代数学 I 第 5 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

4.1 群と部分群の例 (その 2)

前回に引き続き，群と部分群の例について解説する．ただし，今回の例はこれまでに学んだものではなく，多くの方にとって群論の講義ではじめて目にするものではないかと思われる (n 次対称群は見たことがあるかもしれない)．既習の概念を新しい視点 (『群』) からとらえることも面白いが，新しい視点をもつことで初めて数学的に扱える対象を知るということもまた面白いものである．

例 1. X を空でない集合とする．このとき，X から X への全単射写像全体のなす集合

$$B(X) \coloneqq \{f\colon X \to X \mid f \text{ は全単射 }\}^{*1}$$

を考える．このとき，$B(X)$ は写像の合成 $\circ$ を二項演算として，群をなす．

復習

写像 $f\colon X \to Y$ が**全単射**であるとは，

(全射性) 任意の $y \in Y$ に対し，ある $x \in X$ が存在して，$f(x) = y$ となり，かつ
(単射性) 任意の $x_1 \neq x_2$ なる $x_1, x_2 \in X$ に対して，$f(x_1) \neq f(x_2)$ となる

ということである．このとき，各 $y \in Y$ に対し，$f(x_y) = y$ となる $x_y \in X$ が必ずただ 1 つだけ存在するので，y に対してこの x_y を対応させることで，写像 $Y \to X, y \mapsto x_y$ が得られる．これを f の**逆写像**といい，f^{-1} と書く．
写像 $f\colon X \to Y, g\colon Y \to Z$ に対し，写像の合成 $g \circ f\colon X \to Z$ とは，

$$(g \circ f)(x) = g(f(x)),\ x \in X$$

で定まる写像である．$f\colon X \to Y$ が全単射のとき，

$$f^{-1} \circ f = \mathrm{id}_X \text{かつ } f \circ f^{-1} = \mathrm{id}_Y$$

である．ここで，$\mathrm{id}_Z\colon Z \to Z$ は**恒等写像** $z \mapsto z$ ($Z = X$ or Y)．

(I) (結合法則) 任意の $f, g, h \in B(X)$ と任意の $x \in X$ に対し，$((f \circ g) \circ h)(x) = f(g(h(x))) = (f \circ (g \circ h))(x)$ なので，写像として $(f \circ g) \circ h = f \circ (g \circ h)$．

(II) (単位元の存在) 単位元は $\mathrm{id}_X \in B(X)$ である．実際，任意の $f \in B(X)$ と任意の $x \in X$ に対し，$(\mathrm{id}_X \circ f)(x) = f(x) = (f \circ \mathrm{id}_X)(x)$ となるので，写像として $\mathrm{id}_X \circ f = f = f \circ \mathrm{id}_X$ が成立する．

(III) (逆元の存在) 任意の $f \in B(X)$ に対し，$f^{-1} \in B(X)$ であって，上の復習で見たように $f^{-1} \circ f = \mathrm{id}_X = f \circ f^{-1}$ が成立する．

例 2 (n 次対称群)**.** $n \in \mathbb{Z}_{>0}$ とする．$X = \{1, 2, \ldots, n\}$ のとき，例 1 で考えた群 $B(X) = B(\{1, 2, \ldots, n\})$ を n **次対称群 (symmetric group pf degree** n**)** といい，$\mathfrak{S}_n$[*2] と書く．

---

* *e-mail* : `hoya@shibaura-it.ac.jp`

*1 この $B(x)$ という記号は標準的な記号ではなく，この講義で用いる記号である．

*2 この文字はドイツ文字の S である．

$\mathfrak{S}_n$ の各元 σ は全単射写像 $\sigma\colon \{1,2,\dots,n\} \to \{1,2,\dots,n\}$ であるが，この写像は

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

としばしば書かれる．例えば，$\mathfrak{S}_3$ の元

$$\begin{array}{cccc} \sigma\colon & \{1,2,3\} & \longrightarrow & \{1,2,3\} \\ & \cup\!\!\!\!\!\!\text{\rotatebox{90}{}} & & \\ & 1 & \longmapsto & 2 \\ & 2 & \longmapsto & 3 \\ & 3 & \longmapsto & 1 \end{array}$$

は $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ と書かれる．また，$\mathfrak{S}_n$ の単位元 $\mathrm{id}_{\{1,2,\dots,n\}}$ は，$\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$ である．この表示を用いると二項演算，つまり写像の合成は次のように計算することができる：

$\mathfrak{S}_n$ における二項演算

$$\begin{pmatrix} 1 & 2 & \cdots & j_k & \cdots & n \\ i_1 & i_2 & \cdots & i_{j_k} & \cdots & i_n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ j_1 & j_2 & \cdots & j_k & \cdots & j_n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n \\ i_{j_1} & i_{j_2} & \cdots & i_{j_k} & \cdots & i_n \end{pmatrix}$$

例えば，$\mathfrak{S}_3$ においては，

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

となる．右の元から順にたどって計算するということに注意をする (もともと写像の合成であったということを忘れないように！)．さらに，この例から $\mathfrak{S}_3$ は非可換群であるということもわかる．一般に，$n \geq 3$ のとき，$\mathfrak{S}_n$ は非可換群である．また，一般に $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ の $\mathfrak{S}_n$ における逆元は次のように求められる．

$\mathfrak{S}_n$ における逆元の計算

(Step 1) $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ の上下をひっくり返して，$\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$ を考える．

(Step 2) $\begin{pmatrix} i_1 & i_2 & \cdots & i_n \\ 1 & 2 & \cdots & n \end{pmatrix}$ における上下のペアを保ったまま，上段の数字を $1.\dots,n$ に並べ替える．

こうして得られる元が $\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}^{-1}$ である．

例えば，

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \xrightarrow{\text{(Step1)}} \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \xrightarrow{\text{(Step2)}} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

と考えて，$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ である．確かに，

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

となる．一般に，最初に取った元が k の下に i_k が書かれるものであった場合 (つまり $k \mapsto i_k$ という写像であった場合)，この方法で出来上がる元は i_k に下に k が書かれる (つまり $i_k \mapsto k$ という写像になる) ため，確かにこれで逆元が得られるということがわかる．

なお，n 次対称群は集合として

$$\mathfrak{S}_n := \left\{ \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix} \middle| \, i_1,\dots,i_n \text{は } 1,\dots,n \text{ を並べ替えたもの} \right\}$$

となっているので，その位数は $|\mathfrak{S}_n| = n!$ である．

巡回置換，互換

$\sigma \in \mathfrak{S}_n$ が，ある $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$ に対して，

$$\sigma(i_s) = \begin{cases} i_{s+1} & s = 1, \ldots, k-1 \text{ のとき，} \\ i_1 & s = k \text{ のとき，} \end{cases} \qquad \sigma(j) = j,\ j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\} \text{ のとき，}$$

を満たすとき，σ を**巡回置換 (cyclic permutation)** といい，$\sigma = (i_1 \cdots i_k)$ と書く．特に $k = 2$，つまり，$(i_1\ i_2)$ の形の元を**互換 (transposition)** といい，$(i\ i+1)$ の形の互換を**隣接互換 (adjacent transposition)** という．

例えば，$\sigma = (132) \in \mathfrak{S}_4$ は 1 を 3 に，3 を 2 に，2 を 1 に移し，その他は動かさない写像，つまり，

$$\begin{array}{cccc} \sigma\colon & \{1,2,3,4\} & \longrightarrow & \{1,2,3,4\} \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ & 1 & \longmapsto & 3 \\ & 2 & \longmapsto & 1 \\ & 3 & \longmapsto & 2 \\ & 4 & \longmapsto & 4 \end{array}$$

という写像を表す．つまり，$(132) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$ である．他にも，$\sigma' = (24) \in \mathfrak{S}_4$ は

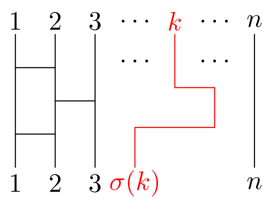
$$\begin{array}{cccc} \sigma'\colon & \{1,2,3,4\} & \longrightarrow & \{1,2,3,4\} \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ & 1 & \longmapsto & 1 \\ & 2 & \longmapsto & 4 \\ & 3 & \longmapsto & 3 \\ & 4 & \longmapsto & 2 \end{array}$$

という写像を表す．つまり，$(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ である．一般に $(i\ j) \in \mathfrak{S}_n (i < j)$ は，

$$(i\ j) = \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ 1 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

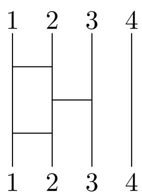
と対応する．

注意 (対称群とあみだくじの関係)**.** 対称群 $\mathfrak{S}_n$ の元は，全単射写像 $\sigma \coloneqq \{1, \ldots, n\} \to \{1, \ldots, n\}$ であったが，これは k から始めると $\sigma(k)$ にたどり着くあみだくじとして表すこともできる (上から下に読む)：

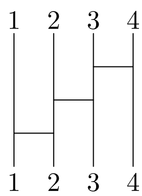


例えば，$\mathfrak{S}_4$ の次の元は以下のようなあみだくじと対応する：

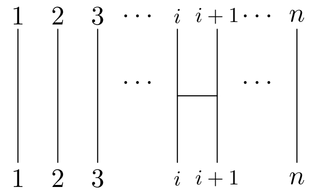
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$:



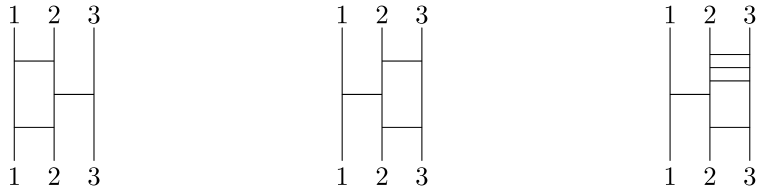
$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$:



また，$\mathfrak{S}_n$ において，隣接互換 $(i\ i+1)$ は以下のような横棒 1 本のあみだくじに対応する：

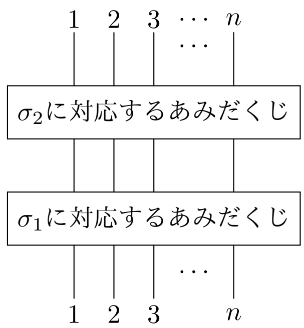


全ての $\mathfrak{S}_n$ の元があみだくじで書けるということは非自明であるが，感覚的には OK であろう．実際にこれは正しい (厳密な証明は補足プリント “巡回置換について” を参照．)．なお，$\mathfrak{S}_n$ の元に対して，対応するあみだくじは 1 通りではない．例えば，



はどれも $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_3$ に対応するあみだくじである．

$\sigma_1, \sigma_2 \in \mathfrak{S}_n$ に対し，$\sigma_1 \circ \sigma_2$ に対応するあみだくじは，σ_1, σ_2 に対応するあみだくじを次のように繋げたものとなる (順番注意！)：



特に，あみだくじは n 本の縦棒に横棒をどんどん付けていって得られるので，上記の考察から，『全ての $\mathfrak{S}_n$ の元があみだくじで書ける』ということは，『全ての $\mathfrak{S}_n$ の元が隣接互換の合成で得られる』という主張に他ならないことに注意しよう．

$\sigma \in \mathfrak{S}_n$ に対し，σ^{-1} に対応するあみだくじは，σ に対応するあみだくじの上下をひっくり返したものとなる．

例 3 (n 次二面体群)**.** 3 以上の整数 n に対し，n 次対称群 $\mathfrak{S}_n$ の元に以下のように名前を付ける：

$$\sigma \coloneqq \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ 2 & 3 & \cdots & k+1 & \cdots & n & 1 \end{pmatrix} = (1\ 2\ \cdots\ n)$$
$$\tau \coloneqq \begin{pmatrix} 1 & 2 & 3 & \cdots & k & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-k & \cdots & 3 & 2 \end{pmatrix}.$$

このとき，

$$D_n \coloneqq \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau\}$$

(e は $\mathfrak{S}_n$ の単位元．二項演算の記号 $\circ$ は省略した．k 乗は k 回合成するという意味) は $\mathfrak{S}_n$ の部分群となる．これを n 次二面体群 **(dihedral group of degree** n**)** という．まず，実際に部分群となることを確かめるために，σ と τ の間の関係を記述しておこう：

命題 4.1

上記の σ と τ について以下が成立する．

(1) $\sigma^n = e$.
(2) $\tau^2 = e$.
(3) $\tau\sigma = \sigma^{-1}\tau, \tau\sigma^{-1} = \sigma\tau$.

証明. 全て直接計算すれば良い．ここでは (3) の 1 つめの式だけ確かめてみよう．まず，

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & 1 & \cdots & k-1 & \cdots & n-2 & n-1 \end{pmatrix}$$

である．これを踏まえると，

$$\begin{aligned} \tau\sigma &= \begin{pmatrix} 1 & 2 & 3 & \cdots & k & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-k & \cdots & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ 2 & 3 & \cdots & k+1 & \cdots & n & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & n-1 & \cdots & n+1-k & \cdots & 2 & 1 \end{pmatrix} \\ \sigma^{-1}\tau &= \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & 1 & \cdots & k-1 & \cdots & n-2 & n-1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \cdots & k & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & n+2-k & \cdots & 3 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & k & \cdots & n-1 & n \\ n & n-1 & \cdots & n+1-k & \cdots & 2 & 1 \end{pmatrix}. \end{aligned}$$

となるので，確かに $\tau\sigma = \sigma^{-1}\tau$ である． □

命題 4.1 から D_n は二項演算と逆元を取る操作について閉じていることが以下のように確かめられる．これは第 4 回講義資料命題 3.5 より D_n が $\mathfrak{S}_n$ の部分群であるということに他ならず，特に D_n は群となる．

<u>逆元を取る操作について閉じていること：</u>まず命題 4.1 (1)，(2) より，

- 各 $k = 0, \dots, n-1$ に対し，$(\sigma^k)^{-1} = \sigma^{n-k}$.
- $\tau^{-1} = \tau$.

である．また，命題 4.1 (3) を繰り返し用いることで，次がわかる．

- 任意の $k \in \mathbb{Z}$ に対し，$\tau\sigma^{-k} = \sigma^k\tau$.

さらに，一般の群 G において以下が成立する：

命題 4.2

G を群とする．このとき，任意の $g, h \in G$ に対し，

$$(gh)^{-1} = h^{-1}g^{-1}.$$

証明. $h^{-1}g^{-1}$ が gh の逆元の満たすべき性質を満たしていることを示せばよい．

$$\begin{aligned} (gh)(h^{-1}g^{-1}) &= g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e \\ (h^{-1}g^{-1})(gh) &= h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e. \end{aligned}$$

より，確かに $h^{-1}g^{-1}$ は gh の逆元 $(gh)^{-1}$ である． □

以上より，D_n の元 $\sigma^k, \sigma^k\tau$ $(k = 0, \dots, n-1)$ に対し，

$$\begin{aligned} (\sigma^k)^{-1} &= \sigma^{n-k} \in D_n \\ (\sigma^k\tau)^{-1} &= \tau^{-1}(\sigma^k)^{-1} = \tau\sigma^{-k} = \sigma^k\tau \in D_n \end{aligned}$$

となることがわかる．

<u>二項演算で閉じていること：</u>一般に証明をしても良いが，必要以上にややこしくなるので，以下の D_7 の例で納得しよう．逆元を取る操作について閉じていることの証明で述べた性質を用いれば良い：

$$\begin{aligned} &\sigma^4\sigma^5 = \sigma^9 = \sigma^2 \in D_7, \qquad (\sigma^2\tau)\sigma^3 = \sigma^2(\tau\sigma^3) = \sigma^2(\sigma^{-3}\tau) = \sigma^{-1}\tau = \sigma^6\tau \in D_7, \\ &(\sigma^2\tau)(\sigma^4\tau) = \sigma^2(\tau\sigma^4)\tau = \sigma^2(\sigma^{-4}\tau)\tau = \sigma^{-2}\tau^2 = \sigma^5 \in D_7. \end{aligned}$$

命題 4.1(3) から，D_n は非可換群であることがわかる (n は 3 以上なので，$\sigma^{-1} = \sigma^{n-1} \neq \sigma$)．さらに，$D_n$ は位数が $2n$ であることが構成からわかる．実際には $\sigma^k, \sigma^k\tau$ $(k = 0, \dots, n-1)$ が全て異なる元であることは

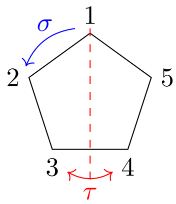
ここでは証明していないが，是非各自チェックしてみて欲しい．なお $n=3$ のとき，$\#D_3 = 2\times 3 = 6$ で，$\#\mathfrak{S}_3 = 3! = 6$ なので，$D_3 = \mathfrak{S}_3$ である．n が 4 以上の時は，$D_n \subsetneq \mathfrak{S}_n$ である．

最後に，この群はいったい何なのか?ということを説明しておこう．D_n は『正 n 角形の板』の対称性と考えることができる．『板』と言っている意味は，表と裏がある (=二面体!) ということである．正 n 角形の板を保つ変換は

『$\frac{2k\pi}{n}$ 回転』と，『(ある固定した対称軸に関して) 折り返してから $\frac{2k\pi}{n}$ 回転』$(k=0,1,\ldots,n-1)$

の $2n$ 個で全てである．このとき，$\frac{2\pi}{n}$ 回転に対応するものが σ であり，ある固定した対称軸に関する折り返しに対応するものが τ である．こう考えると，$\sigma^n = e$ や $\tau^2 = e$ といった性質に親しみがわくであろう．$\tau\sigma = \sigma^{-1}\tau, \tau\sigma^{-1} = \sigma\tau$ も確かめてもらいたい．

D_5 の場合：



なぜこれが対称群 $\mathfrak{S}_5$ の部分群と思えるかというと，上図のように頂点の位置に反時計回りに番号をつけて，各変換によって『どの位置の頂点がどの位置の頂点に行くか』という情報を記録すれば，これは $\{1,\ldots,n\} \to \{1,\ldots,n\}$ という全単射を与えるからである．この対応を考えることで，D_n は $\mathfrak{S}_n$ の部分群として実現されていたのである．このことを念頭において σ と τ の定義を見直してみて欲しい．