# Группа перестановок. Транспозиции. Четные и нечетные перестановки. Порядок элементов

# 1 Перестановки. Группа перестановок

**Определение 1.1.** *Перестановкой будем называть биекцию конечного множества на себя.*

**Определение 1.2.** *Канонической записью перестановки $\pi$ конечного множества, элементы которого пронумерованы от 1 до $n$, будем называть следующую запись:*

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

**Определение 1.3.** *Пусть заданы две перестановки $\pi$ и $\sigma$. Тогда их композиция $\sigma \circ \pi$ определяется следующим образом:*

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

**Замечание 1.1.** *Пусть заданы две следующие перестановки:*

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

*По определению $\pi = \sigma$, но запись перестановки $\sigma$ не является канонической.*

**Определение 1.4.** *Обратной перестановкой к престановке $\pi$ будем называть такую перестановку $\pi^{-1}$, что $\pi \cdot \pi^{-1} = \pi^{-1} \cdot \pi = e$.*

**Замечание 1.2.** *Пусть задана перестановка $\pi$ в канонической записи:*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

*Тогда:*

$$\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix}$$

**Замечание 1.3.** *Нетрудно убедиться, проверив справедливость аксиом группы, что множество всех перестановок $n$-элементного множества с операцией композиции перестановок "$\circ$" образуют группу перестановок, обозначаемую $S_n$.*

# 2 Цикловая запись перестановок

Пусть задана перестановка $\pi$ в канонической записи:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Рассмотрим произвольное число $i \in \{1, 2, \dots, n\}$ и следующий ряд:

$$i \longrightarrow \pi(i) \longrightarrow \pi(\pi(i)) \longrightarrow \dots \longrightarrow t$$

Так как элементов лишь конечное число, то в некоторый момент времени в ряду повторится какое-то число. Пусть в момент первого повтора последний элемент в ряду был $t = \pi^{(m)}(i)$. Покажем, что $t = i$. Действительно, пусть от противного это не так. Тогда при $k < m$ выполнено $t = \pi^{(k)}(i) = \pi^{(m)}(i)$. Так как справедливы аксиомы группы, то введем в рассмотрение $\pi^{-1}(t)$. Ясно, что $\pi^{-1}(t) = \pi^{(k-1)}(t) = \pi^{(m-1)}(t)$. Но рассматривался первый повтор. Получаем противоречие, что и требовалось. Полученное означает, что, начав ряд с произвольного элемента, в какой-то момент будет получен цикл. Значит имеет смысл говорить о цикловой записи перестановки.

**Замечание 2.1.** *Цикл, который был начат с произвольного элемента, может не исчерпывать все элементы исходного n-элементного множества. В качестве примера рассмотрим следующую перестановку в канонической записи:*

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

*Начав цикл с* 1*, получим следующее:*

$$1 \longrightarrow 3 \longrightarrow 5 \longrightarrow 1$$

*Или записывают короче:*

$$\begin{pmatrix} 1 & 3 & 5 \end{pmatrix}$$

*Но несложно видеть, что* 4 *нет в цикле.*

**Определение 2.1.** *Запись цикла*

$$\begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix}$$

*эквивалентна следующему:*

$$\begin{pmatrix} i_1 & i_2 & \dots & i_{k-1} & i_k \\ i_2 & i_3 & \dots & i_k & i_1 \end{pmatrix}$$

**Теорема 2.1.** *Любая перестановка раскладывается на композицию непересекающихся циклов единственным образом с точностью до записи цикла и порядка цикла.*

**Теорема 2.2.** *Непересекающиеся циклы коммутируют.*

**Лемма 2.1.** *Пусть дан цикл* $\begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix}$*. Тогда порядок этого цикла* $ord \begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix}$ *есть* $k$*, то есть*

$$ord \begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix} = k$$

*Доказательство.* Легко получается из применения соответствующей перестановки $k$ раз. □

**Теорема 2.3.** *Пусть перестановка* $\sigma$ *записана в виде композиции непересекающихся циклов, то есть:*

$$\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_k,$$

*где* $|\sigma_i| = c_i \; \forall i \in \{1, \ldots, k\}$*. Тогда справедливо следующее:*

$$ord(\sigma) = HOK(c_1, c_2, \ldots, c_k)$$

*Доказательство.* Так как циклы независимы и коммутируют, то для того, чтобы получить тождественную перестановку, необходимо возвести $\sigma$ в такую степень $m$, что

$$m \vdots c_i \quad \forall i \in \{1, \ldots, k\}$$

При этом порядок $\sigma$ есть наименьшее такое число $m$, откуда немедленно следует требуемое. □

# 3 Транспозиции

**Определение 3.1.** *Транпозицией будем называть цикл длины* 2*:*

$$\begin{pmatrix} i_1 & i_2 \end{pmatrix}$$

**Замечание 3.1.** *Всюду далее, где это уместно, операцию "$\circ$" будем для краткости заменять на операцию умножения.*

**Замечание 3.2.** *Заметим, что:*

$$\begin{pmatrix} i_1 & i_2 & \dots & i_k \end{pmatrix} = \begin{pmatrix} i_1 & i_k \end{pmatrix} \begin{pmatrix} i_1 & i_{k-1} \end{pmatrix} \dots \begin{pmatrix} i_1 & i_3 \end{pmatrix} \begin{pmatrix} i_1 & i_2 \end{pmatrix}$$

*Действительно, в этом несложно убедиться, преобразовав последовательно композицию в правой части равенства.*

**Замечание 3.3.** *Разложение перестановки на композицию транспозиций может не быть единственным. В самом деле, приведём следующий пример:*

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

**Теорема 3.1.** *Для различных разложений перестановки в произведение транспозиций, чётность количества транспозиций сохраняется.*

*Доказательство.* От противного предположим, что существует такая перестановка $\pi$, что:

$$\pi = \underbrace{(\quad)\dots(\quad)}_{\text{чётное число транспозиций}} = \underbrace{(\quad)\dots(\quad)}_{\text{нечётное число транспозиций}}$$

Рассмотрим теперь $\pi^{-1}$ и запишем композицию $\pi \circ \pi^{-1}$ таким образом, что для $\pi$ будем использовать разложение на чётное число транспозиций, а для $\pi^{-1}$ – разложение на нечётное число транспозиций (так можно сделать просто потому, что обратный элемент к композиции транспозиций есть эта композиция, записанная в обратном порядке, что очевидно проверяется непосредственным перемножением). При этом учтём, что по определению $\pi \circ \pi^{-1} = e$:

$$\pi \circ \pi^{-1} = e = \underbrace{(\quad)\dots(\quad)}_{\text{нечётное число транспозиций}} \tag{1}$$

Теперь докажем следующую лемму:

**Лемма 3.1.** *Пусть для некоторого натурального $n \geq 2$ перестановка $e$ раскладывается в композицию $n$ транспозиций. Тогда $e$ раскладывается и в композицию $n-2$ транспозиций.*

*Доказательство.* Рассмотрим некоторое разложение $e$ в композицию $n$ транспозиций:

$$e = \underbrace{(\quad)}_{\sigma_1}\underbrace{(\quad)}_{\sigma_2}\dots\underbrace{(s \quad t)}_{\sigma_p}\dots\underbrace{(\quad)}_{\sigma_n}$$

Возьмём теперь такую транспозицию $\sigma_p = \begin{pmatrix} s & t \end{pmatrix}$ в разложении $e$, что $s$ не встречается в $\sigma_{p+1}, \dots, \sigma_n$. Рассмотрим $\sigma_{p-1}$. Есть лишь несколько случаев:

1. $\sigma_{p-1} = \begin{pmatrix} s & t \end{pmatrix}$. Тогда $\sigma_{p-1}\sigma_p = e \implies$ получили разложение $e$ в $n-2$ транспозиции, что и требовалось.

2. $\sigma_{p-1} = \begin{pmatrix} q & r \end{pmatrix}$, причем $\{q, r\} \cap \{s, t\} = \varnothing$. Значит $\begin{pmatrix} s & t \end{pmatrix}$ и $\begin{pmatrix} q & r \end{pmatrix}$ коммутируют по непересекаемости. Тогда сдвинем $\sigma_p$ влево в разложении $e$:

$$\sigma_{p-1}\sigma_p \longrightarrow \sigma_p\sigma_{p-1}$$

3. $\sigma_{p-1} = \begin{pmatrix} s & r \end{pmatrix}$. Заметим, что:

$$\sigma_{p-1}\sigma_p = \begin{pmatrix} s & r & t \\ t & s & r \end{pmatrix} = \begin{pmatrix} s & t \end{pmatrix}\begin{pmatrix} r & t \end{pmatrix}$$

Тогда, заменив $\sigma_{p-1}\sigma_p$ на полученное выше представление, увидим, что $s$ вновь сдвинулась влево.

4. $\sigma_{p-1} = \begin{pmatrix} t & r \end{pmatrix}$. Заметим, что:

$$\sigma_{p-1}\sigma_p = \begin{pmatrix} s & t & r \\ r & s & t \end{pmatrix} = \begin{pmatrix} s & r \end{pmatrix}\begin{pmatrix} t & r \end{pmatrix}$$

Тогда, заменив $\sigma_{p-1}\sigma_p$ на полученное выше представление, увидим, что $s$ вновь сдвинулась влево.

Либо в некоторый момент времени придём к первому случаю, откуда получим требуемое, либо в конце получим следующее:

$$e = \begin{pmatrix} s & t' \end{pmatrix} \underbrace{\begin{pmatrix} \quad & \quad \end{pmatrix} \dots \begin{pmatrix} \quad & \quad \end{pmatrix}}_{\text{не содержат } s}, \quad s \neq t'$$

Но тогда легко видеть, что после последовательного применения транспозиций в полученном разложении $s$ перейдёт в $t' \neq s$, то есть $s$ не перейдет в себя. Получаем противоречие с тем, что рассматриваемое разложение есть разложение нейтрального элемента. Значит требуемое доказано. □

По доказанной лемме получаем, что из такого разложения

$$e = \underbrace{\begin{pmatrix} \quad & \quad \end{pmatrix} \dots \begin{pmatrix} \quad & \quad \end{pmatrix}}_{\text{нечётное число транспозиций}}$$

следует, что $e$ раскладывается в одну транспозицию (индуктивно уменьшаем длину на 2), что невозможно. Получаем противоречие с (1), а значит требуемое доказано. □

## 4 Четные и нечетные перестановки

**Определение 4.1.** *Перестановку $\pi$ будем называть чётной (нечётной), если существует разложение $\pi$ на композицию чётного (нечётного) числа транспозиций.*

**Замечание 4.1.** *Из теоремы 3.1 очевидно следует:*

1. *Композиция чётной и нечётной перестановки есть нечётная перестановка.*
2. *Композиция двух чётных перестановок есть чётная перестановка.*
3. *Композиция двух нечётных перестановок есть чётная перестановка.*

**Теорема 4.1.** *Пусть дана группа перестановок $S_n$. Тогда в $S_n$ чётных перестановок столько же, сколько нечётных.*

*Доказательство.* Пусть $A_n$ и $B_n$ – множества соответственно чётных и нечётных перестановок $S_n$. Рассмотрим такое отображение $\varphi\colon A_n \to B_n$, что:

$$\forall \pi \in A_n \hookrightarrow \varphi(\pi) = \begin{pmatrix} 1 & 2 \end{pmatrix} \pi$$

Заметим, что если $\pi$ – чётная перестановка, то $\begin{pmatrix} 1 & 2 \end{pmatrix} \pi$ – нечётная перестановка. При этом $\varphi$ инъективно, так как:

$$\forall \pi_1, \pi_2 \in A_n : \pi_1 \neq \pi_2 \hookrightarrow \begin{pmatrix} 1 & 2 \end{pmatrix} \pi_1 \neq \begin{pmatrix} 1 & 2 \end{pmatrix} \pi_2$$

К тому же $\varphi$ сюръективно, так как:

$$\forall \sigma \in B_n \quad \exists \pi = \begin{pmatrix} 1 & 2 \end{pmatrix} \sigma \in A_n : \varphi(\pi) = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \sigma = \sigma$$

Тогда $\varphi$ является биекцией, что и требовалось. □

**Теорема 4.2.** *Пусть дана группа перестановок $S_n$. Пусть также $A_n$ – группа относительно групповой операции $S_n$, имеющая элементами все чётные перестановки $S_n$. Тогда $A_n \triangleleft S_n$.*