代数学 I 第 4 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

前回までは，主に今までに学んだことのある数学的対象の中から群となるものの例を学んできた．その中で学んだ整数の剰余類環 $\mathbb{Z}/n\mathbb{Z}$ は新しいものだったかもしれないが，数を “n で割った余り” に着目して扱うという意味ではそれなりに慣れ親しんだ対象であっただろう．

今回と次回では多くの方にとって群論ではじめて本格的に扱うことになると思われる群の重要な例について学ぶ．今回扱うのは n 次対称群である[*1]．n 次対称群は第 1,2 回講義資料 1.1 節の Galois 理論を簡単に説明したところでも出てきた群であったことを思い出そう．既習の概念を新しい視点 (群の概念) 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．

3.1 n 次対称群

n 次対称群を説明する前に，まず非常に一般的な群の例を見よう．

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

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

を考える[*2]．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[*3]．まず，$f, g \in B(X)$ のとき，$f \circ g$ は再び X から X への写像 $f \circ g \colon X \to X$ であり，

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ \mathrm{id}_X \circ f^{-1} = f \circ f^{-1} = \mathrm{id}_X$$
$$(g^{-1} \circ f^{-1}) \circ (f \circ g) = g^{-1} \circ (f^{-1} \circ f) \circ g = g^{-1} \circ \mathrm{id}_X \circ g = g^{-1} \circ g = \mathrm{id}_X$$

となるので (id_X は X 上の恒等写像)，$f \circ g$ にも逆写像が存在し，$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ である．特に，$f \circ g$ は再び全単射なので，$f \circ g \in B(X)$．これより，写像の合成は確かに二項演算

$$\circ \colon B(X) \times B(X) \to B(X),\ (f, g) \mapsto f \circ g$$

を定める．これが群の二項演算の 3 性質を満たすこと以下のように確かめられる．

(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 X 上の恒等写像 $\mathrm{id}_X \in B(X)$．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 の全単射性から逆写像 $f^{-1} \in B(X)$ が存在するが，このとき第 1 回復習レポート課題解答でも見たように，$f^{-1} \circ f = \mathrm{id}_X = f \circ f^{-1}$ が成立する．

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

*1 n 次対称群は線形代数の講義等でも簡単に扱っているかもしれない．

*2 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．

*3 「写像」「全単射」「写像の合成」といった言葉の定義を忘れた方は，第 1 回復習レポート課題解答を参照すること．

n 次対称群とは上の例 1 で X を有限集合 $\{1,2,\dots,n\}$ として得られる群に他ならない.

定義 3.1

$n \in \mathbb{Z}_{>0}$ とする．$X = \{1,2,\dots,n\}$ のとき，例 1 で考えた群 $B(X) = B(\{1,2,\dots,n\})$ を n **次対称群 (symmetric group pf degree n)** といい，$\mathfrak{S}_n$ と書く.[*4]

定義より $\mathfrak{S}_n$ 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

$$\begin{array}{rccc} \sigma\colon & \{1,2,3\} & \longrightarrow & \{1,2,3\} \\ & \cup & & \cup \\ & 1 & \longmapsto & 2 \\ & 2 & \longmapsto & 3 \\ & 3 & \longmapsto & 1 \end{array}$$

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

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

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,

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

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

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，k を i_k に送る $\mathfrak{S}_n$ の元の逆元は，i_k を k に送る写像である．これは 2 行配列の表示で言うと，k の下に i_k が書かれる元の逆元は，i_k の下に k が書かれるものであるということであり，確かに上の逆元を求める方法はこのような元を与える操作となっていることがわかる．

n 次対称群は集合として

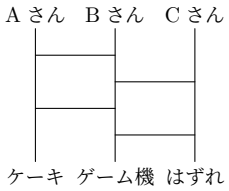
$$\mathfrak{S}_n \coloneqq \left\{ \begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix} \;\middle|\; i_1, \ldots, i_n \text{は } 1, \ldots, n \text{ を並べ替えたもの} \right\}$$

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

以下では，$\mathfrak{S}_n$ の単位元 $\mathrm{id}_{\{1,2,\ldots,n\}}$ を単に e と書くことがある．また，$\mathfrak{S}_n$ における二項演算 (合成) の記号 $\circ$ はしばしば省略する．つまり，$\sigma_1 \circ \sigma_2$ を単に $\sigma_1\sigma_2$ と書いたりする．

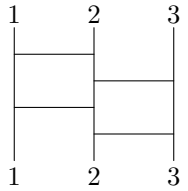
3.2 対称群とあみだくじの関係

プレゼント交換などを行う手段として，“あみだくじ” というものが良く知られている．n 個のプレゼント交換を行いたいときには n 本の縦棒からなるあみだくじを用いる．



あみだくじのルールは各棒の上を上から下に進んで，横棒に当たるたびに必ずその横棒を渡り，渡り終えたらまた下に進むというのを一番下に到着するまで繰り返すというものであった．最後に到達したところに書かれたものが当たるのである．上の例だと A さんはゲーム機，B さんははずれ，C さんはケーキが当たることになる．以下では，あみだくじの横棒としては「隣にある縦棒を結ぶ」という形のもののみを考えることにする．また，あみだくじにおいて「十字路」は現れないものとする．

さて，あみだくじは上の段と下の段を左から順に $1, \ldots, n$ と名付けると，全単射 $\{1, \ldots, n\} \to \{1, \ldots, n\}$ を与える手段の一つとして見ることができる．



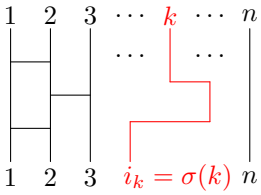
この例だと上から下に読んで，1 は 2，2 は 3，3 は 1 に到達するので，全単射写像

$$\begin{array}{rccc} \sigma\colon & \{1,2,3\} & \longrightarrow & \{1,2,3\} \\ & \cup & & \cup \\ & 1 & \longmapsto & 2 \\ & 2 & \longmapsto & 3 \\ & 3 & \longmapsto & 1 \end{array}$$

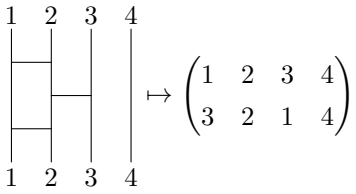
を与えている．この方法で n 本の縦棒からなるあみだくじに，対称群 $\mathfrak{S}_n$ の元を対応させることができる．与えられたあみだくじが各 $k \in \{1, \ldots, n\}$ を i_k に移しているとき，そのあみだくじには

$$\sigma = \begin{pmatrix}1 & 2 & \cdots & n\\ i_1 & i_2 & \cdots & i_n\end{pmatrix} \in \mathfrak{S}_n$$

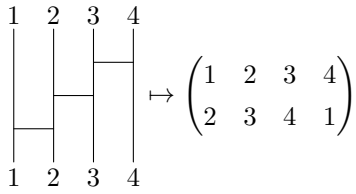
を対応させる．



例 2. 縦棒の数が 4 本のあみだくじは以下のように $\mathfrak{S}_4$ の元に対応する．

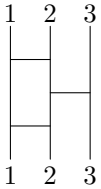


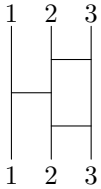
$$\mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

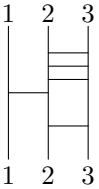


$$\mapsto \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

なお，ここでの対応は「あみだくじの結果」だけを見て考えているので，同じ対称群の元に対応するあみだくじは複数 (一般には無限個) 存在する．例えば，







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．

次に，全ての $\mathfrak{S}_n$ の元があみだくじで書けるかということが気になる．つまりあみだくじで任意の n 個の元の置換が表せるかという問いである．実はこれは正しい．

定理 3.2

任意の $\sigma \in \mathfrak{S}_n$ に対し，σ に対応するあみだくじが存在する．

証明. n に関する数学的帰納法で証明する．$n = 1$ の時は $\mathfrak{S}_1 = \{e\}$ であり，単位元 e は縦棒が 1 本だけのあみだくじに対応するので，定理の主張は正しい．

$n \geq 2$ の場合に，$\mathfrak{S}_{n-1}$ に対しては定理が成り立つと仮定して，定理の主張を証明する．$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$ と書く．ここで，$k = 1, \ldots, n-1$ に対し，

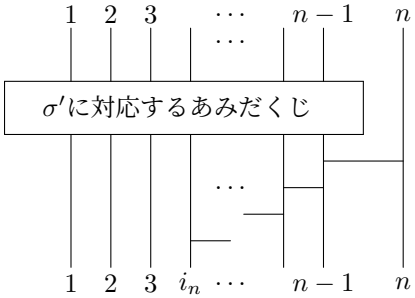
$$i'_k = \begin{cases} i_k & i_k < i_n \text{のとき}, \\ i_k - 1 & i_k > i_n \text{のとき}, \end{cases}$$

とすると，$\{i'_1, \ldots, i'_{n-1}\} = \{1, \ldots, n-1\}$ である[*5]．これより，

$$\sigma' = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ i'_1 & i'_2 & \cdots & i'_{n-1} \end{pmatrix}$$

という $\mathfrak{S}_{n-1}$ の元を考えることができる．帰納法の仮定により，σ' に対応するあみだくじが存在する．これを用いて，以下の n 本の縦棒からなるあみだくじを考える．

[*5] わかりにくいかもしれないので 1 つ例を挙げておこう．$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ のとき，$i_1 = 2, i_2 = 4, i_3 = 5, i_4 = 1, i_5 = 3$ なので，$i'_1 = i_1 = 2, i'_2 = i_2 - 1 = 4 - 1 = 3, i'_3 = i_3 - 1 = 5 - 1 = 4, i'_4 = i_4 = 1$ である．特に，$\{i'_1, i'_2, i'_3, i'_4\} = \{2, 3, 4, 1\} = \{1, 2, 3, 4\}$．言葉で言うと，「$i_n$ を飛ばして小さい順に番号を付けなおしたもの」が $i'_k (k = 1, \ldots, n-1)$ である．



このあみだくじに対応する $\mathfrak{S}_n$ の元を σ_0 と書く．実は $\sigma_0 = \sigma$ であるということを見る．まず，作り方から $\sigma_0(n) = i_n$ である．次に，$k = 1, \ldots, n-1$ で $i'_k < i_n$ のとき，$\sigma_0(k) = i'_k = i_k$ である (「σ' に対応するあみだくじ」を通り抜けた時点で，i_n の縦棒よりも左に到達しており，その場合「σ' に対応するあみだくじ」よりも下に書かれている横棒は進路に影響しない)．最後に，$k = 1, \ldots, n-1$ で $i'_k \geq i_n$ のとき，$\sigma_0(k) = i'_k + 1 = i_k$ であることを見る．この場合，「σ' に対応するあみだくじ」を通り抜けた時点で，i_n の縦棒かそれよりも右に来るので，そのまま進むと，その後横棒を 1 度だけ左から右へ進むことになる．これは $\sigma_0(k) = i'_k + 1 = i_k$ ということに他ならない．

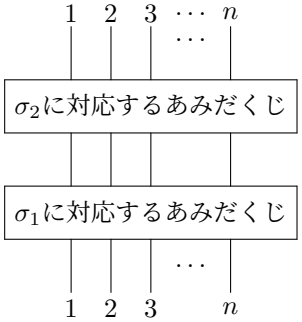
以上より，全ての $k = 1, \ldots, n$ に対して，

$$\sigma_0(k) = i_k = \sigma(k)$$

がわかったので，確かに $\sigma_0 = \sigma$ である．特に，σ は上に書かれたあみだくじに対応する． □

定理 3.2 より，$\mathfrak{S}_n$ の任意の元はあみだくじを用いて表すことができることがわかった．これは対称群における計算を視覚的に行うにあたって便利なことがある．$\mathfrak{S}_n$ における二項演算や逆元を取る操作がどのようにあみだくじで表されるか見ておこう．

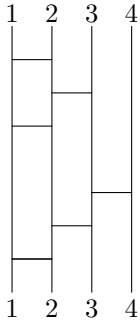
$\sigma_1, \sigma_2 \in \mathfrak{S}_n$ に対し，$\sigma_1 \circ \sigma_2$ に対応するあみだくじは，σ_1, σ_2 に対応するあみだくじを次のように繋げたものとなる (**順番注意！**)：



実際，上のあみだくじは k が「σ_2 に対応するあみだくじ」を抜けたところで $\sigma_2(k)$ の縦棒に到達しており，さらにそこから「σ_1 に対応するあみだくじ」を抜けると $\sigma_1(\sigma_2(k)) = (\sigma_1 \circ \sigma_2)(k)$ の縦棒に到達するので，確かに $\sigma_1 \circ \sigma_2$ に対応している．

$\sigma \in \mathfrak{S}_n$ 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．実際，各 k が i_k に到達するあみだくじの上下をひっくり返すと，i_k が k に到達するあみだくじとなる．これは互いに逆写像の関係になっている．

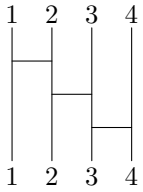
例 3. 例 2 の 2 つのあみだくじを順につなげたもの



を考えると，これは確かに

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

に対応するあみだくじとなる．また，例 2 の 2 つめのあみだくじの上下をひっくり返したもの



を考えると，これは確かに

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

に対応するあみだくじとなる．

3.3 巡回置換，互換

対称群の元の中で特別なものとして，巡回置換，互換というものを導入する．これらは対称群の “基本的な構成要素” として重要な元となる (“基本的な構成要素” の意味については定理 3.7 参照).

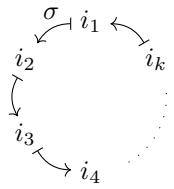
定義 3.3

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

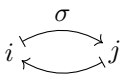
$$\sigma(i_s)=\begin{cases}i_{s+1} & s=1,\dots,k-1\text{ のとき},\\ i_1 & s=k\text{ のとき},\end{cases}\qquad \sigma(j)=j,\ j\in\{1,\dots,n\}\setminus\{i_1,\dots,i_k\}\text{ のとき},$$

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．

巡回置換 $\sigma=(i_1\cdots i_k)$

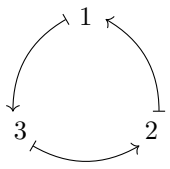


互換 $\sigma=(i\ j)$



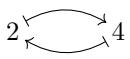
例えば，$\sigma=(132)\in\mathfrak{S}_4$ は 1 を 3 に，3 を 2 に，2 を 1 に移し，その他は動かさない写像，つまり，

$$\begin{array}{rccc}\sigma\colon & \{1,2,3,4\} & \longrightarrow & \{1,2,3,4\}\\ & \cup & & \cup\\ & 1 & \longmapsto & 3\\ & 2 & \longmapsto & 1\\ & 3 & \longmapsto & 2\\ & 4 & \longmapsto & 4\end{array}$$



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

$$\begin{array}{rccc}\sigma'\colon & \{1,2,3,4\} & \longrightarrow & \{1,2,3,4\}\\ & \cup & & \cup\\ & 1 & \longmapsto & 1\\ & 2 & \longmapsto & 4\\ & 3 & \longmapsto & 3\\ & 4 & \longmapsto & 2\end{array}$$



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．

以下は定義から容易に導かれる巡回置換の基本性質である．証明はここでは割愛するので各自考えてみてほしい (上に書いたような巡回置換の「絵」を思い浮かべれば良い)．

命題 3.4

巡回置換 $(i_1\ i_2 \cdots i_k) \in \mathfrak{S}_n$ に対し，以下が成立する．

(1) $(i_1\ i_2 \cdots i_k)^{-1} = (i_k \cdots i_2\ i_1)$.
(2) $1 \leq \ell \leq k-1$ のとき $(i_1\ i_2 \cdots i_k)^{\ell} \neq e$ であり，$(i_1\ i_2 \cdots i_k)^k = e$.

巡回置換 $\sigma = (i_1 \cdots i_k) \in \mathfrak{S}_n$ に対し，

$$S(\sigma) \coloneqq \{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$$

とする[*6]．また単位元 e に対し，$S(e) \coloneqq \emptyset$ とする．つまり，$S(\sigma)$ とは「巡回置換 σ によって非自明に動かされる数の集まり」である．

例 4.

$$S((4\ 6\ 7)) = \{4, 6, 7\}, \qquad S((2\ 4\ 1)) = \{1, 2, 4\}, \qquad S((3\ 4)) = \{3, 4\}.$$

定義 3.5

$\mathfrak{S}_n$ 内の巡回置換の組 $\sigma_1, \ldots, \sigma_s$ が

$$\text{任意の } t \neq t' \text{ に対し，} S(\sigma_t) \cap S(\sigma_{t'}) = \emptyset$$

を満たすとする．このとき $\sigma_1, \ldots, \sigma_s$ は**どの 2 つも互いに素**であると言われる．

例 5.

$$S((1\ 5)) \cap S((2\ 4)) = \emptyset, \quad S((1\ 5)) \cap S((3\ 6\ 8)) = \emptyset, \quad S((2\ 4)) \cap S((3\ 6\ 8)) = \emptyset$$

となるので，$(1\ 5), (2\ 4), (3\ 6\ 8)$ はどの 2 つも互いに素な巡回置換である．

$$S((4\ 6\ 7)) \cap S((2\ 4\ 1)) = \{4\}$$

なので，$(4\ 6\ 7)$ と $(2\ 4\ 1)$ は互いに素でない．

命題 3.6

$\sigma, \sigma' \in \mathfrak{S}_n$ が互いに素な巡回置換のとき，それらは可換，つまり，

$$\sigma\sigma' = \sigma'\sigma$$

である．

証明. $\mathfrak{S}_n$ の元は全単射 $\{1, \ldots, n\} \to \{1, \ldots, n\}$ であったことを思い出すと，$\{1, \ldots, n\}$ から $\{1, \ldots, n\}$ への写像として $\sigma\sigma' = \sigma'\sigma$ であることを言えば良いことになる．

σ, σ' が互いに素なので，$S(\sigma) \cap S(\sigma') = \emptyset$ であることに注意すると，$i = 1, \ldots, n$ は以下の 3 条件のいずれか 1 つだけを満たすことがわかる．

[*6] これはこの講義だけの記号である．

(1) $i \in S(\sigma)$.
(2) $i \in S(\sigma')$.
(3) $i \notin S(\sigma)$ かつ $i \notin S(\sigma')$.

このいずれの場合にも $(\sigma\sigma')(i) = (\sigma'\sigma)(i)$ となることを言えばよい.
(1) のとき： $i, \sigma(i) \in S(\sigma)$ より，$i, \sigma(i) \notin S(\sigma')$．よって，$\sigma'(i) = i, \sigma'(\sigma(i)) = \sigma(i)$ なので,

$$(\sigma\sigma')(i) = \sigma(\sigma'(i)) = \sigma(i) = \sigma'(\sigma(i)) = (\sigma'\sigma)(i).$$

(2) のとき： $i, \sigma'(i) \in S(\sigma')$ より，$i, \sigma'(i) \notin S(\sigma)$．よって，$\sigma(i) = i, \sigma(\sigma'(i)) = \sigma'(i)$ なので,

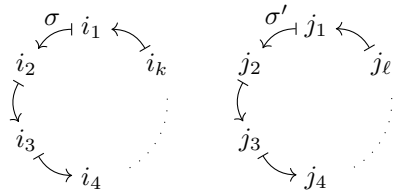
$$(\sigma\sigma')(i) = \sigma(\sigma'(i)) = \sigma'(i) = \sigma'(\sigma(i)) = (\sigma'\sigma)(i).$$

(3) のとき： $i \notin S(\sigma)$ かつ $i \notin S(\sigma')$ より，$\sigma(i) = i$ かつ $\sigma'(i) = i$ なので,

$$(\sigma\sigma')(i) = \sigma(\sigma'(i)) = \sigma(i) = i = \sigma'(i) = \sigma'(\sigma(i)) = (\sigma'\sigma)(i).$$

以上より示すべきことは全て示された. □

命題 3.6 の証明は少し込み入って見えるかもしれない．しかし，再び巡回置換の「絵」を思い出すと，命題 3.6 は以下のように「輪」に重なりが無い (=互いに素)2 つの巡回置換を考えているのだから,「お互いに無関係だとどちらを先に考えても変わりは無い」というごく自然なことを言っているのである.



以下の定理は対称群において巡回置換や (隣接) 互換がそれぞれの意味で “基本的な構成要素” となっていることを主張する定理である.

定理 3.7

n を 2 以上の整数とする．このとき，以下が成立する.

(1) 任意の $\mathfrak{S}_n$ の元は隣接互換 $(i\ i+1), i = 1, \ldots, n-1$ らの合成として書かれる.
(2) 単位元でない任意の $\mathfrak{S}_n$ の元は，どの 2 つも互いに素な巡回置換の合成として書かれる．さらに，自明な巡回置換 (=単位元) を用いないことにすると，合成の順序の違いを除いてこの表示は一意的である.

定理 3.7 (1) においては，(2) のような表示の一意性が成り立たないことに注意する．例えば，$\mathfrak{S}_3$ において，$s_1 = (1\ 2), s_2 = (2\ 3)$ とすると,

$$s_1 s_2 s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s_2 s_1 s_2 = s_1 s_1 s_2 s_1 s_2 = \cdots.$$

である.

命題 3.6 より互いに素な巡回置換は可換なので，定理 3.7 (2) の表示において，どの 2 つも互いに素な巡回置換の合成の順番は任意であるということがわかる．主張内にある「合成の順序の違いを除いて」というのは可換性からここの順番の違いは自明な違いであると考えられるので書かれている[*7].

[*7] 自然数の素因数分解の一意性において，積の順番は気にしなかったり，1 は素数に入れなかったりすることと同様の注意が書かれていると思えば良い.

以下で定理 3.7 を証明するが，特に (2) の証明は少し長い[*8]．このため，どのようにすれば $\mathfrak{S}_n$ の元をどの 2 つも互いに素な巡回置換の合成として書くことができるのか先に例で見て，この主張の正しさを「納得」してもらうことにする．実際この例と同様にすることで，いつでもこのタイプの表示を得ることができる．

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 2 & 8 & 7 & 6 & 9 & 1 & 5 & 10 & 3 \end{pmatrix} \in \mathfrak{S}_{10}$$

とする．まず 1 をとる (これは実際には 1 でなくても何でも良い)．1 の σ による像を次々に計算する：

$$1 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 7 \overset{\sigma}{\mapsto} 1$$

上のように初めに取った 1 に戻ってきたところでストップする (必ずいつか初めの数字に戻る)．次に，上の過程で現れていない数字を任意にとる．ここでは 2 を取る．そして，上と同様に 2 の σ による像を計算する：

$$2 \overset{\sigma}{\mapsto} 2$$

これは，1 回で初めに取った数字に戻ってくる (つまり動かさない) のでここでストップする．さらに，上の過程でまだ今まで一度も出てきてない数字を任意にとる．ここでは 3 をとる．そして，上と同様に 3 の σ による像を次々に計算する：

$$3 \overset{\sigma}{\mapsto} 8 \overset{\sigma}{\mapsto} 5 \overset{\sigma}{\mapsto} 6 \overset{\sigma}{\mapsto} 9 \overset{\sigma}{\mapsto} 10 \overset{\sigma}{\mapsto} 3$$

同様に初めに取った 3 に戻ってくるのでそこでストップする．以上で $1, \dots, 10$ の全ての数が出そろったので，反復の過程をストップする．

以上の過程で出てきた数字のサイクルをその順に並べて巡回置換を作り，その合成をとる．

$$(1\ 4\ 7)(2)(3\ 8\ 5\ 6\ 9\ 10) = (1\ 4\ 7)(3\ 8\ 5\ 6\ 9\ 10)$$

すると，こうして得られる巡回置換たちはその作り方から (どの 2 つも) 互いに素であり，さらに写像として σ と一致する．つまり，

$$\sigma = (1\ 4\ 7)(3\ 8\ 5\ 6\ 9\ 10)$$

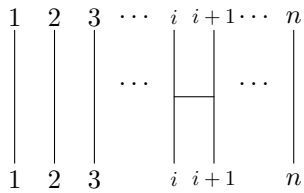
であり，確かに σ を互いに素な巡回置換の合成として書くことができた．

例 6. 他の定理 3.7 (1) の形の表示例も以下に書いておくので，上のアルゴリズムで計算してみてほしい．

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 3 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 4\ 5\ 6)(2\ 7)$
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 5 & 2 & 1 & 6 & 10 & 9 & 7 & 8 \end{pmatrix} = (1\ 3\ 5)(2\ 4)(7\ 10\ 8\ 9)$

定理 3.7 の証明.

(1) $\mathfrak{S}_n$ 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．



ここで定理 3.2 より，任意の $\sigma \in \mathfrak{S}_n$ には 3.2 節での意味で対応するあみだくじが存在した．ここでのあみだくじは上記のような横棒 1 本のあみだくじを有限個つなぐことでできるものである．3.2 節より，あみだくじの連結は対称群 $\mathfrak{S}_n$ における二項演算に対応していたので，これは σ が隣接互換 $(i\ i+1), i = 1, \dots, n-1$ らの合成として書かれるということに対応している[*9]． □

[*8] 講義時間に全てを解説する時間はないと思われるので，講義時間中には概略のみ話す予定です．もし詳細について質問がある場合は直接お願いします．

[*9] この考察から，(1) で表示の一意性が成り立たないことは同じ対称群の元に対応するあみだくじが複数あるということに対応するということがわかる．

(2) まず $\sigma \in \mathfrak{S}_n$ がどの 2 つも互いに素な巡回置換の合成として書かれるということを証明する．

$$k_\sigma \coloneqq \#\{i \in \{1,\dots,n\} \mid \sigma(i) \neq i\}$$

とし，k_σ の値に関する帰納法で証明をする (k_σ は「σ によって非自明に動かされる元の個数」である)．まず，$k_\sigma = 0$ のとき，$\sigma = e$ なので，証明すべき主張は正しい (e は自明な巡回置換と考える)．次に $k_\sigma > 0$ のとき，$k_{\sigma'} < k_\sigma$ となる $\mathfrak{S}_n$ の元 σ' は，どの 2 つも互いに素な巡回置換の合成として書かれることが証明できたと仮定し，σ がどの 2 つも互いに素な巡回置換の合成として書かれることを証明する．

i_0 を $\sigma(i_0) \neq i_0$ を満たす元とする．このとき，$\{1,\dots,n\}$ は有限集合であることから，ある $s,t \in \mathbb{Z}_{>0}, s < t$ が存在して，

$$\sigma^s(i_0) = \sigma^t(i_0)$$

となる．このとき，両辺に σ^{-1} を s 回施すと，

$$i_0 = \sigma^{t-s}(i_0)$$

となる．そこで，$i_0 = \sigma^s(i_0)$ を満たす最小の正の整数 s を s_0 とする (上の考察より，このような s は必ず存在するので，その中で最小のものを取れば良い)．$\sigma(i_0) \neq i_0$ より，$s_0 \geq 2$ であることに注意する．このとき，

$$i_0,\ \sigma(i_0),\ \sigma^2(i_0),\dots,\ \sigma^{s_0-1}(i_0)$$

は全て異なる．なぜなら，$\sigma^{k_1}(i_0) = \sigma^{k_2}(i_0), 0 \leq k_1 < k_2 \leq s_0 - 1$ とすると，上と同様の議論から $i_0 = \sigma^{k_2-k_1}(i_0)$ となるが，$0 < k_2 - k_1 < s_0$ より，これは s_0 の最小性に反するためである．そこで，巡回置換 $\sigma_0 \in \mathfrak{S}_n$ を

$$\sigma_0 \coloneqq (i_0\ \sigma(i_0)\ \cdots\ \sigma^{s_0-1}(i_0))$$

と定義する．さらに，

$$\sigma' \coloneqq \sigma\sigma_0^{-1}$$

とする．このとき，任意の $0 \leq k \leq s_0 - 1$ に対して，

$$\sigma'(\sigma^k(i_0)) = \sigma(\sigma_0^{-1}(\sigma^k(i_0))) = \sigma(\sigma^{k-1}(i_0)) = \sigma^k(i_0)$$

となるので，σ' は $\sigma^k(i_0), 0 \leq k \leq s_0 - 1$ を動かさない．また，$j \in \{1,\dots,n\} \setminus \{i_0, \sigma(i_0),\dots,\sigma^{s_0-1}(i_0)\}$ に対しては，

$$\sigma'(j) = \sigma(\sigma_0^{-1}(j)) = \sigma(j)$$

となる．つまり，$i_0, \sigma(i_0),\dots,\sigma^{s_0-1}(i_0)$ 以外の部分については，σ' と σ は同じ対応を与える．以上より，

$$k_{\sigma'} < k_\sigma$$

となる．これより，帰納法の仮定から σ' はどの 2 つも互いに素な巡回置換 $\sigma_1,\dots,\sigma_t$ を用いて，$\sigma' = \sigma_1 \cdots \sigma_t$ と書かれる．さらに，σ_0 と $\sigma_s, 1 \leq s \leq t$ は互いに素である．なぜなら，σ_0 と σ_s が互いに素でない場合，$S(\sigma_s)$ に，ある $\sigma^k(i_0)$ が含まれることになるが，このとき，$\sigma' = \sigma_1 \cdots \sigma_t$ は $\sigma^k(i_0)$ を非自明に動かす置換となって，σ' が $\sigma^k(i_0), 0 \leq k \leq s_0 - 1$ を動かさないということに矛盾するためである．よって，

$$\sigma = \sigma'\sigma_0 = \sigma_1 \cdots \sigma_t\sigma_0$$

となり，確かに σ がどの 2 つも互いに素な巡回置換として表されることが示された．

次に表示の一意性を証明する．$\sigma = \sigma_1 \cdots \sigma_a = \sigma'_1 \cdots \sigma'_b$ をそれぞれどの 2 つも互いに素な巡回置換の合成による σ の表示とする．このとき，

$$\{\sigma_1,\dots,\sigma_a\} \neq \{\sigma'_1,\dots,\sigma'_b\}$$

と仮定して矛盾を導けば良い．このとき，$\{\sigma_1,\dots,\sigma_a\}$ と $\{\sigma'_1,\dots,\sigma'_b\}$ の対等性と命題 3.6 より，

$$\sigma_1 \notin \{\sigma'_1,\dots,\sigma'_b\}$$

と仮定して一般性を失わない．$i \in S(\sigma_1)$ とすると，

$$\sigma(i) = (\sigma_1 \cdots \sigma_a)(i) = \sigma_1(i) \neq i$$

となるので，$S(\sigma'_1), \ldots, S(\sigma'_b)$ の中にもだた 1 つだけ i を含むものが存在する (そうでなければ $\sigma(i) = (\sigma'_1 \cdots \sigma'_b)(i) = i$ となって矛盾する)．ここで，再び命題 3.6 より $i \in S(\sigma'_1)$ として一般性を失わない．いま σ_1 の決め方より，$\sigma_1 \neq \sigma'_1$．このとき，ある $\ell \in \mathbb{Z}_{>0}$ が存在して，

$$\sigma_1^\ell(i) \neq (\sigma'_1)^\ell(i)$$

となる．ここで，命題 3.6 より，

$$\sigma^\ell = \sigma_1^\ell \cdots \sigma_a^\ell = (\sigma'_1)^\ell \cdots (\sigma'_b)^\ell$$

となるが，

$$\sigma^\ell(i) = (\sigma_1^\ell \cdots \sigma_a^\ell)(i) = \sigma_1^\ell(i) \qquad \sigma^\ell(i) = ((\sigma'_1)^\ell \cdots (\sigma'_b)^\ell)(i) = (\sigma'_1)^\ell(i)$$

より，$\sigma_1^\ell(i) = (\sigma'_1)^\ell(i)$ となって矛盾が生じる．以上より，示すべき一意性は示された． □