Перестановки

Е. А. Максименко

23 ноября 2007 г.

В этом учебном тексте перечислены элементарные свойства перестановок (преобразований конечного множества) в форме простых упражнений.

Содержание

§ 1. Определение перестановки

Всюду будем полагать, что n — положительное целое число. Пусть X_n — множество из n элементов. Так как природа этих элементов нас здесь не интересует, то всюду далее будем считать, что $X_n = \{1, 2, \dots, n\}$. В программировании бывает удобнее начинать нумерацию с нуля, т. е. полагать $X_n = \{0, 1, \dots, n-1\}$.

Отображение конечного множества в себя: запись в виде таблицы из двух строк. Любое отображение $f\colon X_n \to X_n$ можно записать в виде таблицы из двух строк, указывая под каждым элементом a из X_n его образ $f(a)$:

$$f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \downarrow & \downarrow & \dots & \downarrow \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix} \qquad \text{или} \qquad f = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ f(a_1) & f(a_2) & \dots & f(a_n) \end{pmatrix}.$$

В первой строке записаны без повторений все элементы множества X_n, а во второй строке — их образы относительно отображения f. Другими словами, при такой записи перечисляются (по столбцам) все пары вида (a, b), где $a, b \in X$ и $b = f(a)$. Например, запись

$$f = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 4 & 2 & 4 & 1 \end{pmatrix}, \quad \text{как и более подробная запись} \quad f = \begin{pmatrix} 4 & 2 & 1 & 3 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 2 & 4 & 1 \end{pmatrix},$$

означает, что $f(4) = 4$, $f(2) = 2$, $f(1) = 4$, $f(3) = 1$. Ясно, что если поменять местами какие-то столбцы таблицы, то получится то же самое отображение. Если элементы верхней строки расположены по порядку, то такую запись называют стандартной (канонической):

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

Определение перестановки. Перестановкой множества X_n (или перестановкой степени n) называют биективное отображение множества X_n в себя. Множество всех перестановок множества X_n обозначают S_n.

Требования инъективности и сюръективности в определении перестановки. Инъективность означает, что при записи перестановки в виде таблицы из двух строк все элементы в нижней строке (строке образов) *различны*, а сюръективность — что в строке образов присутствуют *все* элементы X_n. Можно доказать, что инъективность, сюръективность и биективность здесь равносильны, так как множество X_n конечное.

Другая терминология: перестановки и подстановки. Некоторые авторы называют биективное отображение X_n в X_n *подстановкой*, а *перестановкой* называют упорядоченный набор вида $(a_1, a_2, \ldots, a_n)$, где элементы $a_1, a_2, \ldots, a_n$ попарно различны и $\{a_1, a_2, \ldots, a_n\} = X_n$. По этой терминологии, если подстановка записана в виде таблицы из двух строк, то верхняя и нижняя строки являются перестановками. Первый довод против этой терминологии состоит в том, что упорядоченные наборы указанного вида («перестановки») естественным образом отождествляются с биективными отображениями («подстановками»). Например, упорядоченный набор чисел $(5, 1, 8, 3, 4, 7, 6, 2)$ естественно отождествить с отображением

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 8 & 3 & 4 & 7 & 6 & 2 \end{pmatrix}.$$

Второй довод — лингвистический. Термин «подстановка» перегружен, а слово «перестановка» скорее ассоциируется с действием (отображением), чем с набором.

Примеры перестановок. Тождественное отображение X_n в себя называют *единичной перестановкой* и часто обозначают через e:

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Транспозицией элементов i и j, где $i, j \in X_n$ и $i \neq j$, называют перестановку $\tau_{i,j}$, которая меняет местами i и j, а остальные элементы оставляет на месте:

$$\tau_{i,j}(k) = \begin{cases} j, & k = i; \\ i, & k = j; \\ k, & k \neq i,\ k \neq j. \end{cases}$$

Например, при $n = 7$

$$\tau_{2,5} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 3 & 4 & 2 & 6 & 7 \end{pmatrix}.$$

Транспозицию $\tau_{i,j}$ называют *простой* (или смежной), если $j = i + 1$. Например, $\tau_{1,2}$ и $\tau_{4,5}$ — простые транспозиции.

Определение лексикографического порядка. Пусть $\varphi, \psi \in S_n$. Говорят, что φ *лексикографически меньше* ψ, если существует такой номер $j \in X_n$, что $\varphi(j) < \psi(j)$ и $\varphi(i) = \psi(i)$ при любом $i < j$.

Проверка свойств лексикографического порядка. Доказать, что отношение лексикографического порядка является строгим линейным порядком на S_n, т. е. оно транзитивно и для любых двух перестановок φ, ψ из S_n выполняется ровно одно из соотношений: либо $\varphi = \psi$, либо φ лексикографически меньше ψ, либо ψ лексикографически меньше φ.

Перечисление перестановок в лексикографическом порядке. Перечислить в лексикографическом порядке (по возрастанию) перестановки из S_1, S_2, S_3 и S_4. Можно писать только нижнюю строку из стандартной записи. Найти число элементов множества S_n.

S_3 **как множество симметрий правильного треугольника.** Симметрией геометрической фигуры X называется любое биективное отображение X на X. Пусть T — правильный треугольник с вершинами A_1, A_2, A_3, пронумерованными против часовой стрелки. Тогда любая его симметрия $f\colon T \to T$ порождает перестановку $\varphi \in S_3$, такую, что

$$A_{\varphi(j)} = f(A_j), \qquad j \in \{1, 2, 3\}.$$

Доказать, что соответствие между симметриями треугольника и множеством S_3 биективно, и выяснить геометрический смысл каждой перестановки из S_3. Можно использовать следующие обозначения: r_α — поворот против часовой стрелки на угол α; h_j — отражение относительно высоты, проведённой из вершины A_j.

§ 2. Композиция перестановок

Определение композиции перестановок. *Композиция перестановок* φ и ψ из S_n определяется как обычная композиция отображений:

$$(\varphi \circ \psi)(j) = \varphi(\psi(j)) \qquad (j \in X_n).$$

Композиция перестановок является перестановкой (композиция биективных отображений биективна). Композицию перестановок часто называют *произведением перестановок* и вместо $\varphi \circ \psi$ пишут просто $\varphi\psi$.

Композиция перестановок: примеры. Пусть $\varphi, \psi \in S_5$,

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}, \qquad \psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}.$$

Тогда $\psi(1) = 5$, $\varphi(5) = 2$, поэтому $(\varphi\psi)(1) = \varphi(\psi(1)) = \varphi(5) = 2$. Аналогичным образом найдём $(\varphi\psi)(j)$ для $j = 2, 3, 4, 5$ и получим:

$$\varphi\psi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}.$$

Для частичного контроля над правильностью вычислений можно убедиться в том, что все элементы в нижней строке различны.

Теперь найдём $\psi\varphi$. Так как $\varphi(1) = 3$, а $\psi(3) = 4$, то $(\psi\varphi)(1) = 4$. Аналогично вычисляя образы элементов $2, 3, 4, 5$, получим:

$$\psi\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}.$$

Этот пример показывает, что в некоторых случаях $\varphi\psi$ может быть не равно $\psi\varphi$.

Композиция перестановки и транспозиции. Пусть $\varphi \in S_n$, $i, j \in X_n$, $i \neq j$. Как получить записи перестановок $\varphi\tau_{i,j}$ и $\tau_{i,j}\varphi$ из записи φ? Сначала можно разобраться на примерах, а затем сформулировать общее правило.

Ассоциативность композиции перестановок. $\varphi(\psi\chi) = (\varphi\psi)\chi$ для любых $\varphi, \psi, \chi \in S_n$. Это вытекает из общего свойства ассоциативности композиции отображений. Напомним доказательство: для любого $j \in X_n$

$$(\varphi(\psi\chi))(j) = \varphi(\psi(\chi(j))), \qquad ((\varphi\psi)\chi)(j) = \varphi(\psi(\chi(j))).$$

Полезно проверить свойство $\varphi(\psi\chi) = (\varphi\psi)\chi$ на примере, выбрав какие-нибудь $\varphi, \psi, \chi \in S_6$.

Определение единичной перестановки. Тождественное отображение множества X_n в себя называют *единичной* (или *тождественной*) перестановкой и обычно обозначают через e.

Основное свойство единичной перестановки. Тождественная перестановка является «нейтральным элементом» относительно операции композиции перестановок:

$$e\varphi = \varphi e = \varphi \qquad \forall \varphi \in S_n.$$

Убедиться в этом на примере и доказать в общем случае.

Единственность нейтрального элемента. Доказать, что если $e' \in S_n$ и

$$e'\varphi = \varphi e' = \varphi \qquad \forall \varphi \in S_n,$$

то $e' = e$. Указание: найти композицию ee' двумя способами: 1) пользуясь тем, что e — нейтральный элемент; 2) пользуясь тем, что e' — нейтральный элемент.

Определение обратной перестановки. Перестановка ψ из S_n называется *обратной* к перестановке φ из S_n, если $\varphi\psi = \psi\varphi = e$.

Существование обратной перестановки. Пусть перестановка φ задана двустрочной записью. Построить перестановку ψ, обратную к φ. Провести доказательство, что она действительно обратна к φ.

Единственность обратной перестановки. Пусть ψ_1 обратна к φ и ψ_2 обратна к φ. Доказать, что $\psi_1 = \psi_2$. Указание: найти композицию $(\psi_1\varphi)\psi_2 = \psi_1(\varphi\psi_2)$ двумя способами: 1) пользуясь тем, что ψ_1 обратна к φ; 2) пользуясь тем, что ψ_2 обратна к φ.

Перестановку, обратную к φ, обозначают через φ^{-1}.

Примеры обратных перестановок. Для следующих перестановок из S_5 найти обратные перестановки:

(1) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$;

(2) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$;

(3) $\varphi = \tau_{i,j}$;

(4) $\varphi = e$.

Свойства операции обращения перестановок. Доказать свойства:

1. $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}$.
2. $(\varphi^{-1})^{-1} = \varphi$.
3. $e^{-1} = e$.

Операция обращения как биекция S_n на S_n. Доказать, что отображение, которое переводит φ в φ^{-1}, является биекцией S_n на S_n.

Запись частного перестановок в виде двух строк. Пусть $\varphi, \psi \in S_n$. Доказать, что

$$\varphi\psi^{-1} = \begin{pmatrix} \psi(1) & \psi(2) & \dots & \psi(n) \\ \varphi(1) & \varphi(2) & \dots & \varphi(n) \end{pmatrix}.$$

Замена элементов в перестановке. Пусть $\varphi, \psi \in S_n$, причём φ задана следующей двустрочной записью:

$$\varphi = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}.$$

Найти удобную двустрочную запись для перестановки $\psi\varphi\psi^{-1}$.

Степени перестановки. Если $\varphi \in S_n$, то степени φ^k, где $k = 0, 1, 2, \dots$, определяются индукцией по k:

$$\varphi^0 = e, \qquad \varphi^{k+1} = \varphi^k\varphi.$$

Из ассоциативности следует, что $\varphi^k\varphi = \varphi\varphi^k$ (провести строгое доказательство индукцией по k). Считают,

$$\varphi^{-k} = (\varphi^{-1})^k.$$

Индукцией по k доказать, что $(\varphi^{-1})^k = (\varphi^k)^{-1}$. Можно строго доказать, что

$$\varphi^{k+m} = \varphi^k\varphi^m, \qquad (\varphi^k)^m = \varphi^{km} \qquad (k, m \in \mathbb{Z}).$$

Если φ и ψ коммутируют, то $(\varphi\psi)^k = \varphi^k\psi^k$. В общем случае это равенство может не выполняться (привести пример).

§ 3. Симметрическая группа

Определение группы. Говорят, что $(G, *)$ — *группа*, если G — множество, $*$ — бинарная (двухаргументная) операция на G, и выполняются следующие свойства («аксиомы группы»):

(1) ассоциативность: $a * (b * c) = (a * b) * c$ для любых $a, b, c \in G$;
(2) существует единственный элемент $e \in G$, такой, что $a * e = e * a = a$ для любого $a \in G$; этот элемент называют единичным (или нейтральным);
(3) для любого элемента $a \in G$ существует единственный элемент $b \in G$, такой что $a * b = b * a = e$; этот элемент называют обратным к a и обычно обозначают через a^{-1}.

Выше было доказано, что для множества S_n с операцией композиции $\circ$ аксиомы группы выполняются. Поэтому $(S_n, \circ)$ — группа. Её называют *симметрической группой* n*-го порядка.*

Единственность единичного и обратного элемента в определении группы. Показать, что в определении группы можно не требовать единственность единичного элемента и единственность обратного элемента, так как эти свойства следуют из остальных условий.

Таблица Кэли для S_3. Построить для группы S_3 таблицу Кэли («таблицу умножения»). В этом таблице строки и столбцы проиндексированы элементами S_3, и на пересечении строки φ и столбца ψ стоит $\varphi\psi$. Удобно использовать геометрические обозначения для элементов S_3. При индексации строк и столбцов сначала перечислить все повороты, а затем все отражения. С помощью этой таблицы для каждого элемента φ из S_3 найти обратный элемент.

О строках и столбцах таблицы Кэли. Заметить, что в каждой строке таблицы Кэли группы S_3 присутствуют все элементы S_3, причём ровно по одному разу. Доказать это свойство в общем виде:

(1) для любых $\varphi, \chi \in S_n$ существует такая $\psi \in S_n$, что $\chi = \varphi\psi$;
(2) если $\varphi, \psi_1, \psi_2 \in S_n$, то $\varphi\psi_1 \neq \varphi\psi_2$.

Аналогичные свойства доказать для столбцов таблицы Кэли.

Вложение S_n в S_m при $n \leqslant m$. Любую перестановку $\varphi \in S_n$ можно доопределить до перестановки $\varphi' \in S_m$, полагая $\varphi'(j) = j$ при $j > n$:

$$\varphi'(j) = \begin{cases} \varphi(j), & j \in \{1, \dots, n\}, \\ j, & j > n. \end{cases}$$

Например, при вложении S_4 в S_6

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \quad \text{переходит в} \quad \varphi' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 5 & 6 \end{pmatrix}.$$

Доказать, что отображение $f\colon S_n \to S_m$, действующее по правилу $f(\varphi) = \varphi'$, инъективно (из $\varphi' = \psi'$ следует $\varphi = \psi$). Это позволяет в некоторых случаях мыслить себе S_n как подмножество S_m.

Найти значения n, при которых группа S_n коммутативна. Говорят, что элементы x и y группы $(G, *)$ коммутируют (перестановочны), если $xy = yx$. Группа $(X, *)$ называется коммутативной (абелевой), если любые её элементы коммутируют между собой, т. е. $x * y = y * x$ для любых $x, y \in X$.

С помощью таблиц Кэли доказать, что группы S_1 и S_2 коммутативны, а S_3 некоммутативна. В каких случаях элементы $\varphi, \psi \in S_3$ перестановочны? Доказать, что при $n > 2$ группа S_n некоммутативна.

§ 4. Циклические перестановки

Определение циклической перестановки. Пусть $a_1, a_2, \ldots, a_k$ — попарно различные элементы X_n. Перестановку φ, действующую по правилу

$$\varphi(a_1) = a_2,\ \varphi(a_2) = a_3,\ \ldots\ ,\ \varphi(a_k) = a_1;$$

$$\varphi(j) = j \qquad \text{при } j \notin \{a_1, a_2, \ldots, a_k\},$$

называют *циклической перестановкой* элементов $a_1, a_2, \ldots, a_k$ или *циклом* из элементов $a_1, a_2, \ldots, a_k$. Обозначение:

$$\varphi = (a_1\ a_2\ \ldots\ a_k)_n.$$

Число n обычно ясно из контекста и не указывается. Пишут просто

$$\varphi = (a_1\ a_2\ \ldots\ a_k).$$

Число k называют *длиной цикла*. Заметим, что цикл длины 2 есть транспозиция, а любой цикл длины 1 совпадает с e и называется вырожденным циклом.

Число способов записи одного цикла. Циклическую перестановку длины k, где $k > 1$, можно записать в указанном виде различными способами:

$$\varphi = (a_1\ a_2\ \ldots\ a_k) = (a_2\ a_3\ \ldots\ a_k\ a_1) = \ldots$$

Найти число различных записей фиксированного цикла длины k.

Циклические перестановки: примеры. Следующие циклические перестановки из группы S_6 перевести в стандартную запись:

$$(1\ 4\ 2\ 5), \qquad (6\ 2\ 1\ 3\ 5\ 4), \qquad (3\ 5), \qquad (4).$$

Для следующих циклических перестановок найти сокращённую запись:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 3 & 6 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Число циклических перестановок. Найти число циклических перестановок длины s в группе S_n. Сначала найти число записей вида $(a_1\ a_2\ \ldots\ a_s)$, где элементы $a_1, a_2, \ldots, a_s$ попарно различны, а затем учесть, что каждый цикл записывается несколькими способами.

Замена элементов в цикле. Найти $\varphi(a_1\ a_2\ \ldots\ a_s)\varphi^{-1}$, где $a_1, a_2, \ldots, a_s$ — попарно различные элементы X_n, $\varphi \in S_n$. Сначала рассмотреть пример:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 6 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 5 & 2 & 6 \end{pmatrix} \begin{pmatrix} 4 & 2 & 5 & 1 & 6 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Перестановка, обратная к циклу. Найти перестановку, обратную к циклической перестановке $(a_1\ a_2\ \ldots\ a_s)$.

Вычисление степеней цикла. Пусть $\varphi = (a_1\ a_2\ \ldots\ a_s)$. Объясните, как вычислить φ^k, где $k \in \mathbb{Z}$. Полезно сначала рассмотреть какой-нибудь конкретный пример.

Независимые циклы коммутируют. Циклы $\varphi, \psi \in S_n$ вида

$$\varphi = (a_1\ a_2\ \ldots\ a_k), \qquad \psi = (b_1\ b_2\ \ldots\ b_l)$$

называются *независимыми*, если они перемещают разные элементы:

$$\{a_1, a_2, \ldots, a_k\} \cap \{b_1, b_2, \ldots, b_l\} = \varnothing.$$

Доказать, что независимые циклы коммутируют: $\varphi\psi = \psi\varphi$. Сначала можно убедиться в этом на примере:

$$\varphi, \psi \in S_6, \qquad \varphi = (3\ 1\ 5), \qquad \psi = (4\ 6).$$

§ 5. Разложение перестановки в композицию независимых циклов

Пример разложения перестановки на независимые циклы. Этот (или аналогичный) пример полезно держать перед собой для лучшего понимания последующих теоретических построений. Пусть

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 7 & 6 & 5 & 2 & 3 \end{pmatrix}.$$

Видим, что $\varphi(1) = 4$, $\varphi(4) = 6$, $\varphi(6) = 2$, $\varphi(2) = 1$. На элементе 1 цикл замкнулся:

$$1 \mapsto 4 \mapsto 6 \mapsto 2 \mapsto 1.$$

Говорят, что элементы $1, 2, 4, 6$ попарно φ-эквивалентными, а множество $\{1, 2, 4, 6\}$ является φ-орбитой точки 1 (это также φ-орбита каждой из точек $2, 4, 6$). Любые две из этих точек можно связать посредством φ, например: $6 = \varphi^2(1)$, $4 = \varphi^{-1}(6) = \varphi^3(6)$, и т. п. Заметим, что на множестве $\{1, 2, 4, 6\}$ перестановка φ действует так же, как цикл $(1\ 4\ 6\ 2)$.

Точка 3 не вошла в орбиту точки 1. Действуем на неё перестановкой φ до тех пор, пока не вернёмся обратно в 3: $3 \mapsto 7 \mapsto 3$. Это соответствует циклу $(3\ 7)$. Осталась точка 5, которая соответствует вырожденному циклу $(5) = e$. Проверить, что

$$\varphi = (1\ 4\ 6\ 2)(3\ 7)(5).$$

φ-эквивалентность. Пусть $\varphi \in S_n$. Элементы $i, j \in X_n$ будем называть φ-*эквивалентными* и писать $i \overset{\varphi}{\sim} j$, если если существует такое $k \in \mathbb{Z}$, что $\varphi^k(i) = j$. Доказать, что это отношение эквивалентности.

Действие степеней перестановки на элемент. Пусть $\varphi \in S_n$, $j \in X_n$. Доказать, что существует такое положительное целое k, для которого $\varphi^k(j) = j$. Указание: так как X_n конечно, то какие-то степени элемента j обязательно совпадут: существуют такие $k_1, k_2 \in \mathbb{Z}$, что $k_1 < k_2$ и $\varphi^{k_1}(j) = \varphi^{k_2}(j)$. Нетрудно догадаться, какое нужно взять k, чтобы $\varphi^k(j) = j$.

Орбита. Пусть $\varphi \in S_n$, $j \in X_n$. *Орбитой* элемента j относительно перестановки φ (короче, φ-орбитой элемента j) называют класс элемента φ по отношению φ-эквивалентности, т. е. множество всех элементов вида $\varphi^k(j)$, где $k \in \mathbb{Z}$. Множество всех φ-орбит есть разбиение X_n.

Пусть k — наименьшая из таких положительных целых степеней p, при которых $\varphi^p(j) = j$. Доказать, что множество $\{\varphi^0(j), \ldots, \varphi^{k-1}(j)\}$ состоит из k элементов и является φ-орбитой j. Доказать, что для любых r,s из φ-орбиты j существует такое $m \in \{0, \ldots, k-1\}$, что $s = \varphi^m(r)$.

Разложение перестановки на независимые циклы. Пусть $\varphi \in S_n$. Доказать, что φ можно представить в виде

$$\varphi = \omega_1 \omega_2 \dots \omega_q,$$

где $\omega_1, \dots, \omega_q$ — независимые нетривиальные циклы, причём такое разложение единственно с точностью до порядка следования циклов.

Существование: пусть $Y_1, \dots, Y_q$ — все φ-орбиты, в которых более одного элемента; $\omega_j = \varphi | Y_j$.

Единственность: если $\varphi = \omega'_1 \omega'_2 \dots \omega'_s$, где $\omega'_1, \dots, \omega'_s$ — независимые нетривиальные циклы, и Y'_j — множество тех $i \in X_n$, для которых $\omega'_j(i) \neq i$, то $Y'_1, \dots, Y'_s$ — все φ-орбиты, в которых более одного элемента, и $\omega'_j = \varphi | Y_j$.

§ 6. Декремент и разложение на транспозиции

Декремент перестановки. Пусть перестановка $\varphi \in S_n$ разложена на k независимых циклов, имеющих длины $l_1, l_2, \ldots, l_k$. Тогда её *декрементом* называется число

$$\operatorname{dec}(\varphi) = \sum_{j=1}^{k} (l_j - 1) = \left(\sum_{j=1}^{k} l_j\right) - k.$$

Показать, что в этом определении можно заменить разложение на независимые циклы разложением на невырожденные независимые циклы.

Декремент перестановки: другая форма определения. Показать, что $\operatorname{dec}(\varphi)$ есть разность между числом действительно перемещаемых элементов и числом невырожденных циклов. (Говорят, что перестановка φ действительно перемещает элемент j, если $\varphi(j) \neq j$.)

Декремент перестановки: примеры. Найти $\operatorname{dec}(\varphi)$ для следующих перестановок φ:
1) $\varphi = e$; 2) φ — цикл длины s; 3) φ — транспозиция;

$$4)\ \varphi = \begin{pmatrix} 1 & 2 & \ldots & (n-1) & n \\ n & (n-1) & \ldots & 2 & 1 \end{pmatrix}.$$

Возможные значения декремента. Доказать, что $\operatorname{dec}(\varphi)$, где $\varphi \in S_n$, принимает все значения от 0 до $n-1$.

Склеивание двух циклов, имеющих один общий элемент. Пусть

$$a_1, \ldots, a_m, a_{m+1}, \ldots, a_k$$

— попарно различные элементы X_n. Доказать, что

$$(a_1\ a_2\ \ldots\ a_m)(a_m\ a_{m+1}\ \ldots\ a_k) = (a_1\ a_2\ \ldots\ a_k).$$

Полезно сначала убедиться в этом на конкретном примере (в S_8):

$$(5\ 3\ 8)(8\ 1\ 7\ 6) = (5\ 3\ 8\ 1\ 7\ 6).$$

Разложение цикла на транспозиции. Пусть $a_1, a_2, \ldots, a_m$ — попарно различные элементы X_n. Доказать, что

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

т. е. любой цикл длины m можно разложить на $m-1$ транспозицию.

Умножение цикла на транспозицию элементов, входящих в цикл. Пусть $a_1, \ldots, a_m$ — попарно различные элементы X_n, $j \in \{1, \ldots, m\}$. Вывести формулы для следующих произведений:

$$(a_1\ a_j)(a_1\ \ldots\ a_m), \qquad (a_1\ \ldots\ a_m)(a_m\ a_j).$$

Изменение цикловой структуры при умножении на транспозицию. Пусть $\varphi \in S_n$, $a, b \in X_n$. Доказать, что если a и b входят в один цикл перестановки φ, то при умножении φ на транспозицию $\tau_{a,b}$ (слева или справа) этот цикл распадается на 2 цикла, а если a и b входят в различные циклы, то при указанном умножении эти циклы сливаются в один.

Изменение декремента при умножении на транспозицию. Пусть $\varphi \in S_n$, $i, j \in X_n$, $i \neq j$. Доказать, что

$$\operatorname{dec}(\varphi\tau_{i,j}) = \begin{cases} \operatorname{dec}(\varphi) - 1, & i \overset{\varphi}{\sim} j; \\ \operatorname{dec}(\varphi) + 1, & i \overset{\varphi}{\nsim} j. \end{cases}$$

Найти и доказать похожую формулу для $\operatorname{dec}(\tau_{i,j}\varphi)$.

Разложение перестановки на минимальное число транспозиций. Доказать, что любую перестановку φ из S_n можно разложить на $\operatorname{dec}(\varphi)$ транспозиций и нельзя разложить на меньшее число транспозиций.

Декремент обратной перестановки. Пусть $\varphi \in S_n$. Доказать, что $\operatorname{dec}(\varphi^{-1}) = \operatorname{dec}(\varphi)$.

Декремент композиции. Пусть $\varphi, \psi \in S_n$. Доказать, что

$$\operatorname{dec}(\varphi\psi) \leqslant \operatorname{dec}(\varphi) + \operatorname{dec}(\psi), \qquad (-1)^{\operatorname{dec}(\varphi\psi)} = (-1)^{\operatorname{dec}(\varphi)}(-1)^{\operatorname{dec}(\psi)}.$$

Разложение транспозиции на простые транспозиции. Показать, что если i, j, k — попарно различные элементы X_n, то

$$\tau_{i,k} = \tau_{i,j}\tau_{j,k}\tau_{i,j}.$$

Вывести отсюда, что любую транспозицию вида $\tau_{i,i+m}$, где m — положительное целое число, можно представить в виде композиции простых транспозиций, число которых равно $2m-1$.

Существование разложения перестановки на простые транспозиции. Доказать, что любую перестановку можно представить в виде композиции конечного числа простых транспозиций.

Цикловая структура перестановки $\psi\varphi\psi^{-1}$. Пусть φ раскладывается в композицию следующих независимых циклов:

$$\varphi = (a_{1,1}\ a_{1,2}\ \ldots\ a_{1,s_1})\ldots(a_{k,1}\ a_{k,2}\ \ldots\ a_{k,s_k}).$$

Найти разложение на независимые циклы перестановки $\psi\varphi\psi^{-1}$.

Инвариантность декремента. Доказать, что для любых φ, ψ из S_n

$$\mathrm{dec}(\psi\varphi\psi^{-1}) = \mathrm{dec}(\varphi).$$

Декремент произведения двух перестановок не зависит от порядка сомножителей. Доказать, что для любых φ, ψ из S_n

$$\mathrm{dec}(\varphi\psi) = \mathrm{dec}(\psi\varphi).$$

Декрементная метрика. Для любых φ, ψ положим

$$d(\varphi, \psi) = \mathrm{dec}(\varphi\psi^{-1}).$$

Доказать, что d является метрикой на S_n, т. е. удовлетворяет следующим условиям:
(1) $d(\varphi, \psi) \geqslant 0$ для любых φ, ψ из S_n;
(2) $d(\varphi, \psi) = 0 \quad \Longleftrightarrow \quad \varphi = \psi$;
(3) $d(\varphi, \psi) = d(\psi, \varphi)$ для любых φ, ψ из S_n;
(4) $d(\varphi, \psi) \leqslant d(\varphi, \chi) + d(\chi, \psi)$ для любых φ, ψ, χ из S_n.
Доказать также, что $d(\varphi, \psi) = \mathrm{dec}(\varphi^{-1}\psi)$.

Смысл декрементной метрики. Пусть $\varphi, \psi \in S_n$. Доказать, что $d(\varphi, \psi)$ есть минимальное число транспозиций, умножая на которые слева можно превратить ψ в φ. Доказать, что $d(\varphi, \psi)$ есть минимальное число транспозиций, умножая на которые справа можно превратить ψ в φ.

§ 7. Число инверсий и разложение на простые транспозиции

Число инверсий перестановки. Пусть $\varphi \in S_n$. Обозначим через $\mathrm{inv}(\varphi)$ *число инверсий* перестановки φ, т. е. число таких пар (i, j), что $i, j \in X_n$, $i < j$ и $\varphi(i) > \varphi(j)$. Инверсии называют также *беспорядками.*

Пример подсчёта числа инверсий. Пусть

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 1 & 6 & 4 \end{pmatrix}.$$

Тогда множество инверсий φ есть

$$\{(1,4), (2,3), (2,4), (2,6), (3,4), (5,6)\},$$

откуда $\mathrm{inv}(\varphi) = 6$. Если перестановка записана в стандартном виде (как выше), то можно для каждого элемента нижней строки найти число тех элементов, которые расположены правее него, но при этом меньше него, и сложить полученные числа:

$$\mathrm{inv}(\varphi) = 1 + 3 + 1 + 0 + 1 + 0 = 6.$$

Или наоборот: для каждого элемента нижней строки найти число тех элементов, которые расположены левее него, но при этом больше него, и сложить полученные числа:

$$\mathrm{inv}(\varphi) = 0 + 0 + 1 + 3 + 0 + 2 = 6.$$

Упражнения на подсчёт числа инверсий. Найти $\mathrm{inv}(\varphi)$ для следующих перестановок:

(1) $\varphi = e$;

(2) $\varphi = \tau_{j,j+1}$;

(3) $\varphi = \tau_{j,j+m}$;

(4) $\varphi = (1\ 2\ 3\ \ldots\ s)$;

(5) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 8 & 1 & 2 & 7 \end{pmatrix}$;

(6) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 7 & 2 & 1 & 5 & 4 & 6 \end{pmatrix}$;

(7) $\varphi = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ n & n-1 & \ldots & 2 & 1 \end{pmatrix}$;

(8) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & 2m-1 & 2m \\ 2 & 1 & 4 & 3 & \ldots & 2m & 2m-1 \end{pmatrix} \qquad (n = 2m)$;

(9) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3m-2 & 3m-1 & 3m \\ 3 & 2 & 1 & 6 & 5 & 4 & \dots & 3m & 3m-1 & 3m-2 \end{pmatrix}$ $(n = 3m)$;

(10) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & 2m-3 & 2m-2 & 2m-1 & 2m \\ 3 & 4 & 5 & 6 & \dots & 2m-1 & 2m & 1 & 2 \end{pmatrix}$ $(n = 2m)$;

(11) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3m-2 & 3m-1 & 3m \\ 2 & 3 & 1 & 5 & 6 & 4 & \dots & 3m-1 & 3m & 3m-2 \end{pmatrix}$ $(n = 3m)$;

(12) $\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \dots & 3m-2 & 3m-1 & 3m \\ 4 & 5 & 6 & 7 & 8 & 9 & \dots & 1 & 2 & 3 \end{pmatrix}$ $(n = 3m)$.

Изменение числа инверсий при умножении на простую транспозицию. Пусть $\varphi \in S_n$, $j \in \{1, \dots, n-1\}$. Доказать, что

$$\mathrm{inv}(\varphi\tau_{j,j+1}) = \begin{cases} \mathrm{inv}(\varphi) + 1, & \varphi(j) < \varphi(j+1), \\ \mathrm{inv}(\varphi) - 1, & \varphi(j) > \varphi(j+1). \end{cases}$$

Полезно представить себе стандартную запись перестановки $\varphi\tau_{j,j+1}$.

О числе инверсий композиции нескольких простых транспозиций. Доказать, что если $\psi_1, \dots, \psi_k$ — простые транспозиции, то

$$(-1)^{\mathrm{inv}(\psi_1 \dots \psi_k)} = (-1)^k, \qquad \mathrm{inv}(\psi_1 \dots \psi_k) \leqslant k.$$

Число инверсий тождественной перестановки. Пусть $\varphi \in S_n$. Доказать, что условие $\mathrm{inv}(\varphi) = 0$ равносильно условию $\varphi = e$.

Существование инверсии соседних элементов в нетождественной перестановке. Пусть $\varphi \in S_n$, $\varphi \neq e$. Доказать, что существует такое число $j \in \{1, \dots, n-1\}$, для которого $\varphi(j) > \varphi(j+1)$.

В нетождественной перестановке существует элемент, стоящий правее своего места. Пусть $\varphi \in S_n$, $\varphi \neq e$. Доказать, что существует такое число $k \in X_n$, что $\varphi^{-1}(k) > k$, т. е. значение k «находится правее положенного места».

Перемещение элемента на своё место. Пусть $\varphi \in S_n$, $\varphi \neq e$, k — минимальное число, которое в перестановке S_n находится правее положенного места, и $j = \varphi^{-1}(k)$. Сколько простых транспозиций необходимо, чтобы «переместить элемент k на место k»? Более формально: на сколько простых транспозиций нужно умножить справа перестановку φ, чтобы получить перестановку φ', для которой $\varphi'(k) = k$? Как связаны между собой $\mathrm{inv}(\varphi)$ и $\mathrm{inv}(\varphi')$?

Разложение перестановки на минимальное число простых транспозиций. Доказать, что любую перестановку $\varphi \in S_n$ можно разложить на $\mathrm{inv}(\varphi)$ простых транспозиций и нельзя разложить на меньшее число простых транспозиций.

Максимальное значение числа инверсий. Найти максимальное значение $\mathrm{inv}(\varphi)$ при φ из S_n.

Возможные значения числа инверсий. Доказать, что $\mathrm{inv}(\varphi)$ принимает все значения от 0 до $\frac{n(n-1)}{2}$, когда φ пробегает S_n.

Число инверсий обратной перестановки. Пусть $\varphi \in S_n$. Показать, что $\mathrm{inv}(\varphi^{-1}) = \mathrm{inv}(\varphi)$. Сначала можно рассмотреть конкретный пример:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 3 & 1 & 5 \end{pmatrix}.$$

Число инверсий композиции перестановок. Пусть $\varphi, \psi \in S_n$. Доказать, что

$$\mathrm{inv}(\varphi\psi) = \mathrm{inv}(\varphi) + \mathrm{inv}(\psi) - 2k,$$

где k — число таких пар (i, j), что

$$i, j \in X_n, \qquad i < j, \qquad \psi(i) > \psi(j), \qquad \varphi(\psi(i)) < \varphi(\psi(j)).$$

Вывести отсюда, что

$$\mathrm{inv}(\varphi\psi) \leqslant \mathrm{inv}(\varphi) + \mathrm{inv}(\psi), \qquad (-1)^{\mathrm{inv}(\varphi\psi)} = (-1)^{\mathrm{inv}(\varphi)}(-1)^{\mathrm{inv}(\psi)}.$$

§ 8. Сигнатура перестановки

Определение сигнатуры через декремент. *Сигнатурой* (*знаком*) перестановки $\varphi \in S_n$ называют число $(-1)^{\operatorname{dec}(\varphi)}$. Сигнатуру перестановки φ обычно обозначают через $\operatorname{sgn}(\varphi)$, $\operatorname{sign}(\varphi)$ или $\varepsilon(\varphi)$. Перестановку φ называют *чётной*, если $\operatorname{sgn}(\varphi) = 1$; *нечётной*, если $\operatorname{sgn}(\varphi) = -1$.

Вычисление сигнатуры через число циклов чётной длины. Пусть φ — перестановка, k — число циклов чётной длины в её разложении. Тогда $\operatorname{sgn}(\varphi) = (-1)^k$.

Изменение сигнатуры при умножении на транспозицию. Пусть $\varphi, \psi \in S_n$, причём ψ — транспозиция. Доказать, что $\operatorname{sgn}(\varphi\psi) = \operatorname{sgn}(\psi\varphi) = -\operatorname{sgn}(\varphi)$.

Сигнатура произведения транспозиций. Пусть $\psi_1, \ldots, \psi_k$ — транспозиции. Доказать, что $\operatorname{sgn}(\psi_1 \cdot \ldots \cdot \psi_k) = (-1)^k$.

Сигнатура и число инверсий. Пусть $\varphi \in S_n$. Доказать, что

$$\operatorname{sgn}(\varphi) = (-1)^{\operatorname{inv}(\varphi)}.$$

Иногда эту формулу берут в качестве определения. Отметим два преимущества $\operatorname{dec}(\varphi)$ перед $\operatorname{inv}(\varphi)$:
1) $\operatorname{dec}(\varphi)$ не зависит от нумерации элементов множества X_n;
2) в большинстве случаев $\operatorname{dec}(\varphi)$ вычисляется проще, чем $\operatorname{inv}(\varphi)$.

Сигнатура перестановки: примеры. Найти $\operatorname{sgn}(\varphi)$ для перестановок из упражнений на декремент и на число инверсий.

Мультипликативность сигнатуры.

$$\operatorname{sgn}(\varphi\psi) = \operatorname{sgn}(\varphi)\operatorname{sgn}(\psi) \qquad (\varphi, \psi \in S_n).$$

Имеется много способов доказательства. Вот самые естественные:

1-й способ: с помощью теорем о $\operatorname{dec}(\varphi\psi)$ или $\operatorname{inv}(\varphi\psi)$.

2-й способ: представить ψ в виде композиции нескольких транспозиций и воспользоваться утверждением об изменении сигнатуры при умножении на транспозицию.

3-й способ: разложить φ и ψ на транспозиции и воспользоваться утверждением о сигнатуре перестановки, разложенной на транспозиции.

Сигнатура единичной и обратной перестановок. Вывести из мультипликативности сигнатуры, что $\operatorname{sgn}(e) = 1$, $\operatorname{sgn}(\varphi^{-1}) = \operatorname{sgn}(\varphi)$.

Сигнатура «самой беспорядочной» перестановки. Вычислить $\operatorname{sgn}(\varphi)$, где
$$\varphi = \begin{pmatrix} 1 & 2 & \dots & (n-1) & n \\ n & (n-1) & \dots & 2 & 1 \end{pmatrix},$$
двумя способами: через $\operatorname{inv}(\varphi)$ и через $\operatorname{dec}(\varphi)$. Рассмотреть 4 случая в зависимости от того, какой остаток даёт n при делении на 4. Записать ответ также с помощью функции $\lfloor\ \rfloor$ (целой части).

Множество A_n. Пусть A_n — множество всех чётных перестановок $\varphi \in S_n$. Найти A_2 и A_3. Доказать, что если $n \geqslant 1$, то $|A_n| = |S_n|/2$. Указание: придумать какую-нибудь биекцию множества A_n на множество $S_n \setminus A_n$.

A_n есть подгруппа S_n. Пусть $(G, *)$ — группа. Множество $H \subset G$ называют подгруппой G, если оно вместе с операцией $*$ (суженной на $H \times H$) само является группой. Для этого необходимо и достаточно, чтобы $x * y^{-1} \in H$ для любых $x, y \in H$. Доказать, что A_n — подгруппа S_n. Её называют *знакопеременной группой порядка* n.

§ 9. Кососимметрические функции

Функции от n аргументов. Будем рассматривать функции, действующие из Y^n в $\mathbb{R}$, где Y — какое-то множество. Примеры:
1) $f\colon \mathbb{R}^n \to \mathbb{R}$, $f(x_1, \ldots, x_n) = x_1 + \ldots + x_n$;
2) $f\colon \mathbb{R}^2 \to \mathbb{R}$, $f(x_1, x_2) = x_1 - x_2$.

Действие перестановки на функцию. Пусть $f\colon Y^n \to \mathbb{R}$, $\varphi \in S_n$. Тогда функция $\varphi f\colon Y^n \to \mathbb{R}$ определяется формулой

$$(\varphi f)(x_1, \ldots, x_n) = f(x_{\varphi(1)}, \ldots, x_{\varphi(n)}), \qquad x_1, \ldots, x_n \in Y.$$

Например, при действии транспозиции $\tau_{i,j}$ на функцию f аргументы с номерами i и j меняются местами:

$$\tau_{i,j} f(x_1, \ldots, x_i, \ldots, x_j, \ldots, x_n) = f(x_1, \ldots, x_j, \ldots, x_i, \ldots, x_n).$$

Последовательное действие двух перестановок на функцию. Пусть $f\colon Y^n \to \mathbb{R}$, $\varphi, \psi \in S_n$. Доказать, что $(\varphi\psi)f = \varphi(\psi f)$.

Условия кососимметричности. Пусть $f\colon Y^n \to \mathbb{R}$. Доказать, что следующие условия равносильны:

(a) $\tau_{j,j+1} f = -f$ для любого $j \in \{1, \ldots, n-1\}$, т. е. f меняет знак при перестановке любых двух соседних аргументов;

(b) $\tau_{i,j} f = -f$ для любых различных $i, j \in \{1, \ldots, n\}$, т. е. f меняет знак при перестановке любых двух аргументов;

(c) $\varphi f = \operatorname{sgn}(\varphi) f$ для любой перестановки $\varphi \in S_n$.

Если выполняются эти условия, то функцию f называют кососимметрической.

Произведение разностей как кососимметрическая функция. Определим функцию $V_n\colon \mathbb{R}^n \to \mathbb{R}$ формулой

$$V_n(x_1, \ldots, x_n) = \prod_{i>j} (x_i - x_j),$$

где произведение берётся по всем парам (i, j), таким, что $i, j \in \{1, \ldots, n\}$ и $i > j$. Например,

$$V_3(x_1, x_2, x_3) = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2).$$

Доказать, что функция V_n кососимметрическая и что $V_n(x_1, \ldots, x_n) \neq 0$, если аргументы $x_1, \ldots, x_n$ попарно различны.

Доказательство мультипликативности сигнатуры с помощью кососимметрических функций. Пусть $f\colon Y^n \to \mathbb{R}$ — какая-нибудь кососимметрическая функция от n аргументов, не равная тождественно нулю (например, $f = V_n$). Пользуясь кососимметричностью f, доказать, что для любых φ, ψ из S_n и любых $x_1, \ldots, x_n$ из Y

$$\operatorname{sgn}(\varphi\psi) f(x_1, \ldots, x_n) = \operatorname{sgn}(\varphi) \operatorname{sgn}(\psi) f(x_1, \ldots, x_n).$$

Вывести отсюда утверждение о мультипликативности сигнатуры.

Анализ доказательства мультипликативности сигнатуры через кососимметрические функции. Выяснить, какие свойства перестановок и какие свойства сигнатуры использованы в доказательстве из предыдущего упражнения.