置換を右に, 2 回目の置換を左に書くということである.

問3 次の置換の積はどのように置き換えられるか.

$$\begin{pmatrix} \text{リ} & \text{ミ} & \text{ブ} \\ \text{ミ} & \text{ブ} & \text{リ} \end{pmatrix} \circ \begin{pmatrix} \text{ブ} & \text{ミ} & \text{リ} \\ \text{リ} & \text{ブ} & \text{ミ} \end{pmatrix}$$

問4 前のページと同じように考えると, 下図の置換はどのように表されるだろうか. P.6 ($\star$) の形で表してみよう.



2.3　3 次対称群

今までは, リンゴ, ミカン, ブドウを用いてきたが, それぞれ, リンゴを 1, ミカンを 2, ブドウを 3 と数字にしてみよう.

そうすると, 初めの置換 $\begin{pmatrix} \text{リ} & \text{ミ} & \text{ブ} \\ \text{ミ} & \text{ブ} & \text{リ} \end{pmatrix}$ は $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ と書き直すことができる.

今後はリンゴ, ミカン, ブドウなどで果物の名前ではなくて, 1, 2, 3 などの数字で考えていくことにする.

P.5 **問 2** でみた S_3 を **3 次対称群**という.

もう少し丁寧に言うと, 集合 $G = \{1, 2, 3\}$ の置換全体からなる集合は群になる. この群を 3 次対称群という. 3 次対称群の元をすべて書き出すと以下のようになる.

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

一般に, 集合 $G = \{1, 2, 3, \cdots, n\}$ の置換全体からなる集合は群になる. この群を $\boldsymbol{n}$ **次対称群**という.

問 5 集合 S_3 に P.6 で定義した積を入れると, 群になることを確認してみよう.

問6 3 次対称群 S_3 は可換群か.

交換法則 $a \circ b = b \circ a$ は常に成り立つとは限らない.

問 7 2 次対称群 S_2, 4 次対称群 S_4 の元をそれぞれすべて書き出せ.

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$$

$$\begin{aligned} S_4 = \Bigg\{ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \\ & \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \Bigg\} \end{aligned}$$

た、大変・・・

問 8 S_n の位数はいくつだろうか.

今後, P.6 で定義した積 $\circ$ は省略する.

2.4 置換の略記法

置換には以下のような略記法がある.

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

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

のように略記する. 上記の書き方は, 1 が 2 に置き換わり, 2 が 1 に置き換わることを意味する. 変化しない 3 は書かない.

また, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ は

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

と略記する. これは, 1 が 2 に, 2 が 3 に, 3 が 1 に置き換わることを意味する.

問9 次の置換を略記せよ.

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

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

(3) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

(4)★ $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ などのように, 初めの状態から何も置き換わらない置換を**恒等置換**といい, e で表す.

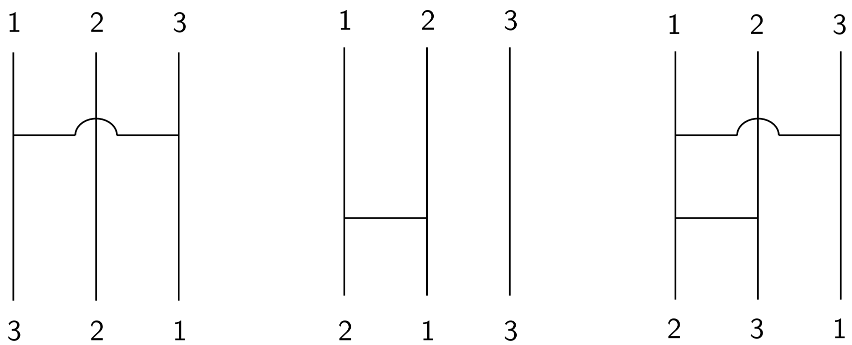
$(1\quad 2)$ のように, S_n の元で i と j が互いに移りあい他の数は変えない置換 $(i\quad j)$ を**互換**という.

$(1\quad 2\quad 3)$ などのように, S_n の元 $(i_1\quad i_2\quad \cdots\quad i_m)$ は

$$i_1 \to i_2 \to \cdots \to i_m \to i_1$$

と移し, 他の $1 \leqq j \leqq n$ は変えない置換である. このような置換を**巡回置換**という.

置換はよくあみだくじに例えられる. 下図は $(1\quad 2\quad 3) = (1\quad 3)(1\quad 2)$ となることを示している. ただし, 普通のあみだくじとは違って, 縦棒を飛び越えることができるようにしておく.



$(1\quad 3)$　　$(1\quad 2)$　　$(1\quad 2\quad 3)$

問10 $(1\quad 2\quad 3) = (1\quad 2)(2\quad 3)$ となることをあみだくじを用いて確かめてみよう.

$(1\quad 2\quad 3) = (1\quad 3)(1\quad 2) = (1\quad 2)(2\quad 3)$ のように, 任意の置換は互換の積で表すことができることが知られている．上図のあみだくじを考えると何となくイメージができるのではないだろうか．ただし, 一意的ではない.

しかし, 任意の置換について, それを互換の積に分解したときの個数が偶数であるか奇数であるかは一意に決まることがわかっている．このことから, S_n の元で奇数個の互換の積で表されるものを**奇置換**, 偶数個の互換の積で表されるものを**偶置換**という．また, 偶置換全体は群となる．これを $\boldsymbol{n}$ **次交代群**といい, $\boldsymbol{A_n}$ で表す.

例えば, 3 次交代群 A_3 とは, 3 次対称群 S_3 の元の中で偶置換全体の集合のことである.

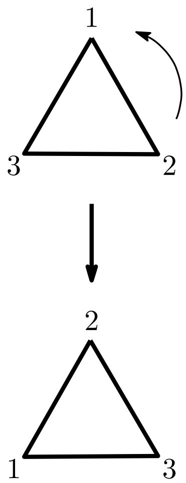
略記法を用いると, S_2, S_3, S_4, A_3, A_4 の元は次のように表すことができる.

$$
\begin{aligned}
S_2 &= \{e, (1\quad 2)\} \\
S_3 &= \{e, (1\quad 2), (1\quad 3), (2\quad 3), (1\quad 2\quad 3), (1\quad 3\quad 2)\} \\
S_4 &= \{e, (1\quad 2), (1\quad 3), (1\quad 4), (2\quad 3), (2\quad 4), (3\quad 4), \\
&\qquad (1\quad 2\quad 3), (1\quad 3\quad 2), (1\quad 2\quad 4), (1\quad 4\quad 2), \\
&\qquad (1\quad 3\quad 4), (1\quad 4\quad 3), (2\quad 3\quad 4), (2\quad 4\quad 3), \\
&\qquad (1\quad 2\quad 3\quad 4), (1\quad 2\quad 4\quad 3), (1\quad 3\quad 2\quad 4), \\
&\qquad (1\quad 3\quad 4\quad 2), (1\quad 4\quad 2\quad 3), (1\quad 4\quad 3\quad 2), \\
&\qquad (1\quad 2)(3\quad 4), (1\quad 3)(2\quad 4), (1\quad 4)(2\quad 3)\}
\end{aligned}
$$

$$
\begin{aligned}
A_3 &= \{e, (1\quad 2\quad 3), (1\quad 3\quad 2)\} \\
A_4 &= \{e, (1\quad 2\quad 3), (1\quad 3\quad 2), (1\quad 2\quad 4), (1\quad 4\quad 2), \\
&\qquad (1\quad 3\quad 4), (1\quad 4\quad 3), (2\quad 3\quad 4), (2\quad 4\quad 3), \\
&\qquad (1\quad 2)(3\quad 4), (1\quad 3)(2\quad 4), (1\quad 4)(2\quad 3)\}
\end{aligned}
$$

3　巡回群

今度は下図のような正三角形の回転を考える．頂点に 1, 2, 3 と番号をふり, 正三角形の重心を中心に, 反時計回りに 120° 回転させる.

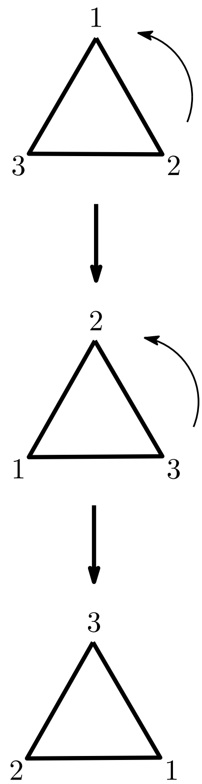


上図の場合, 頂点の番号がそれぞれ, 1 が 2 に, 2 が 3 に, 3 が 1 に置き換わっているので, 先ほどと同じように考えると

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

と表すことができる.

さらに, 反時計回りに 120° 回転させてみよう.



上図の場合は

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = \begin{pmatrix}1 & 3 & 2\end{pmatrix} \qquad (*)$$

と表すことができる. さらに, 反時計回りに 120° 回転させると

$$\begin{aligned}&\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\left\{\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\right\}\\ =&\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\\ =&\begin{pmatrix}1 & 2 & 3\\ 1 & 2 & 3\end{pmatrix} = e \qquad (**)\end{aligned}$$

として, 元に戻ってくる.

ここで, 反時計回りに 120° 回転させるという操作を a とおく. すなわち, $a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ \ 2\ \ 3)$ とおくと, P.17 (∗), (∗∗) は

$$a \circ a = a^2 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$$
$$a \circ (a \circ a) = a^3 = e$$

と表すことができる. ここでは, a を 3 回掛けることを a^3 で表している. 置換の積も結合法則を満たすので, 同じ置換同士の積では順番を考える必要がない. したがって, a や e は数ではなく置換なのだが, 数と同じような記号を用いることにする.

$a^3 = e$ は正三角形を 3 回回転させると元に戻ることを意味している.

問11 a を 4 回, 5 回, 6 回と掛けるとどうなるだろうか.

a を 4 回, 5 回, 6 回と掛けると

$$a^4 = a \circ a^3 = a \circ e = a$$
$$a^5 = a^2 \circ a^3 = a^2 \circ e = a^2$$
$$a^6 = a^3 \circ a^3 = a^3 \circ e = a^3 = e$$

となる. つまり 4 回回転させれば, 1 回回転させたところに戻り, 5 回回転させれば, 2 回回転させたところに戻り, 6 回回転させれば, 2 周して元に戻ることがわかる.

ここで e, a, a^2 に注目すると, **e, a, a^2 の 3 個のうち, どの 2 個の積も e, a, a^2 のどれかになっている**. これを表にすると, 次のようになる.

	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

このことを $\{e, a, a^2\}$ **は積について閉じている**という.

置換群 $\{e, a, a^2\}$ は, 積について閉じていて, すべての元が a の累乗になっている. このような群を**巡回群**という.

もう少し正確に言うと, 群 G の 1 つの元 a があって, $G = \{a^n \mid n \in \mathbb{Z}\}$ となるとき, G は**巡回群**であるといい, このような a を G の**生成元**という.

巡回群の生成元はただ一通りに決まるわけではない. 例えば, 整数の集合 $\mathbb{Z}$ は, 通常の加法に関して 1 を生成元とする巡回群である. また, -1 も生成元である.

$\{i, -1, -i, 1\}$ も通常の乗法に関して, i を生成元とする巡回群である. ただし, i は虚数単位と呼ばれるもので, $i^2 = -1$ である.

ちなみに, 巡回群は可換群である.

4 部分群

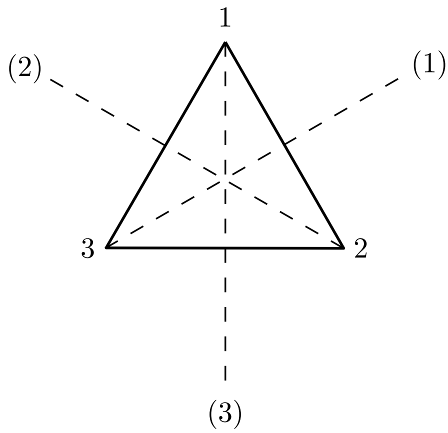
前のページの巡回群 $\left\{e, a, a^2\right\}$ は 3 次対称群 S_3 の一部であった．これを巡回群 $\left\{e, a, a^2\right\}$ は 3 次対称群 S_3 の**部分群**であるという．

すなわち, 群 G の空でない部分集合 H が G の演算によって群となるとき, H を G の**部分群**という．

例えば, 3 の倍数の集合 $3\mathbb{Z} = \{\,3n \mid n \in \mathbb{Z}\} = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$ は, 通常の加法に関して $\mathbb{Z}$ の部分群になっている．

5　正 2 面体群

問12　巡回群で出てきた正三角形の回転に加えて, 裏返しも考えてみよう. このとき, 回転と裏返しを合わせた置換全体の集合はどのように表されるだろうか.



平面上の正 n 角形を, 空間の中において, その形を変えずに裏返したり, 回転させたりしてできる集合は群をなす. この群を**正 2 面体群**といい, $\boldsymbol{D_n}$ で表す.

上の問いからわかるように, 3 次対称群 S_3 と正 2 面体群 D_3 は集合の構造が同じ (同型対応) である. このことを, S_3 と D_3 は**同型**であるという.

参考文献

[1] 志賀浩二, 群論への 30 講, 朝倉書店, 1989 年

[2] 中村亨, ガロアの群論-方程式はなぜ解けなかったのか-, 講談社, 2010 年

[3] 石田信, 代数学入門, 実教出版, 1978 年

[4] 金重明, 13 歳の娘に語るガロアの数学, 岩波書店, 2011 年

[5] 山口周, 大井武男, よくわかる線形代数学, 産業図書, 1993 年