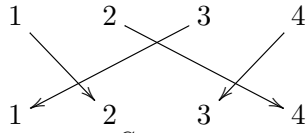


Определение 1. Перестановка чисел $1, \dots, n$ — это взаимно однозначное отображение множества $\{1, \dots, n\}$ на себя. Множество перестановок чисел $1, \dots, n$ обозначается S_n и называется *симметрической группой*.

Задача 1. Сколько элементов в симметрической группе S_n ?

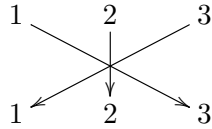
Перестановки записывают таблицами вида $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$; такая таблица означает перестановку $1 \mapsto 2$

(то есть 1 переходит в 2), $2 \mapsto 4$, $3 \mapsto 1$, $4 \mapsto 3$. Вообще, если $\sigma \in S_n$, то $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$. Для наглядности, ту же перестановку можно изобразить картинкой вида



Определение 2. Произведение перестановок $\sigma, \tau \in S_n$ определяется так: $\sigma\tau(i) = \sigma(\tau(i))$ (для произвольных отображений σ и τ такое произведение обычно называется *композицией отображений*). Например, если

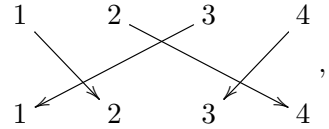
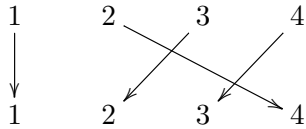
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$



TO

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

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



Отметим, что сначала применяется второй сомножитель, а потом первый.

Задача 2. а) Всегда ли $\sigma\tau = \tau\sigma$? б) Пусть $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$. Найти $\sigma\tau$ и $\tau\sigma$.

Задача 3. а) Найдите перестановку e , удовлетворяющую условию $e\sigma = \sigma e = \sigma$ для любой перестановки $\sigma \in S_n$. Докажите, что такая перестановка единственна (её называют *единичной* или *тождественной*.) б) Докажите, что для любой перестановки σ существует единственная перестановка σ^{-1} такая, что $\sigma\sigma^{-1} = e = \sigma^{-1}\sigma$. (Эта перестановка называется *обратной* к σ . Почему?) в) Докажите, что для любых $\sigma, \tau, \eta \in S_n$ имеет место равенство $\sigma(\tau\eta) = (\sigma\tau)\eta$. г) Докажите, что если $\sigma\tau = \sigma\eta$, то непременно $\tau = \eta$.

Задача 4. Докажите, что для любой перестановки $\sigma \in S_n$ существует такое натуральное число k , что $\sigma^k = e$. Минимальное k с этим свойством называется *порядком* перестановки σ и обозначается $\text{ord } \sigma$.

Задача 5. Найдите порядки перестановок: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$.

Определение 3. Циклом (a_1, a_2, \dots, a_k) называется перестановка, циклически переставляющая элементы a_1, a_2, \dots, a_k (то есть $a_1 \mapsto a_2, a_2 \mapsto a_3, \dots, a_k \mapsto a_1$; имеется в виду, что все элементы a_1, a_2, \dots, a_k различны; все остальные элементы множества $\{1, \dots, n\}$ переходят в себя). Число k называется длиной цикла.

Задача 6. Какие из перестановок в задаче 5 являются циклами?

Задача 7. Каков порядок цикла длины k ? Сколько всего циклов длины k в S_n ?

Задача 8. а) Докажите, что если σ и τ — циклы, множества элементов которых не пересекаются (такие циклы называются *независимыми*), то $\sigma\tau = \tau\sigma$ (циклы *коммутируют*). б) Верно ли, что циклы коммутируют тогда и только тогда, когда они независимы?

Задача 9. Представьте перестановки из задачи 5 в виде произведения независимых циклов.

Задача 10. Докажите, что любую перестановку можно представить в виде произведения независимых циклов. Сколькими способами (с точностью до перестановки множителей)?

Задача 11. а) Пусть порядок перестановки равен двум. Разложим её в произведение независимых циклов. Какими могут быть длины этих циклов? б) Пусть σ — это k -я степень цикла $(1, 2, \dots, n)$. На сколько независимых циклов раскладывается σ ? Каковы длины этих циклов?

Задача 12. Найдите максимальный порядок перестановки а) из S_5 ; б) из S_{13} ; в)* из S_n .

Задача 13. Докажите, что число $\text{ord } \sigma$ делит $n!$ для любой перестановки $\sigma \in S_n$.

Задача 14. Текст зашифрован программой, заменяющей взаимно однозначно каждую букву на некоторую другую. а) Докажите, что существует такое число k , что текст расшифровывается применением k раз шифрующей программы. б) Найдите хотя бы одно такое k .

1	2 а	2 б	3 а	3 б	3 в	3 г	4	5	6	7	8 а	8 б	9	10	11 а	11 б	12 а	12 б	12 в	13	14 а	14 б

[illegible]