1　対称群

X を集合とする．X から X 自身への全単射を X 上の**置換**という．

定理 1.1.　X 上の置換の全体 $S(X)$ は写像の合成を積として群をなす．

証明．　σ, τ を $S(X)$ の元とする．σ, τ は単射であるから，X の二つの元 x, y に対して，

$$x \neq y \Longrightarrow \tau(x) \neq \tau(y) \Longrightarrow \sigma(\tau(x)) \neq \sigma(\tau(y)).$$

ゆえに $\sigma \circ \tau(x) \neq \sigma \circ \tau(y)$ となる．よって合成写像 $\sigma \circ \tau$ は単射である．次に，X の元 z をとれば，σ は全射であるから，$\sigma(y) = z$ となる $y \in X$ が存在する．τ も全射であるから，$\tau(x) = y$ となる $x \in X$ が存在する．よって

$$z = \sigma(y) = \sigma(\tau(x)) = \sigma \circ \tau(x)$$

となって，合成写像 $\sigma \circ \tau$ は全射になる．したがって，$\sigma \circ \tau \in S(X)$ である．

σ, τ, ρ を $S(X)$ の元とする．X の任意の元 x に対して，

$$(\sigma \circ (\tau \circ \rho))(x) = \sigma((\tau \circ \rho)(x)) = \sigma(\tau(\rho(x))),$$
$$((\sigma \circ \tau) \circ \rho)(x) = (\sigma \circ \tau)(\rho(x)) = \sigma(\tau(\rho(x))).$$

したがって，結合法則 $\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho$ が成り立つ．

X 上の恒等写像 id_X は $S(X)$ の元である．$S(X)$ の任意の元 σ と X の任意の元 x に対して，

$$(id_X \circ \sigma)(x) = id_X(\sigma(x)) = \sigma(x),$$
$$(\sigma \circ id_X)(x) = \sigma(id_X(x)) = \sigma(x).$$

すなわち，$id_X \circ \sigma = \sigma \circ id_X = \sigma$ となる．よって id_X は $S(X)$ の単位元である．

$S(X)$ の元 σ は全単射であるから，逆写像 σ^{-1} が存在する．逆写像も全単射なので，$\sigma^{-1} \in S(X)$ である．このとき，

$$\sigma \circ \sigma^{-1} = id_X, \qquad \sigma^{-1} \circ \sigma = id_X$$

であるから，σ^{-1} は σ の逆元である．

以上により，$S(X)$ が群であることが示された．　□

群 $S(X)$ を X 上の**対称群**という．対称群の部分群を**置換群**という．とくに $\Omega_n = \{1, 2, \ldots, n\}$ の上の対称群 $S(\Omega_n)$ を n 次対称群といい，S_n で表す．

以後，$S(X)$ が群であることを意識して，合成写像 $\sigma \circ \tau$ を $\sigma\tau$ と書く．また，$S(X)$ の単位元，すなわち X 上の恒等写像 id_X を 1 と書き，これを**恒等置換**という．さらに，置換 σ の逆写像 σ^{-1} を σ の**逆置換**という．

例 1.2.　$\sigma \in S_n$ がすべての $k \in \Omega_n$ に対して $\sigma(k) \leq k$ を満たすとき，$\sigma = 1$ である．

実際，$\sigma \neq 1$ とすると，$\sigma(k) \neq k$ となる $k \in \Omega_n$ が存在する．このような k の中で最小のものを k_0 とする．このとき $\sigma(k_0) > k_0$ である．なぜなら，もし $\sigma(k_0) < k_0$ ならば，

$$\sigma(\sigma(k_0)) = \sigma(k_0) \Longrightarrow \sigma(k_0) = k_0$$

となり，矛盾が生じるからである．

定理 1.3. X, Y を集合とする．このとき

$$|X| = |Y| \Longrightarrow S(X) \cong S(Y)$$

が成り立つ．

証明. $|X| = |Y|$ のとき，X から Y への全単射 f が存在する．

$$\phi : S(X) \longrightarrow S(Y), \quad \sigma \longmapsto f \circ \sigma \circ f^{-1}$$

と定義すれば，ϕ は群の同型写像である．実際,

$$\phi(\sigma_1) = \phi(\sigma_2) \Longrightarrow f \circ \sigma_1 \circ f^{-1} = f \circ \sigma_2 \circ f^{-1} \Longrightarrow \sigma_1 = \sigma_2$$

より ϕ は単射．$S(Y)$ の元 τ に対して，$\sigma = f^{-1} \circ \tau \circ f$ とおくと,

$$\phi(\sigma) = f \circ (f^{-1} \circ \tau \circ f) \circ f^{-1} = \tau.$$

よって ϕ は全射．さらに

$$\phi(\sigma_1\sigma_2) = f \circ \sigma_1\sigma_2 \circ f^{-1} = f \circ \sigma_1 \circ f^{-1} \circ f \circ \sigma_2 \circ f^{-1} = \phi(\sigma_1)\phi(\sigma_2)$$

より ϕ は準同型写像である．したがって $S(X) \cong S(Y)$. □

n 個の元からなる集合 X の上の対称群 $S(X)$ は同型を除いて一意的に定まる．とくに $S(X)$ は n 次対称群 S_n と同一視できる．

S_n の元 σ と $\Omega_n = \{1, 2, \ldots, n\}$ の元 $a_1, \ldots, a_n$ について，$\sigma(a_i) = b_i$ であるとき，σ を

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

のように表す．

例 1.4. $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}, \tau = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$ のとき,

$$\tau\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}, \qquad \sigma^{-1} = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$$

である．

例 1.5. $\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ のとき，S_n に属する任意の元 τ に対して,

$$\tau\sigma\tau^{-1} = \begin{pmatrix} \tau(a_1) & \tau(a_2) & \cdots & \tau(a_n) \\ \tau(b_1) & \tau(b_2) & \cdots & \tau(b_n) \end{pmatrix}$$

となる．なぜなら,

$$(\tau\sigma\tau^{-1})(\tau(a_i)) = \tau(\sigma(a_i)) = \tau(b_i) \qquad (1 \leq i \leq n)$$

だからである．

$m \leq n$ のとき，S_m を S_n の部分群とみなすことができる．実際，S_m の元 σ に対して，

$$\overline{\sigma}(i) = \begin{cases} \sigma(i), & 1 \leq i \leq m \\ i, & m < i \leq n \end{cases}$$

によって S_n の元 $\overline{\sigma}$ を定めると，写像

$$S_m \longrightarrow S_n, \qquad \sigma \longmapsto \overline{\sigma}$$

は単射準同型になる．

例 1.6. $n \geq 3$ のとき，n 次対称群 S_n は Abel 群ではない．実際，S_3 において，

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

ゆえに，

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

よって S_3 は Abel 群ではない．

$n \geq 4$ のとき，S_n は S_3 に同型な部分群をもつから，可換でない二つの元をもつ．

定理 1.7. n 次対称群 S_n の位数は $n!$ である．

証明. $S(X)$ の元 σ, τ に対して，関係 $\equiv$ を

$$\sigma \equiv \tau \Longleftrightarrow \sigma(n) = \tau(n)$$

によって定めると，$\equiv$ は S_n 上の同値関係になる．$1 \leq i \leq n$ である各整数 i に対して，ρ_i を

$$\rho_i(n) = i, \qquad \rho_i(i) = n, \qquad \rho_i(j) = j \ (j \neq i, j \neq n)$$

であるような S_n の元とする．このとき，関係 $\equiv$ の定義から明らかに

$$i \neq j \Longrightarrow \rho_i \not\equiv \rho_j$$

である．他方，S_n の任意の元 σ に対して，

$$\sigma(n) = i \Longrightarrow \sigma \equiv \rho_i$$

である．すなわち，σ は $\rho_1, \rho_2, \ldots, \rho_n$ のいずれか一つに同値である．ρ_i が属する $\equiv$ による同値類を C_{ρ_i} とすると，

$$S_n = C_{\rho_1} \cup \cdots \cup C_{\rho_n} \quad (\text{直和}).$$

いま，

$$H = \{\sigma \in S_n \mid \sigma(n) = n\}$$

とする．H は S_n の部分群であり，$H \cong S_{n-1}$ である．

$$\begin{aligned} \sigma \in C_{\rho_i} &\Longleftrightarrow \sigma \equiv \rho_i \Longleftrightarrow \sigma(n) = \rho_i(n) \\ &\Longleftrightarrow (\rho_i^{-1}\sigma)(n) = n \Longleftrightarrow \rho_i^{-1}\sigma \in H \\ &\Longleftrightarrow \sigma \in \rho_i H = \{\rho_i \eta \mid \eta \in H\}. \end{aligned}$$

よって $C_{\rho_i} = \rho_i H$ である．したがって，

$$S_n = \rho_1 H \cup \cdots \cup \rho_n H \quad (\text{直和}).$$

さらに，各 i に対して，

$$H \longrightarrow \rho_i H, \qquad \eta \longmapsto \rho_i \eta$$

は全単射である．ゆえに，

$$|\rho_1 H| = |\rho_2 H| = \cdots = |\rho_n H| = |H|.$$

したがって，

$$|S_n| = |\rho_1 H| + |\rho_2 H| + \cdots + |\rho_n H| = n|H| = n|S_{n-1}|.$$

S_1 の元は，一つの元からなる集合 $\{1\}$ の上の全単射である．そのような全単射はただ一つしかない．よって S_1 はただ一つの元からなる．すなわち $|S_1| = 1$.

以上より，n に関する数学的帰納法によって，$|S_n| = n!$ が得られる． □

系 1.7.1. X を有限集合とし，$|X| = n$ とする．このとき，対称群 $S(X)$ の位数は $n!$ である．

証明. 定理 1.3 と定理 1.7 によりわかる． □

定理 1.8. X, Y を有限集合とする．このとき

$$|X| = |Y| \Longleftrightarrow S(X) \cong S(Y)$$

が成り立つ．

証明. $\Longrightarrow$ は定理 1.3 より明らか．

逆に，$|X| = n$ のとき $S(X) = n!$ であるから，$|X| \neq |Y|$ ならば $|S(X)| \neq |S(Y)|$．よって

$$S(X) \cong S(Y) \Longrightarrow |S(X)| = |S(Y)| \Longrightarrow |X| = |Y|$$

である． □

定理 1.9 (Cayley). 任意の群 G は対称群 $S(G)$ のある部分群に同型である．

証明. G の任意の元 g に対して

$$\pi_g : G \longrightarrow G, \qquad x \longmapsto gx$$

は全単射である．そこで写像

$$\pi : G \longrightarrow S(G), \qquad g \longmapsto \pi_g$$

を考える．π は群の単射準同型写像である．実際，G の元 g, h に対して

$$\pi_h \circ \pi_h(x) = \pi_h(gx) = hgx = \pi_{hg}(x) \qquad (\forall x \in G)$$

ゆえ，π は準同型写像である．また

$$\pi_g = \mathrm{id}_G \Longrightarrow gx = x (\forall x \in G) \Longrightarrow g = e$$

より π は単射である．したがって群 G は対称群 $S(G)$ のある部分群に同型である． □

注意 1.10. 定理 1.9 の証明において構成した同型写像 $\pi : G \longrightarrow S(G)$ は，G の**左正則表現**と呼ばれる．

系 1.10.1. 自然数 n に対して，位数 n の有限群は同型なものを除けば有限個しかない．

証明. G を位数 n の有限群とする．定理 1.9 より G は $S(G)$ のある部分群に同型である．一方，1.3 によって $S(G) \cong S_n$ であるから，G は S_n のある部分群に同型である．S_n は有限群であるから，部分集合の全体 $\mathfrak{P}(S_n)$ は有限である．したがって同型なものを除けば位数 n の有限群は有限個しかない． □

2 巡回置換と互換

相異なる数字 $i_1, \ldots i_r \in X$ に対して，巡回的に

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \ldots, \quad \sigma(i_r) = i_1$$

となり，$i_1, \ldots, i_r$ 以外の数字を固定する置換を長さ r の**巡回置換**といい，$(i_1\ i_2\ \cdots\ i_r)$ で表す．とくに長さ 2 の巡回置換 $(i_1\ i_2)$ を**互換**という．置換 σ について，σ が長さ 1 の巡回置換であることと，恒等置換であることとは同値である．

$\sigma = (i_1\ i_2\ \cdots\ i_r)$ を長さ r の巡回置換とする．明らかに $\sigma^r = 1$ である．また，$1 \leq k < r$ であるような任意の整数 k に対しては，

$$\sigma^k(i_1) = i_k \neq i_1 \Longrightarrow \sigma^k \neq 1$$

である．したがって，長さ r の巡回置換 σ の位数は r である．

また，巡回置換の定義から明らかに，$i_1, i_2, \ldots, i_r$ をひとつずつずらした巡回置換

$$(i_2\ \cdots\ i_r\ i_1), \quad (i_3\ \cdots\ i_r\ i_1\ i_2), \quad \ldots, \quad (i_r\ i_1\ \cdots\ i_{r-1})$$

はすべて σ に等しい．一方，$1 < r \leq n$ のとき，n 個の数 $1, 2, \ldots, n$ の中から r 個の数 $i_1, i_2, \ldots, i_r$ を選ぶ仕方は $\dfrac{n!}{(n-r)!}$ 通りである．したがって，S_n に属する長さ r の巡回置換は全部で $\dfrac{1}{r}\dfrac{n!}{(n-r)!}$ 個ある．

例 2.1. $\sigma = (1\ 2\ 3)$, $\tau = (1\ 2)$ とする．積 $\sigma\tau$ による 1, 2, 3 の像はそれぞれ，

$$1 \overset{\tau}{\longmapsto} 2 \overset{\sigma}{\longmapsto} 3,$$
$$2 \overset{\tau}{\longmapsto} 1 \overset{\sigma}{\longmapsto} 2,$$
$$3 \overset{\tau}{\longmapsto} 3 \overset{\sigma}{\longmapsto} 1$$

であるから，$\sigma\tau = (1\ 3)$.

定理 2.2. $\sigma = (i_1\ i_2\ \cdots\ i_r)$ を巡回置換とするとき，$\sigma^{-1} = (i_r\ i_{r-1}\ \cdots\ i_1)$ である．とくに，σ が互換ならば，$\sigma^{-1} = \sigma$ である．

証明. $\tau = (i_r\ i_{r-1}\ \cdots\ i_1)$ とおくと，

$$\sigma\tau(i_k) = \sigma(i_{k-1}) = i_k \qquad (2 \leq k \leq r),$$
$$\sigma\tau(i_1) = \sigma(i_r) = i_1.$$

ゆえに $\sigma\tau = 1$．したがって $\tau = \sigma^{-1}$. □

定理 2.3. S_n の元 σ と巡回置換 $(i_1\ i_2\ \cdots\ i_r)$ に対して，

$$\sigma(i_1\ i_2\ \cdots\ i_r)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_r))$$

が成り立つ．

証明． $\tau = (i_1\ i_2\ \cdots\ i_r)$ とおくと，

$$\begin{aligned}&\sigma\tau\sigma^{-1}(\sigma(i_k)) = \sigma\tau(i_k) = \sigma(i_{k+1}) \quad (1 \le k \le r-1),\\ &\sigma\tau\sigma^{-1}(\sigma(i_r)) = \sigma\tau(i_r) = \sigma(i_1)\end{aligned}$$

であるから，

$$\sigma\tau\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_r))$$

となる． □

定理 2.4. 任意の巡回置換は，いくつかの互換の積で表される．

証明． まず，

$$(i_1\ i_2\ \cdots\ i_r) = (i_1\ i_r)(i_1\ i_2\ \cdots\ i_{r-1})$$

を示す．$\sigma = (i_1\ i_r)$, $\tau = (i_1\ i_2\ \cdots\ i_{r-1})$ とすると，

$$\begin{aligned}&\sigma\tau(i_k) = \sigma(i_{k+1}) = i_{k+1} \qquad (1 \le k \le r-2),\\ &\sigma\tau(i_{r-1}) = \sigma(i_1) = i_r,\\ &\sigma\tau(i_r) = \sigma(i_r) = i_1.\end{aligned}$$

よって，$\sigma\tau = (i_1\ i_2\ \cdots\ i_r)$ である．
したがって，

$$\begin{aligned}(i_1\ i_2\ \cdots\ i_n) &= (i_1\ i_r)(i_1\ i_2\ \cdots\ i_{r-1})\\ &= (i_1\ i_r)(i_1\ i_{r-1})(i_1\ i_2\ \cdots\ i_{r-2})\\ &= \cdots\cdots\\ &= (i_1\ i_r)(i_1\ i_{r-1})\cdots(i_1\ i_2)\end{aligned}$$

となる． □

注意 2.5. 巡回置換を互換の積として表す仕方は一通りではない．例えば，

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 3)(2\ 3)(1\ 2)(1\ 3)$$

となる．

巡回置換 $\sigma = (i_1\ i_2\ \cdots\ i_r)$ に対して，集合 $\{i_1, i_2, \ldots, i_r\}$ を σ の**巡回域**という．σ の巡回域の中にある元の一つを i とすれば，明らかに，

$$\sigma = (i\ \sigma(i)\ \sigma^2(i)\ \cdots\ \sigma^{r-1}(i))$$

と書くことができる．

例 2.6. 巡回置換 $\sigma = (i_1\ i_2\ \cdots\ i_r)$ に対して，$\sigma^{-1} = (i_r\ i_{r-1}\ \cdots\ i_1)$ なので，σ の巡回域と σ^{-1} の巡回域とは一致する．

二つの巡回置換 σ, τ について，それらの巡回域が共通部分をもたないとき，σ, τ は**互いに素**であるという．

例 2.7. 二つの巡回置換 σ, τ が互いに素ならば，任意の置換 ρ に対して，$\rho\sigma\rho^{-1}, \rho\tau\rho^{-1}$ は互いに素な二つの巡回置換である．

定理 2.8. 互いに素な二つの巡回置換は可換である．

証明. $\Omega_n = \{1, 2, \ldots, n\}$ とし，σ, τ を Ω_n 上の巡回置換，A_σ, A_τ を σ, τ の巡回域とする．A_σ, A_τ は Ω_n の部分集合であって，$A_\sigma \cap A_\tau = \phi$ である．したがって，Ω_n の元 i について，

$$\text{(i)}\quad i \in A_\sigma \qquad \text{(ii)}\quad i \in A_\tau \qquad \text{(iii)}\quad i \notin A_\sigma \text{ かつ } i \notin A_\tau$$

の 3 通りが考えられる．

(i) の場合，

$$\begin{aligned} i \in A_\sigma &\Longrightarrow i \notin A_\tau,\ \sigma(i) \notin A_\tau \\ &\Longrightarrow \tau(i) = i,\ \sigma(\tau(i)) = \sigma(i),\ \tau(\sigma(i)) = \sigma(i) \\ &\Longrightarrow \sigma\tau(i) = \tau\sigma(i). \end{aligned}$$

(ii) の場合，

$$\begin{aligned} i \in A_\tau &\Longrightarrow i \notin A_\sigma,\ \tau(i) \notin A_\sigma \\ &\Longrightarrow \sigma(i) = i,\ \tau(\sigma(i)) = \tau(i),\ \sigma(\tau(i)) = \tau(i) \\ &\Longrightarrow \sigma\tau(i) = \tau\sigma(i). \end{aligned}$$

(iii) の場合，

$$\begin{aligned} i \notin A_\sigma \text{ かつ } i \notin A_\tau &\Longrightarrow \sigma(i) = \tau(i) = i \\ &\Longrightarrow \sigma\tau(i) = \tau\sigma(i) = i. \end{aligned}$$

以上より，Ω_n のすべての i について，$\sigma\tau(i) = \tau\sigma(i)$ がいえた．よって $\sigma\tau = \tau\sigma$. □

$\Omega_n = \{1, 2, \ldots, n\}$ とし，σ を Ω_n 上の置換とする．Ω_n の元 x, y に対して，関係 $\sim$ を

$$x \sim y \Longleftrightarrow \sigma^k(x) = y \text{ となるような整数 } k \text{ が存在する}$$

と定義すれば，$\sim$ は Ω_n の上の同値関係である．ただし，$\sigma^0 = 1$ とする．$\sim$ による Ω_n の各同値類を，置換 σ に関する**推移類**という．

x を Ω_n の元とする．x を代表元とする置換 σ の推移類を T_x とするとき，

$$T_x = \{\sigma^k(x) \mid k \in \mathbb{Z}\}$$

と表される．とくに，

$$\sigma(x) = x \Longleftrightarrow T_x = \{x\}$$

が成り立つ．

例 2.9. Ω_n 上の恒等写像 1 に関する推移類はすべてただ一つの元からなる集合である.

例 2.10. 長さ 2 以上の巡回置換 σ に関する推移類で，二つ以上の元をもつものはただ一つしかない．それは σ の巡回域である.

例 2.11. σ, τ を長さ 2 以上の巡回置換であるとし，σ, τ は互いに素であるとする．このとき積 $\sigma\tau$ に関する推移類で，二つ以上の元をもつものは σ の巡回域と τ の巡回域しかない.

定理 2.12. 任意の置換 $\sigma \neq 1$ は，二つずつ互いに素な長さ 2 以上の巡回置換の積として，積の順序を除いて一意的に表される.

証明. $\Omega_n = \{1, 2, \ldots, n\}$ とし，x を Ω の元とする．Ω_n は有限集合だから，$\sigma^r(x) = x$ となるような最小の正の整数 r が存在する．このとき，x を代表元とする σ に関する推移類 T_x は

$$T_x = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^{r-1}(x)\}$$

と表される．いま，σ に関する異なる推移類の全体を $T_1, T_2, \ldots, T_l$ とし，それらの個数をそれぞれ $r_1, r_2, \ldots, r_l$ $(r_1 + r_2 + \cdots + r_l = n)$ とする．また，各推移類 T_i から代表元 x_i をとって，長さ r_i の巡回置換

$$\sigma_i = (\, x_i \;\; \sigma(x_i) \; \sigma^2(x_i) \;\; \cdots \;\; \sigma^{r_i-1}(x_i))$$

を作る．このとき，各推移類 T_j と各 σ_i に対して,

$$x \in T_j \Longrightarrow \sigma(x) = \begin{cases} \sigma(x), & i = j \\ x, & i \neq j \end{cases}$$

となる．したがって各 T_j に対して,

$$\sigma_1 \cdots \sigma_l(x) = \sigma_j(x) = \sigma(x) \qquad (\forall x \in T_j)$$

がいえる．$\Omega_n = T_1 \cup \cdots \cup T_l$ であるから,

$$\sigma_1 \cdots \sigma_l(x) = \sigma(x) \qquad (\forall x \in \Omega_n).$$

ゆえに $\sigma = \sigma_1 \cdots \sigma_l$ がいえた.

各 σ_i の巡回域は T_i である．各 T_i は互いに交わらないから，各 σ_i は二つずつ互いに素である．σ_i の中に長さ 1 の巡回置換，すなわち Ω_n 上の恒等写像が含まれているならば，それらをすべて取り除いた積を考えればよい.

一意性を示すために,

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_l = \tau_1\tau_2 \cdots \tau_m$$

のように，二つずつ互いに素な長さ 2 の巡回置換の積として，二通りに表されているとする．$l \leq m$ と仮定しても一般性を失わない.

σ_1 の巡回域に属する元 x に対して，$\tau_1, \tau_2, \ldots, \tau_m$ の中で，巡回域に x をもつものが必ずある．もしそうでなければ，σ_i, τ_j がすべて長さ 2 以上の巡回置換であるという仮定から，二つの積による x の像は互いに異なるものとなって矛盾が生じる.

互いに素な二つの巡回置換は可換なので，適当に番号を並べかえて τ_1 の巡回域に x が属するとしてよい．このとき $\sigma_1 = \tau_1$ である．なぜなら，もし $\sigma_1 \neq \tau_1$ とすると，$\sigma_1^k(x) \neq \tau_1^k(x)$ なる最小の正の整数 k が存在する．よって

$$\sigma_1^{k-1}(x) = \tau_1^{k-1}(x) \quad \text{かつ} \quad \sigma(\sigma_1^{k-1}(x)) \neq \sigma(\tau_1^{k-1}(x))$$

となって矛盾が生じる．したがって $\sigma_1 = \tau_1$ となって，

$$\sigma_2 \cdots \sigma_l = \tau_2 \cdots \tau_m.$$

同様にして，$\sigma_2 = \tau_2$, $\sigma_3 = \tau_3$, …, $\sigma_l = \tau_l$ がいえる．$l = m$ ならば証明が終わる．

いま，$l < m$ と仮定する．$m = l+1$ のときは $\tau_{l+1} = 1$ となって，τ_{l+1} が長さ 2 以上の巡回置換であるという仮定に矛盾する．$m > l+1$ のとき，

$$1 = \tau_{l+1} \cdots \tau_m \Longrightarrow \tau_m^{-1} = \tau_{l+1} \cdots \tau_{m-1}.$$

τ_m^{-1} も長さ 2 以上の巡回置換だから，上と同様の議論により，$\tau_m^{-1} = \tau_{l+1}$ を得る．ところが τ_m と τ_m^{-1} の巡回域は一致する．このことは τ_m と τ_{l+1} が互いに素であるという仮定に反する．よって一意性が示された． □

注意 2.13. 定理 2.12 の主張の中にある，因子となる巡回置換の長さが 2 以上であるという条件は，

$$(3\ 4\ 5) = (1)(3\ 4\ 5) = (1)(2)(3\ 4\ 5)$$

などの場合を除外するためのものである．

置換 σ が，二つずつ互いに素であるようないくつかの巡回置換 σ_1, σ_2, …, σ_r によって $\sigma = \sigma_1\sigma_2 \cdots \sigma_r$ と表されているとき，各巡回置換 σ_i を σ の**巡回因子**と呼ぶ．

例 2.14. 置換 σ が，二つずつ互いに素であるようないくつかの巡回置換 σ_1, σ_2, …, σ_r によって

$$\sigma = \sigma_1\sigma_2 \cdots \sigma_r$$

と表されているとき，任意の置換 ρ に対して，

$$\rho\sigma\rho^{-1} = (\rho\sigma_1\rho^{-1})(\rho\sigma_2\rho^{-1}) \cdots (\rho\sigma_r\rho^{-1})$$

となる．また，各 $\rho\sigma_i\rho^{-1}$ は二つずつ互いに素である (例 2.7)．したがって各 $\rho\sigma_i\rho^{-1}$ は $\rho\sigma\rho^{-1}$ の巡回因子である．

定理 2.15. n 次対称群 S_n は互換の全体で生成される．すなわち，S_n の任意の元は，いくつかの互換の積で表される．

証明. S_n の任意の元はいくつかの巡回置換の積で表される (定理 2.12)．また，任意の巡回置換はいくつかの互換の積で表される (定理 2.4)．ゆえに S_n の任意の元は，いくつかの互換の積で表される． □

系 2.15.1. $n \geq 2$ のとき，n 次対称群 S_n は互換

$$(1\ 2), \quad (1\ 3), \quad \ldots, \quad (1\ n)$$

によって生成される．

証明. $i \neq 1, j \neq 1$ を満たすような異なる数 i, j に対して，

$$(i\ j) = (1\ i)(1\ j)(1\ i)$$

となる．よって，すべての互換は $(1\ k)$ の形の互換の積で表される． □

系 2.15.2. $n \geq 2$ のとき，n 次対称群 S_n は互換

$$(1\ 2),\quad (2\ 3),\quad \ldots,\quad (n-1\ n)$$

によって生成される．

証明. $\tau_i = (i\ i+1)\,(i = 1, 2, \ldots, n-1)$ で生成される S_n の部分群を H とする．

$$\tau_2(1\ 2)\tau_2^{-1} = (1\ 3),\quad \tau_3(1\ 3)\tau_3^{-1} = (1\ 4),\quad \ldots,\quad \tau_{n-1}(1\ n-1)\tau_{n-1}^{-1} = (1\ n)$$

であるから，H は $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$ を含む．したがって $H = S_n$. □

系 2.15.3. $n \geq 3$ のとき，S_n は互換 $(1\ 2)$ と長さ n の巡回置換 $(1\ 2\ \ldots\ n)$ とで生成される．

証明. $\sigma = (1\ 2\ \ldots\ n)$, $\tau = (1\ 2)$ とし，σ, τ で生成される S_n の部分群を H とする．

$$\sigma\tau\sigma^{-1} = (2\ 3),\quad \sigma^2\tau\sigma^{-2} = (3\ 4),\quad \ldots,\quad \sigma^{n-2}\tau\sigma^{-(n-2)} = (n-1\ n)$$

であるから，H は $(1\ 2)$, $(2\ 3)$, …, $(n-1\ n)$ を含む．したがって $H = S_n$. □

系 2.15.4. S_n は $(1\ 2)$ と $(2\ 3\ \cdots\ n)$ により生成される．

証明. $\sigma = (1\ 2)$, $\tau = (2\ 3\ \cdots\ n)$ で生成される S_n の部分群を H とすれば，

$$\tau\sigma\tau^{-1} = (1\ 3),\quad \tau^2\sigma\tau^{-2} = (1\ 4),\quad \ldots,\quad \rho^{n-2}\sigma\rho^{-(n-2)} = (1\ n)$$

であるから，H は $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$ を含む．したがって $H = S_n$. □

定理 2.16. p を素数とする．p 次対称群 S_p の部分群 H が一つの互換と一つの長さ p の巡回置換を含めば，$H = S_p$ である．

証明. H に含まれる互換を $(i_1\ \ i_2)$ とし，長さ p の巡回置換を $\tau = (j_1\ \ j_2\ \ \cdots\ \ j_p)$ とする．$j_1, j_2, \ldots, j_p$ の中に i_1 が必ずあるから，$j_1 = i_1$ としても一般性を失わない．p は素数だから，τ, τ^2, …, τ^{p-1} の中に必ず $(i_1\ i_2\ k_3\ \cdots\ k_p)$ なる形の巡回置換がある．$(1\ 2)$ と $(1\ 2\ \cdots\ p)$ が S_p を生成するのと同じように，$(i_1\ i_2)$ と $(i_1\ i_2\ k_3\ \cdots\ k_p)$ も S_p を生成する．よって $H = S_p$. □

定理 2.17. S_n の元が互換の積で表されているとき，互換の個数が偶数であるか奇数であるかは，与えられた元によって一意的に決まる．

証明. ある置換が同時に偶数個の互換の積と奇数個の互換の積で表されたとすると，単位元が奇数個の互換の積で表される．そこで単位元が奇数個の互換の積で表されないことを証明する．単位元を奇数個の互換の積で表す最小の奇数を k とおき

$$1 = (i_1\ j_1)(i_2\ j_2)\cdots(i_k\ j_k)$$

が成り立っているとする．さて，互換 $(i\ j)$ と他の互換との積は次のように計算することができる．ここで i, j, a, b は相異なる数字である：

$$\begin{aligned}
&(i\ j)(a\ b) = (a\ b)(i\ j),\\
&(i\ j)(i\ j) = 1,\\
&(i\ j)(i\ a) = (j\ a)(i\ j),\\
&(i\ j)(j\ a) = (j\ a)(i\ a)
\end{aligned}$$

k の取り方から，$(i_1\ j_1) = (i_2\ j_2)$ とはならない．もしそうならば単位元が k 個より少ない奇数個の互換で表される．したがって $(i_1\ j_1)$ と $(i_2\ j_2)$ との積は i_1 が右側の互換のみに含まれる互換の積に置きかえられる．この操作を高々有限回繰り返せば，i_1 を順次右側の互換に移し，最終的に i_1 が一番右側の互換のみに現れるようにすることができる．このような互換の積は i_1 を i_1 に写さないので単位元ではない．よって矛盾． □

偶数個の互換の積で表される置換を**偶置換**，奇数個の互換の積で表される置換を**偶置換**という．

定理 2.18. $n \geq 2$ のとき，S_n の中にある偶置換と奇置換の個数は共にそれぞれ $n!/2$ 個である．

証明. 偶置換全体の集合を A，奇置換全体の集合を B とする．σ を偶置換とすれば，$(1\ 2)\sigma$ は奇置換になる．よって，写像

$$A \longrightarrow B, \qquad \sigma \longmapsto (1\ 2)\sigma$$

が定義できる．A の元 σ, σ' に対して，

$$(1\ 2)\sigma = (1\ 2)\sigma' \Longrightarrow \sigma = \sigma'$$

であるから，上の写像は単射である．ゆえに $|A| \leq |B|$ である．逆に，τ を奇置換とすれば $(1\ 2)\tau$ は偶置換であるから，同じ理由によって $|B| \leq |A|$ がいえる．したがって $|A| = |B|$ である．定理 2.17 より，

$$S_n = A \cup B, \quad A \cap B = \phi, \quad |S_n| = n!$$

だから，

$$n! = |S_n| = |A| + |B|.$$

よって $|A| = |B| = n!/2$ となる． □

3 符号

$n \geq 2$ とする．n 次対称群 S_n の元 σ に対して，

$$\mathrm{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

を σ の**符号**という．

例 3.1. 恒等置換 1 の符号は

$$\mathrm{sgn}(1) = \prod_{1 \leq i < j \leq n} \frac{i - j}{i - j} = 1.$$

例 3.2. $\sigma = (1\ 3)$ の符号は

$$\mathrm{sgn}(\sigma) = \frac{3-2}{1-2}\frac{3-1}{1-3}\frac{2-1}{2-3} = -1.$$

例 3.3. $\sigma = (1\ 4\ 2)$ の符号は

$$\mathrm{sgn}(\sigma) = \frac{4-1}{1-2}\frac{4-3}{1-3}\frac{4-2}{1-4}\frac{1-3}{2-3}\frac{1-2}{2-4}\frac{3-2}{3-4} = 1.$$

定理 3.4. $n \geq 2$ とする．n 次対称群 S_n の任意の元 σ に対して，$\mathrm{sgn}(\sigma) = 1$ または $\mathrm{sgn}(\sigma) = -1$ である．

証明. $i \neq j$ なる $i, j \in \Omega_n$ に対して，

$$a(i, j) = \frac{\sigma(i) - \sigma(j)}{i - j}$$

とおく．$a(i, j) = a(j, i)$ であるから，

$$\begin{aligned}\mathrm{sgn}(\sigma)^2 &= \prod_{i<j} a(i, j) \prod_{i<j} a(i, j) = \prod_{i<j} a(i, j) \prod_{i<j} a(j, i) \\ &= \prod_{i<j} a(i, j) \prod_{j<i} a(i, j) = \prod_{i \neq j} a(i, j).\end{aligned}$$

$i \neq j$ となる $i, j \in \Omega_n$ の組 (i, j) の全体を A とする．σ は Ω_n 上の置換であるから，(i, j) が A 全体を動くとき，$(\sigma(i), \sigma(j))$ も A 全体を動く．したがって，

$$\prod_{i \neq j} a(i, j) = \frac{\displaystyle\prod_{i \neq j} (\sigma(i) - \sigma(j))}{\displaystyle\prod_{i \neq j} (i - j)} = \frac{\displaystyle\prod_{i \neq j} (i - j)}{\displaystyle\prod_{i \neq j} (i - j)} = 1.$$

ゆえに，$\mathrm{sgn}(\sigma)^2 = 1$．よって $\mathrm{sgn}(\sigma) = \pm 1$. □

定理 3.5. sgn は S_n から乗法群 $\mathbb{U}_2 = \{\pm 1\}$ への準同型写像である．

証明. S_n の元 σ, τ に対して，

$$\begin{aligned}\mathrm{sgn}(\sigma\tau) &= \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} \\ &= \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \cdot \frac{\tau(i) - \tau(j)}{i - j} \\ &= \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j}.\end{aligned}$$

第一項について，τ は $\Omega_n = \{1, 2, \ldots, n\}$ 上の置換なので，

$$\begin{aligned}\prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} &= \prod_{\substack{i<j \\ \tau(i)<\tau(j)}} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \prod_{\substack{i<j \\ \tau(i)>\tau(j)}} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \\ &= \prod_{\substack{i<j \\ \tau(i)<\tau(j)}} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \prod_{\substack{j>i \\ \tau(j)<\tau(i)}} \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)} \\ &= \prod_{\substack{i<j \\ \tau(i)<\tau(j)}} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \prod_{\substack{i>j \\ \tau(i)<\tau(j)}} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \\ &= \prod_{\tau(i)<\tau(j)} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} \\ &= \mathrm{sgn}(\sigma).\end{aligned}$$

第二項について，符号の定義から

$$\prod_{i<j} \frac{\tau(i)-\tau(j)}{i-j} = \mathrm{sgn}(\tau).$$

したがって，

$$\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).$$

□

例 3.6. 任意の置換 σ に対して，$\mathrm{sgn}(\sigma^{-1}) = \mathrm{sgn}(\sigma)$ である．実際，

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

ゆえに，$\mathrm{sgn}(\sigma) = \pm 1$ より，

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

定理 3.7. 任意の互換 τ に対して，$\mathrm{sgn}(\tau) = -1$.

証明. まず，$\tau_0 = (1\ 2)$ について，

$$\begin{aligned}
&\frac{\tau_0(1)-\tau_0(2)}{1-2} = \frac{2-1}{1-2} = -1 < 0,\\
&\frac{\tau_0(1)-\tau_0(j)}{1-j} = \frac{2-j}{1-j} > 0 \qquad (j \geq 3),\\
&\frac{\tau_0(2)-\tau_0(j)}{2-j} = \frac{1-j}{2-j} > 0 \qquad (j \geq 3)
\end{aligned}$$

であるから，

$$\mathrm{sgn}(\tau_0) = \frac{\tau_0(1)-\tau_0(2)}{1-2} \prod_{\substack{i<j\\(i,j)\neq(1,2)}} \frac{\tau_0(i)-\tau_0(j)}{i-j} < 0.$$

よって $\mathrm{sgn}(\tau_0) = -1$ である．

一般の互換 $\tau = (k\ l) \neq (1\ 2)$, $k < l$ に対しては，

$$\sigma = \begin{cases} (1\ k)(2\ l), & k \neq 1 \text{ のとき}\\ (2\ l), & k = 1 \text{ のとき}\end{cases}$$

とすると，

$$\tau = \sigma\tau_0\sigma^{-1}$$

であるから，sgn の準同型性によって，

$$\mathrm{sgn}(\tau) = \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau_0)\mathrm{sgn}(\sigma^{-1}) = -\mathrm{sgn}(\sigma)^2 = -1$$

が得られる．

□

置換 $\sigma \in S_n$ の符号 $\mathrm{sgn}(\sigma)$ について，明らかに，

$$\mathrm{sgn}(\sigma) = \begin{cases} 1, & \sigma \text{ が偶置換のとき}\\ -1, & \sigma \text{ が奇置換のとき}\end{cases}$$

が成り立つ．

注意 3.8. 定理 2.17 を，符号 sgn を用いて証明すると次のようになる．

ある置換が同時に偶数個の互換の積と奇数個の互換の積で表されたとすると，S_n の単位元 1 が奇数個の互換 $\sigma_1, \ldots, \sigma_l$ (l は奇数) の積で表される．ところが，

$$\mathrm{sgn}(1) = \mathrm{sgn}(\sigma_1 \cdots \sigma_l) = \mathrm{sgn}(\sigma_1) \cdots \mathrm{sgn}(\sigma_l) = (-1)^l = -1$$

となって矛盾が生じる．

定理 3.9. 長さ r の巡回置換 $\sigma = (i_1\ i_2\ \ldots\ i_r)$ の符号は $\mathrm{sgn}(\sigma) = (-1)^{r-1}$ である．

証明. $(i_1\ i_2\ \ldots\ i_r) = (i_1\ i_r)(i_1\ i_{r-1}) \cdots (i_1\ i_2)$ のように，σ は $r-1$ 個の互換の積で表される．よって，$\mathrm{sgn}(\sigma) = (-1)^{r-1}$ である． □

S_n の元 σ に対して，

$$i < j \quad \text{かつ} \quad \sigma(i) > \sigma(j)$$

となるような，Ω_n の元の組 (i, j) の個数を σ の**反転数**という．

注意 3.10. 置換 σ の反転数が偶数であるか奇数であるかによって値 ± 1 を定めたものが符号 $\mathrm{sgn}(\sigma)$ である．

例 3.11. 恒等置換の反転数は 0 である．

例 3.12. $k < l$ のとき，互換 $(k\ l)$ の反転数は $2(l-k)-1$ である．実際，$\sigma = (k\ l)$ とおく．$i < j$ なる $i, j \in \Omega_n$ に対して，$\sigma(i) > \sigma(j)$ となるのは次の場合である：

(i) $i = k$, $k < j < l$ のとき ($l-k-1$ 通り).

(ii) $i = k$, $j = l$ のとき (1 通り).

(iii) $k < i < l$, $j = l$ のとき ($l-k-1$ 通り).

とくに，$(k\ k+1)$ の形の互換の反転数は 1 である．

定理 3.13. 反転数 l の置換 σ は l 個の $(k\ k+1)$ の形の互換の積として表される．

証明. n に関する数学的帰納法により証明する．

$n = 2$ のとき，S_2 の元は 1 と互換 $(1\ 2)$ だけである．この場合に主張が正しいことは容易に確かめられる．

$n-1$ のとき主張が正しいと仮定する．σ を S_n の元とし，$\sigma(\tau) = n$ とする．$t = n$ ならば，$\sigma \in S_{n-1}$ とみなせるからよい．以下，$t < n$ とし，

$$\tau = \sigma(t\ t+1)(t+1\ t+2) \cdots (n-1\ n)$$

とおく．このとき，

$$\tau(n) = \sigma(t) = n$$

であるから，$\tau \in S_{n-1}$ とみなすことができる．したがって，

$$(\tau \text{ の反転数}) = (\sigma \text{ の反転数}) - (n-t)$$

を示せばよい．そうすれば τ は $l-(n-t)$ 個の $(k\ k+1)$ の形の互換の積として表されて，

$$\sigma = \tau(n-1\ \ n)\cdots(t+1\ \ t+2)(t\ \ t+1)$$

より，σ は l 個の $(k\ k+1)$ の形の互換の積として表される．

i, j を Ω_n の元とし，$i<j$ とする．

(i)　$i<j<t$ のとき，τ の定め方から，$\tau(i)=\sigma(i)$, $\tau(j)=\sigma(j)$ であるから，

$$\tau(i)>\tau(j) \Longleftrightarrow \sigma(i)>\sigma(j).$$

(ii)　$i<t\leq j<n$ のとき，$\tau(i)=\sigma(i)$, $\tau(j)=\sigma(j+1)$ であるから，

$$\tau(i)>\tau(j) \Longleftrightarrow \sigma(i)>\sigma(j+1).$$

(iii)　$t\leq i<j<n$ のとき，$\tau(i)=\sigma(i+1)$, $\tau(j)=\sigma(j+1)$ であるから，

$$\tau(i)>\tau(j) \Longleftrightarrow \sigma(i+1)>\sigma(j+1).$$

(iv)　$j=n$ のとき，常に

$$\tau(i)<\tau(n)=n.$$

以上より，τ の反転数は，$i=t$ または $j=t$ 以外の場合において，$\sigma(i)>\sigma(j)$ となるような (i, j) の個数に等しい．ところが，$\sigma(t)=n$ なので，$j=t$ のときは常に $\sigma(i)<\sigma(j)$ であり，$i=t$ のときは常に $\sigma(i)>\sigma(j)$ である．後者の条件を満たす (i, j) の個数は $t<j\leq n$ なる j の個数，すなわち $n-t$ に等しい．□

例 3.14.　$i<j$ とし，$k=j-i$ とする．互換 $(i\ j)$ について

$$(i\ j)=(i\ \ i+1)(i+1\ \ i+2)\cdots(i+k-2\ \ i+k-1)(i+k-1\ \ i+k)$$
$$(i+k-2\ \ i+k-1)\cdots(i+1\ \ i+2)(i\ \ i+1)$$

が成り立つ．右辺は $2k-1$ 個の積である．

例 3.15.　$\sigma=(1\ 3)(2\ 4)$ の反転数は 4 である．また，

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

と表すことができる．

4　交代群

偶置換全体のなす S_n の部分群を n 次**交代群**といい，A_n で表す．

定理 4.1.　交代群 A_n は対称群 S_n の指数 2 の正規部分群である．

証明. $\mathbb{U}_2 = \{\pm 1\}$ を乗法群とする．準同型写像

$$S_n \longrightarrow \mathbb{U}_2, \qquad \sigma \longmapsto \mathrm{sgn}(\sigma)$$

の核は A_n である．ゆえに A_n は S_n の正規部分群である．さらに準同型定理により

$$S_n/A_n \cong \mathbb{U}_2$$

である．よって $(S_n : A_n) = 2$. □

定理 4.2. $n \geq 3$ のとき，n 次交代群 A_n は長さ 3 のすべての巡回置換で生成される．

証明. 異なる互換の積は次のように計算される．ここで，i, j, a, b は相異なる数字である：

$$(i\ j)(a\ b) = (i\ b\ a)(i\ j\ a), \qquad (i\ j)(i\ a) = (j\ i\ a).$$

交代群 A_n の元はすべて偶数個の互換の積で表される．したがって，任意の偶置換は長さ 3 の巡回置換の積で表される． □

系 4.2.1. $n \geq 3$ のとき，交代群 A_n は

$$(1\ 2\ 3), \quad (1\ 2\ 4), \quad \ldots, \quad (1\ 2\ n)$$

によって生成される．

証明. A_n は長さ 3 の巡回置換の全体で生成される．よって，長さ 3 の巡回置換が $(1\ 2\ l)$ の形の巡回置換の積で表されることを証明すればよい．

まず，$i \geq 3$ に対して，

$$(2\ 1\ i) = (1\ 2\ i)^2$$

である．次に，$i \geq 3, j \geq 3$ を満たすような異なる数 i, j に対して，

$$\begin{aligned}(1\ i\ j) &= (1\ 2\ j)^2(1\ 2\ i)(1\ 2\ j),\\ (2\ i\ j) &= (1\ 2\ j)^2(1\ 2\ i)\end{aligned}$$

となる．最後に，$i \geq 3, j \geq 3, k \geq 3$ を満たすような異なる i, j, k に対して，

$$\begin{aligned}(i\ j\ k) &= (1\ i\ j)(1\ j\ k)\\ &= (1\ 2\ j)^2(1\ 2\ i)(1\ 2\ j)(1\ 2\ k)^2(1\ 2\ j)(1\ 2\ k)\end{aligned}$$

となる．以上より，長さ 3 の巡回置換はすべて $(1\ 2\ l)$ の形の巡回置換の積で表される． □

例 4.3. 3 次の対称群 S_3 の元は次の 6 個である：

(i) 恒等置換 (1 個)

(ii) 互換 (3 個)：

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

(iii) 長さ 3 の巡回置換 (2 個)：

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

例 4.4. 3 次の対称群 S_3 の部分群および正規部分群 H が S_3 の部分群ならば，H の位数 n は 6 の約数である．

(i) $n = 1$ のとき．恒等置換 1 のみからなる群．これは**正規である**．

(ii) $n = 2$ のとき．$< (1\ 2) >= \{1, (1\ 2)\}$ 型が 3 個：

$$< (1\ 2) >, < (1\ 3) >, < (2\ 3) >$$

これらはいずれも正規ではない．

(iii) $n = 3$ のとき．交代群 $A_3 =< (1\ 2\ 3) >$．これは**正規である**．

(iv) $n = 6$ のとき．S_3 自身はもちろん**正規である**．

例 4.5. 4 次の対称群 S_4 の元は次の 24 個である：

(i) 恒等置換 (1 個)

(ii) 互換 (6 個)：

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

(iii) 可換な 2 個の互換の積 (3 個)：

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

(iv) 長さ 3 の巡回置換 (8 個)：

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

(v) 長さ 4 の巡回置換 (6 個)：

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

例 4.6. 4 次の対称群 S_4 の部分群および正規部分群をすべて列挙する．H が S_4 の部分群ならば，H の位数 n は 24 の約数である．

(i) $n = 1$ のとき．恒等置換 1 のみからなる群．これは**正規である**．

(ii) $n = 2$ のとき．

(a) $< (1\ 2) >= \{1, (1\ 2)\}$ 型が 6 個：

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

これらはいずれも正規ではない．

(b) $< (1\ 2)(3\ 4) >= \{1, (1\ 2)(3\ 4)\}$ 型が 3 個：

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

これらはいずれも正規ではない．

(iii) $n=3$ のとき．$<(1\ 2\ 3)>=\{1,(1\ 2\ 3),(1\ 3\ 2)\}$ 型が 4 個：

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

これらはいずれも正規ではない．

(iv) $n=4$ のとき．

(a) $<(1\ 2),(3\ 4)>=\{1,(1\ 2),(3\ 4),(1\ 2)(3\ 4)\}$ 型が 3 個：

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

これらはいずれも正規ではない．

(b) $<(1\ 2\ 3\ 4)>=\{1,(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2)\}$ 型が 3 個：

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

これらはいずれも正規ではない．

(c) $\{1,(1\ 2)(3\ 4),(1\ 3)(2\ 4),(1\ 4)(2\ 3)\}$ は**正規である**．

(v) $n=6$ のとき．$<(1\ 2),(1\ 3)>=\{1,(1\ 2),(1\ 3),(2\ 3),(1\ 2\ 3),(1\ 3\ 2)\}$ 型が 4 個：

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

これらはいずれも S_3 と同型であって，正規ではない．

(vi) $n=8$ のとき．

$$\begin{aligned}&<(1\ 2\ 3\ 4),(1\ 3)>\\&\quad=\{1,(1\ 2\ 3\ 4),(1\ 3)(2\ 4),(1\ 4\ 3\ 2),(1\ 3),(1\ 4)(2\ 3),(2\ 4),(1\ 2)(3\ 4)\}\end{aligned}$$

型が 3 個：

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

これらはいずれも正規ではない．

(vii) $n=12$ のとき．交代群 $A_4=<(1\ 2\ 3),(1\ 2\ 4)>$．これは**正規である**．

(viii) $n=24$ のとき．S_4 自身．これはもちろん**正規である**．

定理 4.7. S_n の正規部分群 N が互換を含めば，$N=S_n$ である．

証明. N に含まれる互換 $(i\ j)$ が存在すると仮定する．任意の互換 $(k\ l)$ に対して，

$$(k\ l)=(l\ j)(k\ i)(i\ j)(k\ i)^{-1}(l\ j)^{-1}\in N$$

となる．よって N はすべての互換を含む． □

定理 4.8. $n\geq 3$ のとき，S_n の正規部分群 N が長さ 3 の巡回置換を含めば，$N=S_n$ または $N=A_n$ である．

証明. N に含まれる長さ 3 の巡回置換 $(i\ j\ k)$ が存在したとする.

$$\sigma = (1\ 3\ k)(1\ 2\ j)(1\ 2\ i)$$

とおくと，N は正規部分群であるから,

$$(1\ 2\ 3) = \sigma(i\ j\ k)\sigma^{-1} \in N$$

となる．また,

$$(1\ 3\ 2) = (1\ 2\ 3)^2 \in N.$$

さらに，$l > 3$ なる任意の整数 l に対して,

$$(1\ 2\ l) = (3\ 2\ l)(1\ 3\ 2)(3\ 2\ l)^{-1} \in N.$$

よって，N は $(1\ 2\ 3)$, $(1\ 2\ 4)$, ..., $(1\ 2\ n)$ を含む．したがって，系 4.2.1 より，$A_n \subseteq N$ である．もし $A_n \subsetneq N$ ならば，N は奇置換 τ を含む．そこで τ を奇数個の互換 τ_1, τ_2, ..., τ_r の積で表す：$\tau = \tau_1\tau_2\cdots\tau_r$．このとき $\tau' = \tau_2\cdots\tau_r$ は偶置換なので，N に属する．したがって $\tau_1 = \tau\tau'^{-1} \in N$．$\tau_1$ は互換だから，定理 4.7 より，$N = S_n$ となる． □

定理 4.9. $n \geq 5$ のとき，n 次対称群 S_n の正規部分群は S_n 自身，交代群 A_n，および $\{1\}$ のみである.

証明. N を S_n の $\{1\}$ 以外の正規部分群とし，σ を 1 でない N の元の一つとする．σ を互いに素な巡回置換の積に分解し，その巡回因子について次のように場合を分けて考える.

(i) σ が長さ 3 以上の巡回因子をもつ場合：

$$\sigma = (1\ 2\ \cdots\ m)\sigma', \qquad m \geq 3$$

とする．ここに，σ' は $(1\ 2\ \cdots\ m)$ 以外の巡回因子の積を表す．N は正規部分群であるから，$(1\ 2)\sigma(1\ 2)^{-1}$ を含む．したがって N は

$$\sigma^{-1}(1\ 2)\sigma(1\ 2)^{-1}$$

を含む．これを計算すると,

$$\begin{aligned}\sigma^{-1}(1\ 2)\sigma(1\ 2)^{-1} &= \sigma'^{-1}(m\ \cdots\ 2\ 1)(1\ 2)(1\ 2\ \cdots\ m)\sigma'(1\ 2)\\ &= (m\ \cdots\ 2\ 1)(1\ 2)(1\ 2\ \cdots\ m)(1\ 2)\\ &= (1\ 2\ m).\end{aligned}$$

ここで，互いに素な二つの巡回置換は可換であることに注意する．したがって定理 4.8 によって，$N = A_n$ または $N = S_n$.

(ii) σ が互いに素な互換の積で書ける場合：σ が互換ならば，定理 4.7 によって $N = S_n$ となる．σ が二つ以上の互換の積で書けるとする.

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

とし，$\sigma' \neq 1$ ならば σ' の巡回因子もすべて互換であるとする.

$$\sigma_1 = (1\ 2\ 3)\sigma(1\ 2\ 3)^{-1} \in N$$

とおけば,

$$\begin{aligned} N \ni \sigma\sigma_1 &= (1\ 2)(3\ 4)\sigma'(1\ 2\ 3)(1\ 2)(3\ 4)\sigma'(1\ 3\ 2) \\ &= (1\ 3)(2\ 4). \end{aligned}$$

ここで, $\sigma'^2 = 1$ であることに注意する. $n \geq 5$ であるから, S_n は $(1\ 3\ 5)$ を含む. したがって

$$(1\ 3\ 5)\sigma\sigma_1(1\ 3\ 5)^{-1} \in N.$$

よって,

$$\begin{aligned} N \ni \sigma\sigma_1(1\ 3\ 5)\sigma\sigma_1(1\ 3\ 5)^{-1} \\ &= (1\ 3)(2\ 4)(1\ 3\ 5)(1\ 3)(2\ 4)(1\ 5\ 3) \\ &= (1\ 3\ 5). \end{aligned}$$

ゆえに N は長さ 3 の巡回置換を含む. したがって定理 4.8 によって, $N = S_n$ または $N = A_n$ である.

□

注意 4.10. 定理 4.9 の証明において, 1, 2, 3, ... のところを, 一般の文字 i_1, i_2, i_3, ... に置き換えて同様に議論すれば, 一般の場合について証明できる.

定理 4.11. 写像 $\varphi : S_n \longrightarrow \{\pm 1\}$ が, S_n の任意の元 σ, τ に対して

$$\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$$

を満たし, しかも $\varphi(\rho) = -1$ となる S_n の元 ρ が存在すれば, $\varphi = \mathrm{sgn}$ となる.

証明. $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ より $\varphi(1) = 1$ となる. また, 写像 φ は全射だから, 準同型定理によって

$$S_n/\ker\varphi \cong \{\pm 1\}$$

となる. よって $\ker\varphi$ は S_n や $\{1\}$ とは異なる S_n の正規部分群である. ところが, そのような S_n の正規部分群は A_n しかないから, $\ker\varphi = A_n$ でなければならない. つまり偶置換に対しては常に $\varphi(\sigma) = 1$ となる. ゆえに $\varphi(\rho) = -1$ を満たす ρ は奇置換でなければならない. 任意の奇置換 τ に対して, $\tau\rho$ は偶置換であるから,

$$\varphi(\tau)\varphi(\rho) = \varphi(\tau\rho) = 1.$$

ゆえに $\varphi(\tau) = -1$ となる. したがって $\varphi = \mathrm{sgn}$ である. □

例 4.12. 3 次交代群 A_3 は位数 3 の巡回群である. よって, A_3 の部分群は A_3 自身と $\{1\}$ しかない. とくに, A_3 は単純群である.

例 4.13. 4 次交代群 A_4 の部分群および正規部分群を列挙する:

(i) 恒等置換のみからなる群 $\{1\}$. これは**正規である**.

(ii) $< (1\ 2)(3\ 4) >= \{1, (1\ 2)(3\ 4)\}$ 型が 3 個：

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

これらはいずれも正規ではない.

(iii) $< (1\ 2\ 3) >= \{1, (1\ 2\ 3), (1\ 3\ 2)\}$ 型が 4 個：

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

これらはいずれも正規ではない.

(iv) $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ は**正規である**.

(v) A_4 自身．もちろん**正規である**.

とくに，A_4 は位数 6 の部分群をもたない.

定理 4.14. $n \geq 3$ とする．交代群 A_n の正規部分群 N が少なくとも一つ長さ 3 の巡回置換を含むならば，$N = A_n$ である.

証明. $(i\ j\ k)$ を N に含まれる長さ 3 の巡回置換とする.

$$\sigma = (1\ 3\ k)(1\ 2\ j)(1\ 2\ i) \in A_n$$

とおくと,

$$(1\ 2\ 3) = \sigma(i\ j\ k)\sigma^{-1} \in N$$

となる．また,

$$(1\ 3\ 2) = (1\ 2\ 3)^2 \in N.$$

さらに，$l > 3$ に対して,

$$(1\ 2\ l) = (3\ 2\ l)(1\ 3\ 2)(3\ 2\ l)^{-1} \in N.$$

よって，N は $(1\ 2\ 3)$, $(1\ 2\ 4)$, ..., $(1\ 2\ n)$ を含む．したがって $N = A_n$.

□

定理 4.15. $n \geq 5$ ならば，交代群 A_n は単純群である．すなわち，A_4 自身と $\{1\}$ のほかに正規部分群をもたない.

証明. N を A_n の $\{1\}$ 以外の正規部分群とし，σ を 1 でない N の元の一つとする．σ を互いに素な巡回置換の積に分解し，その巡回因子について次のように場合を分けて考える.

(i) σ が長さ 4 以上の巡回因子をもつ場合：

$$\sigma = (1\ 2\ \cdots\ m)\sigma', \qquad m > 3$$

とする．ここに，σ' は $(1\ 2\ \cdots\ m)$ 以外の巡回因子の積を表す．N は正規部分群であるから，$(1\ 2\ 3)\sigma(1\ 2\ 3)^{-1}$ を含む．したがって N は

$$\sigma^{-1}(1\ 2\ 3)\sigma(1\ 2\ 3)^{-1}$$

を含む．これを計算すると，

$$\begin{aligned}\sigma^{-1}(1\ 2\ 3)\sigma(1\ 2\ 3)^{-1} &= {\sigma'}^{-1}(m\ \cdots\ 2\ 1)(1\ 2\ 3)(1\ 2\ \cdots\ m)\sigma'(1\ 3\ 2)\\ &= (m\ \cdots\ 2\ 1)(1\ 2\ 3)(1\ 2\ \cdots\ m)(1\ 3\ 2)\\ &= (1\ 3\ m).\end{aligned}$$

ここで，互いに素な二つの巡回置換は可換であることに注意する．したがって定理 4.14 によって，$N = A_n$.

(ii)　σ が長さ 3 の巡回因子を二つ以上もつ場合：

$$\sigma = (1\ 2\ 3)(4\ 5\ 6)\sigma'$$

とする．ここに，σ' は (1 2 3), (4 5 6) 以外の巡回因子の積を表す．N は正規部分群であるから，$(2\ 3\ 4)\sigma(2\ 3\ 4)^{-1}$ を含む．したがって N は

$$\sigma^{-1}(2\ 3\ 4)\sigma(2\ 3\ 4)^{-1}$$

を含む．これを計算すると，

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

よって N は長さ 4 以上の巡回置換 $(1\ 2\ m)$ を含む．したがって，この場合の証明は (i) に帰着される．

(iii)　σ が長さ 3 の巡回因子一つだけ含み，他の巡回因子がすべて互換である場合：

$$\sigma = (1\ 2\ 3)\sigma'$$

とする．$\sigma' \neq 1$ ならば，σ' は二つずつ互いに素であるような互換の積であるとする．このとき ${\sigma'}^2 = 1$ であるから，

$$N \ni \sigma^2 = (1\ 2\ 3){\sigma'}^2 = (1\ 3\ 2).$$

すなわち N は長さ 3 の巡回置換を含む．

(iv)　σ の巡回因子がすべて互換である場合：σ は偶置換であるから，この場合 σ は少なくとも二つの互換を含む．そこで，

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

とし，$\sigma' \neq 1$ ならば σ' の巡回因子もすべて互換であるとする．

$$\sigma_1 = (1\ 2\ 3)\sigma(1\ 2\ 3)^{-1} \in N$$

とおけば，

$$\begin{aligned}N \ni \sigma\sigma_1 &= (1\ 2)(3\ 4)\sigma'(1\ 2\ 3)(1\ 2)(3\ 4)\sigma'(1\ 3\ 2)\\ &= (1\ 3)(2\ 4).\end{aligned}$$

ここで，$\sigma'^2 = 1$ であることに注意する．$n \geq 5$ であるから，A_n は $(1\ 3\ 5)$ を含む．したがって

$$(1\ 3\ 5)\sigma\sigma_1(1\ 3\ 5)^{-1} \in N.$$

よって，

$$\begin{aligned} N &\ni \sigma\sigma_1(1\ 3\ 5)\sigma\sigma_1(1\ 3\ 5)^{-1} \\ &= (1\ 3)(2\ 4)(1\ 3\ 5)(1\ 3)(2\ 4)(1\ 5\ 3) \\ &= (1\ 3\ 5). \end{aligned}$$

ゆえに N は長さ 3 の巡回置換を含む．したがって定理 4.14 によって，$N = A_n$ である．

以上ですべての場合が証明された．

□

5 共役類について

S_n の任意の元 σ は，二つずつ互いに素な巡回置換 $\sigma_1, \sigma_2, \ldots, \sigma_k$ の積に分解することができる：

$$\sigma = \sigma_1\sigma_2\cdots\sigma_k.$$

ここでは，$\sigma_1, \sigma_2, \ldots, \sigma_k$ の中に長さ 1 の巡回置換が入っていてもよいとする．そうすると，上のような巡回置換からなる集合 $\{\sigma_1, \sigma_2, \ldots, \sigma_k\}$ が σ に対してただ一つ定まる．

$\sigma_1, \sigma_2, \ldots, \sigma_k$ の長さをそれぞれ $r_1, r_2, \ldots, r_k$ とするとき，

$$r_1 + r_2 + \cdots + r_k = n \tag{1}$$

とすることができる．さらに，互いに素な二つの巡回置換は可換だから，

$$r_1 \geq r_2 \geq \cdots \geq r_k \tag{2}$$

となるように $\sigma_1, \sigma_2, \ldots, \sigma_k$ を並びかえて番号を付けなおすことができる．こうして，(1), (2) を満たすような組 $(r_1, r_2, \ldots, r_k)$ は σ に対してただ一つ定まる．この $(r_1, r_2, \ldots, r_k)$ を σ の**分解型**という．

定理 5.1. n 次対称群 S_n の 2 つの元 σ, τ が共役であるためには，σ, τ が同じ分解型をもつことが必要十分である．

証明. まず，巡回置換 $(i_1\ i_2\ \cdots\ i_k)$ と S_n の元 ρ について

$$\rho(i_1\ i_2\ \cdots\ i_k)\rho^{-1} = (\rho(i_1)\ \rho(i_2)\ \cdots\ \rho(i_k))$$

が成り立つ．とくに右辺の巡回置換の長さは $(i_1\ i_2\ \cdots\ i_k)$ と同じである．したがって，S_n の元 σ を巡回置換の積に分解して

$$\sigma = (i_1\ i_2\ \cdots\ i_{k_1})(j_1\ j_2\ \cdots\ j_{k_2})\cdots$$

とすれば

$$\rho\sigma\rho^{-1} = \rho(i_1\ i_2\ \cdots\ i_{k_1})\rho^{-1}\rho(j_1\ i_2\ \cdots\ j_{k_2})\rho^{-1}\cdots$$

となる．最初に述べたことから，$\rho\sigma\rho^{-1}$ の分解型と σ の分解型とは同じであることがいえる．したがって σ と τ とが共役ならば，分解型が一致する．

逆に，σ と τ とが同じ分解型ならば，それぞれ巡回置換の積に分解して

$$\sigma = (i_1\ i_2\ \cdots\ i_{k_1})(j_1\ j_2\ \cdots\ j_{k_2})\cdots$$
$$\tau = (i'_1\ i'_2\ \cdots,\ i'_{k_1})(j'_1\ j'_2\ \cdots\ j'_{k_2})\cdots$$

とするとき，置換

$$\rho = \begin{pmatrix} i_1 & i_2 & \cdots & i_{k_1} & j_1 & j_2 & \cdots & j_{k_2} & \cdots \\ i'_1 & i'_2 & \cdots & i'_{k_1} & j'_1 & j'_2 & \cdots & j'_{k_2} & \cdots \end{pmatrix}$$

によって $\rho\sigma\rho^{-1} = \tau$ となり，σ と τ とは共役になる． □

n を正の整数とする．

$$n = r_1 + r_2 + \cdots + r_k, \qquad r_1 \geq r_2 \geq \cdots \geq r_k$$

となる正の整数の組 $(r_1, r_2, \ldots, r_k)$ を n **の分割**という．n の分割の個数を $p(n)$ と書き，これを n の**分割数**という．

このとき，分解型の定義および定理 5.1 から，S_n での共役類の個数は $p(n)$ で与えられることがわかる．

例 5.2. S_3 の共役類は次の 3 つである．

(i) $(1,1,1)$ 型：

$$\{1\}$$

元の個数は 1 個.

(ii) $(2,1)$ 型：

$$\{(1\ 2),\ (1\ 3),\ (2\ 3)\}$$

元の個数は 3 個.

(iii) (3) 型：

$$\{(1\ 2\ 3),\ (1\ 3\ 2)\}$$

元の個数は 2 個.

したがって類等式は

$$6 = 1 + 3 + 2$$

となる．

例 5.3. S_4 の共役類は次の 5 つである．

(i) $(1,1,1,1)$ 型：

$$\{1\}$$

元の個数は 1 個.

(ii) $(2,1,1)$ 型：

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

元の個数は 6 個.

(iii) $(3,1)$ 型：

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

元の個数は 8 個.

(iv) $(2,2)$ 型：

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

元の個数は 3 個.

(v) (4) 型：

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

元の個数は 6 個.

したがって類等式は

$$24 = 1 + 6 + 8 + 3 + 6$$

となる.

定理 5.4. 長さ r の巡回置換 $(1\ 2\ \cdots\ r)$ と可換な S_n のすべての元は

$$(1\ 2\ \cdots\ r)^k\rho, \qquad k = 0, 1\ \ldots, r-1$$

の形をしている．ただし ρ は $1, 2, \ldots, r$ をすべて固定するような S_n の任意の元である.

証明. $(1\ 2\ \cdots\ r)^k\rho$ の形の元が $(1\ 2\ \cdots\ r)$ と可換であることは明らかである．このような形の元は全部で $r\cdot(n-r)!$ 個ある.

いま，$(1\ 2\ \cdots\ r)$ と可換な S_n の元がちょうど $r\cdot(n-r)!$ 個であることを示す．$\sigma = (1\ 2\ \cdots\ r)$ とおく.

$$N(\sigma) = \{\tau \in S_n \mid \tau\sigma = \sigma\tau\}$$

を S_n における σ の正規化群とする．σ と可換な S_n の元の個数は $N(\sigma)$ の位数に一致する．そこで $N(\sigma)$ の位数を求めることにする.

σ の共役類に含まれる元の個数が，指数 $(S_n : A_n)$ に等しいことに注意する．一方，定理 5.1 により，σ の共役類の個数は，σ と同じ長さ r の巡回置換の個数に一致する．それらは $\dfrac{1}{r}\dfrac{n!}{(n-r)!}$ 個ある．したがって，

$$|N(\sigma)| = \frac{|S_n|}{\dfrac{1}{r}\dfrac{n!}{(n-r)!}} = r\cdot(n-r)!$$

となる. □

例 5.5. $n \geq 4$ とする．$(1\ 2)(3\ 4)$ と共役な S_n の元は全部で $\dfrac{1}{8}\dfrac{n!}{(n-4)!}$ 個ある．また，$(1\ 2)(3\ 4)$ と可換な S_n の元は

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

なる形のものがすべてである．ただし ρ は $1, 2, 3, 4$ を固定するような S_n の任意の元である．

例 5.6. A_3 における共役類は

$$\{1\}, \qquad \{(1\ 2\ 3)\}, \qquad \{(1\ 3\ 2)\}$$

の 3 つである．類等式は

$$3 = 1 + 1 + 1.$$

A_3 は Abel 群なので，これらのことは自明である．

例 5.7. A_4 における共役類は

$$\begin{aligned}
&\{1\},\\
&\{(1\ 2\ 3), (1\ 4\ 2), (1\ 3\ 4), (2\ 4\ 3)\},\\
&\{(1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\},\\
&\{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}
\end{aligned}$$

の 4 つである．類等式は

$$12 = 1 + 4 + 4 + 3$$

である．

6 自己同型

群 G から G 自身への準同型写像であって，かつ全単射であるものを G の**自己同型**という．G の自己同型の全体 $\mathrm{Aut}\, G$ は，対称群 $S(G)$ の部分群である．$\mathrm{Aut}\, G$ を G の**自己同型群**という．

群 G の元 g に対して，写像

$$\theta_g : G \longrightarrow G, \qquad x \longmapsto gxg^{-1}$$

は G の自己同型である．この θ_g を g による**内部自己同型**という．それらの全体 $\mathrm{Inn}\, G$ は $\mathrm{Aut}\, G$ の部分群である．$\mathrm{Inn}\, G$ を G の**内部自己同型群**という．G が Abel 群ならば，$\mathrm{Inn}\, G = \{1\}$ である．

定理 6.1. $\mathrm{Inn}\, G$ は $\mathrm{Aut}\, G$ の正規部分群である．

証明. σ を $\mathrm{Aut}\, G$ の元とし，$\theta_g\ (g \in G)$ を $\mathrm{Inn}\, G$ の元とすると，任意の $x \in G$ に対して，

$$\begin{aligned}
(\sigma\theta_g\sigma^{-1})(x) &= \sigma(g\sigma^{-1}(x)g^{-1})(x) = \sigma(g)\sigma(\sigma^{-1}(x))\sigma(g^{-1})\\
&= \sigma(g)x\sigma(g^{-1}) = \sigma(g)x\sigma(g)^{-1}\\
&= \theta_{\sigma(g)}(x).
\end{aligned}$$

ゆえに，

$$\sigma\theta_g\sigma^{-1} = \theta_{\sigma(g)}.$$

これより $\mathrm{Inn}\, G$ が $\mathrm{Aut}\, G$ の正規部分群であることがわかる． □

剰余群 Aut G/Inn G を**外部自己同型類群**といい，Out G で表す．

定理 6.2. G を群，$Z(G)$ を G の中心とする．このとき

$$\mathrm{Inn}\, G \cong G/Z(G)$$

が成り立つ．

証明. G の元 g に対して，θ_g を g による内部自己同型とする．写像

$$\theta : G \longrightarrow \mathrm{Inn}\, G, \qquad g \longmapsto \theta_g$$

は全射準同型である．また，

$$g \in \mathrm{Ker}\, \theta \Longleftrightarrow \theta_g = 1 \Longleftrightarrow gxg^{-1} = x\,(\forall x \in G) \Longleftrightarrow g \in Z(G)$$

より，$\mathrm{Ker}\, \theta = Z(G)$．したがって準同型定理により $\mathrm{Inn}\, G \cong G/Z(G)$ が得られる． □

定理 6.3. S_n を n 次対称群とし，$Z(S_n)$ を S_n の中心とする．このとき

$$Z(S_n) = \begin{cases} S_2, & n = 2 \\ \{1\}, & n \geq 3 \end{cases}$$

が成り立つ．

証明. $S_2 = \{1, (1\ 2)\}$ は Abel 群だから，$Z(S_2) = S_2$．$n \geq 3$ に対して，S_n の元で，$\sigma \neq 1$ なるものをとれば，$\sigma(i) = j$, $i \neq j$ なる二つの数字 i, j が存在する．i, j と異なる数字 k について

$$(\sigma \circ (j\ k))\,(i) = \sigma(i) = j,$$
$$((j\ k) \circ \sigma)\,(i) = (j\ k)\,(j) = k$$

であるから，$\sigma \circ (j\ k) \neq (j\ k) \circ \sigma$．よって $\sigma \notin Z(S_n)$．したがって $Z(S_n) = \{1\}$． □

定理 6.4. S_n を n 次対称群とし，Inn S_n を内部自己同型群とする．このとき

$$\mathrm{Inn}\, S_n = \begin{cases} \{1\}, & n = 2 \\ S_n, & n \geq 3 \end{cases}$$

が成り立つ．

証明. 定理 6.3 と，同型 $\mathrm{Inn}\, S_n \cong S_n/Z(S_n)$ からわかる． □

7 可解群について

定理 7.1. 対称群 S_3 は可解群である．

証明. 正規部分群の列

$$S_3 \rhd A_3 \rhd \{1\}$$

について，剰余群

$$S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$$
$$A_3/\{1\} \cong A_3 = \{1, (1\ 2\ 3), (1\ 2\ 3)^2\}$$

はそれぞれ Abel 群である． □

定理 7.2. 対称群 S_4 は可解群である．

証明. まず，S_4 の部分集合

$$V = \{1,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}$$

は S_4 における正規部分群であるから，とくに A_4 の正規部分群である．

正規部分群の列

$$S_4 \rhd A_4 \rhd V \rhd \{1\}$$

について，剰余群

$$\begin{aligned} S_4/A_4 &\cong \mathbb{Z}/2\mathbb{Z} \\ A_4/V &\cong \mathbb{Z}/3\mathbb{Z} \\ V/\{1\} &\cong V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

はそれぞれ Abel 群である． □

定理 7.3. $n \geq 5$ のとき，交代群 A_n は可解群ではない．また，対称群 S_n も可解群ではない．

証明. A_n の交換子群 $[A_n,\ A_n]$ は A_n に等しい．実際，$i,\ j,\ k,\ l,\ m$ を互いに異なる数字とすると

$$\begin{aligned} (i\ j\ k) &= (i\ j\ l)(i\ k\ m)(l\ j\ i)(m\ k\ i) \\ &= (i\ j\ l)(i\ k\ m)(i\ j\ l)^{-1}(i\ k\ m)^{-1} \\ &= [(i\ j\ l),\ (i\ k\ m)] \end{aligned}$$

である．よって長さ 3 の巡回置換はすべて交換子になる．一方，A_n の任意の元は長さ 3 の巡回置換の積で表される．ゆえに $A_n \subseteq [A_n,\ A_n]$．逆の包含関係は明らかだから $A_n = [A_n,\ A_n]$．よって A_n は可解群ではない．

さらに，$[S_n,\ S_n] = A_n$ である．実際 $i,\ j,\ k$ を互いに異なる数字とすると

$$\begin{aligned} (i\ j\ k) &= (i\ k)(j\ k)(i\ k)(j\ k) \\ &= (i\ k)(j\ k)(i\ k)^{-1}(j\ k)^{-1} \\ &= [(i\ k),\ (j\ k)] \end{aligned}$$

より $A_n \subseteq [S_n,\ S_n]$．ところが A_n は S_n の指数 2 の部分群だから $A_n = [S_n,\ S_n]$ でなければならない．よって S_n も可解群ではない． □