ЛЕКЦИЯ 4

ОБОБЩЕННАЯ АССОЦИАТИВНОСТЬ

ПОДСТАНОВКИ

ЦИКЛОВАЯ СТРУКТУРА ПОДСТАНОВКИ

ОБОБЩЕННАЯ АССОЦИАТИВНОСТЬ

Теорема 1. *Если M — множество с ассоциативной операцией $*$, то результат применения этой операции на n сомножителей не зависит от расстановки скобок при любом натуральном $n \geqslant 3$.*

Доказательство. Докажем утверждение теоремы по полной индукции по числу сомножителей n.

База индукции. База при $n = 3$ содержится в утверждении теоремы о том, что операция $*$ ассоциативна.

Шаг индукции. Пусть для всех $k < n$ результат применения операции на k сомножителях не зависит от расстановки скобок. Докажем это утверждение для данного числа n.

Пусть мы имеем две расстановки скобок в произведении

$$a_1 * a_2 * \cdots * a_{n-1} * a_n,$$

где первая расстановка — слева направо:

$$((\ldots(a_1 * a_2) * \cdots * a_{n-1}) * a_n),$$

вторая — какая-то произвольная расстановка. Докажем, что результат для этой расстановки скобок будет совпадать с результатом для расстановки слева направо.

В любой расстановке скобок есть операция, которая производится последней, что означает, что скобки выглядят так:

$$(a_1 * a_2 * \cdots * a_k) * (a_{k+1} * \ldots a_{n-1} * a_n),$$

где внутри первых и вторых скобок еще как-то расставлены скобки.

Благодаря предположению индукции внутри первых и вторых скобок мы можем расставить скобки произвольным образом.

Расставим в первом выражении их слева направо, а во втором — справа налево:

$$((\dots(a_1 * a_2) * \dots * a_{k-1}) * a_k) * (a_{k+1} * (a_{k+2} \dots (a_{n-1} * a_n) \dots)).$$

Благодаря ассоциативности скобки можно переставить так:

$$(((\dots(a_1 * a_2) * \dots * a_{k-1}) * a_k) * a_{k+1}) * (a_{k+2} \dots (a_{n-1} * a_n) \dots)).$$

Таким образом, за $n - k$ шагов мы придем к расстановке скобок слева направо, что и требовалось. $\square$

ПОДСТАНОВКИ/ПЕРЕСТАНОВКИ

Пусть Ω — конечное множество из n элементов. Поскольку природа этих элементов для нас несущественна, удобно считать, что

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

Элементы множества $S_n = S(\Omega)$ всех взаимно однозначных преобразований $\Omega \to \Omega$, обычно обозначаемые строчными буквами греческого алфавита, называются *перестановками* (иногда — *подстановками*). Отдельно за единичным преобразованием обычно сохраняют обозначение e.

В развернутом наглядном виде произвольную подстановку

$$\pi : i \mapsto \pi(i), \quad i = 1, 2, \ldots, n,$$

обычно изображают в виде

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix},$$

полностью таким способом указывая все образы этой перестановки.

Подстановки $\sigma, \tau \in S_n$ перемножаются в соответствии с общим правилом композиции отображений:

$$(\sigma\tau)(i) = \sigma(\tau(i)).$$

Покажем, что две подстановки могут не коммутировать, а заодно приведем пример перемножения:

Рассмотрим подстановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ и } \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Тогда

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

а

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

Умножение подстановок подчиняется следующим трем важным правилам:

(1) ассоциативность — $\forall \alpha, \beta, \gamma\ (\alpha\beta)\gamma = \alpha(\beta\gamma)$;

(2) S_n обладает единичным элементом e: $\forall \alpha \in S_n\ e\alpha = \alpha e = \alpha$;

(3) для каждой перестановки $\alpha \in S_n$ существует обратная подстановка: $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$.

Такая система (множество с операцией) называется *группой.*

Группа подстановок называется также *симметрической группой порядка* n.

Найдем порядок $|S_n|$ группы S_n. Символ 1 может перейти в любой элемент из n. Выбрав один из этих элементов, получим n возможностей и фиксированный $\sigma(1)$.

Теперь для $\sigma(2)$ существует $n-1$ вариант, так как один вариант уже занят.

И так далее, для числа k существует $n-k+1$ вариантов для $\sigma(k)$.

Все эти варианты перемножаются, получается число $n!$.

Таким образом,

$$|S_n| = n!.$$

Разложим теперь подстановки из S_n в произведение более простых подстановок, называемых *циклами.*

Что такое цикл? Это перестановка, в которой элементы переставляются по циклу:

$$i_1 \mapsto i_2 \mapsto \ldots \mapsto i_{k-1} \mapsto i_k \mapsto i_1.$$

Такой цикл записывается как $(i_1\, i_2\, \ldots i_{k-1}\, i_k)$, но можно также начинать запись с любого другого элемента из цикла: $(i_t\, i_{t+1} \ldots)$.

Любую подстановку можно разложить в произведение циклов, элементы которых не пересекаются.

Теорема 2. *Любая подстановка в S_n раскладывается в произведение независимых циклов. Эти циклы определяются однозначно по подстановке, с точностью до их перестановки.*

Доказательство. Действительно, пусть у нас есть подстановка $\sigma \in S_n$. Посмотрим, куда переходит 1. Если $1 \mapsto 1$, то это и есть маленький цикл длины один. Пусть $i_1 \neq 1$, тогда посмотрим на $\sigma(i_1) = i_{i_1}$. Если $i_{i_1} = 1$, то мы получили цикл длины два. Пусть $i_{i_1} \neq 1$, то посмотрим на образ этого элемента и т.д.

Понятно, что в какой-то момент образ очередного элемента станет равен 1 (если бы повторение произошло на другом элементе, то отображение σ оказалось бы не инъективным). Значит, к нас появился один цикл.

Если этот цикл не заметает все элементы, то рассмотрим следующий на очереди элемент, которого не было в первом цикле. Из него точно так же образуется цикл. Первый и второй циклы не могут пересечься, так как любое пересечение означает, что отображение не инъективно.

Будем продолжать эту процедуру далее, в результате чего получим разложение перестановки в произведение непересекающихся циклов.

Чтобы понять, что такое разложение единственно, заметим лишь, что разбиение множества $\{1, 2, \ldots, n\}$ элементов подстановки на циклы однозначно, потому что только внутри одного цикла можно попасть из одного элемента в другой, переставляя элементы соответственно σ несколько раз.

Если мы уже знаем множество в одном цикле, то сам цикл также формируется однозначно, так как определяется просто образами элементов. $\square$

ЦИКЛОВАЯ СТРУКТУРА ПОДСТАНОВКИ

Давайте для наглядности запишем в виде циклов все подстановки из двух, трех и четырех элементов.

Все подстановки из двух элементов исчерпываются двумя — тождественной e и циклом длины два — $(1\,2)$.

Подстановки из трех элементов бывают такие: тождественная e, циклы длины два — $(1\,2)$, $(1\,3)$, $(2\,3)$ и циклы длины три — $(1\,2\,3)$, $(3\,2\,1)$.

На четырех элементах структура подстановок становится чуть более разнообразной: тождественная e, циклы длины два — $(1\,2)$, $(1\,3)$, $(1\,4)$, $(2\,3)$, $(2\,4)$, $(3\,4)$, циклы длины три — $(1\,2\,3)$, $(3\,2\,1)$, $(1\,2\,4)$, $(4\,2\,1)$, $(1\,3\,4)$, $(4\,3\,1)$, $(2\,3\,4)$, $(4\,3\,2)$, циклы длины четыре — $(1\,2\,3\,4)$, $(4\,3\,2\,1)$, $(1\,2\,4\,3)$, $(3\,4\,2\,1)$, $(1\,3\,2\,4)$, $(4\,2\,3\,1)$ и пары циклов длины два — $(1\,2)(3\,4)$, $(1\,3)(2\,4)$ и $(1\,4)(2\,3)$.

Циклы длины два называют *транспозициями.*

Пусть π — произвольная подстановка из S_n. Ее *степень* π^s определяется по индукции:

$$\pi^s = \begin{cases} \pi(\pi^{s-1}), & \text{если } s > 0, \\ e, & \text{если } s = 0, \\ \pi^{-1}((\pi^{-1})^{-s-1}), & \text{если } s < 0. \end{cases}$$

При таком определении очевидно, что

$$\pi^s\pi^t = \pi^{s+t} = \pi^t\pi^s, \quad t, s \in \mathbb{Z}.$$

Так как мы рассматриваем подстановки на конечном числе элементов, то на самом деле для каждой подстановки $\pi \in S_n$ найдется однозначно определенное натуральное число $q = q(\pi)$ такое, что все различные степени нашей подстановки содержатся в множестве

$$\langle\pi\rangle = \{e, \pi, \pi^2, \ldots, \pi^{q-1}\}$$

и $\pi^q = e$.

Это число q называется еще *порядком* подстановки π.

Получается, что рассмотренные выше перестановки имели порядки $1, 2, 3, 4$.

Теорема 3. *Если подстановка σ разложена в произведение непересекающихся циклов:*

$$\sigma = \sigma_1\sigma_2\ldots\sigma_m,$$

длины которых равны $l_1, l_2, \ldots, l_m$, соответственно, то порядок подстановки σ равен наименьшему общему кратному чисел $l_1, \ldots, l_m$.

Доказательство. Так как независимые циклы коммутируют, то

$$\sigma^k = \sigma_1^k \sigma_2^k \dots \sigma_m^k.$$

Для того, чтобы $\sigma^k = e$, необходимо и достаточно, чтобы

$$\sigma_1^k = e,\ \sigma_2^k = e, \dots, \sigma_m^k = e,$$

а это равносильно тому, что

$$l_1, l_2, \dots, l_m | k.$$

Таким образом, наименьшее подходящее k — это наименьшее общее кратное чисел $l_1, l_2, \dots, l_m$. □