# 群論と対称性

花木章秀・2012 年度前期大学院講義

2012 年 3 月 27 日

## 1 群の作用

$X$ を集合、$G$ を群とする。$G$ が $X$ に (左から) **作用する**とは、写像 $f : G \times X \to X$ が定義されていて、以下の条件を満たすこととする。ここで $g \in G$, $x \in X$ に対して $f(g, x)$ を $gx$ と表すことにする。

(1) $g, h \in G$, $x \in X$ に対して $(gh)x = g(hx)$ が成り立つ。

(2) $x \in X$ に対して $1_G x = x$ が成り立つ。

$G$ が $X$ に作用するとき $X$ を **(左)** $G$**-集合**ともいう。同様に右からの作用、右 $G$-集合も定義される。特に断らない限り左からの作用のみを考えるが、右からの作用についても同様のことが成り立つ。

$X, Y$ を $G$-集合とする。$X$ から $Y$ への ($G$-集合としての) **同型**とは、全単射 $f : X \to Y$ で、$g \in G$, $x \in X$ に対して

$$f(gx) = gf(x)$$

が成り立つものである。$X$ から $Y$ への同型が存在するとき $X$ と $Y$ は**同型である**という。

$X$ を $G$-集合とする。$x, y \in X$ に対して $gx = y$ となる $g \in G$ が存在するとき $x \sim y$ と定めると、$\sim$ は $X$ 上の同値関係となる。この同値関係による $x \in X$ を含む同値類は

$$Gx = \{gx \mid g \in G\}$$

となる。これを $G$ による $X$ の**軌道**、または $X$ の $G$**-軌道**という。$X$ 自身が一つの軌道であるとき、すなわち、任意の $x, y \in X$ に対して $gx = y$ となる

$g \in G$ が存在するとき、$G$ の $X$ の作用は**可移である**という。このとき $X$ は**可移な $G$-集合**であるともいう。

$X$ を $G$-集合とし $Y$ をその一つの軌道とするとき、$Y$ も自然に $G$-集合の構造をもち、この作用は可移である。したがって、任意の $G$-集合は可移な $G$-集合の和集合となる。

$x \in X$ に対して

$$G_x = \{g \in G \mid gx = x\}$$

とおいて、これを $G$ における $x$ の**安定化部分群**という。実際、これは $G$ の部分群である。

**命題 1.1.** $X$ を $G$-集合とし $x \in X$ とする。このとき $f : G/G_x \to Gx$ を $f(gG_x) = gx$ で定めれば $f$ は全単射である。よって $|G : G_x| = |Gx|$ が成り立つ。

$H$ を $G$ の部分群とする。$G$ の $H$ による左剰余類の集合 $G/H$ には以下のようにして $G$-集合の構造が入る。

**命題 1.2.** $X$ を可移な $G$-集合とし、$x \in X$ とする。このとき $X$ と $G/G_x$ は $G$-集合として同型である。

# 2 Schreier-Sims アルゴリズム

この節では [1] に従って、置換群の計算に関するアルゴリズムを解説する。

$G$ を $n$ 次置換群、すなわち対称群 $S_n$ の部分群とし、その生成元が与えられているものとする。

$$G = \langle \sigma_1, \cdots, \sigma_r \rangle$$

このとき次の問題を考える。

1. $G$ の位数を求める。
2. $\tau \in S_n$ に対して $\tau \in G$ を判定する。

具体的な場合にこれを計算するために Schreier-Sims アルゴリズムがある。

## 2.1 軌道の計算

$i \in X = \{1, \cdots, n\}$ に対して、$i$ を含む軌道 $Gi$ を求める。生成元の集合を $S = \{\sigma_1, \cdots, \sigma_r\}$ とする。$X^1 = \{i\}$ とおいて、帰納的に

$$X^{k+1} = X^k \cup \{\sigma_\ell(j) \mid 1 \leq \ell \leq r,\ j \in X^k\}$$

と定める。このとき

$$X^1 \subset X^2 \subset \cdots \subset X^k \subset \cdots$$

となる。$X$ は有限集合なので、この列は止まる。すなわち、ある $m$ があって $X^m = X^{m+1} = \cdots$ となる。このとき $X^m$ が $i$ を含む軌道 $Gi$ となる[1]。また、この計算過程を保存しておけば $j \in Gi$ に対して $\sigma_{\ell_p}\sigma_{\ell_{p-1}} \cdots \sigma_{\ell_1}(i) = j$ となる $\sigma_{\ell_p}\sigma_{\ell_{p-1}} \cdots \sigma_{\ell_1} \in G$ も求めることが出来る。

$i$ の安定化部分群 $G_i$ による左剰余類を考える。$G/G_i$ と $Gi$ の間には自然な全単射 $\tau G_i \mapsto \tau(i)$ がある。したがって、上のようにして、各 $j \in Gi$ に対して $\tau_j(i) = j$ となる $\tau_j \in G$ を求めておけば $\{\tau_j \mid j \in Gi\}$ が $G/G_i$ の完全代表系となる。また $|Gi| = |G : G_i|$ であるから、軌道の長さと安定化部分群の位数が分かれば $G$ の位数も分かる。上記の方法で軌道の長さは分かるので、あとは安定化部分群の位数が分かればよい。安定化部分群は $\{1, \cdots, n\} - \{i\}$ 上の置換群となるので $n-1$ 次置換群である。これに対して同じことを繰り返すことによって $G$ の位数は計算できる。具体的に書くと以下のようになる。

$G = G_{[0]}$ とおいて

$$G_{[k+1]} = (G_{[k]})_{k+1} = \bigcap_{s=1}^{k+1} G_s$$

とおく。すなわち $G_{[k]}$ は $1, \cdots, k$ をすべて固定する元の集合である。また $G_{[n]} = 1$ である。このとき $|G_{[k]}(k+1)| = |G_{[k]} : G_{[k+1]}|$ なので

$$\begin{aligned} |G| &= |G_{[0]} : G_{[1]}| \cdot |G_{[1]} : G_{[2]}| \cdots |G_{[n-1]} : G_{[n]}| \\ &= |G_{[0]}1| \cdot |G_{[1]}2| \cdots |G_{[n-1]}n| \end{aligned}$$

である。

しかしこのためには安定化部分群の生成元を求める必要がある。

[1]実際に計算するときは $X^1 = Y^1 = \{i\}$ として $Y^{k+1} = \{\sigma_\ell(j) \mid 1 \leq \ell \leq r,\ j \in Y^k\} - X^k$, $X^{k+1} = X^k \cup Y^{k+1}$ とすれば計算量を減らすことが出来る。

## 2.2 安定化部分群の生成元 - Schreier の補題

**定理 2.1** (Schreier の補題)**.** $G = \langle g_1, \cdots, g_r \rangle$ とする。$H$ を $G$ の指数 $n$ の部分群とし、左剰余類の代表系を $x_1 = 1, x_2, \cdots, x_n$ とする。また $gH$ の代表元を $\overline{g}$ で表す。このとき $H = \langle (\overline{g_j x_i})^{-1} g_j x_i \mid 1 \leq i \leq n,\ 1 \leq j \leq r \rangle$ が成り立つ。(ただし $G$ が無限群の場合には生成元にその逆元も含むようにしておく。有限群の場合にはその必要はない。)

*Proof.* $S = \{(\overline{g_j x_i})^{-1} g_j x_i \mid 1 \leq i \leq n,\ 1 \leq j \leq r\}$ とおく。任意の $g \in G$ に対して $gH = \overline{g}H$ であるから $\overline{g}^{-1} g \in H$ である。よって $S \subset H$ である。

$(\overline{g_j x_i})^{-1} g_j x_i \in S$ の逆元を考える。$\overline{g_j x_i} = x_k$、すなわち $g_j x_i H = x_k H$ とする。このとき $x_i H = g_j^{-1} x_k H$ なので $\overline{g_j^{-1} x_k} = x_k$ である。よって

$$((\overline{g_j x_i})^{-1} g_j x_i)^{-1} = x_i^{-1} g_j^{-1} x_k = (\overline{g_j^{-1} x_k})^{-1} g_j^{-1} x_k \in S$$

である。よって $S^{-1} = S$ となる。

$S$ が $H$ を生成することを示す。$h \in H$ とする。

$$h = g_{j_m} g_{j_{m-1}} \cdots g_{j_2} g_{j_1}$$

と書くことが出来る。$x_{\ell_1} = x_1 = 1$ として、帰納的に $x_{\ell_{i+1}} = \overline{g_{j_i} x_{\ell_i}}$ で $\ell_i$ を定める。$H \supset S \ni (\overline{g_{j_i} x_{\ell_i}})^{-1} g_{j_i} x_{\ell_i} = x_{\ell_{i+1}}^{-1} g_{j_i} x_{\ell_i}$ である。このとき

$$h = x_{\ell_{m+1}} (x_{\ell_{m+1}}^{-1} g_{j_m} x_{\ell_m}) \cdots (x_{\ell_3}^{-1} g_{j_2} x_{\ell_2}) (x_{\ell_2}^{-1} g_{j_1} x_{\ell_1})$$

である。$h \in H$ なので $x_{\ell_{m+1}} = 1$ となり、$h$ は $S$ の元の積で書ける。したがって $S$ は $H$ を生成する。 □

この定理を $n$ 次置換群に適用すれば、安定化部分群の生成元を求めることができる。したがって Schreier-Sims アルゴリズムによって生成元によって定義された置換群の位数を求めることが出来る[2]。次に対称群の元が置換群に含まれるかどうかを判定する方法を考える。このてまに strong generating set という概念を定義する。

[2] この方法では得られる生成元の数が極めて大きくなってしまい、ある程度大きな群に対しては計算機を用いても実際に行うことはは難しい。生成元の数を少なくする方法 (Jerrum's filter) を後に説明する。

## 2.3 Strong generating sets

これまでと同様に $G = \langle \sigma_1, \cdots, \sigma_r \rangle$ を $n$ 次置換群とする。また $G_{[k]} = \bigcap_{s=1}^{k} G_s$ である。$G_{[k]}/G_{[k+1]}$ の代表元を $s_{k,1}, \cdots, s_{k,\ell_k}$ とする。生成元が与えられれば剰余類の代表を求めることが出来ることは既に見たので、これは計算可能である。

$\tau \in G$ とする。まず $\tau G_{[1]} = s_{1,j_1} G_{[1]}$、すなわち $\tau(1) = s_{1,j_1}(1)$、となる $j_1$ がただ一つ存在する。このとき $s_{1,j_1}^{-1}\tau \in G_{[1]}$ である。次に $s_{1,j_1}^{-1}\tau G_{[2]} = s_{2,j_2} G_{[2]}$ なる $s_{2,j_2}$ をとる。これを繰り返すと $s_{n,j_n}^{-1} \cdots s_{1,j_1}^{-1}\tau \in G_{[n]} = 1$ となる。したがって

$$\tau = s_{1,j_1} \cdots s_{n,j_n}$$

が成り立つ。これは $S = \{s_{k,j} \mid 1 \le k \le n,\ 1 \le j \le \ell_k\}$ が $G$ を生成することを意味する。また作り方から、この表示の一意性が分かる。このようにして作った生成系 $S$ を $G$ の strong generating set という。簡単にいうと、1 の行き先から $s_{1,j_1}$ を決め、2 の行き先から $s_{2,j_2}$ を決めるといった方法である。

strong generating set を求めると、これを使って対称群 $S_n$ の元が $G$ に含まれるかどうかを判定することが出来る。$\tau \in S_n$ とする。

(1) $\tau(1) \in G1$ を判定する。すなわち $\tau(1) = s_{1,j_1}(1)$ なる $j_1$ が存在するかどうかを見る。存在しないならば $\tau \notin G$ である。

(2) $\tau(1) = s_{1,j_1}(1)$ とする。$s_{1,j_1}^{-1}\tau \in G_{[1]}$ である。ここで $s_{1,j_1}^{-1}\tau(2) \in G_{[1]}(2)$ かどうか、すなわち $s_{1,j_1}^{-1}\tau(2) = s_{2,j_2}(2)$ なる $j_2$ が存在するかどうかを見る。存在しないならば $\tau \notin G$ である。

(3) 以下、これを繰り返し $s_{n-1,j_{n-1}}^{-1} \cdots s_{1,j_1}^{-1}\tau \in G_{[n]} = 1$ となれば $\tau \in G$ である。

これで、この節のはじめに述べた問題に答えることができた。ただし $G$ の元を生成元の積で書くということは、strong generating set $S$ の元の積で書くということではないので、$S$ の各元を $\sigma_1, \cdots, \sigma_r$ の積で書いておき、それぞれ置き換える必要がある。また、このままの方法では実際の計算を行うことは計算量が大きすぎて出来ない。Schreier の補題によって求める $G_{[k]}$ の生成元の数が大きくなりすぎるからである。これを解決する方法を次の節で学ぶ。

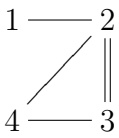
## 2.4 Jerrum's filter

次の定理がこの節で証明することである。

**定理 2.2.** $S_n$ $(n \geq 2)$ の部分群は高々 $n-1$ 個の元で生成される。特に、任意に与えられた生成系から $n-1$ 個以下の生成系を求めることが出来る。

$X = \{1, \cdots, n\}$ とする。$1 \neq g \in S_n$ に対して、$i(g) = \min\{i \in X \mid gi \neq i\}$ とおく。また $e(g) = \{i(g),\ gi(g)\}$ とおく。定義から $i(g) < gi(g)$ である。

$1 \notin S \subset S_n$ に対して頂点集合 $X = \{1, \cdots, n\}$ をもつグラフ $\Gamma_S$ を $e(S) = \{e(\sigma) \mid \sigma \in S\}$ を辺集合として定義する。ただし重複辺を許すものとする。例えば $S_4 \supset S = \{(1\ 2\ 3), (2\ 3\ 4), (2\ 3), (2\ 4), (3\ 4)\}$ ならば




となる。グラフの**サイクル**とは、ある点からはじめて、いくつかの異なる辺をつないで、元の点に戻る点の列であるとする。ある 2 点間に重複辺があるときには、その 2 辺をつないでこれをサイクルと考える。上の例では $[2-3-4-2]$ と $[2-3-2]$ がサイクルである。

定理 2.2 の証明のために、次の命題を示す。

**命題 2.3.** $S_n$ $(n \geq 2)$ の部分群 $G$ の生成系 $S$ で $\Gamma_S$ がサイクルを含まないようなものが存在する。

サイクルを含まないグラフは forest (tree の disjoint union) なので、その辺の数は高々 $n-1$ である。したがってこの命題を示せば定理は証明されたことになる。$\Gamma_S$ が高々 1 つのサイクルをもつ置換の集合 $S$ に対して $m(S) = \sum_{g \in S} i(g)$ とおく。

*Proof of* 命題 *2.3.* $G = \langle \sigma_1, \cdots, \sigma_\ell \rangle$ とし生成元の数 $\ell$ に関する帰納法で示す。$\ell = 1$ ならば命題は明らかである。$\ell \geq 2$ とする。また $g = \sigma_\ell$ とおく。$H = \langle \sigma_1, \cdots, \sigma_{\ell-1} \rangle$ に帰納法の仮定を適用すれば $H = \langle S \rangle$ で $\Gamma_S$ がサイクルを含まないものが存在する。$\Gamma_{S'}$ がサイクルを含まず $G = \langle S, g \rangle = \langle S' \rangle$ となる $S'$ を求めたい。

- $g = 1$ ならば $S' = S$ とすればよい。
- $\Gamma_{S \cup \{g\}}$ がサイクルを含まないならば $S' = S \cup \{g\}$ とすればよい。

よって $\Gamma_{S\cup\{g\}}$ がサイクルを含むと仮定する。$S_1 = S\cup\{g\}$ とおく。$\Gamma_S$ がサイクルを含まないので $\Gamma_{S_1}$ は唯一つのサイクル $C$ をもつ[3]。このサイクル上の点で最小のものを $i$ とする。$i$ からはじめて順番に $C$ の辺を与える置換を $g_1,\cdots,g_m$ とする。辺が $i(g_i)$ から $gi(g_i)$ の向きのとき $\varepsilon_i = 1$ とし、逆のとき $\varepsilon_i = -1$ とし、$h = g_m^{\varepsilon_m}\cdots g_1^{\varepsilon_1}$ とおく。このとき $hi = i$ で、$i$ と $i(g_i)$ の定義から $j < i$ に対しても $hj = j$ である。$S_1$ に含まれる $g_1$ の代わりに $h$ を加えたものを $S_2$ とおくと、$S_2$ も $G$ を生成する。

- $h = 1$ ならば $S_1$ から $g_1$ を除いたものを $S'$ とすればよい。
- $\Gamma_{S_2}$ がサイクルを含まないならば $S' = S_2$ とすればよい。

$\Gamma_{S_2}$ がサイクルを含むとする。$S_1$ から $g_1$ を除いた集合で出来るグラフはサイクルを含まないので$\Gamma_{S_2}$ は唯一つのサイクルを含む。このとき $i(h) > i = i(g_1)$ なので $m(S_2) > m(S_1)$ である。この操作を繰り返すと $m(S_i)$ の狭義短調増加列が得られるが、$|S_i| \le n$ なので $m(S_i) \le n^2$ であり、増加列は停止する。したがって条件をみたす生成系が得られる。 □

**注意 2.4.** 定理 2.2 の評価は精密化され、$n \ge 3$ のとき $S_n$ の部分群は高々 $\lfloor n/2\rfloor$ 個の元で生成されることが知られている。ただしこの限界を与える生成元を求めるアルゴリズムは知られていないようである。

# 3 具体例

$\sigma = (1\ 2\ 3)$, $\tau = (3\ 4\ 5)$ として

$$S_5 \supset G = \langle\sigma,\tau\rangle$$

を考える。

$$1 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} 3 \overset{\tau}{\cdots\!\!>} 4 \overset{\tau}{\cdots\!\!>} 5$$

[3]辺 $[a-b]$ を付け加えて二つのサイクル $[a-b-x_1-\cdots-x_\ell-a]$, $[a-b-y_1-\cdots-y_m-a]$ ができたとすると、$[a-b]$ を加えなくてもサイクル $[b-x_1-\cdots-x_\ell-a-y_m-\cdots-y_1-b]$ が存在することになる。

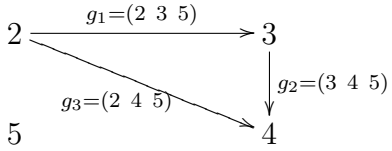
これにより $G$ は $\{1,2,3,4,5\}$ 上に可移に作用する。$G_1$ による剰余類の代表と軌道との間の関係は以下のようになる。

| $G/G_1$ | $G1$ |
|---|---|
| $1$ | $1$ |
| $\sigma$ | $2$ |
| $\sigma^2$ | $3$ |
| $\tau\sigma^2$ | $4$ |
| $\tau^2\sigma$ | $5$ |

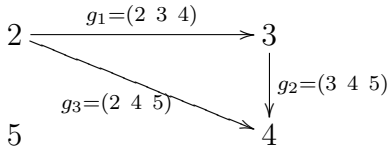
これに Schreier の補題を適用すれば $G_1$ の生成元が求められる。

$$G_1 = \langle (3\ 4\ 5),\ (2\ 4\ 5),\ (2\ 3\ 5),\ (2\ 3\ 4) \rangle$$

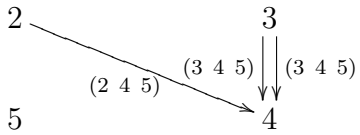
生成元が $4 = 5 - 1$ なので必要なわけではないが Jerrum's filter にかけてみよう。$S = \{(3\ 4\ 5),\ (2\ 4\ 5),\ (2\ 3\ 5)\}$ で以下のようにサイクルを含むグラフが得られる ($1$ は動かないので書かない)。




サイクルの一番小さい点 $2$ に注目して $h = g_3^{-1} g_2 g_1 = 1$ となる。したがって $S$ から $g_1$ を取り除き、新たに $(2\ 3\ 4)$ を加えて $S = \{(3\ 4\ 5),\ (2\ 4\ 5),\ (2\ 3\ 4)\}$ とする。グラフは




である。$m(S) = 2+3+4 = 9$ である。上と同様にして $h = g_3^{-1} g_2 g_1 = (3\ 4\ 5)$ が得られる。$g_1$ を $h$ に取り替えると、グラフは




となり $m(S) = 3 + 3 + 4 = 10$ である。このとき $h = 1$ となるので $(3\ 4\ 5)$ を一つ取り除いて $S = \{(3\ 4\ 5),\ (2\ 4\ 5)\}$ が生成系となる。

# References

[1] P. J. Cameron, *Permutation groups*, London Mathematical Society Student Texts, vol. 45, Cambridge University Press, Cambridge, 1999.