巡回置換について

大矢 浩徳 (OYA Hironori)

本資料では，第 6 回講義資料の定理 5.4 の厳密な証明を与える．まず，定理 5.4 を思い出そう．

定理 5.4

n を 2 以上の整数とする．各 $i = 1, \dots, n-1$ に対し $s_i \coloneqq (i\ i+1) \in \mathfrak{S}_n$ とする．このとき，以下が成立する：

(1) 任意の $\mathfrak{S}_n$ の単位元でない元はどの 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，長さ 1 の巡回置換 (=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．

(2) 任意の $\mathfrak{S}_n$ の元は隣接互換 $s_i, i = 1, \dots, n-1$ らの合成として書かれる．

巡回置換について 2 つの補題を準備する．証明はいずれも各用語の定義より容易である．

補題 1.

$\sigma \in \mathfrak{S}_n$ を巡回置換とし，$i \in S(\sigma)$ とする．このとき，m を $\sigma^m(i) = i$ を満たす最小の m とすると[*1]，

$$\sigma = (i\ \sigma(i) \cdots \sigma^{m-1}(i))$$

である．特に，$S(\sigma) = \{i, \sigma(i), \dots, \sigma^{m-1}(i)\}$ である．

補題 2 (命題 5.3)

$\sigma_1, \dots, \sigma_s$ を $\mathfrak{S}_n$ 内のどの 2 つも互いに素な巡回置換とする．このとき，

$$(\sigma_1 \cdots \sigma_s)(i) = \begin{cases} \sigma_t(i) & \text{ある } t \text{ について } i \in S(\sigma_t) \text{ となるとき，} \\ i & \text{全ての } t = 1, \dots, s \text{ に対して，} i \notin S(\sigma_t) \text{ のとき，} \end{cases}$$

となる．特に，σ と σ' 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．

以下の定理 5.4 (1) の証明は少し込み入っているように見えるので，証明の前に実際にどのようにすれば任意の $\mathfrak{S}_n$ 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ということを例で見ておくと良い．実際に，定理 5.4 (1) の証明は以下の方法を一般的な言葉に置き換えただけのものである．

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

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

$$1 \overset{\sigma}{\mapsto} 3 \overset{\sigma}{\mapsto} 2 \overset{\sigma}{\mapsto} 4 \overset{\sigma}{\mapsto} 8 \overset{\sigma}{\mapsto} 1$$

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 (必ず初めの数字にいつか戻る)．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 5 を取る．そして，上と同様に 5 の σ による像を次々に計算

[*1] このような m の存在は巡回置換の定義よりわかる．

する：

$$5 \overset{\sigma}{\mapsto} 7 \overset{\sigma}{\mapsto} 9 \overset{\sigma}{\mapsto} 5$$

同様に初めに取った 5 に戻ってくるのでそこでストップする．さらに，上の過程で今まで一度も出てきてない数字を任意にとる．ここでは，6 をとる．そして，上と同様に 6 の σ による像を次々に計算する：

$$6 \overset{\sigma}{\mapsto} 10 \overset{\sigma}{\mapsto} 6$$

同様に初めに取った 6 に戻ってくるのでそこでストップする．ここで，$1, \dots, 10$ の全ての数が出そろったので，以上の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．

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

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，さらに補題 2 から写像として σ と一致する．よって，

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

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．

以下の定理 5.4 (1) の証明はこの方法がいつでも可能であるということを抽象的に書いたものである．

定理 5.4 の証明. (1) 任意の元 $\sigma \in \mathfrak{S}_n$ をとる．このとき 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示す．各 $i \in \{1, \dots, n\}$ に対して，

$$\Sigma_i := \{\sigma^m(i) \mid m \in \mathbb{Z}\} \subset \{1, \dots, n\}$$

とおく．このとき，

主張 1. 各 $i, i' \in \{1, \dots, n\}$ に対し，

$$\Sigma_i \cap \Sigma_{i'} \neq \emptyset \Leftrightarrow \Sigma_i = \Sigma_{i'}.$$

主張 *1* の証明．$i = \sigma^0(i) \in \Sigma_i$ なので Σ_i は空集合ではないため，$\Leftarrow$ 方向は明らか．$\Rightarrow$ 方向を示す．$\Sigma_i \cap \Sigma_{i'}$ は空集合でないので，その元 i'' を取ると定義よりある $\ell, \ell' \in \mathbb{Z}$ が存在して，$i'' = \sigma^{\ell}(i) = \sigma^{\ell'}(i')$ と書ける．このとき，

$$\Sigma_i = \{\sigma^{m+\ell}(i) \mid m \in \mathbb{Z}\} = \{\sigma^m(i'') \mid m \in \mathbb{Z}\} = \{\sigma^{m+\ell'}(i') \mid m \in \mathbb{Z}\} = \Sigma_{i'}.$$

□

主張 1 より，$\{i_1, \dots, i_s\} \subset \{1, \dots, n\}$ であって，

(a) $\Sigma_{i_1} \cup \cdots \cup \Sigma_{i_s} = \{1, \dots, n\}$
(b) 任意の $t \neq t'$ に対し，$\Sigma_{i_t} \cap \Sigma_{i_{t'}} = \emptyset$

を満たすものが次の手続きで取れる：

(Step 0) $i_1 = 1$ とする．$\Sigma_{i_1} = \{1, \dots, n\}$ ならばここで終了する ($s = 1$)．$\Sigma_{i_1} \neq \{1, \dots, n\}$ のとき Step1 に進む．

(Step s') $i_1, \dots, i_{s'} \in \{1, \dots, n\}$ が，(b) を満たすとする．

Case 1： $\Sigma_{i_1} \cup \cdots \cup \Sigma_{i_{s'}} = \{1, \dots, n\}$ ならば，ここで終了する ($s = s'$).

Case 2： $\Sigma_{i_1} \cup \cdots \cup \Sigma_{i_{s'}} \neq \{1, \dots, n\}$ のとき，$i_{s'+1} \in \{1, \dots, n\} \setminus \Sigma_{i_1} \cup \cdots \cup \Sigma_{i_{s'}}$ を任意にとる．このとき $k = 1, \dots, s'$ に対し，$\Sigma_{i_{s'+1}} \ni i_{s'+1} \notin \Sigma_{i_k}$ なので，主張 1 より $\Sigma_{i_{s'+1}} \cap \Sigma_{i_k} = \emptyset$ である．よって，$i_1, \dots, i_{s'}, i_{s'+1} \in \{1, \dots, n\}$ は再び (b) を満たし，Step $(s'+1)$ に進む．

$\Sigma_{i_1} \cup \cdots \cup \Sigma_{i_{s''}}$ よりも $\Sigma_{i_1} \cup \cdots \cup \Sigma_{i_{s''}} \cup \Sigma_{i_{s''+1}}$ は真に大きいため，これらの Step を繰り返せばいずれ (a) が成立し，手続きが終了する．

さてこのとき $t = 1, \ldots, s$ に対し，$\sigma^m(i_t) = i_t$ を満たす最小の正の整数を m_t とする[*1]．このとき，

- 任意の $0 \leq k < k' < m_t$ に対し，$\sigma^k(i_t) \neq \sigma^{k'}(i_t)$

となる．なぜなら，もし $\sigma^k(i_t) = \sigma^{k'}(i_t)$ なる $0 \leq k < k' < m_t$ が存在したとすると両辺に σ^{-k} を適用して，$i_t = \sigma^{k'-k}(i_t)$ となり，$0 < k' - k < m_t$ より，これは m_t の最小性に反するからである．よって，

$$\sigma_t := (i_t\ \sigma(i_t) \cdots \sigma^{m_t-1}(i_t))$$

とすると，これは意味を持つ巡回置換である．定義から $S(\sigma_t) = \Sigma_{i_t}$ であることに注意すると，Σ_{i_t} らの性質 (b) より，$\sigma_1, \ldots, \sigma_s$ はどの 2 つも互いに素な巡回置換の組である．よって，

$$\sigma = \sigma_1 \cdots \sigma_s$$

を言えばよい．各 $i \in \{1, \ldots, n\}$ の両辺の写像による像を比較する．Σ_{i_t} らの性質 (a)，(b) より，i に対してただ一つ t が定まり，$i \in \Sigma_{i_t}$ となる．このとき，ある m が存在して，$i = \sigma^m(i_t)$ と書けるが，補題 2 と σ_t の定義より，

$$(\sigma_1 \cdots \sigma_s)(i) = \sigma_t(i) = \sigma_t(\sigma^m(i_t)) = \sigma^{m+1}(i_t) = \sigma(i).$$

今 i は任意だったので，写像 $\{1, \ldots, n\} \to \{1, \ldots, n\}$ として，$\sigma = \sigma_1 \cdots \sigma_s$，つまり，対称群 $\mathfrak{S}_n$ の元として $\sigma = \sigma_1 \cdots \sigma_s$ である．

次に，σ を単位元でないとして，σ を

$$\sigma = \sigma_1^{(1)} \cdots \sigma_{s_1}^{(1)} = \sigma_2^{(2)} \cdots \sigma_{s_2}^{(2)}$$

と，長さ 1 の巡回置換 (=単位元) を含まない互いに素な巡回置換の合成として 2 通りの方法で表示したとする．このとき，$\{\sigma_1^{(1)}, \ldots, \sigma_{s_1}^{(1)}\} = \{\sigma_1^{(2)}, \ldots, \sigma_{s_2}^{(2)}\}$ であることを言えばよい．背理法で示す．補題 2 より，互いに素な巡回置換どうしは可換なので $\sigma_1^{(1)}$ が $\{\sigma_1^{(2)}, \ldots, \sigma_{s_2}^{(2)}\}$ に含まれないとして一般性を失わない (必要があれば 2 つの表示を入れ替える)．ここで，$\sigma_1^{(1)} \neq e$ なので $i \in S(\sigma_1^{(1)})$ をとり，$i \in S(\sigma_t^{(2)})$ なる $t = 1, \ldots, s_2$ をとる (存在しないとき $\sigma_t^{(2)} = e$ とする)．このとき，仮定から $\sigma_1^{(1)} \neq \sigma_t^{(2)}$ なので補題 1 より，ある整数 m が存在して，$(\sigma_1^{(1)})^m(i) \neq (\sigma_t^{(2)})^m(i)$ となる．しかしこのとき，補題 2 より，

$$\sigma^m(i) = (\sigma_1^{(1)})^m(i) \neq (\sigma_t^{(2)})^m(i) = \sigma^m(i)$$

なので矛盾．よって，表示の一意性が示された．

(2)[*2] (1) より， 任意の $\mathfrak{S}_n$ の元は巡回置換の合成として書けるので，巡回置換が s_i らの合成で表されることを示せばよい．今 $(i_1 \cdots i_k)$ を巡回置換とすると，

$$(i_1 \cdots i_k) = (i_1\ i_2)(i_2\ i_3) \cdots (i_{k-1}\ i_k) \tag{1}$$

となることが直接各 $i \in \{1, \ldots, n\}$ の両辺の写像による像を比較することで，容易に確かめられる．これより，互換が s_i らの合成で表されることを示せば十分である．この事実を各互換 $(i\ j), i < j$ に対して，$j - i$ の値に関する帰納法で示す．$j - i = 1$ のとき，$(i\ j) = (i\ i+1) = s_i$ なので良い．$j - i > 1$ のとき，

$$s_{j-1}(i\ j-1)s_{j-1} = (j-1\ j)(i\ j-1)(j-1\ j) = (i\ j) \tag{2}$$

となることが直接各 $i \in \{1, \ldots, n\}$ の両辺の写像による像を比較することで，容易に確かめられる．今，帰納法の仮定より $(i\ j-1)$ は s_i らの合成で表されることがわかっているので，(2) より $(i\ j)$ も s_i らの合成で表される．帰納法により，証明すべきことは全て示された． □

[*1] さらに詳しく説明すると，Σ_{i_t} は有限集合なので，ある $m_1, m_2 (m_1 < m_2)$ が存在して，$\sigma^{m_1}(i_t) = \sigma^{m_2}(i_t)$ となる．両辺に σ^{-m_1} を適用すると $i_t = \sigma^{m_2-m_1}(i_t)$ となるので，$\sigma^m(i_t) = i_t$ を満たす正の整数 m は必ず存在する．

[*2] ここでは (1) を用いた証明を行うが，(1) を用いなくても直接証明できる．例えば，$\mathfrak{S}_{n-1} \hookrightarrow \mathfrak{S}_n$ という自然な埋め込みを用いて，n に関する数学的帰納法を用いる証明もある．考えてみよ．