Лекция 10

Определение 1. *Перестановка* длины (степени, порядка) n – это упорядоченный в каком-нибудь порядке набор чисел $1, 2, \ldots, n$.

Подстановка длины (степени, порядка) n – это биекция из множества $\{1, 2, \ldots, n\}$ в множество $\{1, 2, \ldots, n\}$.

Будем записывать подстановку σ в 2 строки:

$$\begin{pmatrix} \ldots & i & \ldots \\ \ldots & \sigma(i) & \ldots \end{pmatrix}$$

Например, подстановка $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$ соответствует биекции $\{1, 2, 3, 4, 5\} \to \{1, 2, 3, 4, 5\}$, которая переводит $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 5$, $4 \mapsto 1$, $5 \mapsto 3$.

Множество подстановок длины n обзначается S_n.

Заметим, что одной и той же подстановке соответствуют разные таблицы из 2-х строк. Важно лишь что под чем стоит:

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

Однако каждую подстановку можно записать в *стандартном виде*, то есть так, чтобы верхяя строка была упорядочена по возрастанию.

Лемма 1. *Количество перестановок длины n равно количеству подстановок длины n.*

Доказательство. Установим биекцию: перестановке сопоставим подстановку, у которой в стандартном виде нижняя строка совпадает с данной перестановкой. □

Лемма 2. $|S_n| = n!$.

Доказательство. Так как количество подстановок и перестановок одинаковое, будем считать перестановки длины n. Оформим подсчет в виде последовательного заполнения элементов перестановки слева-направо. Первый элемент можно выбрать n способами. Для второго есть $n-1$ вариант (нельзя на 2 место ставить то число, которое поставили на первое). Для третьего элемента существует $n-2$ варианта и т.д. В итоге получаем $n(n-1)(n-2)\ldots 1 = n!$ вариантов. □

Определение 2. Пусть $\sigma, \delta \in S_n$. *Произведением* (композицией) этих подстановок называется подстановка $\sigma\delta = \sigma \circ \delta \in S_n$.

Имеем $\sigma \circ \delta(i) = \sigma(\delta(i))$.

$$\sigma\delta = \begin{pmatrix} \ldots & i & \ldots \\ \ldots & \sigma(\delta(i)) & \ldots \end{pmatrix} = \begin{pmatrix} \ldots & \delta(i) & \ldots \\ \ldots & \sigma(\delta(i)) & \ldots \end{pmatrix} \begin{pmatrix} \ldots & i & \ldots \\ \ldots & \delta(i) & \ldots \end{pmatrix}.$$

Пример 1.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 5 & 1 & 3 & 7 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 5 & 4 & 7 & 3 & 2 \end{pmatrix}$$

Теорема 1 (Свойства произведения подстановок)**.**

- *Ассоциативность* $(\sigma\delta)\xi = \sigma(\delta\xi)$.
  Как мы видели, ассоциативность верна для любых отображений.
- *Обобщенная ассоциативность (следствие ассоциативности).*
- *Рассмотрим тождественную подстановку*

  $$\mathrm{id} = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ 1 & 2 & 3 & \ldots & n \end{pmatrix}.$$

  Для любой подстановки $\sigma \in S_n$ имеем $\sigma\,\mathrm{id} = \mathrm{id}\,\sigma = \sigma$.
- *Для любой подстановки $\sigma \in S_n$ существует единственная обратная подстановка $\sigma^{-1} \in S_n$ такая, что $\sigma\,\sigma^{-1} = \sigma^{-1}\sigma = \mathrm{id}$. Подстановка σ^{-1} получается из σ, если поменять 1-ю и 2-ю строки местами.*
- *При $n > 2$ коммутативность отсутствует. $\sigma\,\delta \neq \delta\,\sigma$.*

Пример 2 (Пример отсутствия коммутативности)**.**

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

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

Определение 3. Подстановка $\sigma \in S_n$ называется *циклом*, если существуют числа $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$ такие что $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$,..., $\sigma(a_{k-1}) = a_k$, $\sigma(a_k) = a_1$, $\sigma(i) = i$ при $i \notin \{a_1, \ldots, a_k\}$.

Данный цикл будем обозначать $(a_1, a_2, \ldots, a_k)$. Число k назовем длиной цикла. При этом

$$(a_1, a_2, \ldots, a_k) = (a_2, a_3, \ldots, a_k, a_1) = \ldots = (a_k, a_1, a_2, \ldots, a_{k-1})$$

Легко видеть, что $(a) = \mathrm{id}$. Цикл дины 2 называется *транспозицией*.

Определение 4. Два цикла называются *независимыми*, если для них множества $\{a_1, \ldots, a_k\}$ не пересекаются. То есть подвижные элементы одного цикла являются неподвижными для другого.

Каждой подстановке σ можно сопоставить ориентированный граф $\Gamma(\sigma)$ на n вершинах $v_1, \ldots, v_n$. При этом из v_i есть стрелка в v_j, если и только если $\sigma(i) = j$. Если $\sigma(i) = i$, получаем петлю.

Лемма 3. *Для любой подстановки σ граф $\Gamma(\sigma)$ есть объединение нескольких ориентированных циклов.*

Доказательство. Из каждой вершины выходит ровно одна стрелка и в каждую вершину входит ровно одна стрелка. Пойдем по стрелкам из некоторой вершины. Войдя в некоторую вершину мы всегда будем иметь возможность выйти. В силу конечности количества вершин, мы придем в ту вершину, в которой уже были. Рассмотрим первую такую вершину. Это та вершина, из которой мы начинали (в остальные вершины идут стрелки из тех, где мы уже были). Получим ориентированный цикл. Далее встанем на любую, не вошедшую в него вершину, и пойдем по стрелкам. Получим еще один цикл. И т.д. □

Теорема 2 (Разложение в независимые циклы)**.** *Любая подстановка $\sigma \in S_n$ есть произведение независимых циклов.*

Доказательство. Рассмотрим граф $\Gamma(\sigma)$ и запишем все его циклы. Произведение этих (независимых) циклов и есть перестановка σ. В самом деле, если $\sigma(i) = j$, то i и j являются подвижными элементами ровно одного цикла и неподвижными для всех остальных. При произведении (идем по множителям справа-налево) сперва много раз i переходит в i, затем i переходит в j, а затем много раз j переходит в j. □

Так как циклы длины 1 – это тождественные подстановки, их можно исключить из данного произведения.

Пример 3.

$$\begin{pmatrix}1&2&3&4&5&6&7\\2&4&7&1&5&6&3\end{pmatrix}=(1,2,4)(3,7)(5)(6)=(1,2,4)(3,7).$$

Замечание 1. В записи подстановки в виде произведения независимых циклов не важен порядок циклов (независимые циклы коммутируют) и не важно, с какого элемента начинать цикл (но последовательность, что за чем идет важна). Например,

$$(1,2,3,4)(5,6)(7,8,9) = (8,9,7)(3,4,1,2)(6,5).$$

Определение 5. Пусть α – перестановка длины n. Тогда пара (i, j) называется *инверсией* для α, если $i > j$ и при этом i стоит левее, чем j.

Определение 6. *Четность* перестановки α – это четность количества инверсий в ней.

Определение 7. *Четность* подстановки σ – это четность ее нижней строки в стандартном виде.

Эквивалентно, четность σ равна четности количества пар (a, b) таких, что $a < b$ и $\sigma(a) > \sigma(b)$. (Такие пары мы называем *инверсиями* в подстановке.)

Теорема 3. *Пусть $\sigma \in S_n$. Умножение на транспозицию $\tau = (i, j)$ слева меняет числа i и j в нижней строке. Умножение на $\tau = (i, j)$ справа меняет числа i и j в верхней строке, или, что эквивалентно, меняет числа $\sigma(i)$ и $\sigma(j)$ в нижней строке.*

Доказательство. Если $a \notin \{i, j\}$, то $\tau(a) = a$. Значит, если $\sigma(x) \notin \{i, j\}$, то $\tau\sigma(x) = \sigma(x)$. Если же $\sigma(x) = i$, то $\tau\sigma(x) = j$, и наоборот, если $\sigma(x) = j$, то $\tau\sigma(x) = i$. Это доказывает первое утверждение.

Если же рассматривать $\sigma\tau$, то при $a \notin \{i, j\}$, получаем $\sigma\tau(a) = a$. Кроме того $\sigma\tau(i) = \sigma(j)$ и $\sigma\tau(j) = \sigma(i)$. Это доказывает второе утверждение. □

Лемма 4. *При умножении справа на транспозицию $\tau = (i, i+1)$ подстановка σ меняет четность.*

Доказательство. Рассмотримнижнюю строку подстановки σ в стандартном виде. Обозначим ее α. При умножении справа на τ в α поменяются местами элементы u и v на местах i и $i + 1$, получится α', которая соответствует подстановке σ'.

Пусть $a, b \notin \{i, i+1\}$. Тогда пара (a, b) является или не является инверсией для σ и σ' одновременно. В самом деле на местах a и b в α и α' стоят одинаковые числа.

Пара (i, a) является инверсией для σ тогда и только тогда, когда $(i + 1, a)$ является инверсией для σ'. И наоборот, пара $(i + 1, a)$ является инверсией для σ тогда и только тогда, когда (i, a) является инверсией для σ'. В самом деле, $\sigma(i)$ теперь стоит на месте $i+1$. Но если $a > i$, то $a > i+1$ (напомним, $a, \notin \{i, i + 1\}$), и если $a < i$, то $a < i + 1$.

Таким образом, количество инверсий кроме $(i, i + 1)$ в подстановках σ и σ' одинаково. Однако, пара $(i, i + 1)$ является инверсией ровно для одной из двух подстановок σ и σ'. Это доказывает, что четности у σ и σ' разные. □

Лемма 5. *При умножении справа на транспозицию $\tau = (i, j)$ подстановка σ меняет четность.*

Доказательство. Представим транспозицию (i, j) в виде произведения нечетного числа транспозиций соседних элементов. Считаем $j > i$.

$$(i, j) = (i, i + 1)(i + 1, i + 2) \dots (j - 2, j - 1)(j - 1, j)(j - 2, j - 1) \dots (i + 1, i + 2)(i, i + 1).$$

Так как при умножении слева на каждую транспозицию соседних четность меняется, то она поменяется. □

Лемма 6. *Любую подстановку σ можно представить в виде произведения некоторого количества транспозиций.*

Доказательство. Начнем с тождественной подстановки и будем делать послевовательно образы элементы нужными. Пусть $\sigma(1) = a$, домножим id на транспозицию $(1, a)$ слева и получим δ_1 такое, что $\delta_1(1) = a$. Пусть $\sigma(2) = b$, $\delta_1(2) = b'$. Если $b = b'$, то $\delta_2 = \delta_1$. Если $b \neq b'$, то $\delta_2 = (b, b')\delta_1$. Легко видеть, что $\delta_2(1) = a, \delta_2(2) = b$. И т.д. $\delta_{n-1} = \sigma$. □

Так как при умножении на транспозицию четность меняется, получаем.

Теорема 4. *Четность подстановки σ – это четность количества транспозиций в любом разложении σ на транспозиции.*

Определение 8. *Знак* подстановки σ – это

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, \text{ если } \sigma \text{ четная,} \\ -1, \text{ если } \sigma \text{ нечетная.} \end{cases}$$

Теорема 5. $\operatorname{sgn}(\sigma\delta) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\delta)$.

Доказательство. Пусть $\sigma = \tau_1 \dots \tau_k$, $\delta = \eta_1 \dots \eta_m$ – разложения в произведения транспозиций. Тогда $\sigma\delta = \tau_1 \dots \tau_k\eta_1 \dots \eta_m$. □

Следствие 1. $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$.

Доказательство.

$$1 = \operatorname{sgn}(\mathrm{id}) = \operatorname{sgn}(\sigma^{-1})\operatorname{sgn}(\sigma).$$

□

Заметим, что

$$(a_1, \dots, a_k) = (a_1, a_2) \dots (a_{k-1}, a_k).$$

Следствие 2. $\operatorname{sgn}(a_1, \ldots, a_k) = (-1)^{k-1}$.

Определение 9. *Декремент* подстановки σ – это число $d(\sigma)$, равное n минус количество независимых циклов (тут циклы длины 1 считаются).

Теорема 6. $\operatorname{sgn}(\sigma) = (-1)^{d(\sigma)}$

Доказательство. Пусть длины независимых циклов $k_1, \ldots, k_m$. Тогда

$$\operatorname{sgn}(\sigma) = \prod_{i=1}^{m} (-1)^{k_i - 1} = (-1)^{\left(\sum_{i=1}^{m} k_i\right) - m} = (-1)^{n-m} = (-1)^{d(\sigma)}.$$

□

Лемма 7. *Четных и нечетных подстановок в S_n при $n \geq 2$ одинаковое число, то есть по $\frac{n!}{2}$.*

Доказательство. Отображение $\Phi\colon \sigma \to (1,2)\sigma$ устанавливает биекцию между четными и нечетными подстановками. В самом деле, если $(1,2)\sigma = (1,2)\delta$, то умножая это равенство на $(1,2)^{-1} = (1,2)$ получаем $\sigma = \delta$. Это доказывает инъективность Φ. Пусть теперь β – некоторая нечетная подстановка. Тогда $\beta = (1,2)\alpha$, для $\alpha = (1,2)\beta$ – четная подстановка. Это доказывает сюръективность Φ.

Так как Φ – биекция, четных и нечетных подстановок одинаковое количество. Так как в сумме их $n!$, количество четных равно количеству нечетных и равно $\frac{n!}{2}$. □