2 Подстановки

2.1 Свойства отображений

Тождественное отображение множества X в себя будет обозначаться ε_X или просто ε. Таким образом, $\varepsilon(x) = x\ \forall x \in X$. Напомним, что композицией отображений $f : X \to Y$ и $g : Y \to Z$ называется отображение $g \circ f : X \to Z$ такое, что $g \circ f(x) = g(f(x))$.

Теорема. *Рассмотрим отображения $f : X \to Y$, $g : Y \to Z$ и $h : Z \to U$. Тогда $(h \circ g) \circ f = h \circ (g \circ f)$.*

Доказательство. Для любого $x \in X$ имеем

$$(h \circ g) \circ f(x) = (h \circ g)(f(x)) = h(g(f(x))),$$

$$h \circ (g \circ f)(x) = h((g \circ f)(x)) = h(g(f(x))).$$

Следовательно, $h(g(f(x))) = h(g(f(x)))$. □

Отображение $f : X \to Y$ называется *инъективным*, если из того, что $f(x_1) = f(x_2)$ следует $x_1 = x_2$. Оно называется *сюръективным*, если для любого $y \in Y$ существует $x \in X$ такое, что $f(x) = y$. Отображение $f : X \to Y$ называется *биективным* если оно инъективно и сюръективно.

Пусть дано отображение $f : X \to Y$. *Обратным* к нему называется отображение $f^{-1} : Y \to X$ такое, что $f \circ f^{-1} = \varepsilon_Y$ и $f^{-1} \circ f = \varepsilon_X$.

Предложение. (1) *Обратное отображение к* $f : X \to Y$ *существует* $\iff$ f *биективно.*

(2) *Если обратное отображение к* $f : X \to Y$ *существует, то оно единственно.*

Доказательство. . . . . . □

2.2 Подстановки

Рассмотрим множество $\Omega_n := \{1, \ldots, n\}$. Подстановкой называется любое биективное отображение $\sigma : \Omega_n \to \Omega_n$. Множество всех подстановок обозначим через S_n. Каждая подстановка однозначно $\sigma \in S_n$ задается $2 \times n$-таблицей (матрицей)

$$\begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

где $\{i_1, \ldots, i_n\} = \Omega_n$ и $j_k := \sigma(i_k)$. Такая запись не единственна: при перестановке столбцов мы получаем ту же подстановку. Таким образом, каждая подстановка может быть записана в стандартном виде

$$\begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

Назовем *перестановкой* из n элементов строку $(i_1, \ldots, i_n)$, где $i_k \in \Omega_n$ и $i_k \neq i_l$ при $k \neq l$. Ясно, что для перестановки $(i_1, \ldots, i_n)$ всегда выполнено $\{i_1, \ldots, i_n\} = \Omega_n$.

Предложение. *Число число всех подстановок равно числу всех перестановок и равно* $n!$.

Произведением подстановок σ_1, $\sigma_2 \in S_n$ назовем их композицию $\sigma_1 \circ \sigma_2 \in S_n$. Тождественная подстановка обозначается через ε.

Свойства подстановок.

- $(\sigma\circ\varphi)\circ\delta = \sigma\circ(\varphi\circ\delta)$ для всех $\sigma, \varphi, \delta \in S_n$ (ассоциативность);
- $\sigma \circ \varepsilon = \varepsilon \circ \sigma = \sigma$ для всех $\sigma \in S_n$;
- $\forall\ \sigma \in S_n\ \exists\ \sigma^{-1} \in S_n \quad \sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \varepsilon$.

Определение. *Транспозицией* называется подстановка $\tau \in S_n$ такая, что существуют i, $j \in \{1, \ldots, n\}$, $i \neq j$ такие, что $\tau(i) = j$, $\tau(j) = i$ и $\tau(k) = k$ при $k \notin \{i, j\}$. Эта транспозиция обозначается $\sigma = [i, j]$.

Теорема. *Любая подстановка* $\sigma \in S_n$ *представляется в виде произведения транспозиций:* $\sigma = \tau_1 \circ \cdots \circ \tau_r$.

Доказательство. Индукция по n. Предположим, что утверждение верно для $n - 1$. Пусть

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i_1 & i_2 & \cdots & i_{n-1} & i_n \end{pmatrix}$$

Если $i_n \neq n$, то рассмотрим транспозицию $\tau = (n, i_n)$. Если же $i_n = n$, то положим $\tau = \varepsilon$. В обоих случаях

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ i'_1 & i'_2 & \cdots & i'_{n-1} & n \end{pmatrix}$$

Рассмотрим подстановку

$$\sigma' = \begin{pmatrix} 1 & 2 & \cdots & n-1 \\ i'_1 & i'_2 & \cdots & i'_{n-1} \end{pmatrix} \in S_{n-1}$$

По предположению индукции она раскладывается в произведение транспозиций: $\sigma' = \tau'_1 \circ \cdots \tau'_m$, $\tau'_i = [k_i, l_i] \in S_{n-1}$, $k_i \ l_i \in \{1, \ldots, n-1\}$, $k_i \neq l_i$. Рассмотрим транспозиции $\tau_i = [k_i, l_i] \in S_n$. Очевидно, что $\tau \circ \sigma = \tau_1 \circ \cdots \circ \tau_m$. Поэтому $\sigma = \tau \circ \tau_1 \circ \cdots \circ \tau_m$. □

Для перестановки $\Pi = (i_1, \ldots, i_n)$ и подстановки $\sigma \in S_n$ положим $\sigma(\Pi) = (\sigma(i_1), \ldots, \sigma(i_n))$. Ясно, что $\sigma(\Pi)$ – перестановка и $\delta \circ \sigma(\Pi) = \delta(\sigma(\Pi))$.

Следствие. *Любые две перестановки из одинакового числа элементов могут быть получены друг из друга применением конечного числа транспозиций.*

Доказательство. Пусть $\Pi = (i_1, \ldots, i_n)$ и $\Pi' = (j_1, \ldots, j_n)$. Рассмотрим подстановку

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

По теореме $\sigma = \tau_1 \circ \cdots \circ \tau_r$, где τ_k – транспозиции. Тогда

$$\Pi' = \sigma(\Pi) = \tau_1 \circ \cdots \tau_r(\Pi) = \tau_1(\tau_2(\cdots \tau_r(\Pi)))$$

□

Рассмотрим перестановку $\Pi = (i_1, \ldots, i_k, \ldots, i_l, \ldots, i_n)$. По определению перестановки $i_k \neq i_l$ при $k \neq l$. Пусть $k < l$. Если $i_k > i_l$, то мы будем говорить, что элементы i_k и i_l образуют инверсию. *Четностью* перестановки назовем четность общего числа инверсий.

Пример. Пусть $1 \leq i < j \leq n$. Число инверсий в перестановке

$$(1, 2, \ldots i-1, j, i+1, \ldots, j-1, i, j+1, \ldots, n-1, n)$$

равно $j - i + \underbrace{1 + \cdots + 1}_{j-i-1} = 2(j-i) - 1$. Поэтому перестановка – нечетная.

Лемма. *Четность перестановки меняется при применении транспозиции.*

Доказательство. Пусть $\Pi = (i_1, \ldots, i_n)$, пусть $\tau = [a, b]$, $a \neq b$. Ясно, что $a = i_k$, $b = i_l$ для некоторых $i_k \neq i_l$, $k < l$. Таким образом, $\Pi = (i_1, \ldots, i_k, \ldots, i_l, \ldots, i_n)$ и $\tau = [i_k, i_l]$. Тогда $\tau(\Pi) = (i_1, \ldots, i_l, \ldots, i_k, \ldots, i_n)$. Обозначим через r_α (соотв. s_α)) число инверсий, которые образует число, стоящее на месте α в Π (соотв. $\tau(\Pi)$) со всеми последующими. Рассмотрим сначала

случай $l = k + 1$. Если $\alpha < k$ или $\alpha > k + 1$, то $r_\alpha = s_\alpha$). Для $\alpha = k$ и $\alpha = k + 1$ имеем

$$s_k = \begin{cases} r_{k+1} + 1 & \text{если } i_k < i_{k+1} \\ r_{k+1} & \text{если } i_k > i_{k+1} \end{cases}$$

$$s_{k+1} = \begin{cases} r_k & \text{если } i_k < i_{k+1} \\ r_k - 1 & \text{если } i_k > i_{k+1} \end{cases}$$

В итоге получаем $\sum s_\alpha = \sum r_\alpha \pm 1$. Остается заметить, что для произвольных k и $l > k + 1$ мы имеем

$$[i_k, i_l] = [i_k, i_{k+1}] \circ [i_{k+1}, i_l] \circ [i_{k+1}, i_k]$$

и таким образим каждая транспозиция $[i_k, i_l]$ раскладывается в композицию нечетного числа транспозиций "соседних" элементов. □

Определение. Четностью подстановки

$$\sigma = \begin{pmatrix} i_1 & i_2 & \cdots & i_{n-1} & i_n \\ j_1 & j_2 & \cdots & j_{n-1} & j_n \end{pmatrix}$$

называется четность суммы числа инверсий в первой и второй строках. Согласно предыдущей лемме четность подстановки не зависит от вида записи (при транспозиции столбцов меняется четность числа инверсий в обоих строках). Знаком σ называется

$$\operatorname{sgn}(\sigma) := (-1)^{\text{четность } (\sigma)}.$$

Пример. Согласно предыдущему примеру транспозиция является нечетной подстановкой.

Предложение.
- $\operatorname{sgn}(\sigma_1 \circ \sigma_2) = \operatorname{sgn}(\sigma_1)\operatorname{sgn}(\sigma_2)$.
- $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.

Множество всех четных подстановок мы обозначим через A_n.

Предложение. *Число четных подстановок равно числу нечетных подстановок и равно* $n!/2$.

Доказательство. Зафиксируем некоторую нечетную подстановку τ (например, транспозицию). Согласно сказанному выше $\forall \sigma \in A_n \quad \tau \circ \sigma \in S_n \setminus A_n$. Следовательно, имеется отображение $f : A_n \to S_n \setminus A_n$, $f(\sigma) = \tau \circ \sigma$. Легко показать, что оно биективно. Следовательно, множества A_n и $S_n \setminus A_n$ равномощны. □

2.3 Циклы

Определение. Пусть $\sigma \in S_n$. Элемент $j \in \{1, \ldots, n\}$ называется *неподвижным* для σ, если $\sigma(j) = j$ и *подвижным*, если $\sigma(j) \neq j$. Множество всех неподвижных элементов мы обозначим через $F(\sigma)$, а множество всех подвижных – через $M(\sigma)$.

Замечание. Ясно, что $M(\sigma_1 \circ \sigma_2) \subset M(\sigma_1) \cup M(\sigma_2)$ и $F(\sigma_1 \circ \sigma_2) \supset F(\sigma_1) \cap F(\sigma_2) \quad \forall \sigma_1, \sigma_2 \in S_n$.

Лемма. *Если для подстановок* $\sigma, \varphi \in S_n$ *выполнено* $M(\sigma) \cap M(\varphi) = \emptyset$, *то* $\sigma \circ \varphi = \varphi \circ \sigma$ *(т.е.* σ *и* φ *коммутируют).*

Определение. Подстановка $\sigma \in S_n$ называется *циклом* (*циклической подстановкой*), если $M(\sigma) = \{i_1, \ldots, i_m\}$ и

$$\sigma(i_k) = \begin{cases} i_{k+1} & \text{при } k = 1, \ldots, m-1, \\ i_1 & \text{при } k = m. \end{cases}$$

Такая подстановка обозначается $\sigma = [i_1, \ldots, i_m]$. Число m называется *длиной* цикла.

Цикл длины 2 – это транспозиция. Запись $\sigma = [i_1, \ldots, i_m]$ не единственна. Ясно, что $[i_1, \ldots, i_m] = [i_2, \ldots, i_m, i_1] = [i_3, \ldots, i_m, i_1, i_2]$ и т. д.

Циклы $\sigma = [i_1, \ldots, i_m]$ и $\varphi = [j_1, \ldots, j_l]$ называются *независимыми*, если $M(\sigma) \cap M(\varphi) = \emptyset$.

Теорема. *Любая подстановка* $\sigma \in S_n$ *представляется в виде произведения независимых циклов* $\sigma = \sigma_1 \circ \cdots \sigma_l$. *Это произведение единственно с точностью до порядка множителей.*

Доказательство. Докажем утверждение индукцией по числу элементов в $M(\sigma)$. Пусть $i_1 \in M(\sigma)$ – подвижный элемент. Положим $i_k := \sigma^{k-1}(i_1)$. Таким образом, $i_{k+1} = \sigma(i_k)$. Все элементы $i_1, i_2, \cdots \in \Omega_n$ не могут быть различны. Поэтому $i_{k+r} = i_k$ для некоторых $k,\ r \in \mathbb{N}$. Выберем $k,\ r \in \mathbb{N}$ – так, что r –

наименьшее, удовлетворяющее этому условию. Тогда для все числа $i_1, \ldots, i_r$ различны и

$$i_{r+1} = \sigma^r(i_1) = \sigma^{-(k-1)}(\sigma^{k-1+r}(i_1)) =$$
$$= \sigma^{-(k-1)}(i_{k+r}) = \sigma^{-(k-1)}(i_k) = \sigma^{-(k-1)}(\sigma^{k-1}(i_1)) = i_1.$$

Положим $\sigma_1 := [i_1, \ldots, i_r]$ и $\sigma' = \sigma \circ \sigma_1^{-1}$. Имеем

$$\sigma'(i_k) = \begin{cases} \sigma(i_r) = i_1 & \text{при } k = 1, \\ \sigma(i_{k-1}) = i_k & \text{при } k = 2, \ldots, r \end{cases}$$

т.е. $i_k \in F(\sigma') \quad k = 1, \ldots, r-1$. Если же $j \notin \{i_1, \ldots, i_r\}$, то $\sigma'(j) = \sigma(j)$. Таким образом, $M(\sigma) = M(\sigma') \cup M(\sigma_1)$ и $M(\sigma') \cap M(\sigma_1) = \emptyset$. $\square$