

置換群 練習問題の解答例 (by 山田)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix} \in \mathcal{S}_6.$$

[1] (1)

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 6 & 4 & 1 & 5 \\ 4 & 6 & 2 & 1 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 3 & 5 \end{pmatrix}.$$
$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 6 & 4 & 1 & 5 & 2 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$$
$$\sigma^{-1} = \begin{pmatrix} 3 & 6 & 4 & 1 & 5 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}, \quad \tau^{-1} = \begin{pmatrix} 3 & 2 & 6 & 4 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 6 & 3 \end{pmatrix}.$$

(2)

$$(\sigma\tau)^{-1} = \begin{pmatrix} 4 & 6 & 2 & 1 & 3 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 6 & 2 \end{pmatrix} = \tau^{-1}\sigma^{-1}.$$
$$(\tau\sigma)^{-1} = \begin{pmatrix} 6 & 5 & 4 & 3 & 1 & 2 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 2 & 1 \end{pmatrix} = \sigma^{-1}\tau^{-1}.$$
$$\tau^{-1}\sigma\tau = \tau^{-1}(\sigma\tau) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix}.$$

(3)–(7)

x	σ	τ	$\sigma\tau$	$\tau\sigma$
(3) x	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 4 & 1 & 5 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 1 & 3 & 5 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 1 & 2 \end{pmatrix}$
x^2	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 5 & 4 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 6 & 4 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 6 & 5 \end{pmatrix}$
x^3	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 6 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 1 & 6 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 2 & 1 \end{pmatrix}$
x^4	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$
x^5	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$			
x^6	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$			
(4) 位数	6	4	4	4
(5) 軌道	1,3,4	1,3,6,5	1,4	1,6,2,5
(6) 巡回	(1,3,4)(2,6)	(1,3,6,5)	(1,4)(2,6,5,3)	(1,6,2,5)(3,4)
(7) 偶奇	奇	奇	偶	偶

(3)–(7) 続き

x	σ	σ^{-1}	$\tau^{-1}\sigma\tau$
(3) x	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix}$
x^2	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix} = (1,4,3)$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{pmatrix} = (1,3,4)$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 3 & 1 & 4 & 6 \end{pmatrix} = (1,5,4)$
x^3	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix} = (2,6)$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix} = (2,6)$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix} = (2,3)$
x^4	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 5 & 6 \end{pmatrix} = (1,3,4)$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 1 & 3 & 5 & 6 \end{pmatrix} = (1,4,3)$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix} = (1,4,5)$
x^5	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 3 & 5 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 1 & 4 & 6 \end{pmatrix}$
x^6	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$
(4) 位数	6	6	6
(5) 軌道	1,3,4	1,4,3	1,4,5
(6) 巡回	(1,3,4)(2,6)	(1,4,3)(2,6)	(1,4,5)(2,3)
(7) 偶奇	奇	奇	奇

[2] (a1) 置換 $\sigma \in \mathcal{S}_n$ に対して、次のアルゴリズムを適用する：

(0) 動く数字がなくなるまで下記の (1) に続いて (k) を反復する ($k = 2, 3, \dots$)

(1) まず 1 の σ による軌道を調べる. (1 が動かない場合は省略)

(k) σ で動く数字のうち、調べた軌道のどれにも含まれていない数字のうち最小のものの σ による軌道を調べる.

高々 (1) と (k) の反復を n 回操作すれば (0) の状況になり終了する. それぞれの軌道は巡回置換になっており, (k) の条件「どれにも含まれていない数字」により, 軌道どうしは交わらない. $\square$

(a2) 巡回置換は互換の積： $(i_1, i_2, \dots, i_r) = (i_1, i_2)(i_2, i_3) \cdots (i_{r-1}, i_r)$ $\square$

補足：従って長さ r の巡回置換の符号は $\text{sgn}((i_1, i_2, \dots, i_r)) = (-1)^{r-1}$.

(a3) 互換は隣接置換の積： $I < J$ と仮定する. $2(J - I) - 1$ 個の積に分解する.

$$(I, J) = (I, I+1)(I+1, I+2) \cdots (J-2, J-1)(J-1, J) \\ (J-2, J-1) \cdots (I+1, I+2)(I, I+1). \quad \square$$

(A) 任意の置換は互換の積：(a1) と (a2) による.

(a2) の証明によれば, 交わらない巡回置換を互換に分解したとき, それぞれから現れる互換は交わらない. なお, 軌道の交わりがない巡回置換の積は交換可能. $\square$

(B) 置換の偶奇は分解に依らない：差分 A から $A(\sigma)$ への変化を考察する。
置換の符号は準同型性質をもつ： $\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau)$. 互換 1 個の符号はマイナスであることから、分解によって個数が変わっても、個数の偶奇までは変わらない。□

(1) 積と偶奇の関係： $\sigma\tau$ の分解の 1 つとして σ の分解と τ の分解の積が考えられる。(B) で示した通り、他の分解を選んでも偶奇は変わらない。置換の符号は互換の積への分解の個数の偶奇なので、整数の和と同じになる。□

(2) 逆元と偶奇の関係： σ の分解と σ^{-1} の分解の積は $\sigma\sigma^{-1} = 1$ の分解をなす。1 は偶置換なので (1) から主張が得られる。□

(3) 偶置換・奇置換の個数：1 つの互換 σ を固定する。「左から σ をかける」操作 F_σ ($F_\sigma(x) = \sigma x$) は偶置換を奇置換に、奇置換を偶置換に変え、

$$F_\sigma : \{ \text{偶置換} \} \rightarrow \{ \text{奇置換} \}, \quad F_\sigma : \{ \text{奇置換} \} \rightarrow \{ \text{偶置換} \},$$

2 回施すと元に戻る： $F_\sigma(F_\sigma(\tau)) = \sigma^2\tau = \tau$. このことから F_σ が全単射であることがわかる。従ってそれらの個数は等しい。それぞれ $n!/2$ 個 □

(4) 位数は高々 $n!$ ：置換 σ の累乗を $n!$ 乗まで考える。 $\sigma, \sigma^2, \sigma^3, \dots, \sigma^{n!}$.
もしこの中に単位元 1 が含まれていれば終了 ($\sigma^k = 1$ なら位数は k かそれより小さい). 含まれていないとすれば S_n の元の個数は $n!$ 個なので、この中に少なくとも 1 組 $\sigma^k = \sigma^l$ ($k < l$) となる組があるはず。このとき σ^{-k} をかけて $\sigma^{l-k} = 1$ を得る。位数は $l-k$ ($< n!$) かそれより小さい。(ただしこの場合、結局 1 が含まれていないことに矛盾する。) □

3 具体例ではなく抽象的に説明できる。

(1) $\tau\sigma$ は $\sigma\tau$ の τ^{-1} による共役： $(\tau^{-1})^{-1}(\sigma\tau)\tau^{-1} = \tau\sigma(\tau\tau^{-1}) = \tau\sigma$.

(2) 共役元の位数は等しい： $(\tau^{-1}\sigma\tau)^n = \tau^{-1}\sigma\tau \cdot \tau^{-1}\sigma\tau \cdot \tau^{-1}\sigma\tau \cdots \tau^{-1}\sigma\tau = \tau^{-1}\sigma^n\tau$.
により、 $(\tau^{-1}\sigma\tau)^k = \tau^{-1}\sigma^k\tau = 1 \Leftrightarrow \sigma^k = 1$ となるため。

(3) σ が巡回置換で $\sigma(i_k) = i_{k+1}$ ($k = 1, 2, \dots, r-1$) のとき
 $\tau^{-1}\sigma\tau$ による $\tau^{-1}(i_k)$ の像は確かに

$$(\tau^{-1}\sigma\tau)(\tau^{-1}(i_k)) = (\tau^{-1}\sigma)(\tau(\tau^{-1}(i_k))) = (\tau^{-1}\sigma)(i_k) = \tau^{-1}(\sigma(i_k)) = \tau^{-1}(i_{k+1})$$

となる。 $\sigma(i_r) = i_1$ についても同様。

具体例では： σ の巡回置換への分解は $(1, 3, 4)(2, 6)$. $\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 6 & 3 \end{pmatrix}$ で写すと

$(5, 1, 4)(2, 3) = (1, 4, 5)(2, 3)$. $\tau^{-1}\sigma\tau$ の巡回置換への分解が得られる。

$$(4) [\sigma, \tau]^{-1} = (\sigma\tau\sigma^{-1}\tau^{-1})^{-1} = (\tau^{-1})^{-1}(\sigma^{-1})^{-1}\tau^{-1}\sigma^{-1} = \tau\sigma\tau^{-1}\sigma^{-1} = [\tau, \sigma].$$

$$\begin{aligned} (5) \quad [\tau^{-1}\omega\tau, \tau^{-1}\sigma\tau] &= \tau^{-1}\omega\tau \cdot \tau^{-1}\sigma\tau \cdot (\tau^{-1}\omega\tau)^{-1}(\tau^{-1}\sigma\tau)^{-1} \\ &= \tau^{-1}\omega\tau \cdot \tau^{-1}\sigma\tau \cdot \tau^{-1}\omega^{-1}\tau \cdot \tau^{-1}\sigma^{-1}\tau^{-1} \\ &= \tau^{-1}\omega\sigma\omega^{-1}\sigma^{-1}\tau^{-1} = \tau^{-1}[\omega, \sigma]\tau. \end{aligned}$$

以上