.

Лекция 1

Симметрическая группа перестановок

Содержание лекции:
В настоящей лекции мы коротко напомним об основных свойствах перестановок и действий с ними. В дайльнейшем приведенные здесь факты окажутся полезными.

Ключевые слова:
Перестановка, транспозиция, инверсия, четность перестановки, подстановка, четность подстановки, композиция подстановок, циклические подстановки.

Авторы курса:

Трифанов А. И. Москаленко М. А.

Ссылка на ресурсы:
`mathdep.ifmo.ru/geolin`

1.1 Перестановки

Nota bene Здесь мы будем рассматривать некоторое конечное множество M_n, состоящее из n элементов

$$M = \{a, b, \ldots, x, y, z\},$$

которые могут быть перенумерованы при помощи первых n натуральных чисел. Так как свойства элементов множества M не будут играть никакой роли, примем, что элементами M являются сами числа $1, 2, \ldots, n$, то есть

$$M = \{1, 2, \ldots, n\}.$$

Перестановкой элементов конечного множества M_n называется всякое упорядоченное расположение всех его элементов.

Пример 1.1. Некоторые перестановки из 4 чисел:

$$(1, 2, 3, 4), \quad (3, 2, 1, 4), \quad (4, 2, 3, 1).$$

Лемма 1.1. *Число перестановок из n символов равно*

$$1 \cdot 2 \cdot \ldots \cdot n = n!.$$

►
Произвольная перестановка из n элементов имеет вид

$$(x_1, x_2, \ldots, x_n),$$

где x_i можно выбрать $(n - i + 1)$ различными способами. Число различных перестановок равно числу способов придать различные значения элементам x_i.
◄

Транспозицией на множестве перестановок называется преобразование, при котором меняются местами какие-либо два символа перестановки, а остальные символы остаются на месте.

Лемма 1.2. *От любой перестановки из n символов можно перейти к любой другой перестановке из тех же символов при помощи конечного числа транспозиций.*
►
Данное утверждение эквивалентно утверждению о том, что все $n!$ перестановок из n символов можно расположить в таком порядке, что каждая следующая будет получаться из предыдущей одной транспозицией, причем начинать можно с любой перестановки. Используем индукцию:

- База индукции:

$$(1, 2) \to (2, 1), \quad (2, 1) \to (1, 2).$$

- Предположение: пусть доказано для перестановок из $(n-1)$ элементов.
- Переход: рассмотрим перестановку, состоящую из n элементов

$$(x_1, x_2, \ldots, x_n),$$

по индукционному предположению все перестановки, у которых x_1 стоит на первом месте можно упорядочить согласно требованиям теоремы, причем начиная с данной перестановки. В последней из полученных таким образом перестановок совершаем транспозицию символа x_1 с произвольным другим символом, например x_2 и упорядочим все перестановки, у которых на первом месте стоит x_2. Таким образом перебираются все перестановки из n элементов.

◄

Пример 1.2. Пример упорядочения перестановок из 3 символов согласно доказательству:

$$(1,2,3) \to (1,3,2) \to (2,3,1) \to (2,1,3) \to (3,1,2) \to (3,2,1).$$

Говорят, что в перестновке числа x_i и x_j образуют **инверсию**, если

$$x_i > x_j, \quad i < j.$$

Перестановка называется **четной**, если ее символы составляют четное число инверсий, и **нечетной** - в противном случае.

Nota bene Перестановка $(1,2,3,\ldots,n)$ четная при любом n, так как не содержит инверсий. Она называется базовой перестановкой.

Пример 1.3. Перестановки и четности:

$$\begin{array}{ccccc} (2,1,3,4) & - & 1 \text{ инверсия} & - & \text{нечетная;} \\ (4,1,3,2) & - & 4 \text{ инверсии} & - & \text{четная.} \end{array}$$

Лемма 1.3. *Всякая транспозиция меняет четность перестановки.*

►

Сначала рассмотрим случай, когда транспонируемые символы стоят рядом:

$$(\ldots, x_i, x_j, \ldots).$$

В том случае транспозиция элементов x_i и x_j не меняет инверсий, которые данные элементы образуют со всеми остальными (x_i и x_j остались справа от предстоящих элементов и слева от последующих). Однако, если x_i и x_j не образовывали инверсию,

то после транспозиции будут. Таким образом число инверсий изменилось на одну, то есть сменило четность.

Докажем теперь общий случай, когда x_i и x_j не стоят рядом, то есть между ними находятся $k \geq 1$ элементов. Тогда, чтобы совершить транспозицию x_i и x_j необходимо совершить $2k+1$ транспозиций: по k транспозиций каждого из x_i и x_j с этими k символами и еще одна транспозиция - переставить местами x_i и x_j. Таким образом общее число транспозиций нечетное и следовательно четность перестановки изменится.
◄

Лемма 1.4. *При $n \geq 2$ число четных перестановок из n символов равно числу нечетных, то есть равно $n!/2$.*
►
Все перестановки из n символов можно упорядочить так, что каждая получается из предыдущей одной транспозицией. Транспозиция меняет четность перестановки и значит любые две соседние перестановки будут иметь противоположные четности. Теперь утверждение следует из замечания о том, что при $n \geq 2$ число $n!/2$ - четное.
◄

1.2 Подстановки

Подстановкой степени n будем называть следующий символ

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

который *содержит* в каждой из строк перестановку из n элементов множества M_n и *определяет* в какой из элементов нижней строки переходит каждый элемент верхней строки.

Пример 1.4. Рассмотрим конкретный случай:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \Rightarrow \quad 1 \to 2, \quad 2 \to 1, \quad 3 \to 3.$$

Nota bene Каждая подстановка $\sigma : M_n \to M_n$ степени n определяет взаимно однозначное отображение множества M_n на себя:

$$\sigma : \quad (x_1, x_2, \dots, x_n) \mapsto (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}).$$

Пример 1.5. Действие подстановки на перестановку:

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

Подстановка называется **четной**, если четности соответствующих ей двух перестановок совпадают и **нечетной** - в противном случае.

Nota bene Сформулируем несколько *очевидных* лемм, следующих прямо из определения подстановки:

Лемма 1.5. *Общее число подстановок степени n равно $n!$*

Лемма 1.6. *Число четных подстановок равно числу нечетных и равно $n!/2$.*

Лемма 1.7. *Четная подстановка не меняет четность перестановки, тогда как нечетная подстановка - меняет.*

1.3 Симметрическая группа

Определим на множестве S_n подстановок степени n операцию **композиции подстановок**. Пусть $\sigma, \chi \in S_n$ две подстановки:

$$\sigma = \begin{pmatrix}1 & 2 & \dots & n\\ \sigma(1) & \sigma(2) & \dots & \sigma(n)\end{pmatrix}, \quad \chi = \begin{pmatrix}1 & 2 & \dots & n\\ \chi(1) & \chi(2) & \dots & \chi(n)\end{pmatrix},$$

тогда результатом их композиции будет следующий символ

$$\chi\circ\sigma = \begin{pmatrix}1 & 2 & \dots & n\\ \chi(\sigma(1)) & \chi(\sigma(2)) & \dots & \chi(\sigma(n))\end{pmatrix} = \begin{pmatrix}1 & 2 & \dots & n\\ (\chi\circ\sigma)(1) & (\chi\circ\sigma)(2) & \dots & (\chi\circ\sigma)(n).\end{pmatrix}$$

Nota bene Композиция подстановок является подстановкой.

Пример 1.6. Пусть даны две подстановки:

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

Найдем их композицию:

$$\chi\circ\sigma = \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 1 & 4\end{pmatrix}, \quad \sigma\circ\chi = \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix}.$$

Nota bene Композиция подстановок - некоммутативная операция:

$$\chi \circ \sigma \neq \sigma \circ \chi.$$

Лемма 1.8. *Операция композиции ассоциативна:*

$$\forall \sigma, \chi, \varphi \quad (\sigma \circ \chi) \circ \varphi = \sigma \circ (\chi \circ \varphi)$$

Лемма 1.9. *На множестве S_n относеительно закона композиции существует нейтральный элемент:*

$$\exists\, \mathrm{id} \in S_n : \quad \forall \sigma \in S_n \quad \sigma \circ \mathrm{id} = \sigma = \mathrm{id} \circ \sigma.$$

►
Предъявляем:

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

◄

Лемма 1.10. *Для каждого элемента $\sigma \in S_n$ сущесвует обратный σ^{-1}:*

$$\forall \sigma \in S_n \quad \exists \sigma^{-1} \in S_n : \quad \sigma \circ \sigma^{-1} = \mathrm{id} = \sigma^{-1} \circ \sigma.$$

►
Предъявляем:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix},$$

◄

Теорема 1.1. *Операция композиции на множестве S_n индуцирует структуру некоммутативной группы - группы автоморфизмов $\mathrm{Aut}(M_n)$ множества M_n.*

Nota bene Всякая транспозиция $t_{ij}^{(n)}$ элементов x_i и x_j перестановки является элементом $S_n = \mathrm{Aut}(M_n)$:

$$t_{ij}^{(n)} = \begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & j & \dots & i & \dots \end{pmatrix}$$

Лемма 1.11. *Всякая подстановка σ представима в виде произведения транспозиций.*
►
Все перестановки из n чисел можно получить из одной из них последовательным применением транспозиций. Следовательно, всякая подстановка может быть получена из тождественной подстановки путем последовательного применения транспозиций в нижней строке, то есть последовательных композиций с подстановками вида $t_{ij}^{(n)}$.
◄

Пример 1.7. Разложение подстановки в композицию транспозиций:

$$\begin{pmatrix}1&2&3&4&5\\2&5&4&3&1\end{pmatrix} = (1,2)(1,5)(3,4), \quad (i,j) \triangleq t_{ij}^{(5)}.$$

Nota bene Разложение подстановки в композицию транспозиций не единственно.

Лемма 1.12. *При любом разложении подстановки в композицию транспозиций четность числа элементов композиции совпадает с четностью подстановки.*

Циклической (или циклом) называется подстановка, которая переставляет элементы некоторого подмножества $A \subset M_n$ циклическим образом. При этом мощность множества A называется **длиной цикла**.

Пример 1.8. Рассмотрим цикл:

$$\langle 1,3,2\rangle = (1 \to 3 \to 2 \to 1),$$

Ему соответствует следующая подстановка:

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

Nota bene Всякая транспозиция является циклической подстановкой:

$$t_{ij}^{(n)} = \langle i,j\rangle$$

Два цикла степени n называются **независимыми**, если они не имеют общих переставляемых символов.

Пример 1.9. Пример независимых циклов для подстановки степени 6:

$$\langle 1,5\rangle, \quad \langle 2,3,4\rangle.$$

Лемма 1.13. *Всякая подстановка может быть единственным образом разложена в композицию попарно независимых циклов.*

Пример 1.10. Разложение подстановки степени 5 в композицию циклов:

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

Nota bene Наконец, напомним наиболее важные комбинаторные понятия:

- **сочетанием** из n по k называется набор из k элементов, выбранных из n-элементного множества, в котором *не учитывается* порядок элементов. Число сочетаний равно
$$C_n^k = \frac{n!}{k!(n-k!)}.$$
- **размещением** из n по k называется набор из k элементов, выбранных из n-элементного множества, в котором *учитывается* порядок элементов. Число сочетаний равно
$$A_n^k = \frac{n!}{(n-k)!}.$$