1 ЦИКЛЫ

Продолжаем изучать перестановки. Будем заниматься циклами, транспозициями, четностью и порядком перестановок.

Пусть у нас есть такая перестановка:

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,4\,7\,8\,6\,2\,1\,5 \end{pmatrix}$$

Возведем ее в квадрат (возьмем композицию с самой собой):

$$\sigma^2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 7\,8\,1\,5\,2\,4\,3\,6 \end{pmatrix}$$

Теперь возведем в 3-ю степень:

$$\sigma^3 = \sigma \circ \sigma^2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 1\,5\,3\,6\,4\,8\,7\,2 \end{pmatrix}$$

Замечаем, что внутри перестановки σ есть три числа (1 3 7), которые переходят друг в друга. Они так и будут ходить по кругу при возведении σ в последовательные степени. Такая структура называется **циклом**.

Выделив цикл (1 3 7) в перестановке σ, мы можем заметить, что остальные ее 5 элементов тоже переходят друг в друга. Таким образом, мы получили представление перестановки σ в виде **произведения двух непересекающихся циклов**:

$$\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,4\,7\,8\,6\,2\,1\,5 \end{pmatrix} = (1\,3\,7)(2\,4\,8\,5\,6)$$

Так как эти циклы не пересекаются, они перестановочны, и σ^m есть произведение m -тых степеней этих циклов («произведение» означает «композиция»).

По аналогии с циклом из 3-х элементов (циклом длины 3), который в 3-й степени дает Id, цикл из 5-ти элементов (цикл длины 5) дает Id, будучи возведенным в 5-ю степень.

Следовательно, наша перестановка σ даст Id при возведении в $3 \cdot 5 = 15$-ю степень.

Далее мы покажем, что перестановка дает Id при возведении в степень, равную наименьшему общему кратному (НОК) длин всех независимых циклов, на которые раскладывается эта перестановка).

Мы получили на основе нашей перестановки σ множество из 15-ти различных перестановок, которое образует **группу**:

$$\{Id, \sigma, \sigma^2, \sigma^3 \dots, \sigma^{14}\}$$

Здесь возникает аналогия с арифметикой остатков (вычетов) по модулю 15.

Точно так же, как остатки являются группой по сложению, эти перестановки образуют группу по композиции, так как выполнены условия:

- замкнутость относительно композиции;
- композиция ассоциативна: $\sigma \circ (\tau \circ \delta) = (\sigma \circ \tau) \circ \delta$;
- существует **нейтральный** элемент (Id) такой, что: $\sigma \circ Id = Id \circ \sigma = \sigma$;
- существует **обратный** элемент: $\sigma \circ \tau = \tau \circ \sigma = Id$.

24 ПОРЯДОК ПЕРЕСТАНОВКИ

Вспомним утверждение из урока 22:

УТВЕРЖДЕНИЕ

Для любой перестановки

$\sigma = \begin{pmatrix} 1\ 2\ \dots\ n \\ i_1, i_2, \dots i_n \end{pmatrix}$, где $i_1, i_2, \dots i_n$ — числа $1, 2, \dots, n$, взятые в произвольном порядке,

существует такое $m \in \mathbb{N}$, что $\sigma^m = Id$.

ДОКАЗАТЕЛЬСТВО

1-Й СПОСОБ.

Используем представление перестановки в виде произведения независимых циклов и возьмем НОК их длин.

Алгоритм разложения на независимые циклы:

1) Начиная с 1, выписываем цепочку переходящих друг в друга элементов, пока мы наконец не получим 1.

2) Берем следующий элемент, не вошедший в этот 1-й цикл, и делаем то же самое.

3) Повторяем, пока все n элементов не будут перечислены в циклах.

Возьмем m = НОК длин всех этих циклов и возведем перестановку σ в степень m. Длина каждого из циклов делит НОК, поэтому каждый из этих циклов обратится в Id при возведении в степень m. А, значит, и вся перестановка σ обратится в Id при возведении в степень m.

2-Й СПОСОБ.

Выпишем для произвольной перестановки σ такую последовательность:
$Id, \sigma, \sigma^2, \sigma^3, \dots$
Вспомним, что всего существует $n!$ различных перестановок на n символах.
По принципу Дирихле, если мы продолжим выписывать последовательность до $\sigma^{n!}$, то какие-то две перестановки σ^k и σ^{k+l} обязательно совпадут. Получим:
$\sigma^k = \sigma^{k+l} = \sigma^k \sigma^l$.
Мы знаем, что для σ^k существует обратная к ней (нейтрализующая) перестановка $(\sigma^k)^{-1}$, композиция с которой дает Id. Домножим наше равенство на $(\sigma^k)^{-1}$:

$$Id = (\sigma^k)^{-1}\sigma^k = (\sigma^k)^{-1}\sigma^k\sigma^l = ((\sigma^k)^{-1}\sigma^k)\sigma^l = Id \circ \sigma^l = \sigma^l$$

Тем самым мы получили, что l — именно такая степень, что $\sigma^l = Id$.

УТВЕРЖДЕНИЕ ДОКАЗАНО

Мы не знаем, является ли l минимальной такой степенью, что $\sigma^l = Id$. Докажем следующее утверждение:

УТВЕРЖДЕНИЕ

Пусть d — минимальная степень такая, что $\sigma^d = Id$.
Тогда l делится на d.

ДОКАЗАТЕЛЬСТВО

От противного. Пусть l при делении на d дает остаток r ($r<d$).
Тогда:
$Id = \sigma^l = \sigma^{ds+r} = \sigma^{ds}\sigma^r = (\sigma^d)^s\sigma^r = (Id)^s\sigma^r = \sigma^r$.
Это противоречит тому, что d — минимальная степень, обращающая перестановку σ в Id.

УТВЕРЖДЕНИЕ ДОКАЗАНО

Такое число d называется **порядком** перестановки.

ПОРЯДОК ПЕРЕСТАНОВОК ПРИ n = 3

Найдем разложение в произведение циклов и порядок всех 6 перестановок на 3-х символах:

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = Id$ имеет порядок 1;

$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$,

имеют порядок 2;

$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$,

имеют порядок 3.