代数学 I 第 6 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

前回は n 次対称群と呼ばれる群を導入し，有限個のものの置換を群論的にとらえるということを行った．また，その中ではあみだくじとの対応も観察し，視覚的に二項演算を計算するということも行った．今回は n 次対称群についてもう少し解説を行い，その後 n 次二面体群と呼ばれるまた新しい群について学ぶ．n 次二面体群は正 n 角形の対称性の成す群とも考えられるものである．

5.1　転倒数，符号，交代群

本節では n を 2 以上の自然数とする．

定義 5.1

対称群 $\mathfrak{S}_n$ の元 σ に対し，$1 \leq i < j \leq n$ であって，$\sigma(i) > \sigma(j)$ を満たす組 (i, j) の数を**転倒数 (number of inversions)** と呼び，$\operatorname{inv}\sigma$ と書く．つまり，転倒数とは，言葉で書くと「σ によって大小関係が入れ替わるような数の組の個数」であり，数式で書くと，

$$\operatorname{inv}\sigma \coloneqq \#\{(i,j) \mid i,j \in \{1,\dots,n\}, 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}$$

である．さらに，

$$\operatorname{sgn}\sigma \coloneqq (-1)^{\operatorname{inv}\sigma}$$

とし，これを σ の**符号 (sign)** と呼ぶ．$\operatorname{sgn}\sigma = 1$ のとき，σ を**偶置換**，$\operatorname{sgn}\sigma = -1$ のとき，σ を**奇置換**とよぶ．

例 1. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \in \mathfrak{S}_4$ として，$\operatorname{inv}\sigma, \operatorname{sgn}\sigma$ を計算してみる．まず，2 行配列による表示がどのような全単射を表していたか思い出そう (第 5 回講義資料 4.1 節)．このとき k の下には $\sigma(k)$ を書くのであったから，

$$\sigma(1) = 2 \qquad \sigma(2) = 4 \qquad \sigma(3) = 1 \qquad \sigma(4) = 3$$

である．よって，$1 \leq i < j \leq 4$ であって，$\sigma(i) > \sigma(j)$ を満たす組 (i, j) は

$$(1,3),\ (2,3),\ (2,4)$$

の 3 つである．よって，

$$\operatorname{inv}\sigma = 3, \qquad \operatorname{sgn}\sigma = (-1)^3 = -1$$

となり，σ は奇置換である．同様に，$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_4$ として，$\operatorname{inv}\sigma', \operatorname{sgn}\sigma'$ を計算してみる．$1 \leq i < j \leq 4$ であって，$\sigma'(i) > \sigma'(j)$ を満たす組 (i, j) は

$$(1,2),\ (1,3),\ (1,4),\ (2,3),\ (2,4),\ (3,4)$$

の 6 つである ($1 \leq i < j \leq 4$ なる (i, j) 全てが出ていることに注意)．よって，

$$\operatorname{inv}\sigma' = 6, \qquad \operatorname{sgn}\sigma' = (-1)^6 = 1$$

* *e-mail*：hoya@shibaura-it.ac.jp

となり，σ' は偶置換である．一般に，

$$\sigma_0 = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ n & n-1 & \cdots & 2 & 1 \end{pmatrix} \in \mathfrak{S}_n$$

とすると，$1 \leq i < j \leq n$ であれば必ず，$n+1-i = \sigma_0(i) > \sigma_0(j) = n+1-j$ となるので，

$$\mathrm{inv}\,\sigma_0 = {}_n\mathrm{C}_2 = \frac{n(n-1)}{2}$$

となる．これは $\mathfrak{S}_n$ において転倒数が最大の元で，転倒数がこの値になるのは σ_0 のみである．

対称群 $\mathfrak{S}_n$ およびその元の符号については線型代数で $n \times n$ 行列の行列式を定義する時に出てきている[*1]．習った時には “対称群” や “符号” と言った言葉は聞かなかったかもしれないが，実はここで導入したものと同じである．

線型代数の復習：行列式

n を正の整数とする．$n \times n$ 行列

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} = (a_{ij})_{i,j=1,\ldots,n}$$

に対して，A の行列式 $\det(A)$ は以下で定義される．

$$\det(A) \coloneqq \sum_{\sigma \in \mathfrak{S}_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

例 2. $\mathfrak{S}_2$ においては，

$\mathfrak{S}_2$の元	転倒数	符号	$\mathfrak{S}_2$の元	転倒数	符号
$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$	0	1	$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$	1	-1

となるので，

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

である．$\mathfrak{S}_3$ においては，

$\mathfrak{S}_3$の元	転倒数	符号	$\mathfrak{S}_3$の元	転倒数	符号
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	0	1	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	1	-1
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	2	1	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	1	-1
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	2	1	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	3	-1

となるので，

$$\det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31}$$

(サラスの方法)

となる．

[*1] 行列式は見た目が異なる同値な定義がいくつかあるのでここに書いたものを “定義” ではなく，“性質” として勉強した人もいるかもしれない．いずれにせよ見たことはある式であると仮定して講義は進めるので復習しておいてほしい．

群論に戻ろう．以下の命題が示すように実は任意の互換は奇置換である．

命題 5.2

任意の $1 \leq i < j \leq n$ に対し，

$$\mathrm{inv}(i\ j) = 2(j-i)-1, \qquad \mathrm{sgn}(i\ j) = -1.$$

証明． 2 行配列の表示を用いると，

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

であったことに注意すると，$1 \leq k < \ell \leq n$ であって，$\sigma(k) > \sigma(\ell)$ を満たす組 (k, ℓ) は

$$\begin{gathered}(i, i+1), (i, i+2), \ldots, (i, j-1), (i, j), \\ (i+1, j), (i+2, j), \ldots, (j-1, j)\end{gathered}$$

の $2(j-1-i)+1 = 2(j-i)-1$ 個である．よって，$\mathrm{inv}(i\ j) = 2(j-i)-1$．また，$2(j-i)-1$ は奇数なので，このとき，$\mathrm{sgn}(i\ j) = -1$ である． □

命題 5.3

任意の $1 \leq k \leq n-1$ と $\sigma \in \mathfrak{S}_n$ に対し，

$$\mathrm{sgn}\,(\sigma(k\ k+1)) = -\,\mathrm{sgn}\,\sigma.$$

証明．

$$\sigma = \begin{pmatrix} 1 & \cdots & k & k+1 & \cdots & n \\ i_1 & \cdots & i_k & i_{k+1} & \cdots & i_n \end{pmatrix}$$

と書くと，

$$\sigma(k\ k+1) = \begin{pmatrix} 1 & \cdots & k-1 & k & k+1 & k+2 & \cdots & n \\ i_1 & \cdots & i_{k-1} & i_{k+1} & i_k & i_{k+2} & \cdots & i_n \end{pmatrix}$$

となる．これより，σ と $\sigma(k\ k+1)$ の転倒数を比べると，

(1) $i_k < i_{k+1}$ のとき，$\mathrm{inv}\,(\sigma(k\ k+1)) = \mathrm{inv}\,\sigma + 1$.
(2) $i_k > i_{k+1}$ のとき，$\mathrm{inv}\,(\sigma(k\ k+1)) = \mathrm{inv}\,\sigma - 1$.

となる．(1)，(2) いずれの場合も，$\mathrm{inv}\,(\sigma(k\ k+1))$ と $\mathrm{inv}\,\sigma$ の偶奇は異なるので，符号の定義より，

$$\mathrm{sgn}\,(\sigma(k\ k+1)) = -\,\mathrm{sgn}\,\sigma.$$

□

以下は符号の重要な性質である．

定理 5.4

任意の $\sigma, \sigma' \in \mathfrak{S}_n$ に対し，

$$\mathrm{sgn}(\sigma\sigma') = \mathrm{sgn}\,\sigma\,\mathrm{sgn}\,\sigma'.$$

また，σ が互換 $(a_1\ b_1), \ldots, (a_m\ b_m)$ を用いて，

$$\sigma = (a_1\ b_1)\cdots(a_m\ b_m)$$

と書かれているとき，

$$\mathrm{sgn}\,\sigma = (-1)^m.$$

特に，σ を互換の合成として書くとき，それに必要な互換の数の偶奇は σ によってあらかじめ定まっている．

証明. 第 5 回講義資料定理 4.7 (1) より，ある $i_1, \dots, i_k, j_1, \dots, j_\ell \in \{1, \dots, n-1\}$ が存在して，

$$\sigma = (i_1\ i_1+1) \cdots (i_k\ i_k+1), \qquad \sigma' = (j_1\ j_1+1) \cdots (j_\ell\ j_\ell+1)$$

と書ける．このとき，命題 5.3 を繰り返し用いると，

$$\begin{aligned}
\operatorname{sgn} \sigma &= \operatorname{sgn}((i_1\ i_1+1) \cdots (i_k\ i_k+1)) \\
&= -\operatorname{sgn}((i_1\ i_1+1) \cdots (i_{k-1}\ i_{k-1}+1)) \\
&= (-1)^2 \operatorname{sgn}((i_1\ i_1+1) \cdots (i_{k-2}\ i_{k-2}+1)) \\
&\cdots \\
&= (-1)^{k-1} \operatorname{sgn}((i_1\ i_1+1)) = (-1)^k.
\end{aligned}$$

同様に，$\operatorname{sgn} \sigma' = (-1)^\ell$．また，

$$\sigma\sigma' = (i_1\ i_1+1) \cdots (i_k\ i_k+1)(j_1\ j_1+1) \cdots (j_\ell\ j_\ell+1)$$

より，上と同様に考えて，$\operatorname{sgn}(\sigma\sigma') = (-1)^{k+\ell}$．以上より，

$$\operatorname{sgn}(\sigma\sigma') = (-1)^{k+\ell} = (-1)^k(-1)^\ell = \operatorname{sgn} \sigma \operatorname{sgn} \sigma'.$$

また，$\sigma = (a_1\ b_1) \cdots (a_m\ b_m)$ であるとき，上で示したことを繰り返し用いると，

$$\operatorname{sgn} \sigma = \operatorname{sgn}(a_1\ b_1) \cdots \operatorname{sgn}(a_m\ b_m)$$

となる．命題 5.2 より，$\operatorname{sgn}(a_s\ b_s) = -1\ (s = 1, \dots, m)$ となるので，

$$\operatorname{sgn} \sigma = (-1)^m$$

である．ここでの考察より，σ が互換の m 個の合成として書けるとき，$\operatorname{sgn} \sigma = 1$ なら m は偶数で，$\operatorname{sgn} \sigma = -1$ なら m は奇数でなければならない．よって，定理の最後の主張も示された． □

n 文字の置換を互換の合成で表した時にその偶奇が決まっているという性質は，例えば “15 パズル” と呼ばれるパズルの可解性を調べるのに用いることができる*2．「15 パズル　対称群」というようなキーワードで検索すると面白い記事がいろいろと見つかると思うので，興味のある方は調べてみてほしい．またルービックキューブ等も含めたパズルと群論の関係については，David Joyner 著・川辺 治之訳 “群論の味わい —置換群で解き明かすルービックキューブと 15 パズル—” という本もあるので興味のある方は手に取ってみると良いであろう*3．

以下はあみだくじと上記の話を関連させる系である．対称群の元の符号は，第 5 回講義資料 4.2 節の意味で対応するあみだくじがわかると以下のように直ちに計算できることができる．

系 5.5

あみだくじが対称群の元 $\sigma \in \mathfrak{S}_n$ に対応しているとき，

$$\operatorname{sgn} \sigma = \begin{cases} 1 & \text{横棒の本数が偶数のとき}, \\ -1 & \text{横棒の本数が奇数のとき}, \end{cases}$$

特に，あみだくじはその結果によって横棒の本数の偶奇があらかじめ定まっている．

証明. 第 5 回講義資料定理 4.7 (1) の証明を思い出すと，あみだくじの各横棒は隣接互換に対応していた．これより，横棒の数が m 本のあみだくじが σ に対応しているとき，σ は m 個の隣接互換の合成として書けることがわかる．よって定理 5.4 より，このとき

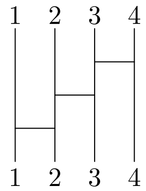
$$\operatorname{sgn} \sigma = (-1)^m.$$

*2 15 パズルというものはおそらく皆様も一度は見たことがあるであろうパズルである．初期状態では 4×4 のマス目に 1 から 15 までの数字の書いたタイルがランダムに入っており，1 マスだけが空いている．この空きマスを利用してタイルをずらしながら 1 から 15 までの数字を順に揃えるというパズルである．

*3 私の研究室 (5384) に来て頂ければお見せします．

つまり，m が偶数のとき $\operatorname{sgn}\sigma = 1$，$m$ が奇数のとき $\operatorname{sgn}\sigma = -1$ となる．また，この考察からあみだくじの結果が $\sigma \in \mathfrak{S}_n$ で与えられるとき，$\operatorname{sgn}\sigma = 1$ であればその横棒の本数は必ず偶数で，$\operatorname{sgn}\sigma = -1$ であればその横棒の本数は必ず奇数であるということもわかる．つまり，あみだくじの横棒の本数の偶奇はその結果からあらかじめ決まっているということがわかる． □

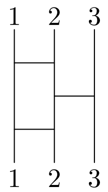
例 3. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \in \mathfrak{S}_4$ は以下のあみだくじに対応する．

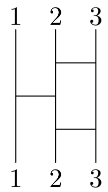


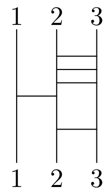
よって，横棒の本数は 3 本で奇数なので，

$$\operatorname{sgn}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = -1.$$

第 5 回講義資料例 2 でも挙げたように，







はいずれも $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in \mathfrak{S}_3$ に対応するあみだくじである．これらを見るとたしかに，横棒の本数は左から順に 3 本，3 本，5 本となっており，いずれも奇数であることが見てとれる．系 5.5 より，これは

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

であることからあらかじめ決まっていることであるという説明ができる．

この節の最後に符号を用いて定義される $\mathfrak{S}_n$ の重要な部分群について述べておこう．

定義 5.6

n 次対称群 $\mathfrak{S}_n$ の元のうち偶置換のみを集めてできる $\mathfrak{S}_n$ の部分集合

$$\mathfrak{A}_n := \{\sigma \in \mathfrak{S}_n \mid \operatorname{sgn}\sigma = 1\}$$

を n 次交代群 **(alternating group of degree n)** と呼ぶ．[*4]

命題 5.7

n 次交代群 $\mathfrak{A}_n$ は n 次対称群 $\mathfrak{S}_n$ の位数 $n!/2$ の部分群である．特に，$\mathfrak{S}_n$ において偶置換と奇置換はちょうど同じ数存在する．

証明. $\operatorname{sgn} e = 1$ なので，$e \in \mathfrak{A}_n$．よって，$\mathfrak{A}_n$ は空ではない．任意の $\sigma, \sigma' \in \mathfrak{A}_n$ に対し，定理 5.4 より，

$$\operatorname{sgn}(\sigma\sigma') = \operatorname{sgn}\sigma \operatorname{sgn}\sigma' = 1 \cdot 1 = 1$$

なので，$\sigma\sigma' \in \mathfrak{A}_n$．再び定理 5.4 より，任意の $\sigma \in \mathfrak{A}_n$ に対し，

$$\operatorname{sgn}\sigma^{-1} = 1 \cdot \operatorname{sgn}\sigma^{-1} = \operatorname{sgn}\sigma \operatorname{sgn}\sigma^{-1} = \operatorname{sgn}(\sigma\sigma^{-1}) = \operatorname{sgn} e = 1$$

[*4] $\mathfrak{A}$ はドイツ文字の A である．普通に「エー」と読めば良い．

となるので，$\sigma^{-1} \in \mathfrak{A}_n$．以上より，$\mathfrak{A}_n$ は $\mathfrak{S}_n$ の部分群である (第 1, 2 回講義資料命題 1.5)．

次に位数について考える．任意の $\sigma \in \mathfrak{A}_n$ に対し，命題 5.3 より，

$$\operatorname{sgn}(\sigma(1\ 2)) = -\operatorname{sgn}\sigma = -1$$

となるので，$\sigma(1\ 2) \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ である ($\mathfrak{S}_n \setminus \mathfrak{A}_n$ は奇置換全体のなす集合である)．逆に，$\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$ のとき，同様に

$$\operatorname{sgn}(\sigma(1\ 2)) = -\operatorname{sgn}\sigma = 1$$

となるので，$\sigma(1\ 2) \in \mathfrak{A}_n$ である．これより，写像

$$\begin{aligned} \iota_1 &\colon \mathfrak{A}_n \to \mathfrak{S}_n \setminus \mathfrak{A}_n,\ \sigma \mapsto \sigma(1\ 2), \\ \iota_2 &\colon \mathfrak{S}_n \setminus \mathfrak{A}_n \to \mathfrak{A}_n,\ \sigma \mapsto \sigma(1\ 2). \end{aligned}$$

を定義することができる．このとき，$(1\ 2)(1\ 2) = e$ より，

$$\iota_2 \circ \iota_1 = \mathrm{id}_{\mathfrak{A}_n}, \qquad \iota_1 \circ \iota_2 = \mathrm{id}_{\mathfrak{S}_n \setminus \mathfrak{A}_n}$$

となる．よって，ι_1, ι_2 は互いに逆写像の関係にある全単射写像である．これより，特に $\mathfrak{A}_n$ と $\mathfrak{S}_n \setminus \mathfrak{A}_n$ の元の個数は等しい (つまり $\mathfrak{S}_n$ において偶置換と奇置換の個数は等しい) ことがわかり，$\mathfrak{A}_n$ の位数は $\mathfrak{S}_n$ の位数のちょうど半分 $n!/2$ であることがわかる． □

例 4. 例 2 における計算より，

$$\mathfrak{A}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

である．これは確かに位数 $3!/2 = 3$ の群である．

5.2　n 次二面体群

本節では n を 3 以上の整数とする．本節では n 次対称群 $\mathfrak{S}_n$ の元に以下のように名前を付ける[*5]．

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

定義 5.8

上の記号のもとで，

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

とする (k 乗は k 回合成するという意味)．これを，n 次二面体群 **(dihedral group of degree n)** という．

注意 1. $n = 3$ のとき，$D_3 = \mathfrak{S}_3$ である．実際，

$$\begin{aligned} e &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & \sigma &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & \sigma^2 &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\ \tau &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & \sigma\tau &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & \sigma^2\tau &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{aligned}$$

である．n が 4 以上の時は，$D_n \subsetneq \mathfrak{S}_n$ である．これは D_n の元の個数が高々 $2n$ 個，$\mathfrak{S}_n$ の元の個数が $n!$ 個であることからわかる．

[*5] これまでの節では $\mathfrak{S}_n$ の任意の元を表すときに σ としばしば書いていたが，この節では常に $(1\ 2\ \cdots\ n)$ を表すことにするので注意せよ．

実は D_n は $\mathfrak{S}_n$ の部分群となる．この群の "意味" については本講義資料の最後に解説することにして，まずは部分群であ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 5.9

上記の $\sigma, \tau \in D_n$ について以下が成立する．

(1) $\sigma^n = e$.

(2) $\tau^2 = e$．すなわち，$\tau^{-1} = \tau$.

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

証明. (1) は第 5 回講義資料命題 4.4 (2) よりわかる．(2) は直接計算すれば直ちにわかる．次に (3) の 1 つめの式を確かめてみよう．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．最後に $\tau\sigma = \sigma^{-1}\tau$ の両辺に左と右から τ を合成すると，

$$\tau\tau\sigma\tau = \tau\sigma^{-1}\tau\tau \quad \Leftrightarrow \quad \sigma\tau = \tau\sigma^{-1} \qquad (\tau^2 = e \text{ より})$$

となる．よって，(3) の 2 つめの式 $\tau\sigma^{-1} = \sigma\tau$ も成立する． □

それでは以下の定理を証明しよう．

定理 5.10

n 次二面体群 D_n は $\mathfrak{S}_n$ の位数 $2n$ の部分群である．

まず，D_n は定義より明らかに空集合ではない．よって，この定理の証明するためには

(1) D_n が二項演算で閉じていること．

(2) D_n が逆元を取る操作について閉じていること．

(3) D_n の位数が $2n$ であること，つまり，$e, \sigma, \sigma^2, \ldots, \sigma^{n-1}, \tau, \sigma\tau, \sigma^2\tau, \ldots, \sigma^{n-1}\tau$ が全て異なる元であること．

の 3 つを示せば良いことがわかる (第 1, 2 回講義資料命題 1.5)．これらを順に確かめる．

(1) の証明：まず命題 5.9 (1), (3) を繰り返し用いることで，以下は直ちにわかる．

補題 5.11

D_n において以下が成立する．

(1) 任意の $k, \ell \in \mathbb{Z}$ に対し，$\sigma^{k+\ell n} = \sigma^k$．特に，任意の $m \in \mathbb{Z}$ に対し，ある $r \in \{0, 1, \ldots, n-1\}$ が存在して，$\sigma^m = \sigma^r \in D_n$ となる．

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

なお補題 5.11 (1) 後半の主張は，任意の $m \in \mathbb{Z}$ に対し，

$$m = qn + r$$

を満たす $q \in \mathbb{Z}, 0 \leq r < n$ が存在することから (q は m を n で割った商，r は余り)，補題 5.11 (1) 前半の主張より，

$$\sigma^m = \sigma^{qn+r} = \sigma^r$$

となって示される．さて，命題 5.9 (2)，補題 5.11 (2) より，任意の $k, \ell \in \{0, 1, \ldots, n-1\}$ に対して，

$$\begin{aligned} &\sigma^k \sigma^\ell = \sigma^{k+\ell} && (\sigma^k \tau)\sigma^\ell = \sigma^k(\tau\sigma^\ell) = \sigma^k(\sigma^{-\ell}\tau) = \sigma^{k-\ell}\tau \\ &\sigma^k(\sigma^\ell \tau) = \sigma^{k+\ell}\tau && (\sigma^k\tau)(\sigma^\ell\tau) = \sigma^k(\tau\sigma^\ell)\tau = \sigma^k(\sigma^{-\ell}\tau)\tau = \sigma^{k-\ell}\tau^2 = \sigma^{k-\ell} \end{aligned}$$

となる．ここで，補題 5.11 (1) より，ある $r_1, r_2 \in \{0, 1, \ldots, n-1\}$ が存在して，$\sigma^{k+\ell} = \sigma^{r_1}, \sigma^{k+\ell} = \sigma^{r_2}$ となるので，上記の計算結果は全て D_n に属する元となる．よって，D_n は二項演算で閉じている．
(2) の証明：まず一般の群 G において以下が成立する．

補題 5.12

G を群とする．このとき，任意の $g, h \in G$ に対し，

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

補題 5.12 の証明. $h^{-1}g^{-1}$ 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． □

命題 5.9 (2)，補題 5.11，補題 5.12 より，D_n の元 $\sigma^k, \sigma^k\tau$ $(k = 0, \ldots, n-1)$ に対し，

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

となることがわかる．よって，D_n が逆元を取る操作について閉じていることが示された．
(3) の証明：$\sigma = (1\ 2\ \cdots\ n)$ より，$k = 0, 1, \ldots, n-1$ について，σ^k による 1 の像を見ると，

$$\sigma^k(1) = (1\ 2\ \cdots\ n)^k(1) = k+1$$

となる．よって，1 の像が全て異なるので，σ^k $(k = 0, 1, \ldots, n-1)$ は相異なる元である．次に，ある $k_1, k_2 \in \{0, 1, \ldots, n-1\}$ に対して，$\sigma^{k_1}\tau = \sigma^{k_2}\tau$ となったと仮定すると，この両辺に右から τ を合成して，

$$\sigma^{k_1}\tau^2 = \sigma^{k_2}\tau^2\text{，つまり，}\sigma^{k_1} = \sigma^{k_2} \quad \text{(命題 5.9 (2) より)}$$

となる．このとき上で証明したことより，$k_1 = k_2$．これより $\sigma^k\tau$ $(k = 0, 1, \ldots, n-1)$ も相異なる元であることがわかった．最後に任意の $k_1, k_2 \in \{0, 1, \ldots, n-1\}$ に対して，$\sigma^{k_1} \neq \sigma^{k_2}\tau$ となることを示せば良い．再びそれぞれの写像による 1 の像を考えると，

$$\sigma^{k_1}(1) = k_1 + 1, \qquad \sigma^{k_2}\tau(1) = \sigma^{k_2}(1) = k_2 + 1$$

となるので，$k_1 \neq k_2$ のとき，$\sigma^{k_1} \neq \sigma^{k_2}\tau$ である．さらに，$k_1 = k_2$ のときも，$\sigma^{k_1} = \sigma^{k_1}\tau$ であったとすると両辺に左から σ^{-k_1} を合成すると $e = \tau$ となって矛盾するので，やはり $\sigma^{k_1} \neq \sigma^{k_1}\tau$ である．以上より，(3) の主張は示された．

以上より，定理 5.10 の証明が完了した．

例 5. 7 次二面体群 D_7 における計算例を以下に示す．

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

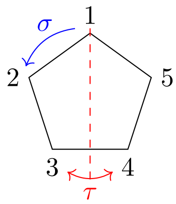
なお，命題 5.9 (3) から D_n は非可換群であることに注意する (n は 3 以上なので，$\sigma^{-1} = \sigma^{n-1} \neq \sigma$)．

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

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

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持てるであろう．$\tau\sigma=\sigma^{-1}\tau, \tau\sigma^{-1}=\sigma\tau$ も確かめてもらいたい．

D_5 の場合：



なぜこれが対称群 $\mathfrak{S}_n$ 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，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ることで，各変換は $\{1,\ldots,n\}\to\{1,\ldots,n\}$ 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 の定義を是非見直してみて欲しい．