УДК 519.17

Шевцова Мария Витальевна

к.ф.-м.н., доцент кафедры математики

Белгородский государственный университет

Белгород

Shevtsova Maria Vitalievna

Belgorod University

shevtsova\_m@bsu.edu.ru

Демченко Алексей Алексеевич

студент

Белгородский государственный университет

Белгород

Demchenko Alexey Alekseevich

Belgorod University

alex2311200@yandex.ru

**ГРУППЫ ПЕРЕСТАНОВОК**

**PERMUTATION GROUPS**

**Аннотация.** В статье рассматриваются теоретические подходы, которые используются для изучения групп перестановок. Перестановки являются важным понятием в математике, теории кодирования и других областях, где важно изучать различные варианты элементов с перемещением данных между собой. Группы перестановок - это коллекции перестановок, которые обладают определенными свойствами и структурой.

**Abstract:** The article discusses the theoretical approaches that are used to study permutation groups. Permutations are an important concept in mathematics, coding theory, and other fields where it is important to study various permutations of elements. Permutation groups are collections of permutations that have certain properties and structure.

**Ключевые слова:** группы, перестановки, свойства групп перестановок, обозначения групп, перестановки-произведение групп, нейтральный элемент, инверсии групп.

**Keywords:** groups, permutations, properties of permutation groups, notation of groups, permutations-product of groups, neutral element, inversions of groups.

**Основные свойства, обозначения и терминология групп перестановок**

Группа перестановок – это подгруппа симметричной группы; то есть ее элементы являются перестановками данного множества. Таким образом, это подмножество симметричной группы, которая является замкнутой относительно композиции перестановок, содержит единичную перестановку и содержит обратную перестановку каждого из своих элементов.[5] Общее свойство конечных групп подразумевает, что конечное непустое подмножество симметричной группы является группой перестановок тогда и только тогда, когда оно замкнуто при перестановочной композиции.[5]

Степень группы перестановок конечного множества - это количество элементов в наборе. Порядок группы (любого типа) - это количество элементов (мощность) в группе. Согласно теореме Лагранжа, порядок любой конечной группы перестановок степени n должен делиться на n! поскольку n-факториал – это порядок симметричной группы Sn.

Поскольку перестановки являются биекциями множества, они могут быть представлены двухстрочной нотацией Коши.[2, 94 с.] В этом обозначении перечислен каждый из элементов *M* в первой строке, и для каждого элемента его изображение под перестановкой под ним во второй строке. Если *σ* является перестановкой множества *M = {x1, x2, …, xn}*, то

$σ=\left(\begin{matrix}x\_{1}&x\_{2}\\σ(x\_{1})&σ(x\_{2})\end{matrix} \begin{matrix}x\_{3}&…&x\_{n}\\σ(x\_{3})&…&σ(x\_{n})\end{matrix}\right)$.

Например, конкретная перестановка множества {1, 2, 3, 4, 5} может быть записана как

$$σ= \left(\begin{matrix}1&2\\2&5\end{matrix} \begin{matrix}3&4&5\\4&3&1\end{matrix}\right)$$

это означает, что *σ* удовлетворяет *σ*(1) = 2, *σ*(2) = 5, *σ*(3) = 4, *σ*(4) = 3 и *σ*(5) = 1. Элементы *M* не обязательно должны располагаться в каком-либо особом порядке в первой строке, поэтому ту же самую перестановку также можно записать как

$σ= \left(\begin{matrix}3&2\\4&5\end{matrix} \begin{matrix}5&1&4\\1&2&3\end{matrix}\right)$.

Перестановки также часто записываются в циклической нотации (или же циклическая форма)[3], так что при заданном множестве *M = {1, 2, 3, 4}*, перестановка *g* из *M* с *g*(1) = 2, *g*(2) = 4, *g*(4) = 1 и *g*(3) = 3 будет записана как (1, 2, 4)(3), или, чаще, (1, 2, 4), поскольку значение 3 остается неизменным; если объекты обозначаются отдельными буквами или цифрами, запятые и пробелы также можно исключить, и у нас есть обозначения, такие как (124). Перестановка, написанная выше в двухстрочной нотации, будет записана в циклической нотации как

*σ* = (125)(34).

**Композиция перестановок-произведение группы**

Произведение двух перестановок определяется как их композиция в виде функций, поэтому *σ \* π* это функция, которая отображает любой элемент *x* множества в *σ*(*π*(*x*)). Обратите внимание, что крайняя правая перестановка применяется к аргументу первой из-за способа написания композиции функции.[1][5] Некоторые авторы предпочитают, чтобы крайний левый фактор действовал первым, но с этой целью перестановки должны записываться справа от их аргумента, часто в виде верхнего знака, поэтому перестановка, *σ* действующая на элемент, *x* приводит к изображению *xσ*. В соответствии с этим соглашением произведение задается через *xσ\*π* = (*xσ*)*π* .[3] [4] Однако это дает другое правило для умножения перестановок. Это соглашение обычно используется в литературе по группам перестановок, но в этой статье используется соглашение, в котором крайняя правая перестановка применяется первой.

Поскольку композиция двух биекций всегда дает другую биекцию, произведение двух перестановок снова является перестановкой. В двухстрочной системе счисления произведение двух перестановок получается путем перестановки столбцов второй (самой левой) перестановки таким образом, чтобы ее первая строка была идентична второй строке первой (самой правой) перестановки. Затем произведение может быть записано как первая строка первой перестановки поверх второй строки модифицированной второй перестановки.[5] Например, учитывая перестановки,

$P= \left(\begin{matrix}1&2\\2&4\end{matrix} \begin{matrix}3&4&5\\1&3&5\end{matrix}\right)$ и $Q= \left(\begin{matrix}1&2\\5&4\end{matrix} \begin{matrix}3&4&5\\3&2&1\end{matrix}\right)$,

произведение *QP* равно:

$QP= \left(\begin{matrix}1&2\\5&4\end{matrix} \begin{matrix}3&4&5\\3&2&1\end{matrix}\right)\left(\begin{matrix}1&2\\2&4\end{matrix} \begin{matrix}3&4&5\\1&3&5\end{matrix}\right)= \left(\begin{matrix}2&4\\4&2\end{matrix} \begin{matrix}1&3&5\\5&3&1\end{matrix}\right)\left(\begin{matrix}1&2\\2&4\end{matrix} \begin{matrix}3&4&5\\1&3&5\end{matrix}\right)= \left(\begin{matrix}1&2\\4&2\end{matrix} \begin{matrix}3&4&5\\5&3&1\end{matrix}\right)$.

Композиция перестановок, когда они записаны в циклической нотации, получается путем сопоставления двух перестановок (со второй, записанной слева), а затем упрощения до формы непересекающегося цикла, если это необходимо. Таким образом, приведенный выше продукт был бы задан:

$Q\*P=\left(15\right)\left(24\right)\*(1243)=(1435)$.

Поскольку композиция функций ассоциативна, то же самое относится и к операции произведения перестановок:

$\left(σ\*π\right)\*ρ=σ\*\left(π\*ρ\right)$.

Поэтому произведения двух или более перестановок обычно записываются без добавления круглых скобок для выражения группировки; они также обычно записываются без точки или другого знака, обозначающего умножение (точки в предыдущем примере были добавлены для подчеркивания, поэтому будут записываться просто как *σπρ*).

**Нейтральный элемент и инверсии**

Перестановка идентификаторов, которая сопоставляет каждый элемент множества самому себе, является нейтральным элементом для этого продукта. В двухстрочной записи идентификатор равен

$\left(\begin{matrix}1&2\\1&2\end{matrix} \begin{matrix}3&…&n\\3&…&n\end{matrix}\right)$.

В циклической записи, *e* = (1)(2)(3)...(*n*), которая по соглашению также обозначается просто или четно.[5]

Поскольку биекции имеют обратные значения, то же самое делают и перестановки, и обратная *σ* -1 от *σ* снова является перестановкой. Очевидно, что всякий раз, когда *σ*(*x*)=*y*, также имеется *σ* -1(*y*)=*x*. В двухстрочной записи обратное может быть получено путем перестановки двух строк (и сортировки столбцов, если требуется, чтобы первая строка располагалась в заданном порядке). Например

$\left(\begin{matrix}1&2\\2&5\end{matrix} \begin{matrix}3&4&5\\4&3&1\end{matrix}\right)^{-1}= \left(\begin{matrix}2&5\\1&2\end{matrix} \begin{matrix}4&3&1\\3&4&5\end{matrix}\right)= \left(\begin{matrix}1&2\\5&1\end{matrix} \begin{matrix}3&4&5\\4&3&2\end{matrix}\right)$.

Чтобы получить результат, обратный одному циклу, мы меняем порядок его элементов на обратный. Таким образом,

(125) -1 = (521) = (152).

Чтобы получить значение, обратное произведению циклов, мы сначала меняем порядок циклов на обратный, а затем берем значение, обратное каждому из них, как указано выше. Таким образом,

[(125)(34)] -1 = (34)-1 (125)-1 = (43)(521) = (34)(152).

Наличие ассоциативного произведения, элемента идентификации и обратных значений для всех его элементов превращает множество всех перестановок из *M* в группу Sym(*M*); группу перестановок.

**Заключение**

Группы перестановок – это подгруппы симметричных групп, состоящие из различных вариантов множества. Они обладают рядом свойств, таких как замкнутость относительно композиции перестановок, наличие единичной перестановки и обратной перестановки каждого элемента.

Композиция перестановок, или их произведение, определяется как композиция соответствующих функций. Произведение двух перестановок также является перестановкой, а запись произведения может быть представлена как перестановка столбцов и строк в двухстрочной нотации или сопоставлением двух перестановок в циклической нотации.

В целом, изучение групп перестановок является важной темой в математике, которая имеет много применений в различных областях, включая криптографию, комбинаторику и теорию алгоритмов.

**Список литературы:**

1. Биггс Н. Л.; Уайт, А. Т.; Группы перестановок и комбинаторные структуры. Издательство Кембриджского университета, 1979. – 140 с.
2. Вуссинг Х., Генезис концепции абстрактной группы: вклад в историю возникновения теории абстрактных групп, 2007. – 334 с.
3. Джеррум М., "Компактное представление групп перестановок". Журнал алгоритмов. Том 7 выпуск 1: 1986. – 157 с.
4. Кэмерон П. Дж., Группы перестановок. Издательство Кембриджского университета., 1999. – 232 с.
5. Ротман Д. Дж.; Первый курс абстрактной алгебры с приложениями, 2006. – 3-е изд. – 616 с.