Лекция 9. Теорема Кэли. Группа перестановок. Порядок элементов. Транспозиции.

#вшпи #дискретная_математика #теория

Автор конспекта: Гридчин Михаил

Замечание. В этом конспекте будем считать, что знак $(\circ)$ обозначает композицию и вычисляется *справа налево*, а произведение с опусканием знака или $(\cdot)$ обозначает групповую операцию.

Теорема Кэли

Теорема Кэли. Пусть G - конечная группа. $|G| =: n$. Тогда $\exists H < S_n : G \cong H$. То есть всякая конечная группа изоморфна некоторой подгруппе группы перестановок из n элементов. Другими словами $G \cong L_G < S_n$.
$\square$
Так как G - конечная группа, пронумеруем все элементы этой группы, как $g_2, g_2, \dots g_n$.
Рассмотрим левые сдвиги $L_a, a \in G$:

$$\begin{aligned} &g_1 \to ag_1 \\ &g_2 \to ag_2 \\ &\dots \\ &g_n \to ag_n \end{aligned}$$

Поскольку все получившиеся элементы лежат в G, а также они все различны (иначе умножим на a^{-1} слева и получим равенство, см. предыдущие лекции), получаем, что L_a - это какая-то перестановка исходных элементов $g_1, g_2, \dots, g_n$ (взаимно однозначное соответствие). Рассмотрим L_a для всех $a \in G$. Заметим, что они образуют группу. Действительно, $L_e = e'$ (тождественная перестановка, $\forall g_i \in G \implies eg = g$).
$L_a \circ L_{a^{-1}} = L_{a^{-1}} \circ L_a = L_e$. Действительно, $\forall g_i \in G \implies g_i = a^{-1}ag_i$. Также по определению $L_a \circ L_b = L_{ab} \implies L_a \circ (L_b \circ L_c) = (L_a \circ L_b) \circ L_c = L_{abc}$. Таким образом, доказали существование нейтрального элемента, обратного элемента и ассоциативность. Докажем теперь, что эта группа изоморфна группе G. Действительно, во первых мы доказали, что L_a - биекция $\forall a \in G$. А также мы показали, что $L_a \circ L_b = L_{ab} \implies$ по определению $G \cong L_G$.
Поскольку $|L_G| = n$ и $L_G < S_n$, а также L_G - группа относительно той же групповой операции, что и S_n (композиция), то доказали альтернативную формулировку теоремы.
$\blacksquare$

Группа перестановок

Def. *Перестановкой* назовём биекцию конечного множества на себя.

Def. *Перестановка в канонической записи* длины n обозначается следующим образом:

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

Note. Перестановка - это также таблично заданная функция.

Def. *Произведение перестановок* длины n определим следующим образом:

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

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

Def. *Неканонической записью перестановки* длины n назовём такую перестановку, в которой аргументы могут быть перемешаны. При этом если $\pi(i) = i$, то этот столбец можно опустить.
Пример.

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

Def. *Обратной перестановкой* π^{-1} к перестановке π длины n назовём перестановку:

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

Def. *Циклом* длины k перестановки длины n назовём последовательность элементов, где каждый элемент переходит в следующий, а последний - в первый и будем обозначать:

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

Note. Цикл - это биекция k-элементного множества на себя.
Note. Из предыдущего замечания следует, что цикл - это элемент группы перестановок.

Def. *Цикловой записью перестановки* длины n

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

Определяется представление перестановки в виде произведения непересекающихся циклов.

Пример. Рассмотрим перестановку

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

У неё есть следующие циклы:

$$1 \to 3 \to 5 \to 1$$
$$2 \to 4 \to 2$$

Значит

$$\pi = (1, 3, 5)(2, 4)$$

Утверждение. Любую перестановку можно разложить в непересекающиеся циклы.
Утверждение. Циклы перестановки коммутируют, то есть, если a и b - циклы, то $a \cdot b = b \cdot a$ и они задают одну и ту же перестановку. Доказательство по определению.
Утверждение. Любая перестановка раскладывается в произведение (композицию) **непересекающихся** циклов единственным образом с точностью до записи цикла и порядка циклов.

Утверждение. Порядок цикла длины k равен k, то есть $ord(i_1, i_2, \ldots, i_k) = k$
□
Действительно, по определению цикла элемент i_1 переходит в элемент i_2 и так далее, то есть

$$i_1 \to i_2 \to \ldots \to i_k \to i_1$$

Количество переходов равно k, а значит порядок каждого элемента равен k, значит и порядок всего цикла равен k. То есть $(i_1, i_2, \ldots, i_k)^k = (i_1, i_2, \ldots, i_k)$.
■

Def + теорема. Если перестановка записана в виде непересекающихся циклов длины $c_1, c_2, \ldots, c_m$, то *порядком данной перестановки* равен $НОК(c_1, c_2, \ldots, c_m)$.
□
Действительно, поскольку порядок перестановки должен делиться на порядок каждого цикла (чтобы элемент i перешёл сам в себя), а циклы не пересекаются, то $ord(\pi) = НОК(c_1, c_2, \ldots, c_m)$.
■

Транспозиции

Def. *Транспозиция* - это цикл длины 2. То есть цикл (i_1, i_2).
Note. Транспозиция - это элемент группы перестановок
Note. Для транспозиции (a_i, a_j) обратная транспозиция - (a_i, a_j), то есть $(a_i, a_j)^2 = e = \mathrm{id}$.

Теорема. Любая перестановка представима в виде произведения транспозиций.
□
Нестрогое доказательство: из курса алгоритмов или из детского сада известно, что

существуют сортировки сравнением. А значит, перестановка - это какое-то количество применённых операций $swap(a_i, a_j)$, что и задаёт транспозицию.

Строгое доказательство: Докажем сначала, что любой цикл можно разложить в произведение транспозиций. Действительно, рассмотрим цикл длины m:

$$(a_1 \quad a_2 \quad \dots \quad a_m)$$

Такой цикл можно представить в виде произведения транспозиций следующим образом:

$$(a_1 \quad a_2 \quad \dots \quad a_m) = (a_1 \quad a_m)\,(a_1 \quad a_{m-1}) \cdots (a_1 \quad a_3)\,(a_1 \quad a_2)$$

В данной записи умножение выполняется справа налево, как композиция функций. Действительно, элемент a_i, где $i \in \{2, 3, \dots, m-1\}$ сначала перейдёт в a_1, а на следующем шаге перейдёт в a_{i+1}, а далее к нему не будет выполнено никаких операций. Элемент a_1 перейдёт в a_2 на самом первом шаге, а далее к нему не будет выполнено никаких операций. Элемент a_m перейдёт в a_1 на последнем шаге. В результате получаем, что $\forall i \in \{1, 2, \dots, m\} : a_i \to a_{i+1 \pmod m}$. Значит, любой цикл представим в виде произведения транспозиций. Но любая перестановка представима в виде непересекающихся и коммутирующих циклов, а значит, что она представима и в виде произведения транспозиций.
■

Теорема. Пусть перестановка π задана произведением транспозиций:

$$\pi = t_1 t_2 \dots t_k$$

Тогда

$$\boxed{\pi^{-1} = t_k^{-1} t_{k-1}^{-1} \dots t_1^{-1} = t_k t_{k-1} \dots t_2 t_1}$$

□
Поскольку транспозиция - это элемент группы перестановок, то для транспозиций выполняется та же аксиоматика групп, что и для перестановок. Тогда если положим

$$\pi = t_1 t_2 \dots t_k$$

То для π^{-1} будет выполнено

$$\pi^{-1} = (t_1 t_2 \dots t_k)^{-1} = t_k^{-1} t_{k-1}^{-1} \dots t_1^{-1}$$

Докажем этот факт по индукции.

БАЗА. $k = 1$: $(t_1)^{-1} = t_1^{-1}$. Очевидно верно
ШАГ. Предположим, что предположение верно для k, докажем для $k+1$.
Пусть $\sigma = t_1 t_2 \dots t_k t_{k+1} = \sigma' t_{k+1}$, где $\sigma' = t_1 t_2 \dots t_k$. Тогда:

$$\sigma^{-1} = (\sigma' t_k)^{-1} = t_{k+1}^{-1} (\sigma')^{-1} = t_{k+1}^{-1} t_k^{-1} \dots t_1^{-1}$$

Получили требуемое.

Теперь, поскольку $t = t^{-1}$, получаем второе требуемое равенство.

■

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

□

Предположим противное, что для перестановки π существует разложение на чётное количество транспозиций и на нечётное количество транспозиций. Вспомним, что π^{-1} представляет обратное произведение транспозиций для π . Рассмотрим произведение $\pi \circ \pi^{-1}$, как произведение их транспозиций в одном и в другом случае.

$$\pi \circ \pi^{-1} = e = \underbrace{\sigma_1 \sigma_2 \dots \sigma_k}_{\text{нечётное количество}}$$

Докажем, что если e раскладывается в n транспозиций, то e раскладывается и в $n-2$ транспозиции. Рассмотрим в произведении такое $\sigma_p = (s, t)$, что элемент s правее $(\forall i > p)$ не встречается. Рассмотрим σ_{p-1}. Есть несколько случаев.

1. $\sigma_{p-1} = (s, t)$, тогда $\sigma_{p-1}\sigma_p = e$.
2. $\sigma_{p-1} = (q, r)$, $\{q, r\} \cap \{s, t\} = \varnothing$. То есть они не пересекаются, следовательно, они коммутируют. Поменяем местами: $\sigma_{p-1}\sigma_p = \sigma_p\sigma_{p-1}$. То есть мы сместили выбранный s элемент левее
3. $\sigma_{p-1} = (s, r)$. Тогда $\sigma_{p-1}\sigma_p = \begin{pmatrix} s & r & t \\ t & s & r \end{pmatrix} = (s, t)(r, t)$. То есть мы опять сдвигаем s влево.
4. $\sigma_{p-1} = (t, r)$. Тогда $\sigma_{p-1}\sigma_p = \begin{pmatrix} s & t & r \\ r & s & t \end{pmatrix} = (s, r)(t, r)$. То есть мы опять сдвигаем s влево.

   Поймём, что произойдёт с s. Либо в какой-то момент подойдёт первый случай, и s сократится, либо получим, что s содержится в первой транспозиции, а правее не будет ни одной транспозиции, содержащей s (по построению). То есть

$$e = (s, t')\underbrace{(\dots)\cdots(\dots)}_{\text{не содержат } s}$$

   Тогда s отображается в t'. Может ли быть такое, если $t' \neq s$? Нет, поскольку в итоге s должен перейти в s, чтобы перестановка была нейтральной. Значит, такого быть не может и в какой-то момент s сократится с какой-то ещё скобкой. То есть в какой-то момент выполнится критерий первого случая.

   Повторяя описанные выше действия, каждый раз сокращаются ровно 2 скобки, но поскольку изначально их было нечётное количество, то в конце концов останется одна скобка из двух разных элементов, а такого быть не может. Значит, наше предположение было неверным, и чётность количества транспозиций сохраняется.

   ■

Def. Чётность количества транспозиций в перестановке назовём *чётностью перестановки*.
Утверждение. В группе перестановок одинаковое количество чётных и нечётных перестановок. Доказательство почти тривиально (умножим на транспозицию (a_1, a_2))
Утверждение. Множество чётных перестановок образует подгруппу группы перестановок.
Утверждение. Подгруппа чётных перестановок является нормальной.