ЛЕКЦИЯ 4

РАЗЛОЖЕНИЕ ПОДСТАНОВОК НА ЦИКЛЫ

СТЕПЕНИ ПОДСТАНОВОК

ЧЕТНОСТЬ ПОДСТАНОВОК

РАЗЛОЖЕНИЕ ПОДСТАНОВКИ НА ЦИКЛЫ

Разложим теперь подстановки из S_n в произведение более простых подстановок, называемых *циклами*.

Что такое цикл? Это перестановка, в которой элементы переставляются по циклу:

$$i_1 \mapsto i_2 \mapsto \cdots \mapsto i_{k-1} \mapsto i_k \mapsto i_1.$$

Такой цикл записывается как $(i_1\, i_2\, \ldots\, i_{k-1}\, i_k)$, но можно также начинать запись с любого другого элемента из цикла: $(i_t\, i_{t+1}\, \ldots)$.

Любую подстановку можно разложить в произведение циклов, элементы которых не пересекаются.

Теорема 1. *Любая подстановка в S_n раскладывается в произведение независимых циклов. Эти циклы определяются однозначно по подстановке, с точностью до их перестановки.*

Доказательство. Действительно, пусть у нас есть подстановка $\sigma \in S_n$. Посмотрим, куда переходит 1. Если $1 \mapsto 1$, то это и есть маленький цикл длины один. Пусть $i_1 \neq 1$, тогда посмотрим на $\sigma(i_1) = i_{i_1}$. Если $i_{i_1} = 1$, то мы получили цикл длины два. Пусть $i_{i_1} \neq 1$, то посмотрим на образ этого элемента и т.д.

Понятно, что в какой-то момент образ очередного элемента станет равен 1 (если бы повторение произошло на другом элементе, то отображение σ оказалось бы не инъективным). Значит, к нас появился один цикл.

Если этот цикл не заметает все элементы, то рассмотрим следующий на очереди элемент, которого не было в первом цикле. Из него точно так же образуется цикл. Первый и второй циклы не могут пересечься, так как любое пересечение означает, что отображение не инъективно.

Будем продолжать эту процедуру далее, в результате чего получим разложение перестановки в произведение непересекающихся циклов.

Чтобы понять, что такое разложение единственно, заметим лишь, что разбиение множества $\{1, 2, \ldots, n\}$ элементов подстановки на циклы однозначно, потому что только внутри одного цикла можно попасть из одного элемента в другой, переставляя элементы соответственно σ несколько раз.

Если мы уже знаем множество в одном цикле, то сам цикл также формируется однозначно, так как определяется просто образами элементов. $\square$

ЦИКЛОВАЯ СТРУКТУРА ПОДСТАНОВКИ

Давайте для наглядности запишем в виде циклов все подстановки из двух, трех и четырех элементов.

Все подстановки из двух элементов исчерпываются двумя — тождественной e и циклом длины два — $(1\,2)$.

Подстановки из трех элементов бывают такие: тождественная e, циклы длины два — $(1\,2)$, $(1\,3)$, $(2\,3)$ и циклы длины три — $(1\,2\,3)$, $(3\,2\,1)$.

На четырех элементах структура подстановок становится чуть более разнообразной: тождественная e, циклы длины два — $(1\,2)$, $(1\,3)$, $(1\,4)$, $(2\,3)$, $(2\,4)$, $(3\,4)$, циклы длины три — $(1\,2\,3)$, $(3\,2\,1)$, $(1\,2\,4)$, $(4\,2\,1)$, $(1\,3\,4)$, $(4\,3\,1)$, $(2\,3\,4)$, $(4\,3\,2)$, циклы длины четыре — $(1\,2\,3\,4)$, $(4\,3\,2\,1)$, $(1\,2\,4\,3)$, $(3\,4\,2\,1)$, $(1\,3\,2\,4)$, $(4\,2\,3\,1)$ и пары циклов длины два — $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ и $(1\,4)(2\,3)$.

Циклы длины два называют *транспозициями*.

Пусть π — произвольная подстановка из S_n. Ее *степень* π^s определяется по индукции:

$$\pi^s = \begin{cases} \pi(\pi^{s-1}), & \text{если } s > 0, \\ e, & \text{если } s = 0, \\ \pi^{-1}((\pi^{-1})^{-s-1}), & \text{если } s < 0. \end{cases}$$

При таком определении очевидно, что

$$\pi^s \pi^t = \pi^{s+t} = \pi^t \pi^s, \quad t, s \in \mathbb{Z}.$$

Так как мы рассматриваем подстановки на конечном числе элементов, то на самом деле для каждой подстановки $\pi \in S_n$ найдется однозначно определенное натуральное число $q = q(\pi)$ такое, что все различные степени нашей подстановки содержатся в множестве

$$\langle \pi \rangle = \{e, \pi, \pi^2, \ldots, \pi^{q-1}\}$$

и $\pi^q = e$.

Это число q называется еще *порядком* подстановки π.

Получается, что рассмотренные выше перестановки имели порядки $1, 2, 3, 4$.

Теорема 2. *Если подстановка σ разложена в произведение непересекающихся циклов:*

$$\sigma = \sigma_1 \sigma_2 \ldots \sigma_m,$$

длины которых равны $l_1, l_2, \ldots, l_m$, соответственно, то порядок подстановки σ равен наименьшему общему кратному чисел $l_1, \ldots, l_m$.

Доказательство. Так как независимые циклы коммутируют, то

$$\sigma^k = \sigma_1^k \sigma_2^k \ldots \sigma_m^k.$$

Для того, чтобы $\sigma^k = e$, необходимо и достаточно, чтобы

$$\sigma_1^k = e,\ \sigma_2^k = e, \ldots, \sigma_m^k = e,$$

а это равносильно тому, что

$$l_1, l_2, \ldots, l_m | k.$$

Таким образом, наименьшее подходящее k — это наименьшее общее кратное чисел $l_1, l_2, \ldots, l_m$. $\square$

ЧЕТНОСТЬ ПОДСТАНОВОК

Лемма 1. *Каждая подстановка $\pi \in S_n$ является произведением транспозиций.*

Доказательство. В силу того, что любая подстановка раскладывается в произведение непересекающихся циклов, нам достаточно доказать, что любой цикл $(i_1\, i_2\, \ldots\, i_{k-1}\, i_k)$ раскладывается в произведение транспозиций.

Это разложение можно предъявить в явном виде:

$$(i_1\, i_2\, \ldots\, i_{k-1}\, i_k) = (i_1\, i_2)(i_2\, i_3)\ldots(i_{k-1}\, i_k).$$

$\square$

Определение 1. У подстановки

$$\begin{pmatrix} 1 & 2 & \ldots & k & \ldots & n \\ i_1 & i_2 & \ldots & i_k & \ldots & i_n \end{pmatrix}$$

инверсией называется такая пара столбиков $\begin{pmatrix} l \\ i_l \end{pmatrix}$ и $\begin{pmatrix} k \\ i_k \end{pmatrix}$, что $l < k$, но $i_l > i_k$.

Определение 2. *Четностью* подстановки $\sigma \in S_n$ называется четность количества всех инверсий в этой подстановке.

Очевидно, что тождественная подстановка является четной, так как не содержит ни одной инверсии.

Транспозиция $(i\, j)$ всегда нечетна.

Теорема 3. *Умножение на транспозицию (слева или справа) меняет четность подстановки.*

Замечание 1. Предварительно заметим, что умножение на транспозицию слева или справа меняет у подстановки ровно два элемента во второй строчке.

Доказательство. Соответственно сформулированному замечанию нам надо показать, что если в подстановке поменять два элемента во второй строчке, то ее четность изменится на противоположную.

Пусть для начала эти элементы являются соседними, то есть

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots n & \\ i_1 & i_2 & \dots & i_k & i_{k+1} & \dots & i_n \end{pmatrix},$$

после умножения на транспозицию

$$\sigma' = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots n & \\ i_1 & i_2 & \dots & i_{k+1} & i_k & \dots & i_n \end{pmatrix}.$$

Все инверсии, которые существовали между столбцами с номерами меньше k или больше $k+1$, либо между одним из таким столбцов и либо k-м, либо $k+1$-м, сохранятся (так как порядок следования между этими парами столбцов не изменится. Если между столбцами с номерами k и $k+1$ не было инверсии, то они появится, если же инверсия была, то она исчезнет.

Таким образом, число инверсий в подстановке σ' на одну отличается (на одну больше или на одну меньше), чем число инверсий в подстановке σ.

Значит, эти две подстановки имеют различную четность.

Если же мы поменяли в подстановке σ не соседние столбики, а столбики, которые находились на расстоянии m друг от друга, то это означало бы, что мы делаем сначала $m-1$ перестановку соседних столбиков (после чего они становятся соседними), далее меняем эти два столбика местами и за $m-1$ шаг возвращаем столбик на место. На это уйдет $2m-1$ операция, в которой мы меняем местами элементы в соседних столбиках, то есть произойдет нечетное число изменений четности подстановки.

Таким образом, постановка σ поменяет четность. $\square$

Следствие 1. *Если подстановку σ разложить в произведение транспозиций двумя способами, то четность числа транспозиций в разложениях будет одинаковой.*

Следствие 2. *Четность подстановки равна четности числа транспозиций в ее разложении.*

Лемма 2. *Четность цикла длины k равна четности числа $k-1$.*

Доказательство. Очевидно следует из разложения цикла длины k в произведение $k-1$ транспозиции. $\square$

Теорема 4. *Если подстановка $\sigma = \tau_1\tau_2\ldots\tau_m$ разложена в произведение m независимых циклов длин $l_1, l_2, \ldots, l_m$ соответственно, то ее четность равна*

$$(-1)^{\sum\limits_{i=1}^{m}(l_i-1)}.$$

Доказательство. Очевидно следует из предыдущих леммы и следствий. $\square$

Теорема 5. *Множество всех четных перестановок (обозначаемое через A_n) замкнуто относительно операций умножения и взятия обратной перестановки (то есть является группой).*

Доказательство. Очевидно следует из предыдущих теорем. $\square$

Так как все подстановки делятся на четные и нечетные, рассмотрим разбиение

$$S_n = A_n \cup \overline{A}_n, \quad \overline{A}_n = S_n \setminus A_n.$$

Установим биективное соответствие между множествами A_n и $\overline{A}_n$, сопоставляя каждой подстановке $\sigma \in A_n$ подстановку $\sigma \cdot (1\,2) \in \overline{A}_n$.

Очевидно, что такое соответствие является биективным, откуда получаем, что четные подстановки составляют ровно половину от всех подстановок.