Лекция 1. Перестановки

1.1 Понятие перестановки

Пусть n — произвольное натуральное число. Рассмотрим множество $M = \{1, 2, \ldots, n\}$, состоящее из первых n натуральных чисел.

Определение 1.1. *Перестановкой* называется любой упорядоченный набор, составленный из (всех) элементов множества M.

Вообще говоря, с точки зрения определения 1.1 нам не важна природа элементов множества M. Это могут быть любые объекты: карандаши из коробки, ученики из класса, звёзды на небе и т.д. Перестановка — это некоторый способ их все упорядочить, выстроить один за другим от первого до последнего.

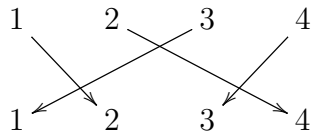
Другой подход к перестановкам предлагает смотреть на них, как на отображения.

Определение 1.2. *Перестановкой* называется взаимно однозначное отображение $\sigma\colon M \to M$.

Перестановки удобно записывать в виде таблиц из двух строк и n столбцов, называемых *подстановками*. В первой строке подстановки перечисляются элементы множества M, а во второй — их образы при отображении σ. При этом порядок столбцов в такой записи роли не играет, поэтому одну и ту же перестановку можно записать в виде подстановки различными способами. Например, так:

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

Пример 1.3. Пусть $n = 4$. Рассмотрим следующий упорядоченный набор первых четырёх натуральных чисел: $2, 4, 1, 3$. Он является перестановкой, которая в виде отображения представляется так:



Она же, записанная разными подстановками:

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

Определение 1.4. Множество всех перестановок из n элементов обозначается S_n.

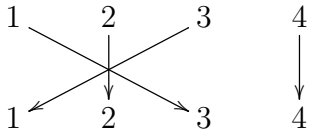
Ясно, что количество элементов в S_n (то есть количество всех перестановок из n элементов) равно $n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$. Действительно, образ числа 1 (то есть число, в которое переходит 1) можно выбрать n способами, образ числа 2 можно выбрать уже из оставшихся $n-1$ чисел и т. д.

1.2 Перемножение перестановок

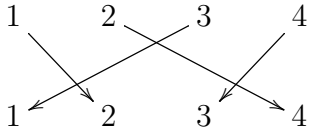
Определение 1.5. *Произведением* перестановок $\sigma, \tau \in S_n$ называется композиция отображений $\sigma\tau(i) = \sigma(\tau(i))$. Отметим, что сначала применяется второй сомножитель, а потом первый.

Пример 1.6. Пусть перестановки τ и σ такие, как показано ниже:

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

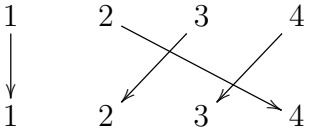


$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$



Тогда их произведение имеет следующий вид:

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



По сути, чтобы получить произведение перестановок $\sigma\tau$, мы проходим сначала по стрелочкам внутри перестановки σ, а затем — внутри перестановки τ. Например, 3 переходит в 1 при действии σ, а 1 переходит в 2 при действии τ. Значит, $\sigma\tau$ переведёт 3 в 2. То же самое с точки зрения формального определения звучит так: $\sigma\tau(3) = \sigma(\tau(3)) = \sigma(1) = 2$.

Записывая перестановки в виде подстановки, удобно вычислять произведение следующим образом: в перестановке σ переставляем столбцы так, что первая строчка в σ совпадает с последней строчкой в τ. Тогда произведением будет перестановка, у которой первая строчка — стандартная, а вторая строчка — это вторая строчка из σ. Вот как это будет выглядеть в нашем случае: $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$.

Определение 1.7. Перестановка $e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$ называется тождественной.

Определение 1.8. Пусть $\sigma \in S_n$. Перестановка $\tau \in S_n$ называется *обратной* к перестановке σ, если $\sigma\tau = \tau\sigma = e$. Обратная перестановка обозначается σ^{-1}.

На практике для того, чтобы получить перестановку, обратную данной, нужно поменять направление стрелочек (если мы имеем дело с записью в виде отображения) или поменять местами строки (если перестановка записана в виде подстановки).

Пример 1.9. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

Замечание 1.10. Знакомый с теорией групп читатель, конечно, догадался, что множество перестановок из n элементов образует группу относительно операции умножения (композиции). Эта группа, как и всё множество перестановок, обозначается S_n и при $n > 2$ не является коммутативной.

Определение 1.11. *Циклом* $(a_1, a_2, \dots, a_k)$ называется перестановка, циклически переставляющая элементы $a_1, a_2, \dots, a_k$. То есть имеется в виду, что все элементы $a_1, a_2, \dots, a_k$ различны, $a_1 \mapsto a_2$, $a_2 \mapsto a_3$, $\dots$, $a_k \mapsto a_1$, а остальные элементы множества $\{1, \dots, n\}$ переходят в себя.

Число k называется *длиной* цикла.

Любую перестановку можно представить в виде произведения циклов, все элементы которых различны. Такие циклы называются *независимыми*. Каждый цикл в таком разложении данной

перестановки σ имеет вид $(l, \sigma(l), \sigma(\sigma(l)), \ldots)$. Это означает, что циклы образуются, когда мы последовательно «проходим» по элементам перестановки: сначала берём один элемент (это l), потом берём то, во что он переходит (то есть $\sigma(l)$), потом то, во что переходит следующий элемент (во что переходит $\sigma(l)$) и так далее. Как только мы возвращаемся к исходному элементу, этот процесс заканчивается, и цикл образован. Сформировав первый цикл, мы берём один из незадействованных в нём элементов и тем же способом образуем на его основе второй цикл. Затем аналогично создаём третий цикл и так далее.

Пример 1.12. $\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix} = (1,2,4)(3,5)$. Здесь 1 переходит в 2, 2 переходит в 4, а 4 — снова в 1. Таким образом, эти три элемента образуют цикл $(1,2,4)$. Точно так же 3 переходит в 5, а 5 — в 3, и мы обретаем ещё один цикл: $(3,5)$.

Каждый цикл сам по себе тоже можно представить в виде подстановки:

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

Произведение двух независимых циклов не зависит от того, в каком порядке мы их перемножаем. Это следует напрямую из определения умножения перестановок и определения независимых циклов. А вот если в циклах встречаются одинаковые элементы, порядок умножения может быть важен.

Пример 1.13. $(1,2,4)(3,5,6) = (3,5,6)(1,2,4) = \begin{pmatrix}1&2&3&4&5&6\\2&4&5&1&6&3\end{pmatrix}$ — это произведение независимых циклов. Пример произведения циклов, не являющихся независимыми:

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

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

Пусть $\sigma = (1,2,\ldots,k) = \begin{pmatrix}1&2&\ldots&k-1&k\\2&3&\ldots&k&1\end{pmatrix}$ — цикл длины k. Рассмотрим последовательность перестановок, получающихся умножением σ на себя несколько раз:

$$\sigma^2 = \sigma\cdot\sigma = \begin{pmatrix}1&2&\ldots&k-1&k\\3&4&\ldots&1&2\end{pmatrix},$$

$$\sigma^3 = \sigma^2\cdot\sigma = \begin{pmatrix}1&2&\ldots&k-1&k\\4&5&\ldots&2&3\end{pmatrix},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma^{k-1} = \sigma^{k-2}\cdot\sigma = \begin{pmatrix}1&2&\ldots&k-1&k\\k&1&\ldots&k-2&k-1\end{pmatrix},$$

$$\sigma^k = \sigma^{k-1}\cdot\sigma = \begin{pmatrix}1&2&\ldots&k-1&k\\1&2&\ldots&k-1&k\end{pmatrix}.$$

Мы видим, что $\sigma^k = e$, причём для всех натуральных чисел $m < k$ выполнено $\sigma^m \neq e$. Оказывается, подобный факт имеет место для любой перестановки. Он лежит в основе следующего определения.

Определение 1.14. Пусть $\sigma \in S_n$. Наименьшее натуральное число k такое, что $\sigma^k = e$, называется *порядком* перестановки σ и обозначается $\operatorname{ord}\sigma$.

Как мы видели выше, порядок цикла длины k равен k. Посмотрим теперь, как искать порядок произвольной перестановки. Для этого разложим её в произведение независимых циклов:

$$\sigma = (a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2}) \ldots (t_1, t_2, \ldots, t_{k_l}).$$

Поскольку циклы независимы, порядок их перемножения роли не играет, а значит,

$$\sigma^m = (a_1, a_2, \ldots, a_{k_1})^m (b_1, b_2, \ldots, b_{k_2})^m \ldots (t_1, t_2, \ldots, t_{k_l})^m.$$

Вся перестановка станет тождественной тогда, когда каждый её сомножитель из числа независимых циклов обратится в e. Порядки всех независимых циклов нам известны — это их длины. Значит, $\operatorname{ord}\sigma = \text{НОК}(k_1, k_2, \ldots, k_l)$.

Подытоживая, сформулируем доказанное выше в виде отдельного утверждения.

Утверждение 1.15. *Пусть* $\sigma = (a_1, a_2, \ldots, a_{k_1})(b_1, b_2, \ldots, b_{k_2}) \ldots (t_1, t_2, \ldots, t_{k_l})$ *— представление перестановки в виде произведения независимых циклов. Тогда* $\operatorname{ord}\sigma = НОК(k_1, k_2, \ldots, k_l)$.

1.3 Чётность перестановок

Определение 1.16. *Транспозицией* называется цикл длины 2.

Важность введённого понятия трудно переоценить, хотя на первый взгляд неискушённого читателя это может быть незаметно.

Утверждение 1.17. *Любая перестановка может быть представлена в виде произведения транспозиций.*

Доказательство. Рассмотрим произвольную перестановку $\sigma \in S_n$ и разложим её в произведение независимых циклов. Ясно, что если нам удастся разложить каждый из циклов в произведение транспозиций, то и вся перестановка окажется представлена в виде произведения транспозиций. Таким образом, достаточно доказать утверждение 1.17 для циклов.

Рассмотрим произвольный цикл $(a_1, a_2, \ldots, a_k)$. Заметим, что его можно представить в виде следующего произведения: $(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_2, \ldots, a_{k-1})$. Следовательно, продолжая процесс по индукции, в итоге получим $(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_2)$. □

Определение 1.18. *Беспорядок* или *инверсия* в перестановке σ — это такая пара (i, j), что $i < j$ и $\sigma(i) > \sigma(j)$. Перестановка называется *чётной*, если число беспорядков в ней чётно, и *нечётной* в противном случае.

Замечание 1.19. Важно в каждый момент времени и в каждом конкретном место осознавать, что означает запись (i, j), потому что её можно понимать и как транспозицию, переводящую i в j, а j в i, и как пару из двух элементов — i и j.

Пример 1.20. В перестановке $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$ пара $(1, 3)$ является беспорядком, потому что $\sigma(1) = 2 > 1 = \sigma(3)$, а пара $(1, 2)$ — не является, так как $\sigma(1) = 2 < 3 = \sigma(2)$. Всего в этой перестановке два беспорядка: $(1, 3)$ и $(2, 3)$. Поэтому она — чётная.

Теорема 1.21. *При умножении на транспозицию чётность перестановки меняется.*

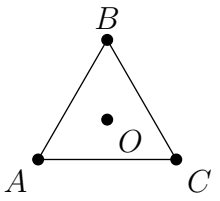
Доказательство. Рассмотрим произвольную перестановку $\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ и умножим её на транспозицию (i, j). Вот что получится:

$$\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & \dots & a_i & \dots & a_j & \dots & a_n \end{pmatrix} (i, j) = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & \dots & a_j & \dots & a_i & \dots & a_n \end{pmatrix}.$$

Заметим, что при таком умножении образы элементов i и j поменялись местами. Поэтому если в исходной перестановке пара (i, j) была беспорядком, то в полученной она беспорядком не будет, и наоборот. То есть общее количество беспорядков за счёт пары (i, j) меняется на 1.

Посмотрим теперь, что произойдёт с другими парами. Свойство быть или не быть беспорядком, очевидно, не меняется для пары (l, m), если не меняются образы[1] элементов l и m. Поэтому нас интересуют только те пары, один из элементов которых равен i или j. Оказывается, такие пары дополняют друг друга. В самом деле, рассмотрим, например, пары (i, m) и (m, j) (здесь $i < m < j$). Если, скажем, $a_i < a_m < a_j$, то в исходной перестановке ни одна из этих пар не является беспорядком, а в полученной беспорядками будут обе. То есть общее количество беспорядков за счёт этих пар изменится на 2. Если же, например, $a_m < a_i < a_j$, то и до умножения на транспозицию, и после него среди этих пар беспорядок ровно один. Легко убедиться, что и во всех остальных случаях картина будет такой же: во всех дополняющих друг друга парах число беспорядков либо не меняется, либо меняется на 2.

Итак, при умножении на транспозицию количество беспорядков в перестановке изменяется на нечётное число. Значит, меняется и чётность перестановки. Теорема доказана. □



Перестановки удобно использовать для описания преобразований различных множеств, обладающих заданными свойствами. Рассмотрим, например, группу движений плоскости, переводящих правильный треугольник ABC в себя. При каждом таком движении вершина треугольника переходит в другую вершину, а потому если мы отождествим точки A, B и C с числами 1, 2 и 3, любое движение будет соответствовать перестановке из трёх элементов. Например, повороту треугольника на 120° по часовой стрелке относительно его центра O сопоставляется перестановка $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, а симметрии относительно прямой BO — $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Важно отметить, что при таком сопоставлении чётные перестановки соответствуют движениям, сохраняющим ориентацию плоскости (то есть поворотам), а нечётные — движениям, которые ориентацию меняют (осевым симметриям).

Похожим образом множество перестановок S_4 отождествляется с группой преобразований правильного тетраэдра, причём чётные перестановки соответствуют его вращениям, а нечётные — зеркальным симметриям. Другими словами, тетраэдр, сложенный из бумаги, можно повернуть так, чтобы получился его образ при применении чётной перестановки. А вот нечётная перестановка переведёт такую бумажную модель в объект, увидеть который можно будет только в зеркале.

[1] То есть то, во что они переходят.