

§7. 置換

集合 $\{1, 2, \dots, n\}$ から $\{1, 2, \dots, n\}$ への全単射は n 文字の置換と呼ばれる。ここではこの置換の基本的な性質を学ぶ。

● 7-1 : 置換の表記法

集合 $\{1, 2, \dots, n\}$ から $\{1, 2, \dots, n\}$ への全単射を n 文字の置換という。 n 文字の置換 σ を表わすには、次のような表を用いると便利である：

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

この表においては、上段の数字と下段の数字の組 $\left[\begin{smallmatrix} i \\ \sigma(i) \end{smallmatrix} \right]$ が重要で、これをひと固まりとして、並べ方の順番を変えた表は同じ置換を表わすと約束する。

例 7-1-1 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$ は $\sigma = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ と表わすこともでき、どちらも

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

により定まる 4 文字の置換 $\sigma : \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ を表わす。

n 文字の置換全体からなる集合を \mathfrak{S}_n という記号で表わす。 \mathfrak{S} はアルファベットの S に対応するドイツ文字である。

2 つの置換 $\sigma \in \mathfrak{S}_m$ と $\tau \in \mathfrak{S}_n$ が写像として等しいとき $\sigma = \tau$ と表わす。すなわち、

$$\sigma = \tau \iff \begin{cases} \bullet n = m, \text{ かつ,} \\ \bullet \text{すべての } i = 1, \dots, n \text{ について } \sigma(i) = \tau(i). \end{cases}$$

● 7-2 : 置換の積

2 つの n 文字の置換 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ と $\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix}$ から、

$$\sigma\tau := \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}$$

という n 文字の置換 $\sigma\tau$ を定義することができる。これを σ と τ の積という。積 $\sigma\tau$ は合成写像 $\sigma \circ \tau : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ のことに他ならない。

例 7-2-1 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \in \mathfrak{S}_4$ について、

$$(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(4) = 3,$$

$$(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(3) = 1,$$

$$(\sigma \circ \tau)(3) = \sigma(\tau(3)) = \sigma(1) = 4,$$

$$(\sigma \circ \tau)(4) = \sigma(\tau(4)) = \sigma(2) = 2$$

であるから、 $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ である。同様にして、 $\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ がわかる。したがって、 $\sigma\tau \neq \tau\sigma$ である。

● 7-3 : 逆置換と恒等置換

n 文字の置換 $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$ に対して、各 $\sigma(i)$ を i に写すような置換

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

を考えることができる。この置換を σ の逆置換といい、記号 σ^{-1} で表わす。

例 7-3-1 置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ の逆置換は $\sigma^{-1} = \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ である。

1 から n までの各数字 i に対して、 i 自身を対応させる n 文字の置換 (つまり、 $\{1, \dots, n\}$ 上の恒等写像) を \mathfrak{S}_n における恒等置換といい、記号 1_n で表わす (e で表わすこともある) :

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

前後の文脈から、数字の 1 と混乱する恐れのない場合には、 1_n を単に 1 で表わす。任意の置換 $\sigma \in \mathfrak{S}_n$ に対して、 $\sigma 1_n = 1_n \sigma = \sigma$, $\sigma \sigma^{-1} = \sigma^{-1} \sigma = 1_n$ が成り立つ。

● 7-4 : 巡回置換

巡回置換とは、ある異なる k 個 ($k \geq 2$) の数字 i_1, \dots, i_k を

$$i_1 \mapsto i_2, \quad i_2 \mapsto i_3, \quad \dots, \quad i_{k-1} \mapsto i_k, \quad i_k \mapsto i_1$$

のように写し、それ以外の数字は動かさないような置換のことをいう。このような置換を $(i_1 i_2 \cdots i_k)$ のように表わす。 k を巡回置換 $(i_1 i_2 \cdots i_k)$ の長さという。

例 7-4-1 \mathfrak{S}_5 において、 $(2 3 4 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 5 & 2 \end{pmatrix}$.

定理 7-4-2

任意の置換は (互いに共通の文字を含まない) 巡回置換の積で表わされる。

上の定理を例を用いて説明する。

例 7-4-3 7 文字の置換 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 3 & 1 & 6 & 2 \end{pmatrix}$ を互いに共通の文字を含まない巡回置換の積の形に表わそう。まず、 σ を次々に合成していったときに、1 がどのような数字に写されていくのかを追跡すると、次のようになる。

$$1 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 1$$

次に、上の中に登場しない数字、例えば、2 について同様の考察を行なうと、

$$2 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 2.$$

今までに登場しなかった数字は 6 のみであり、これは σ により動かされない。したがって、

$$\sigma = (7 2)(1 4 3 5)$$

のように表わされる。 □

● 7-5 : 互換

$(i j)$ の形で表される巡回置換、すなわち、長さ 2 の巡回置換を互換と呼ぶ。

例 7-5-1 \mathfrak{S}_4 における互換 (13), (23), (14), (12) の積 (13)(23)(14)(12) は 4 文字の置換 $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$ に等しい。実際、 $\sigma = (13)(23)(14)(12)$ とおくと、 σ の下で、1 は

$$1 \xrightarrow{(12)} 2 \xrightarrow{(14)} 2 \xrightarrow{(23)} 3 \xrightarrow{(13)} 1$$

のように写される (合成をとる順番に注意)。同様に、2, 3, 4 はそれぞれ σ によって 4, 2, 3 に写されることがわかる。□

巡回置換 $(i_1 i_2 \cdots i_k)$ は、次のように、互換の積に表わされる。

$$(7-5 a) \quad (i_1 i_2 \cdots i_k) = (i_1 i_2)(i_2 i_3) \cdots (i_{k-2} i_{k-1})(i_{k-1} i_k).$$

このことと [定理 7-4-2] より、次を得る。

定理 7-5-2

任意の置換は有限個の互換の積として書くことができる。

n 文字の置換は上の定理より互換の積として表わされるが、その表わし方には一意性はない。

例 7-5-3 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$ について、 $\sigma = (34)(23)(12)(45)(34) = (35)(14)(24)$.

● **7-6 : 置換の符号とその性質**

$n \geq 2$ とする。 n 文字の置換 $\sigma \in \mathfrak{S}_n$ に対して、

$$(7-6 a) \quad \text{sgn } \sigma := \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \in \mathbb{Q}$$

とおく。ここで、 $\prod_{1 \leq i < j \leq n}$ は $1 \leq i < j \leq n$ を満たすすべての整数の組 (i, j) に渡って積をとることを意味する。

(7-6 a) を用いて $\text{sgn } \sigma$ を計算するのは大変であるが、以下で述べる定理を用いると簡単に計算することができる。

定理 7-6-1 (置換の符号の性質)

任意の $\sigma, \tau \in \mathfrak{S}_n$ に対して、次が成り立つ。

(1) $\text{sgn}(\sigma\tau) = (\text{sgn } \sigma)(\text{sgn } \tau)$.

したがって、 $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$ (各 $i = 1, 2, \dots, k$ に対して σ_i は互換) のとき、 $\text{sgn } \sigma = (-1)^k$.

(2) $\text{sgn}(1_n) = 1$.

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

この定理の (1) を証明するために、次の補題を用いる。

補題 7-6-2

σ が互換のとき、 $\text{sgn } \sigma = -1$ である。

(証明)

$\sigma = (k \ l) \ (1 \leq k < l \leq n)$ とおく。 $N = \#\{(\sigma(i), \sigma(j)) \mid 1 \leq i < j \leq n, \sigma(i) > \sigma(j)\}$ とおく ($\#$ は集合の元の個数を表わす) と、

$$\prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)) = (-1)^N \prod_{1 \leq i < j \leq n} (j - i)$$

とかけるから、 N が奇数であることを示せばよい。 N は、数字 $k \ (k = 1, 2, \dots, n)$ よりも左側にある数字の中で k より大きい数字の個数を n_k とおくと、 $N = n_1 + n_2 + \dots + n_n$ により計算できる。数え上げにより、 $n_{k+1} = \dots = n_{l-1} = 1, n_k = l - k$ であり、これら以外の n_i は 0 であることがわかる。故に、 $N = (l - k - 1) + (l - k) = 2(l - k) - 1$ であり、 $\text{sgn } \sigma = (-1)^{2(l-k)-1} = -1$ である。 \square

(定理 7-6-1 の証明)

(1) まず、 $\{1, \dots, n\}$ の相異なる 2 元からなる部分集合 $\{i, j\} \ (i \neq j)$ の全体 \mathcal{S} を考える。 $I = \{i, j\} \in \mathcal{S}$ および $\sigma, \tau \in \mathfrak{S}_n$ に対して、

$$a_I(\sigma, \tau) := \frac{\sigma(j) - \sigma(i)}{\tau(j) - \tau(i)}$$

とおくと、 $\text{sgn } \sigma$ は次のように表わすことができる： $\text{sgn } \sigma = \prod_{I \in \mathcal{S}} a_I(\sigma, 1_n)$ 。

写像 $I = \{i, j\} \in \mathcal{S} \mapsto \tau(I) = \{\tau(i), \tau(j)\} \in \mathcal{S}$ は \mathcal{S} 上の全単射であるから、

$$\text{sgn } \sigma = \prod_{I \in \mathcal{S}} a_{\tau(I)}(\sigma, 1_n) = \prod_{I \in \mathcal{S}} a_I(\sigma\tau, \tau)$$

と書くこともできる。したがって、

$$\begin{aligned} \text{sgn}(\sigma\tau) &= \prod_{I \in \mathcal{S}} a_I(\sigma\tau, 1_n) = \prod_{I \in \mathcal{S}} (a_I(\sigma\tau, \tau) a_I(\tau, 1_n)) \\ &= \left(\prod_{I \in \mathcal{S}} a_I(\sigma\tau, \tau) \right) \left(\prod_{I \in \mathcal{S}} a_I(\tau, 1_n) \right) = (\text{sgn } \sigma)(\text{sgn } \tau) \end{aligned}$$

となる。特に、 $\sigma \in \mathfrak{S}_n$ が $\sigma = \sigma_1 \sigma_2 \dots \sigma_k$ (各 $i = 1, 2, \dots, k$ に対して σ_i は互換) と表わされるとき、[補題 7-6-2] を用いて、 $\text{sgn } \sigma = \text{sgn}(\sigma_1 \sigma_2 \dots \sigma_k) = \text{sgn}(\sigma_1) \text{sgn}(\sigma_2) \dots \text{sgn}(\sigma_k) = (-1)^k$ となることがわかる。

(2) 置換の符号の定義により、直ちに $\text{sgn}(1_n) = 1$ とわかる。

(3) (1) と (2) より、 $\text{sgn}(\sigma^{-1}) \text{sgn } \sigma = \text{sgn}(\sigma^{-1} \sigma) = \text{sgn}(1_n) = 1$ を得る。したがって、 $\text{sgn}(\sigma^{-1})$ と $\text{sgn } \sigma$ は同符号である。また、(1) の後半部分の主張により、 $\text{sgn } \sigma \in \{\pm 1\}$ であるから、 $\text{sgn}(\sigma^{-1}) = \text{sgn } \sigma$ であることがわかる。 \square

注意. n 文字の置換 σ を互換の積による表示は何通りもあるが、(1) から、置換を互換の積で表わしたときの互換の個数の偶奇は一定なことがわかる。すなわち、置換 $\sigma \in \mathfrak{S}_n$ を次のように 2 通りの互換の積に書いたとする：

$$\sigma = \tau_1 \tau_2 \dots \tau_k = \rho_1 \rho_2 \dots \rho_l,$$

(但し、各 $i = 1, 2, \dots, k$ に対して τ_i は互換、各 $j = 1, 2, \dots, l$ に対して ρ_j は互換)

このとき、 k が偶数 (resp. 奇数) ならば、 l も偶数 (resp. 奇数) である。

例 7-6-3 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}$ は $\sigma = (35)(14)(24)$ のように奇数個の互換の積で表わされるから、 $\text{sgn } \sigma = -1$ である。