Перестановки: все что вы хотели знать о них, но боялись спросить

Это сводка основных определений, примеров и фактов о перестановках. За доказательствами отсылаем читателя к подробным учебниками, например,

- А. И. Кострикин, «Введение в алгебру. Часть I. Основы алгебры».
- Э. Б. Винберг, «Курс алгебры».

Знаком «↯» отмечены места, в которых мы советуем читателю остановиться и обдумать прочитанное (в частности, восстановить детали доказательства). Все ошибки, разумеется, принадлежат автору.

1. Основные определения

Пусть X — произвольное множество. **Перестановкой** на множестве X называется любое биективное отображение $\sigma : X \to X$. Нас будут интересовать только перестановки конечных множеств. Элементы конечного множества из n элементов будем обозначать просто натуральными числами от 1 до n. Итак, пусть $X = \{1, \dots, n\}$. Перестановку $\sigma : X \to X$ удобно тогда записывать в виде следующей таблицы

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix},$$

которую во многих учебниках называют **подстановкой**, соответствующей перестановке σ.

Замечание 1. Существуют определенные разногласия по поводу употребления терминов «перестановка» и «подстановка», однако отличия тут скорее лежат в лингвистической плоскости, чем в математической. Не желая вдаваться в обсуждение этих отличий (см., например, П. С. Александров, «Лекции по аналитической геометрии», Приложение), мы, следуя учебнику Кострикина, будем везде использовать термин «перестановка»[1].

Множество всех перестановок на множестве из n элементов обозначается S_n. Поскольку в нижней строке таблицы сверху каждое число от 1 до n встречается по одному разу, S_n содержит ровно $n!$ элементов.

Запись перестановки, в которой в верхней строчке числа записаны строго по возрастанию, называется *канонической записью*. Ясно, однако, что перестановка столбцов в таблице никак не менят само отображение σ. Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 2 & 1 & 4 & 3 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

— одна и та же подстановка в S_4. Иногда бывает удобно использовать неканоническую запись. Однако, любая перестановка приводится к каноническому виду изменением порядка столбцов.

[1] Это оправдывается, в частности, тем, что в англоязычной литературе такой путаницы нет: везде используется термин «permutation».

Поскольку перестановка на X — это биективное отображение $X \to X$, имеет смысл говорить о композиции таких отображений: для $i \in \{1, \dots, n\},\ \sigma, \tau \in \mathrm{S}_n$ имеем

$$\tau \circ \sigma :\ i \overset{\sigma}{\mapsto} \sigma(i) \overset{\tau}{\mapsto} \tau(\sigma(i))$$

Подчеркнем, что запись $\tau \circ \sigma$ обозначает, что сперва применяется отображение σ, а уже потом — отображение τ.

Замечание 2. Вообще говоря, это *не* то же самое, что сначала применить отображение τ, а затем — отображение σ.

Композицию перестановок принято называть их **произведением**. Причина этого в том, что все перестановки из S_n с операцией взятия их композиции образуют **группу**. Это означает следующее:

(1) Произведение двух перестановок есть снова перестановка (очевидно).

(2) Произведение ассоциативно:

$$\sigma \circ (\tau \circ \rho) = (\sigma \circ \tau) \circ \rho$$

(требует некоторой проверки).

(3) Существует **тождественная перестановка**

$$e = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix},$$

соответствующая тождественному отображению $X \to X$, такая что

$$e \circ \sigma = \sigma \circ e = \sigma$$

для любой $\sigma \in \mathrm{S}_n$ (очевидно).

(4) Наконец, для любой перестановки $\sigma \in \mathrm{S}_n$ существует **обратная** перестановка σ^{-1}, такая что

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = e.$$

Очевидно, что σ^{-1} имеет вид

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

(запись не каноническая).

Пример 1. Найдем произведение $\tau\sigma$ двух перестановок из S_4:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

В соответствии с нашей договоренностью о порядке, в котором берется композиция двух отображений, умножение начинаем со второй перестановки:

$$\begin{aligned} \tau\sigma(1) &= \tau(\sigma(1)) = \tau(2) = 3, \\ \tau\sigma(2) &= \tau(\sigma(2)) = \tau(3) = 1, \\ \tau\sigma(3) &= \tau(\sigma(3)) = \tau(1) = 4, \\ \tau\sigma(4) &= \tau(\sigma(4)) = \tau(4) = 2. \end{aligned}$$

Таким образом,

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

Замечание 3. Согласно Замечанию 2, в общем случае $\sigma\tau \neq \tau\sigma$. Если $\sigma\tau = \tau\sigma$, то говорят, что σ и τ **коммутируют** между собой.

2. Циклы

Циклической перестановкой (циклом) называется перестановка, переводящая i_1 в i_2, i_2 в i_3, …, i_{k-1} в i_k и i_k в i_1. Такой цикл кратко записывается в виде $(i_1 i_2 \dots i_k)$. Цикл все равно откуда начинать. Поэтому, например,

$$(i_1 i_2 \dots i_k) = (i_2 i_3 \dots i_k i_1).$$

Любая перестановка представима в виде произведения циклов. Для этого нужно взять любое число i_1 в верхней строке и посмотреть, в какое i_2 оно переводится, затем найти i_2 в верхней строке и посмотреть, в какое i_3 оно переходит, и так далее до тех пор, пока не встретится i_m, переходящее в i_1. В результате выделяется сомножитель (цикл)

$$(i_1 i_2 i_3 \dots i_m).$$

Затем среди $1, \dots, n$ берется любое число, не входящее в уже найденный цикл, и процедура повторяется для этого числа.

Пример 2.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 4 & 2 & 5 & 8 & 10 & 9 & 6 & 7 \end{pmatrix} = (1342)(5)(689)(7,10)$$

Заметим, что 5 осталось на месте. Числа, которые переходят сами в себя, принято опускать в такой записи перестановки, то есть писать просто $(1342)(689)(7,10)$.

Заметим, что на самом деле описанный метод дает запись перестановки в виде **непересекающихся циклов** (то есть ни одно число не входит в два цикла сразу). *Разложение перестановки в произведение непересекающихся циклов единственно с точностью до изменения порядка сомножителей.*

Замечание 4. Причина того, что соможители можно менять местами, состоит в том, что непересекающиеся циклы, очевидно, коммутируют между собой ϟ.

Транспозицией называется цикл длины 2. *Любой цикл представляется в виде произведения транспозиций*, и такое разложение можно указать явно (ϟ):

Предложение 1. *Имеем*

$$(i_1 i_2 \dots i_k) = (i_1 i_2)(i_2 i_3) \dots (i_{k-1} i_k)$$

В частности, *любая перестановка раскладывается в произведение транспозиций.*

Замечание 5. В отличие от разложения на независимые циклы, разложение в произведение транспозиций, вообще говоря, *не единственно*[2]. Например, в S_4 имеем

$$(123) = (13)(12) = (23)(13) = (13)(24)(12)(14).$$

[2]А сами транспозиции в таком разложении могут быть зависимы и не обязаны коммутировать.

3. Знак перестановки

Определение знака перестановки часто дается в терминах *инверсий*, но мы сразу дадим более полезное в реальных вычислениях определение.

Предложение-определение 1. Пусть $\sigma \in \mathrm{S}_n$ и

$$\sigma = \tau_1 \tau_2 \dots \tau_k$$

— произвольное разложение σ в произведение транспозиций. Тогда число

$$\operatorname{sgn} \sigma = (-1)^k,$$

называемое **знаком** или **четностью** σ, полностью определяется σ и не зависит от способа разложения σ в произведение транспозиций. Подстановки, имеющие знак 1, называются **четными**, (-1) — **нечетными**.

Следствие 1. *Транспозиции — нечетные перестановки.*

Используя предыдущее следствие и Предложение 1, получаем

Следствие 2. *Четность цикла длины k равна $(-1)^{k-1}$.*

Как ведет себе знак перестановки при перемножении перестановок? Ответ дает

Предложение 2. *Пусть $\sigma, \tau \in \mathrm{S}_n$. Тогда*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau.$$

Следствие 3. *Множество всех четных перестановок образует группу. Эта группа обозначается A_n и называется* **знакопеременной группой**. *Отображение*

$$\operatorname{sgn} : \mathrm{S}_n \to \mathbb{Z}_2$$

является гомоморфизмом групп, ядро[3] которого есть A_n.

Пример 3. Найдем четность перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 4 & 2 & 5 & 8 & 10 & 9 & 6 & 7 \end{pmatrix}$$

Как мы видели выше, $\sigma = (1342)(689)(7,10)$. Значит,

$$\operatorname{sgn}\sigma = (-1)^{4-1}(-1)^{3-1}(-1) = 1.$$

4. Порядок перестановки

В любой группе G имеет смысл понятие **порядка** элемента $g \in G$. В частности, порядок $\sigma \in \mathrm{S}_n$ — это такое наименьшее натуральное число n, что $\sigma^n = e$ — тождественная перестановка. Порядок σ мы будем обозначать $\operatorname{ord}\sigma$.

Пример 4. Порядок транспозиции равен 2. Более общо, порядок цикла длины k равен k (☡).

Замечание 6. Не следует думать, что для $\sigma \in \mathrm{S}_n$ всегда верно $\sigma^n = e$. Например, для $(12) \in \mathrm{S}_3$ имеем $(12)^3 = (12)^2(12) = (12)$. Верно, однако, что $\operatorname{ord}\sigma$ делит $|\mathrm{S}_n| = n!$ (но это редко помогает ввиду быстрого роста $n!$).

[3] Ядром гомоморфизма групп $f : G \to H$ называется множество $f^{-1}(1)$.

Замечание 7. Если $\sigma^n = e$, то $\operatorname{ord}\sigma$ делит n. Действительно, пусть $\operatorname{ord}\sigma = k$ и $n \geqslant k$. Разделим n на k с остатком: $n = kq + r$, $r < k$. Тогда

$$e = \sigma^n = \sigma^{kq}\sigma^r = \sigma^r,$$

но это противоречит тому, что k — наименьшее натуральное число, такое что $\sigma^k = e$.

Порядок произвольной перестановки, разложенной в произведение *независимых* циклов, вычисляется при помощи следующего утверждения:

Предложение 3 (ϟ)**.** *Пусть*

$$\sigma = \tau_1\tau_2\dots\tau_k$$

— разложение σ в произведение независимых циклов длин $\ell_1, \dots, \ell_k$ соответственно. Тогда

$$\operatorname{ord}\sigma = \text{НОК}(\ell_1, \dots, \ell_k).$$

Замечание 8. Для доказательства нужно заметить, что, ввиду независимости τ_i, эти циклы попарно коммутируют между собой, а потому

$$(\tau_1\tau_2\dots\tau_k)^n = \tau_1^n\tau_2^n\dots\tau_k^n$$

(для некоммутирующих перестановок τ_1 и τ_2 мы могли бы лишь записать $(\tau_1\tau_2)^2 = \tau_1\tau_2\tau_1\tau_2$).

Пример 5. Порядок перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 4 & 2 & 5 & 8 & 10 & 9 & 6 & 7 \end{pmatrix} = (1342)(689)(7,10)$$

равен $\text{НОК}(4, 3, 2) = 12$.

5. Примеры решения задач

Разложение перестановки в произведение независимых циклов является основным средством при решении большинства задач (вместе с соображениями, касающимися порядка перестановки).

Задача 1. Вычислить

$$\sigma = \begin{pmatrix} 4 & 3 & 7 & 9 & 2 & 5 & 1 & 6 & 8 & 10 \\ 2 & 8 & 9 & 6 & 1 & 5 & 10 & 3 & 7 & 4 \end{pmatrix}^{2017}.$$

Решение. Раскладывая в произведение независимых циклов, получаем

$$[(1,10,4,2)(38796)]^{2017} = (1,10,4,2)^{2017}(38796)^{2017} = \{2017 = 4\cdot 504 + 1 = 5\cdot 403 + 2\} =$$
$$= ((1,10,4,2)^4)^{504}(1,10,4,2)\cdot((38796)^5)^{403}(38796)^2 =$$
$$= (1,10,4,2)(38796)^2 = (1,10,4,2)(37689).$$

Мы сразу получили запись результата в виде произведения независимых циклов. При необходимости можно перейти и к развернутой записи:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 1 & 7 & 2 & 5 & 8 & 6 & 9 & 3 & 4 \end{pmatrix}$$

□

Задача 2. В группе S_5 решить уравнение

$$\sigma^2 = (345).$$

Решение. Перестановка $\sigma \in \mathrm{S}_5$ может раскладываться в произведение независимых циклов только следующими способами:

$$(ab),\quad (ab)(cd),\quad (ab)(cde),\quad (abc),\quad (abcd),\quad (abcde).$$

Возведение в квадрат первой и второй перестановок даст тождественную; следовательно, они нам не подходят. Кроме того, не подходят и последние две перестановки, поскольку

$$(abcd)^2 = (ac)(bd),\quad (abcde)^2 = (acebd).$$

С другой стороны,

$$[(ab)(cde)]^2 = (ced),\quad (abc)^2 = (acb).$$

Это дает возможности $c = 3$, $e = 4$, $d = 5$ и $a = 3$, $c = 4$, $b = 5$. В результате получаем ответ: либо $\sigma = (12)(354)$, либо $\sigma = (354)$. □

Задача 3. В группе S_n решить уравнение

$$\sigma^3 = (123).$$

Решение. Заметим, что $\sigma^9 = e$. Согласно Замечанию 7, $\operatorname{ord}\sigma$ делит 9, откуда $\operatorname{ord}\sigma \in \{1, 3, 9\}$. Поскольку $\sigma \neq e$ и, по условию, $\sigma^3 = (123)$, остается рассмотреть лишь случай $\operatorname{ord}\sigma = 9$. Поскольку порядок перестановки есть наименьшее общее кратной длин независимых циклов, входящих в ее разложение, в записи σ должен присутствовать *хотя бы один* цикл длины 9, то есть разложение на независимые циклы имеет вид

$$\sigma = (i_1 i_2 \dots i_9)\tau_1 \dots \tau_k,$$

откуда

$$\sigma^3 = (i_1 i_4 i_7)(i_2 i_5 i_8)(i_3 i_5 i_9)\tau_1^3 \dots \tau_k^3,$$

что, очевидно, не может быть равно (123). □

Задача 4 (Различные системы порождающих в S_n). Докажите, что всякая перестановка $\sigma \in \mathrm{S}_n$ может быть представлена как произведение циклов вида:

(а) $(12),\ (13), \dots, (1, n)$;
(б) $(12),\ (23), \dots, (n-1, n)$;
(в) $(12),\ (123\dots n)$.

Доказательство. Такие задачи решаются методом «взять и увидеть».

(а) Тут нужно увидеть, что любая транспозиция (ij) представляется в виде

$$(ij) = (1i)(1j)(1i).$$

Осталось вспомнить, что любая перестановка записывается в виде произведений транспозиций.

(б) Докажем, что любая транспозиция вида $(1k)$ может быть получена как произведение транспозиций из пункта (б), а затем воспользуемся уже доказанным пунктом (а). Доказывать будем индукцией по k. База $k = 2$ очевидна. Предположим, что это верно для k и докажем для $k + 1$. Для этого просто нужно заметить, что

$$(1, k+1) = (1k)(k, k+1)(1k)$$

и воспользоваться предположением индукции.

(в) Здесь мы сведем все к пункту (б), где мы раскладывали произвольную перестановку в произведение транспозиций вида $(k, k+1)$. А именно, положим $\gamma = (123\dots n)$ и заметим, что

$$\gamma^{-1}(k, k+1)\gamma = (k-1, k).$$

Домножая слева на γ^{-1}, а справа на γ подходящее число раз, из любой транспозиции $(k, k+1)$ можно получить таким образом транспозицию (12).

□

В решении Задачи 4в мы использовали операцию *сопряжения*. Напомним, что $\tau, \sigma \in \mathrm{S}_n$ называются *сопряженными*, если

$$\tau = \delta\sigma\delta^{-1}$$

для некоторой $\delta \in \mathrm{S}_n$. Это важное понятие, которое часто встречается в различных задачах.

Задача 5. Докажите, что для любой $\sigma \in \mathrm{S}_n$ имеем

$$\sigma(i_1 i_2 \dots i_k)\sigma^{-1} = (\sigma(i_1)\sigma(i_2)\dots\sigma(i_k)).$$

Решение. Положим $\tau = (i_1 i_2 \dots i_k)$. Поскольку в левой и правой частях доказываемого равенства стоят перестановки, достаточно показать, что они одинаково действуют на каждый $j \in \{1, \dots, n\}$. Докажем это, например, для $j = \sigma(i_1)$ (для остальных — полностью аналогично). Нам нужно показать, что применение перестановки в левой части к $\sigma(i_1)$ дает $\sigma(i_2)$. Имеем:

$$\sigma\tau\sigma^{-1}[\sigma(i_1)] = \sigma\tau(\sigma^{-1}\sigma)[i_1] = \sigma[\tau(i_1)] = \sigma(i_2).$$

□

Следствие 4. *Если*

$$\tau = (i_1 i_2 \dots i_k)(j_1 j_2 \dots j_s)\dots$$

— разложение τ в произведение независимых циклов, то

$$\sigma\tau\sigma^{-1} = \Big(\sigma(i_1)\sigma(i_2)\dots\sigma(i_k)\Big)\Big(\sigma(j_1)\sigma(j_2)\dots\sigma(j_s)\Big)\dots$$

Доказательство. Действительно,

$$\sigma\tau\sigma^{-1} = \sigma(i_1 i_2 \dots i_k)\sigma^{-1}\sigma(j_1 j_2 \dots j_s)\sigma^{-1}\sigma\dots$$

□

Из этой задачи вытекает важный теоретический факт:

Предложение 4. *Две перестановки в S_n сопряжены тогда и только тогда, когда они имеют одинаковую цикловую структуру, то есть их разложения в произведение независимых циклов для любого k содержат одинаковое число циклов длины k.*

Задача 6. Найдите все перестановки, коммутирующие с $\tau = (146)(35) \in \mathrm{S}_6$.

Решение. Нам нужно найти все σ, такие что $\sigma\tau = \tau\sigma$ или, что эквивалентно, $\tau = \sigma\tau\sigma^{-1}$. Согласно предыдущей задаче,

$$\sigma\tau\sigma^{-1} = \big(\sigma(1)\sigma(4)\sigma(6)\big)\big(\sigma(3)\sigma(5)\big) = (146)(35)$$

(заметим, что автоматически $\sigma(2) = 2$). Следовательно, имеются следующие возможности:

- $\sigma(1) = 1,\ \sigma(4) = 4, \sigma(6) = 6$;
- $\sigma(1) = 4,\ \sigma(4) = 6, \sigma(6) = 1$;
- $\sigma(1) = 6,\ \sigma(4) = 1, \sigma(6) = 4$.

Получаем ответ: $\sigma \in \{e, (146), (164), (35), (146)(35), (164)(35)\}$ ϟ. □