ЛЕКЦИЯ 3

ОБРАТНЫЕ ОТОБРАЖЕНИЯ

ОБОБЩЕННАЯ АССОЦИАТИВНОСТЬ

ПОДСТАНОВКИ

ОБРАТНЫЕ ОТОБРАЖЕНИЯ

Композиция отображений $X \to X$ некоммутативна, то есть $fg \neq gf$. В этом легко убедиться на примере, когда $X = \{a, b\}$, $f(a) = b$, $f(b) = a$, $g(a) = a$, $g(b) = a$.

Некоторые отображения имеют *обратные*. Предположим, что $f : X \to Y$ и $g : Y \to X$ — какие-то отображения, так что композиции fg и gf определены. Если $fg = e_Y$, то f называется *левым обратным* к g, а g — *правым обратным* к f.

Когда произведения в любом порядке являются единичными отображениями:

$$fg = e_Y, \quad gf = e_X,$$

то f и g — просто взаимно *обратные* отображения. В этом случае пишут $g = f^{-1}$.

Понятно, что тогда из $v = f(u)$ следует $u = f^{-1}(v)$.

Лемма 1. *Если у отображения $f : X \to Y$ есть обратное отображение $g : Y \to X$, то оно определено однозначно.*

Доказательство. Действительно, пусть у отображения $f : X \to Y$ есть еще обратное отображение $h : Y \to X$. Рассмотрим произвольный элемент $v \in Y$. Из того, что $fg = fh = e_Y$, следует

$$fg(v) = fh(v) = v.$$

Пусть $g(v) = u$, $h(v) = u'$. Значит, $f(u) = f(u') = v$. Так как $gf = hf = e_X$, получаем

$$u = gf(u) = g(v) = h(v).$$

Таким образом, $g(v) = h(v)$ для любого $v \in Y$, поэтому $g = h$. $\square$

Лемма 2. *Если*

$$f : X \to Y, \quad g : Y \to X$$

— любые отображения, для которых $gf = e_X$*, то* f *инъективно, а* g *сюръективно.*

Доказательство. Пусть $x, x' \in X$, $f(x) = f(x')$.

Тогда

$$x = e_X(x) = (gf)(x) = g(fx) = g(fx') = (gf)x' = e_X(x') = x'.$$

Значит, f инъективно.

Если теперь x — любой элемент из X, то

$$x = e_X(x) = (gf)x = g(fx),$$

что доказывает сюръективность отображения g. □

Теорема 1. *Отображение $f : X \to Y$ тогда и только тогда имеет обратное, когда оно взаимно однозначно (биективно).*

Доказательство. Предположим вначале, что f обладает обратным, $g = f^{-1}$. Тогда из предыдущей леммы вытекает, что f инъективно и сюръективно, то есть биективно.

Теперь предположим, что f биективно. Это значит, что для любого $y \in Y$ мы можем найти *единственный* элемент $x \in X$ такой, что $f(x) = y$. Положив $g(y) = x$, мы определим отображение $g : X \to Y$ со свойствами обратного к f отображения. Значит, $f^{-1} = g$. □

Следствие 1. *Из биективности отображения $f : X \to Y$ вытекает биективность обратного отображения, причем*

$$(f^{-1})^{-1} = f.$$

Пусть, далее, $f : X \to Y$, $h : Y \to Z$ — биективные отображения.

Тогда биективна и их композиция hf, причем

$$(hf)^{-1} = f^{-1}h^{-1}.$$

Доказательство. По предыдущей теореме биективность f влечет существование f^{-1}, что в силу той же теоремы эквивалентно биективности f^{-1}.

Условия $f^{-1}f = e_X$, $ff^{-1} = e_Y$ сразу дают условие $(f^{-1})^{-1} = f$.

Далее, по условию и доказанной теореме существуют обратные отображения

$$f^{-1} : Y \to X \text{ и } h^{-1} : Z \to Y$$

и их композиция

$$f^{-1}h^{-1} : Z \to X.$$

Из равенств

$$(hf)(f^{-1}h^{-1}) = ((hf)f^{-1})h^{-1} = (h(ff^{-1}))h^{-1} = hh^{-1} = e_Z,$$
$$(f^{-1}h^{-1})(hf) = f^{-1}(h^{-1}(hf)) = f^{-1}(h^{-1}h)f = f^{-1}f = e_X$$

вытекает, что $f^{-1}h^{-1}$ — обратное отображение к hf. □

Отображение следования $\sigma : \mathbb{N} \to \mathbb{N}$, сопоставляющее каждому натуральному числу следующее за ним натуральное число, является инъективным, но не сюръективным.

Для конечных множеств подобное невозможно:

Теорема 2. *Если X — конечное множество и отображение $f : X \to X$ инъективно, то оно сюръективно.*

Доказательство. Нам нужно только показать, что f сюръективно, то есть для любого $x \in X$ существует $x' \in X$ такое, что $f(x') = x$. Положим

$$f^k(x) = f(f \dots (fx) \dots) = f(f^{k-1}x), \quad k = 0, 1, 2, \dots$$

В силу конечности X в этой последовательности должны быть повторения. Пусть, скажем, $f^m(x) = f^n(x)$, $m >$. Если $n > 0$, то из $f(f^{m-1}x) = f(f^{n-1}x)$ и из инъективности f следует равенство $f^{m-1}(x) = f^{n-1}(x)$. Повторив достаточное число раз сокращение f, мы придем к равенству

$$f^{m-n}(x) = f^0(x) = e_X(x) = x.$$

В таком случае для $x' = f^{m-n-1}(x)$ выполнено как раз $f(x') = x$. □

Легко понять, что сюръективное преобразование конечного множества в себя также биективно.

Говорят, что два множества X и Y имеют *одинаковую мощность*, если между ними существует биективное отображение.

Множества той же мощности, что и $\mathbb{N}$, называются *счетными*.

ОБОБЩЕННАЯ АССОЦИАТИВНОСТЬ

Теорема 3. *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,

$$|S_n| = n!.$$