置換の計算

栗野俊一 * <kurino@math.cst.nihon-u.ac.jp>

2007/01/23 版

1　置換と互換

1.1　置換

定義 1 (置換) n 個の要素を、置き換えるような操作 *(*関数*)* を **置換** と呼ぶ[1]。従って、厳密には、n 個の要素をもつ有限集合 $A_n = \{x|x \in N, 1 \leq x \leq n\}$ を考え、その A_n 上の一対一変換[2]が置換となる。

例えば、$A_3 = \{1, 2, 3\}$ 上の写像で、1 を 2、 2 を 3、 そして 3 を 1 に対応させるようなものは、A_3 の置換 (の一つ..) である。この時、この変換を σ と呼ぶことにすれば、$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$ が、それぞれ成立することを意味する。

置換は、(定義により..) 有限集合上の対応なので、その対応関係を直接、表の形で、書き下すことができる[3]。例えば、上記の A_3 上の置換 σ を、この表形式で表した結果は次のようになる。

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

これは、次のような関数表と同じ意味である。

x	1	2	3
$\sigma(x)$	2	3	1

また、同様にして、

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}(1) = 2, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}(2) = 3, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}(3) = 1$$

となる。

*日本大学理工学部数学科

[1]「置き換る」ので置換。

[2]関数の中で、値域と定義域が共に等しい A であった場合、その関数を特に、A 上の**変換** と呼ぶ。なお、有限集合上の一対一の変換は自動的に、上への写像になり、したがって、全単射 (逆変換を持つこと) になる点に、注意。

[3]有限集合上の関数は、このように値の対応関係を明示的に記すことで、表現できることは、当り前のことのようだが、指摘しないと気が付かないことも多い。実際、計算機上で、このことを要求すると、できないことが多い。有限集合上の関数が、表で記述できるということは、計算機を使う上でも大変重要である。なぜなら、計算機上の関数というのは、原理的には、有限集合上の関数にしかならないと考えることができるからである。すなわち、計算機上の関数は、いつでも、表の形で表現できる。

なお、この表は、上下の対応だけが本質なので、列を入れ替えても同じ置換を表す。
すなわち、

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

である (他にも、沢山ある。考えてみよう) [4]。
A_n 上の置換の表現は、上の行を $1, 2, .., n$ という昇順の形に固定しても、下の行が $n!$ だけの種類があり、それらは異なる置換となる[5]ので、A_n 上の置換の種類は、$n!$ 種あることがわかる。

定義 2 (対称群) A_n 上の全ての置換を集めた集合を、S_n で表し、**対称群**[6]と呼ぶ。

1.2 置換の積

$\sigma, \tau \in S_n$ とする。すなわち、σ, τ が、共に A_n 上の置換であるとする。すると、σ で写した像を再び、τ で写すことによって、新しい置換を作ることができる。

定義 3 (置換の積) $\sigma, \tau \in S_n$ とする。この時、σ, τ の合成関数 μ を $\mu(x) = \tau(\sigma(x))$ で、定義する。すなわち、$y = \sigma(x), z = \tau(y)$ の時に、$z = \mu(x)$ となるような関数 μ を考え、これを **置換の積** と呼び、$\tau\sigma$ [7]で表す。

例えば、A_5 上の置換 σ, τ を、それぞれ次のように与える。

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

すると、

x	1	2	3	4	5	←この行と、
$y = \sigma(x)$	2	5	1	3	4	
$z = \tau(y)$	1	2	4	3	5	←この行を取る

となるので、その積 $\tau\sigma$ は、次のようになる。

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

これは単純に、上の行に $1 \sim 5$ を並べ、更に、下の行に、$\tau\sigma(1) \sim \tau\sigma(5)$ を並べるだけでできる。
よって、次のように、σ を上、τ を下に並べて、対応を考えればよい。

[4]二つの関数 f, g に対して、定義域 S 上での $f = g$ の定義は、$\forall x (\in S)[f(x) = g(x)]$ である。同じ置換が上記のように異なる表現になっても、この意味で、同じ定義域内であれば、同じ関数になることを確かめよう。
[5]逆に、上の行が、$1, 2, .., n$ でない場合は、上の行が昇順になるように、列ごと整理すれば、同じ関数が違う形に表記されていただけであることがわかる。
[6]単なる集合ではなく、「群」と呼ぶ理由は、この集合 S_n が、関数の合成に関して、群を成すためである。
[7]σ と τ の積は、$\tau\sigma$ と、適用する順と逆に並べること注意。これは、関数としての合成を考えると、こちらの方が自然だからである。なお、この $\tau\sigma$ と、τ, σ の積である $\sigma\tau$ は一般には異なる置換になるので注意。

$$
\begin{aligned}
\sigma &= \begin{pmatrix} 1 & 2 & \boxed{3} & 4 & 5 \\ & & \downarrow & \downarrow & \\ 2 & 5 & \boxed{1} & 3 & 4 \end{pmatrix} \\
& \qquad\quad / \qquad\quad / \\
\tau &= \begin{pmatrix} \boxed{1} & 2 & 3 & 4 & 5 \\ \downarrow & & \downarrow & & \\ \boxed{4} & 1 & 3 & 5 & 2 \end{pmatrix} \\
\\
\tau\sigma &= \begin{pmatrix} 1 & 2 & \boxed{3} & 4 & 5 \\ 1 & 2 & \boxed{4} & 3 & 5 \end{pmatrix}
\end{aligned}
$$

これは、また、次のように考えることができる。

まず、τ は、上の行が σ の下の行と同じになるように、列ごと並び換えても、元の置換 τ と同じである。すなわち、

$$
\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 1 & 3 & 4 \\ 1 & 2 & 4 & 3 & 2 \end{pmatrix}
$$

である。よって、

$$
\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 5 & 1 & 3 & 4 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}
$$

すなわち、

$$
\begin{array}{rcl}
\sigma &=& \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} \\
& & \;\;\downarrow \;\; \downarrow \;\; \downarrow \;\; \downarrow \;\; \downarrow \\
\tau &=& \begin{pmatrix} 2 & 5 & 1 & 3 & 4 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}
\end{array}
\begin{array}{l}
\leftarrow \text{この行と、} \\
\left.\begin{array}{l} \\ \\ \\ \end{array}\right\} \leftarrow \text{この二行を揃える} \\
\leftarrow \text{この行を取る}
\end{array}
$$

$$
\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}
$$

ともできる。

1.3 恒等置換

置換の積を考えると、次のような特別な置換は、特別な性質があることが解る。

定義 4 (恒等置換) 置換の中で、要素を何も動かさない置換、すなわち、要素を並べて表現すると、

$$
\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}
$$

となる置換を**恒等置換** あるいは **単位置換** と呼び 1_n で表す。当然のことながら $\forall i \in 1..n[1_n(i) = i]$ である。

この要素は、置換の積に関して、単位元となる。すなわち、$\forall \sigma \in S_n[\sigma 1_n = 1_n \sigma = \sigma]$ となる。

1.4 逆置換

置換は、全単射なので、逆変換を持つ。

定義 5 (逆置換) 置換 σ に対して、その逆変換を、元の置換の**逆置換**と呼び、σ^{-1} で表す。

置換 σ とその逆置換 σ^{-1} は、互いに逆変換 ($(\sigma^{-1})^{-1} = \sigma$) なので、合成すると単位置換になる。すなわち $\sigma\sigma^{-1} = \sigma^{-1}\sigma = 1_n$ である。

与えられた置換から、逆置換を求めるのは簡単で、上の行と下の行を交換すればよい。

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$

例えば、

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 5 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

となる。

1.5 互換

定義 6 (互換) 置換の中で、特に、二つの異なる要素、i 番目と j 番目の要素の交換だけを行うような置換を、特別に **互換**[8]と呼び、その交換する二つの要素 i, j を利用して、(i, j) で表す。

互換は、置換の一種なので、当然、対応する要素を並べた表形式でも表現できる。例えば、A_5 上の、2 と 4 を交換する互換 $(2, 4)$ は、普通の表現にすると、次のような形になる。

$$(2, 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$$

従って、$\sigma = (2, 4)$ の時、$\sigma(1) = 1, \sigma(2) = 4, \sigma(3) = 3, \sigma(4) = 2, \sigma(5) = 5$ である[9]。

互換は、着目している、i 番目と j 番目の要素以外の要素は変更しないことに注意しよう。

[8]「互いに交換する」の意味で、互換。

[9]一般の置換の場合は、それがどの集合 A_n 上の置換であるかによって、表現が異なることになるが、互換の場合は、A_n (の、特に n) を明示する必要がないことに注意。

1.6 置換の互換の積による表現

互換は常に置換だが、任意の置換は必ずしも互換とは限らない。しかし、互換を組合せる（すなわち、幾つかの互換の積を取る..）ことにより、任意の置換と同じ変換を実現することができる。この事実を述べたのが、次の定理である。

定理 7 任意の置換は、いくつかの互換の積で表現することができる。すなわち、

$$\forall\sigma \in S_n, \exists\tau_1, \tau_2, .., \tau_m : \text{互換 } s.t.\ \sigma = \tau_m..\tau_2\tau_1$$

である。

例えば、次の A_3 の置換 (σ) は、互換ではないが、二つの互換（$(2,3)$ と、$(1,3)$）の積に一致する。

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (2,3)(1,3)$$

1.7 置換から互換の積への変換

置換を互換の積に変換する方法は色々とあるが、その一つは、置換の下の行を、互換を利用して、整列してゆく方法である[10]。

まず、次の性質に注意しよう。

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & n \\ a_1 & a_2 & \cdots & a_i & \cdots & a_j & a_n \end{pmatrix}, \qquad \tau = (i,j)$$

の時、

$$\begin{aligned} \sigma\tau &= \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ a_1 & a_2 & \cdots & a_i & \cdots & a_j & \cdots & a_n \end{pmatrix}\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ a_1 & a_2 & \cdots & a_j & \cdots & a_i & \cdots & a_n \end{pmatrix} \end{aligned}$$

すなわち、ある置換 τ に、右から、互換 (i,j) をかけるということは、その置換の下の行の i 番目の要素と j 番目の要素を交換する[11]という意味を持つ。

この性質を利用すれば、例えば、次のようにして、与えられた置換を、順に互換を右からかけて、恒等置換に変換することができる。

[10]これは、基本変形を利用して、逆行列を求める場合と全く同じ考え方である。
[11]実は、左からかけた場合は、上の要素を交換する。

$$
\begin{array}{ccccccccc}
 & & & & & & & & \text{互換} \\
\left(\begin{array}{c} 1 \\ 2 \end{array}\right. & \begin{array}{c} 2 \\ 4 \end{array} & \begin{array}{c} 3 \\ 1 \end{array} & \begin{array}{c} 4 \\ 6 \end{array} & \begin{array}{c} 5 \\ 7 \end{array} & \begin{array}{c} 6 \\ 3 \end{array} & \left.\begin{array}{c} 7 \\ 5 \end{array}\right) & & \\
1 & & 2 & & & & & & (1,3) \\
 & 2 & 4 & & & & & & (2,3) \\
 & & 3 & & & 4 & & & (3,6) \\
 & & & 4 & & 6 & & & (4,6) \\
 & & & & 5 & & 7 & & (5,7)
\end{array}
$$

このことは、要するに、

$$
\left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 6 & 7 & 3 & 5 \end{array}\right)(1,3)(2,3)(3,5)(4,6)(5,7) = 1_7
$$

を意味する。
即ち、

$$
\left(\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 6 & 7 & 3 & 5 \end{array}\right) = ((1,3)(2,3)(3,5)(4,6)(5,7))^{-1} = (5,7)(4,6)(3,5)(2,3)(1,3)
$$

である[12]。

1.8 置換の符号

実は、置換を互換の積に表現する場合、その表現の方法は何通りもある[13]。例えば、以下のようにである。

$$
\left(\begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array}\right) = (1,2)(1,3) = (1,3)(2,3) = (1,2)(2,3)(1,3)(1,2)
$$

すなわち、同じ個数でも、異なる互換の積で表現できる[14]し、また、積の個数も必ずしも一定していない。
しかしながら、実は、どの場合も積の個数が奇数が偶数かは、その置換によって定まっている。上記の例では、何れに場合も、偶数個の互換の積となっている。逆に、奇数個のどのような互換の積を作っても、上記の置換にはならなということである。
この性質を示したものが次の定理である。

定理 8 置換は幾つかの互換の積で表現できるが、その互換の個数の偶奇性はいつも一定である。

このように置換は、それが、偶数個の互換の積で表現できるか、あるいは、奇数個の互換の積で表現できるかの二つに分類できる。そこで、それらを区別して、名前を付けることにする。

[12]ここで、$(\tau\sigma)^{-1} = \sigma^{-1}\tau^{-1}$ と、$(i,j)^{-1} = (j,i) = (i,j)$ を利用した。
[13]原理的には、いくらでも長い互換の積が作れるので、その方法は無限通りあることになる。
[14]端的にいえば、$(1,2)(2,1) = 1_n$ なので、$\sigma = \tau_1\tau_2$ であれば、$\sigma = \tau_1\tau_2 1_n = \tau_1\tau_2(1,2)(2,1)$ となる。即ち、特定な置換を表現する互換の積の列はいくらでも長くできる。

定義 9 (偶置換と奇置換) ある置換 σ が、偶数の個の互換 $\tau_1, \tau_2, .., \tau_{2m}$ の積で表現できたとする *(* すなわち $\sigma = \tau_{2m}..\tau_2\tau_1$ が成立 *)*。その時、この置換 σ は **偶置換** であると呼ぶ。同様にして、σ が奇数個の互換の積で表現できる場合は、**奇置換** と呼ぶ。

また、この偶置換と奇置換の違いを表現する標数として、次の符号というものも定義する。

定義 10 (置換の符号) 置換 σ に対して、**符号** を次のように定め、$sgn\ \sigma$ で表す。

$$sgn\ \sigma = \begin{cases} +1 & (\sigma \text{ が偶置換の時}) \\ -1 & (\sigma \text{ が奇置換の時}) \end{cases}$$

1.9 符号の計算

符号の計算は、定義通りに行えば、計算できる。すなわち、与えられた置換 σ を互換の積に変形し、その積に現れる互換の個数を数えて、それが偶数ならば $+1$ 、奇数ならば -1 とすればよい。
しかし、次のような視角的に解りやすい方法[15]がある。

手段 11 (交点を利用した置換の符号の計算) 次の手順で、置換の符号を計算する。

1. 置換の上の行と下の行の同じ番号を線で結ぶ。
2. ただし、交点は、必ず二本の線だけが交わるようにする *(* 三本以上が一点で交わらないように線をずらすなどの工夫をする。*)*
3. 交点の個数を n とする。
4. $sgn\ \sigma = (-1)^n$ として答えを求める。

[15] 鈴木君が教えてくれた。