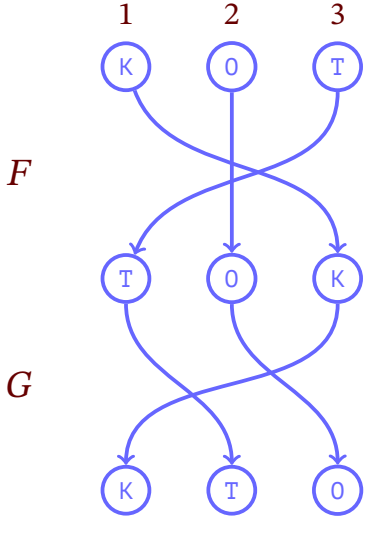
А. Шень

Перестановки



$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

Москва
Издательство МЦНМО
2020

А. Шень

Перестановки

Москва
Издательство МЦНМО
2020

УДК 519.83
ББК 22.1
Ш47

Шень А.
Ш47 Перестановки М.: МЦНМО, 2020. — 16 с.: ил.

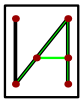
ISBN 978-5-4439-2776-3

В жизни «перестановками» называют самые разные вещи; эта книжка содержит начальные сведения о том, что математики называют «группой перестановок конечного множества». Мы покажем, как можно разделить перестановки на «чётные» и «нечётные» и как это помогает проанализировать известную головоломку «игра 15», как перестановка разлагается в циклы и почему это бывает полезно, почему повторение одного и того же действия с «кубиком Рубика» рано или поздно вернёт его в исходное положение, и разберём задачи, при решении которых перестановки оказываются полезными. Обычно эти вопросы относят к курсам «высшей алгебры» для студентов младших курсов, но они вполне элементарны, и никаких сведений, выходящих за пределы средних классов школы, мы не используем. (Хотя, конечно, привычка к несложным математическим рассуждениям пригодится.)

ББК 22.1

Оригинал-макет предоставлен автором. Электронная версия книги является свободно распространяемой и доступна по адресу `ftp://ftp.mccme.ru/users/shen/perm.zip`
В качестве иллюстраций к игре «15» использованы свободно распространяемые материалы проекта `Wikimedia`.

12+

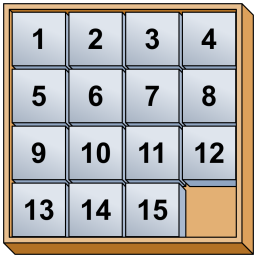


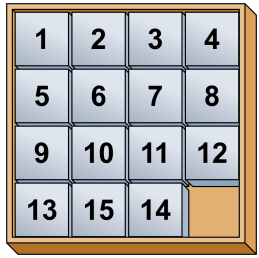
Предупреждение. Автор является научным сотрудником лаборатории LIRMM в г. Монпелье (Франция) и может рассматриваться de facto правительством России как «иностранный агент» в смысле поправок к закону об «иностранных агентах», принятых 21.11.2019.

ISBN 978-5-4439-2776-3

1. Игра «15»

Поместим в квадратную коробочку фишки с номерами $1, 2, \ldots, 15$, оставив одно место пустым. Фишки можно двигать, не вынимая из коробочки: на пустое место можно переместить любую из соседних фишки, и так несколько раз. Можно ли таким образом переставить две фишки, скажем, 14 и 15, оставив остальные на месте?





На практике удобнее решать эту задачу «с конца»: начать с конфигурации, где 14 и 15 переставлены, и пытаться вернуться к исходному порядку. (В любом случае нам надо переставить две последние фишки; какие цифры на них написаны, значения не имеет). Попробуйте это сделать — сейчас есть довольно много сайтов, где можно играть (поищите слова “15 puzzle online”), но и настоящие головоломки тоже продаются.

Говорят, что в своё время (в XIX веке) был объявлен приз за решение этой задачи — безо всякого риска, так как это невозможно. Но люди про это не знали (или не верили) и пытались решить.[1]

2. Упрощённый вариант

Для начала мы разберёмся с упрощённым вариантом головоломки. Напишем какое-нибудь слово, скажем,

КОНУС

(это слово осмысленное, но в дальнейшем мы будем называть «словами» любые цепочки букв, не заботясь о том, являются ли они словами русского языка). За один шаг разрешается переставить в нём любые две буквы

[1] Часто изобретение этой головоломки приписывают Сэму Ллойду, но, видимо, зря, см. `https://en.wikipedia.org/wiki/15_puzzle#History`.

местами. Например, можно переставить О и У, получив слово КУНОС, на следующем шаге переставить ещё какие-то две буквы и так далее.

1 Можно ли получить из слова КОНУС слово СУКНО за четыре шага?

2 Можно ли, начав со слова КОНУС, вернуться в исходное положение после 10 шагов? после 11 шагов?

Первое сделать легко: переставив одну и ту же пару букв два раза подряд, мы ничего не изменим, и так пять раз. А вот второе, сколько бы вы ни пробовали, сделать не удастся (так что автор мог бы смело пообещать приз, ничем не рискуя). Но как в этом убедиться?

На самом деле верен более общий факт: *если на каждом шаге разрешается поменять два объекта местами, мы не можем вернуться в исходное положение, сделав нечётное число шагов*. Это верно для любого количества объектов. Для двух это совсем очевидно:

$$АР \to РА \to АР \to РА \to АР \to \ldots$$

на каждом шаге порядок меняется, и после чётного числа шагов буквы идут в исходном порядке, а после нечётного — в обратном.

Теперь возьмём трёхбуквенное слово, скажем, КОТ. Есть три пары букв для обмена, так что за один шаг мы можем получить слова

КТО ТОК ОКТ

(включая и бессмысленные). На втором шаге мы должны взять одно из этих слов и поменять местами какие-то буквы. Пару для обмена можно выбрать тремя способами. Один из этих способов вернёт слово в исходное положение, а два других дадут новые слова:

$$КТО \to КОТ\ ТКО\ ОТК$$
$$ТОК \to КОТ\ ТКО\ ОТК$$
$$КТО \to КОТ\ ТКО\ ОТК$$

(проверьте). Видно, что во всех случаях получаются одни и те же три слова

КОТ ТКО ОТК

(после двух шагов). А что можно получить за три? для этого надо к этим трём словам применить все возможные перестановки, получатся уже знакомые три слова

КТО ТОК ОКТ

(три шага дают то же самое, что один шаг). Поэтому за четыре шага можно получить то же самое, что за два, и так далее.

Видно, что мы разбили все варианты на две группы по три слова, и на каждом шаге переходим из одной группы в другую:

КОТ ТКО ОТК ↔ КТО ТОК ОКТ

Значит, вернуться в исходную группу (в частности, получить слово КОТ) можно только за чётное число шагов.

3 Что будет для слова из чётырех букв, скажем, КРОТ? Покажите, что все варианты (сколько их?) тоже разбиваются на две группы, и обмен двух букв местами переводит нас из одной группы в другую.

С ростом количества букв перебрать все варианты становится труднее, так что нужно какое-то общее рассуждение. Мы изложим его, предварительно объяснив терминологию.

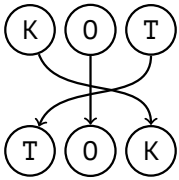
4 Петя сказал младшей сестре, что подарит ей шоколадку, если она сделает в слове СИНУС одиннадцать попарных обменов и получит исходное слово. В чём был его просчёт?

3. Перестановки

Пусть есть n предметов, которые можно переставлять местами. Скажем, n человек сидят на n стульях, и могут пересаживаться (но на каждом стуле остаётся по одному человеку). Или n шаров лежат в n ящиках, и мы можем их перекладывать произвольным образом (но тоже оставляя в каждом ящике по шару). Или на доске написано n букв, которые можно менять местами, и так далее. Схема перекладывания (пересадки и т.п.) называется «перестановкой».[2]

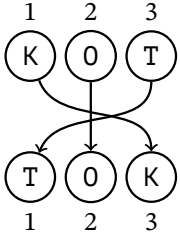
Как можно задать (записать, изобразить) перестановку? Можно нарисовать «посадочные места» и показать, откуда куда надо пересаживаться. Например, на этом рисунке

[2]Когда-то (см., например, учебник А. Г. Куроша *Курс высшей алгебры*, М.: ОГИЗ Гостехиздат, 1948, § 7) такие схемы, то есть взаимно однозначные отображения конечного множества на себя, называли «подстановками», а слово «перестановка» сохраняли для записанных в каком-то порядке чисел $1, 2, \ldots, n$, но мы не будем так педантичны.



мы меняем местами первую и последнюю букву в слове КОТ и получаем слово ТОК.

Конечно, рисовать каждый раз картинку неудобно. Можно пронумеровать места для букв, скажем, слева направо, и составить таблицу, указывающую, в какую позицию перемещается каждая буква.



$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

На рисунке столбец $\begin{pmatrix} 1 \\ 3 \end{pmatrix}$ означает, что буква с первого места (то есть К) переходит на третье, и так далее. В общем случае можно сказать так: таблица

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

задаёт перестановку с n позициями, пронумерованными от 1 до n. В ней элемент с позиции 1 перемещается на позицию k_1, с позиции 2 на позицию k_2 и так далее.

5 Буквы слова САТИР занимают пять позиций, пронумерованных слева направо числами $1, 2, \ldots, 5$. Напишите, какое слово получится после перестановки

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

6 Запишите перестановку, переводящую слово КОНУС в слово СУКНО. (Позиции букв в слове КОНУС нумеруются слева направо числами от 1 до 5.)

Математики сказали бы, что перестановка представляет собой взаимно однозначное отображение множества позиций (то есть $\{1, 2, \ldots, n\}$ при нашей нумерации) на себя. Перестановка

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

переводит (*отображает*) *число i в число k_i*. Отображения они называют ещё функциями и говорят, что наша перестановка является функцией, *значение которой на числе i равно k_i*.

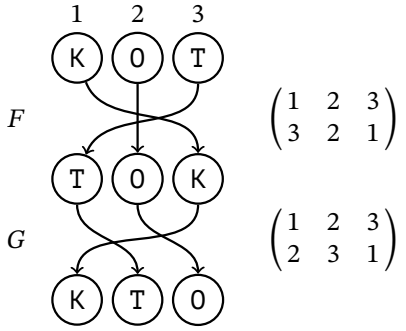
Если договориться, что мы всегда нумеруем позиции числами $1, \ldots, n$ и пишем их в верхней строке по порядку, то первую строку можно не писать для экономии места. Достаточно написать вторую. Программисты сказали бы, что перестановка представляет собой массив элементов `perm[1]..perm[n]`, в котором каждое число от 1 до n встречается по одному разу (так как мы не можем записать в одну позицию две буквы и ни одна позиция не остаётся пустой). Впрочем, другие программисты с ними бы не согласились и сказали, что удобнее нумеровать позиции от 0 до $n-1$, как принято во многих популярных языках программирования.

Среди всех перестановок n элементов есть *тождественная*, в которой ничего не переставляется (каждый элемент остаётся где был). В нашей записи она будет выглядеть как

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

4. Произведение перестановок

В нашей задаче шла речь о последовательном выполнении нескольких перестановок друг за другом. Математики это называют *произведением* перестановок. Например, можно сначала переставить буквы в слове КОТ, получив слово ТОК (поменять первую букву с третьей), а затем переставить буквы в слове ТОК, получив слово КТО.



$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \qquad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

Такое последовательное выполнение называют *произведением*, или *композицией* перестановок, и говорят, что произведение перестановок

$$F = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} \quad \text{и} \quad G = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

равно перестановке

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

Правда, среди математиков нет согласия, в каком порядке записывать F и G в произведении: слева F, справа G или наоборот. С одной стороны, мы обычно читаем и выполняем операции слева направо (в большинстве языков), так что логично в нашем примере писать $F \cdot G = H$. С другой стороны, если использовать обозначения для функций, то $H(i) = G(F(i))$: чтобы найти, куда перестановка H отображает позицию i (куда переходит элемент с позиции i), надо сначала найти позицию $j = F(i)$, а потом посмотреть, куда переходит элемент с позиции j при перестановке G. Так что иногда пишут $H = G \circ F$, обозначая произведение (композицию) кружочком. Мы будем придерживаться второго порядка.

7 Найдите $F \circ F$, если $F = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$.

Для каждой перестановки можно найти *обратную* — то, что надо сделать, чтобы вернуть элементы на прежние места. Если в перестановке элемент с позиции i переставляется в позицию j, то в обратной перестановке элемент с позиции j переставляется в позицию i. Говоря научно, *произведение перестановки и обратной к ней равно тождественной перестановке.* Если мы договорились называть последовательное выполнение перестановок произведением, то обратную к перестановке F логично

обозначать F^{-1}. Тогда можно записать

$$F^{-1} \circ F = I,$$

где I — тождественная перестановка. Заметим, что и в другом порядке получится тоже тождественная перестановка:

$$F \circ F^{-1} = I \ :$$

если $F(i) = j$, то при перестановке F^{-1} позиция j переходит в i, а затем при перестановке F обратно в j. Как сказали бы математики, *левая и правая обратные перестановки совпадают*.

8 Найдите обратную к перестановке

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

Мы называем композицию перестановок «произведением», но тут надо иметь в виду, что это «произведение» не обладает свойством коммутативности: при перестановке сомножителей произведение может меняться.

9 Приведите пример двух перестановок F и G, для которых $F \circ G \neq G \circ F$. (Такой пример есть уже для трёхэлементного множества.)

10 (для знакомых с программированием) Представляя перестановки как массивы из n элементов, напишите программу для вычисления произведения перестановок и обратной перестановки. (И то, и другое можно сделать за $O(n)$ действий.)

5. Транспозиции (обмены)

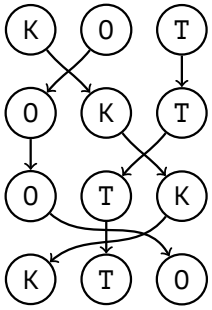
Нас интересуют перестановки, в которых два элемента меняются местами, а остальные остаются где были. Если мы меняем местами позиции i и j, и $i < j$, то перестановка записывается так:

$$\begin{pmatrix} 1 & \ldots & i-1 & i & i+1 & \ldots & j-1 & j & j+1 & \ldots & n \\ 1 & \ldots & i-1 & j & i+1 & \ldots & j-1 & i & j+1 & \ldots & n \end{pmatrix}.$$

Это длинно, и поэтому мы будем сокращённо записывать эту перестановку как (ij). При этом мы требуем $i \neq j$, но разрешаем j быть и больше i, и меньше i. Скажем, (25) и (52) — законные обозначения одной и той

же перестановки, в которой позиции 2 и 5 меняются местами. Конечно, при этом надо отдельно указать, чему равно n, то есть сколько всего у нас позиций.

Такие перестановки называют *транспозициями*.[3]



11 Для перестановок трёх элементов найдите композицию (13) ∘ (23) ∘ (12). (Это тоже будет транспозиция — каких элементов?)

Напомним, что мы договорились сначала выполнять перестановку справа, так что мы сначала переставляем первый и второй элементы, потом второй и третий, потом первый и третий.

12 Какая перестановка будет обратной к транспозиции (ij)?

Чтобы привыкнуть к введённой терминологии, давайте докажем, что *всякая перестановка может быть представлена как произведение транспозиций*. Говоря по-простому, если нам разрешено пересаживать сидящих на стульях по двое (на каждом шаге двое меняются местами, а остальные не двигаются), то можно в итоге пересадить их в любом порядке. Почему? Понятное дело: сначала поместим на первый стул того, кто там должен сидеть (обменяв его с другим, если он ещё не там), и больше уже его никогда не будем трогать. Затем посадим на второй стул того, кто должен там сидеть, и так далее, пока все не будут сидеть на своих местах.

Для программистов представление (любой) перестановки в виде произведения транспозиций означает, что любой массив можно отсортировать обменами (на каждом шаге мы меняем местами два элемента).

13 Это рассуждение показывает, что *всякая перестановка n элементов представляется как произведение не более чем ... транспозиций* — что нужно вставить на место многоточия?

(На первый взгляд кажется, что n — потому что мы по очереди сажаем всех на свои места. Но на самом деле достаточно $n - 1$, потому что на последнем шаге остальные места заняты, и последний и так сидит где надо.)

[3]Наверно, лучше было бы называть их *обменами* — в конце концов, не называем же мы перестановки «пермутациями». Тем не менее терминология уже стала традиционной, так что и мы будем говорить «транспозиции».

14 Приведите пример перестановки 4 элементов, которая не представляется в виде произведения двух или менее транспозиций.

15 Приведите пример перестановки 10 элементов, которая не представляется в виде произведения 8 или менее транспозиций.[4]

Пронумеровав позиции от 1 до n, мы можем говорить о транспозициях соседних элементов, то есть (12), (23),..., $(n{-}1\ n)$. Легко понять, что любую перестановку можно разложить в произведение транспозиций *соседних* элементов. Если в очереди за один шаг человек может обменяться местами с предыдущим (или следующим, если смотреть с точки зрения предыдущего), то за несколько шагов они могут встать в любом порядке.

16 В очереди Аня стоит раньше Бени, и между ними стоят k человек. Сколько шагов нужно, чтобы Аня встала на место Бени и наоборот, а остальные остались где были? На каждом шаге стоящий в очереди может поменяться местами с соседом.

Подсчёт тут несложный: сначала Беня должен встать сразу за Аней, для чего поменяться с каждым из k стоявших между ними. Потом Беня меняется с Аней, после чего Аня должна встать на то место, где стоял Беня, для этого поменявшись (к своей невыгоде) с теми же k людьми. Всего получается $2k + 1$ шагов. Другими словами, *транспозиция двух элементов, между которыми есть k промежуточных, разлагается в произведение $2k + 1$ транспозиций соседних элементов*. (Бывают и другие разложения, но нам важно, что есть разложение с $2k + 1$ элементами.)

Число $2k + 1$ нечётно, и это для нас будет ключевым наблюдением в доказательстве обещанного утверждения, которое приводится в следующем разделе.

Для программистов транспозиции соседних элементов соответствуют тому, что называют «пузырьковой сортировкой» — элементы всплывают как пузырьки, меняясь местами с соседними.

17 Сколько транспозиций соседних элементов нужно, чтобы получить перестановку

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ n & n-1 & \ldots & 1 \end{pmatrix},$$

обращающую порядок элементов, и почему нельзя обойтись меньшим числом транспозиций соседних элементов?

[4] Основная сложность в этой задаче не в том, чтобы придумать пример такой перестановки, а в том, чтобы доказать, что эта перестановка действительно не представляется в виде произведения меньшего числа транспозиций. Одно из возможных рассуждений тут использует разложение перестановки в произведение циклов, о котором мы будем говорить дальше.

(Указание. Полезно считать общее число «беспорядков», то есть количество пар элементов, которые стоят не в том порядке, в котором надо.)

6. Доказательство

Мы обещали доказать, что после нечётного числа обменов предметы не могут занять первоначальные места. Теперь это можно сформулировать научно:

Теорема. *Произведение нечётного числа транспозиций не может быть тождественной перестановкой.*

Доказательство. Ключевой момент тут такой: достаточно доказывать теорему для транспозиций *соседних* элементов. Почему?

Мы видели, что если элементы не соседние и между ними стоит k промежуточных, то их транспозицию (обмен) можно заменить на произведение $2k+1$ транспозиций соседних элементов. При этом общее число транспозиций увеличивается на $2k$ (вместо одной становится $2k+1$). Но чётность при этом не меняется: если в произведении было нечётное число транспозиций, то и теперь будет большее, но тоже нечётное число. Значит, если произведение нечётного числа транспозиций было тождественным, то после таких замен будет другое, но тоже нечётное число транспозиций соседних элементов, так что достаточно доказать невозможность для соседних.

Для случая транспозиций соседних элементов это легко объяснить на языке очередей. Представим себе, что люди стояли в очереди, произошло несколько обменов, когда человек в очереди менялся местами с соседом, но в итоге все вернулись на исходные места. Почему число обменов было обязательно чётным?

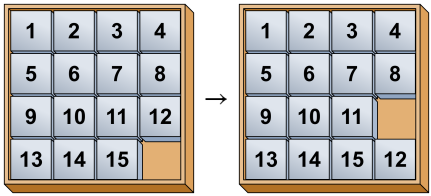
Выберем двух людей в очереди и посмотрим, когда они менялись друг с другом (не обращая внимания пока на моменты, когда они менялись с кем-то ещё или когда менялись другие люди). Каждый такой обмен меняет взаимный порядок этих двоих. Поэтому, если они в итоге остались в прежнем порядке, то их обменов было чётное число.

Остаётся заметить, что каждый обмен — это обмен какой-то пары. Если разбить все обмены на группы по этому признаку (какая пара людей менялась), то в каждой группе будет чётное число обменов, как мы выяснили. А сумма чётных чисел (по группам) всегда чётна.

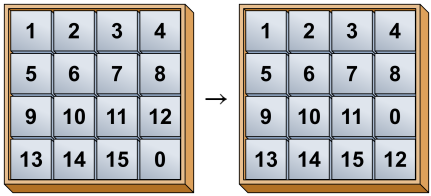
Теорема доказана. □

7. Игра «15»: невозможность

Разобравшись с нашей более простой игрой (перестановка букв), мы можем применить аналогичные рассуждения и к игре «15». Ситуация здесь сложнее, так как мы не переставляем фишки друг с другом, а сдвигаем фишку на пустое место. Но и это можно рассматривать как транспозицию, если представить себе, что на пустом месте стоит невидимая фишка (можно написать на ней, скажем, нуль). Например, ход



сдвигает фишку «12» вниз на пустое место и теперь может рассматриваться как обмен фишки «12» с виртуальной фишкой «0»:



Чем это помогает? Представим себе, что можно вернуть игру «15» с переставленными фишками «14» и «15» в исходное положение за N ходов. Это означает, что в нашей новой игре с 16 фишками (включая нулевую) можно вернуться в исходное положение после $1 + N$ транспозиций: сначала мы меняем местами «14» и «15», а потом делаем ещё N транспозиций с участием виртуальной фишки. Отсюда по доказанной нами теореме мы заключаем, что это возможно, лишь если $1 + N$ чётно, то есть если N нечётно.

Ну и что? Мы доказали, что нельзя вернуться в игре «15» в исходное положение при чётном N (сделав чётное число ходов). Но, может быть, можно вернуться, сделав нечётное число ходов? В игре число ходов может быть любым. Оказывается, что есть другое препятствие, не позволяющее сделать это за нечётное число ходов. Оно тоже связано с пустым местом, и проще — учение о перестановках тут не нужно.

18 Попробуйте догадаться, в чём состоит это препятствие (почему в игре «15» нельзя вернуться в исходное положение за нечётное число ходов), не читая дальше.

Вот в чём тут дело. Когда мы делаем ход игры, пустое место перемещается в соседнюю клетку (вверх, вниз, вправо или влево). Если после N ходов пустая клетка оказалась где была, то это значит, что она сделала поровну ходов влево и вправо, а также поровну ходов вверх и вниз. Значит, общее число ходов по горизонтали (влево + вправо) чётно, и общее число ходов по вертикали (вверх + вниз) чётно. Следовательно, и N тоже чётно как сумма двух чётных чисел (вертикаль + горизонталь).

19 Как изложить это рассуждение немного иначе, раскрасив поле игры в шахматном порядке?

Теперь мы видим, что нельзя решить поставленную в игре «15» задачу ни за чётное, ни за нечётное число ходов — следовательно, она неразрешима. Что и требовалось доказать.[5]

8. Чётные и нечётные перестановки

Решая задачу о транспозициях в слове КОТ (раздел 2), мы разделили шесть слов, получающихся перестановками, на две группы про три слова: одни получались после чётного числа обменов, другие — после нечётного. Аналогичная классификация возможна для перестановок произвольного конечного множества.

Будем называть перестановку *чётной*, если она представляется как произведение чётного числа транспозиций, и *нечётной*, если она представляется как произведение нечётного числа транспозиций.

Чтобы эта терминология была корректной, нужно, чтобы нечётными были в точности те перестановки, которые не являются чётными.[6] Таким

[5] Примерно это же доказательство невозможности было опубликовано вскоре после того, как игра стала популярной, см. Wm. Woolsey Johnson (Annapolis, Md.), Notes on the "15" puzzle, *American Journal of Mathematics*, vol. 2, no. 4 (December 1879), 397–404, https://www.jstor.org/stable/2369492. Там же опубликована заметка William E. Story, в которой даётся описание позиций игры, из которых можно вернуться в начальную (мы разбираем этот вопрос в разделе 11). После этих двух заметок идёт примечание редакции, в котором они оправдываются и говорят, что поместили эти заметки не потому, что игра «15» стала популярна в народе и девять из десяти американцев любого пола из возраста о ней слышали, а потому только, что она иллюстрирует важнейшие понятия математики.

[6] К сожалению, не всегда употребляемая в этом смысле терминология корректна: часто говорят о неубывающих функциях, для которых $f(x) \geqslant f(y)$ при $x > y$, и убывающих функциях, для которых $f(x) < f(y)$ при $x > y$. При этом, скажем, функция $y = x^2$ не

образом, мы должны доказать две вещи:

- перестановка не может быть одновременно чётной и нечётной;
- любая перестановка попадает хотя бы в один из классов (чётные и нечётные)

Второе очевидно: мы знаем, что всякая перестановка разлагается в произведение транспозиций, и в этом произведении либо нечётное, либо чётное число сомножителей. А вот первое немного сложнее. Не может ли быть так, что перестановка двумя способами разлагается в произведение транспозиций, и в одном случае сомножителей чётное число, а в другом нечётное? Что мешает этому случиться?

Представим себе, что какая-то последовательность из n транспозиций даёт тот же результат, что другая последовательность из k транспозиций. Тогда выполним сначала n транспозиций из первой последовательности, а потом k транспозиций второй последовательности, но в обратном порядке. (Так сказать, проиграем второе видео задом наперёд). Получим последовательность из $n+k$ транспозицией, которая вернёт всё в исходное положение. По доказанной нами теореме из этого следует, что $n+k$ чётно. Значит, n и k одной чётности — что и требовалось доказать.

В учебнике высшей алгебры то же рассуждение было бы написано более формально. Примерно так: пусть

$$F = T_n \circ \ldots \circ T_2 \circ T_1 = T'_k \circ \ldots \circ T'_2 \circ T'_1,$$

где F — произвольная перестановка, а T_i и T'_i — транспозиции. Умножим это равенство справа на $T_1 \circ \ldots \circ T_n$:

$$T_n \circ \ldots \circ T_2 \circ T_1 \circ T_1 \circ T_2 \circ \ldots \circ T_n = T'_k \circ \ldots \circ T'_2 \circ T'_1 \circ T_1 \circ T_2 \circ \ldots \circ T_n.$$

Поскольку $T_i \circ T_i$ — тождественная[7] перестановка при любом i, в левой части все члены сокращаются по очереди и остаётся тождественная перестановка. Получаем представление тождественной перестановки в виде произведения $k+n$ транспозиций в правой части. Значит, по доказанной теореме $k+n$ чётно, поэтому k и n имеют одинаковую чётность. Утверждение доказано.[8]

попадает ни в те, ни в другие. Примерно такая же ерунда происходит с «чётными» и «нечётными» функциями, но, к счастью, эти названия редко применяются за пределами школы.

[7]Как могли убедиться жители России в 2008–2012 годах.

[8]Критики-педанты заметили бы, что мы неявно используем ассоциативность умножения $F \circ (G \circ H) = (F \circ G) \circ H$, позволяя себе опускать скобки в произведении нескольких перестановок.

20 Покажите, что для умножения чётных и нечётных перестановок действуют те же правила, что с числами: произведение двух перестановок одинаковой чётности будет чётным, а двух перестановок разной чётности — нечётным.

21 Покажите, что обратная перестановка имеет ту же самую чётность, что и исходная.

22 Определите, чётна или нечётна перестановка

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

Чтобы найти чётность перестановки, можно действовать согласно определению, постепенно помещая элементы на нужные места с помощью транспозиций. В нашем примере это будет так:

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \\ 3 & 2 & 4 & 5 & 1 \end{array}$$

(если писать только нижнюю строку для краткости). Видно, что понадобилось три транспозиции, так что перестановка нечётна. Можно действовать и наоборот, начав с исходной перестановки и постепенно помещая элементы на свои места (это соответствует тому, что мы представляем обратную перестановку в виде произведения транспозиций).

Есть другой способ узнать, чётна или нечётна перестановка

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ k_1 & k_2 & \ldots & k_n \end{pmatrix}$$

Посмотрим, сколько пар элементов изменили свой порядок при переходе от верхней строки к нижней. Точнее, пусть есть два номера i, j от 1 до n, причём разные. Будем считать, что $i < j$. Пару (i, j) назовём *беспорядком*, если $k_i > k_j$ (стоящие под i и j элементы идут в обратном порядке).

23 В каких перестановках будет меньше всего и больше всего беспорядков? Сколько?

Следующая теорема показывает, что можно узнать чётность перестановки, подсчитав в ней беспорядки.

Теорема. *В чётной перестановке число беспорядков чётное, а в нечётной — нечётное.*

Эта теорема легко следует из такого утверждения:

Лемма. *При умножении перестановки на транспозицию число беспорядков меняется на нечётное число.*

В самом деле, лемма показывает, что для произведения n транспозиций каждый раз (при увеличении n на единицу) чётность меняется, то есть соответствует чётности n. Осталось доказать лемму.

Доказательство леммы. Утверждение леммы можно наглядно сформулировать так: в строку записаны n чисел $1, \dots, n$ в каком-то порядке (каждое по одному разу), и мы считаем число беспорядков — случаев, когда большее число стоит слева от меньшего. Надо доказать, что при обмене двух чисел в этой строке количество беспорядков изменяется на нечётное число.

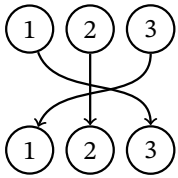
Как и раньше, полезно сначала посмотреть, что будет, когда мы меняем местами два числа i, j, стоящие в строке рядом. Тогда число беспорядков меняется ровно на единицу (уменьшается или увеличивается). В самом деле, положение чисел i и j по отношению к остальным числам строки не меняется, так что единственный беспорядок, который появляется или пропадает — это сама пара i, j. (Если $i < j$, то при замене ij на ji беспорядок появляется, а если $i > j$, то пропадает.)

Почему количество беспорядков изменится на нечётное число, если обменять местами несоседние числа? Пусть мы меняем местами числа, между которыми стоит k других чисел. Тогда эту операцию можно разложить в $2k+1$ обменов соседних чисел (см. раздел 5). Каждый обмен соседних меняет чётность числа беспорядков (число беспорядков меняется на 1), значит, после $2k+1$ обменов чётность изменится. Лемма доказана. □

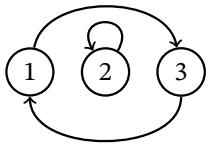
24 (для знакомых с программированием) Напишите программу, определяющую чётность перестановки. (Можно подсчитать число беспорядков, это требует $O(n^2)$ шагов для перестановки n элементов. Можно сортировать массив обменами, считая число обменов — если это делать по-простому, то будет тоже $O(n^2)$, но эффективные алгоритмы сортировки дадут $O(n \log n)$. На самом деле несложно вычислить чётность за $O(n)$ шагов, исходя из определения и постепенно возвращая элементы на свои места — надо только хранить прямую и обратную перестановки.)

9. Циклы

Мы изображали перестановку с помощью стрелок (показывающих, откуда и куда пересаживаются):



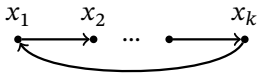
$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$



Спрашивается, зачем мы рисовали каждую позицию дважды (в верхней и нижней строке)? Почему бы не нарисовать это на одной схеме? Так получится даже нагляднее: хорошо видно, что будет, если применять одну и ту же перестановку много раз (чему равно произведение $F \circ F \circ F$ .... Видно, что буквы позиции 1 и 3 на каждом шаге меняются местами, а позиция 2 остаётся на месте.

25 Чему равно F^{1001} (композиция 1001 перестановок, равных F)?

Что можно увидеть на таких картинках, которые называют *графами перестановок*? Возьмём какую-то вершину (кружочек, позицию) x_1 и будем из неё идти по стрелкам. Что при этом может получиться? Из x_1 может вести стрелка в себя (позиция остаётся на месте), а может вести в другую вершину x_2. Куда может вести стрелка из x_2? Может вести в какую-то новую вершину x_3, может вести в x_1 (тогда получится цикл длины 2). А может ли она вести в x_2? Нет, потому что туда уже есть стрелка из x_1 (а два человека не могут сесть на одно место, это не будет перестановкой). И так далее.



Формально говоря, *циклом длины k* называют последовательность из k различных вершин $x_1, \ldots, x_k$, для которой стрелки ведут из каждой в следующую, а из конца в начало (конечно, тот же самый цикл можно начать с любой другой вершины, так что для симметрии можно рисовать вершины по кругу). При $k = 1$ цикл состоит из единственной вершины, которая остаётся на месте.

После сказанного несложно заметить, что *всякая вершина в графе перестановки входит в некоторый цикл*. В самом деле, пойдём по стрелкам $x_1 \to x_2 \to \ldots$; рано или поздно появится вершина, которая уже была (потому что вершин конечное число). При этом никакая вершина, кроме x_1, появиться не может, потому что в неё уже есть стрелки, а две стрелки в одну вершину вести не может. Мы доказали такое утверждение:

Теорема. *Граф любой перестановки состоит из одного или нескольких непересекающихся циклов.*

(Почему циклы не могут пересекаться? цикл получается из любой своей вершины движением по стрелкам, так что если есть общая вершины, то и циклы одинаковы.)

Мы уже использовали обозначение (ij) для цикла из двух элементов, то есть транспозиции, которая переводит i в j и наоборот. Можно по аналогии обозначить через (ijk) цикл $i \to j \to k \to i$, и так далее. Цикл из одного элемента $i \to i$ тогда будет обозначаться просто как (i). С использованием этих обозначений перестановку

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

записывают как (13)(2).

26 Запишите перестановку

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

в виде произведения циклов. [Ответ: (1345)(2)]

Слово «произведение» тут можно понимать буквально (как композицию), при этом порядок тут не важен, поскольку в каждом цикле движение независимо.

Что можно сказать о чётности цикла? По определению цикл из двух элементов нечётен, потому что это просто транспозиция.

27 Разложите произведение (композицию) перестановок $(1234567) \circ (34)$ на множестве $\{1, 2, \dots, 6, 7\}$ в произведение непересекающихся циклов. (В исходном произведении циклы пересекаются.)

28 Найдите чётность цикла из k элементов.

По определению надо представить этот цикл в виде произведения транспозиций и посмотреть, чётное или нечётное число транспозиций. Это несложно: цикл

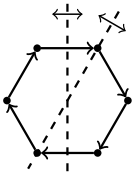
$$\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix}.$$

получается так: 1 проходит вправо через 2 (меняется местами с 2), потом проходит через 3, через 4, ..., наконец, проходит вправо через n (меняется с n). Всего $n-1$ транспозиций. Значит, при чётном n перестановка будет **не**чётной, а при нечётном n — чётной.

Теперь, зная про чётность цикла, легко определить чётность любой перестановки, разложив её в произведение (непересекающихся) циклов.

Разложение перестановки на непересекающиеся циклы бывает полезно в разных задачах. При советской власти, когда продавать квартиры было по большей части нельзя (как «государственную собственность»), люди переезжали из одной квартиры в другую в результате обменов. Простейший обмен — когда одни переезжают на место других, и наоборот, то есть транспозиция. Его выполнить сравнительно легко: одновременно перевозим мебель на грузовиках туда и обратно. Можно одновременно сделать несколько непересекающихся транспозиций: A меняется с B, одновременно C меняется с D и так далее. Будем считать, что это выполнимо за один день (любое количество транспозиций параллельно). Так вот, школьникам тогда давали такую задачу: доказать, что любой обмен можно осуществить за два дня. Вот точная формулировка:

29 Назовём перестановку *однодневной*, если она разлагается в произведение непересекающихся циклов длин 1 и 2. Докажите, что любую перестановку можно представить в виде композиции двух однодневных.



Разложение перестановки на непересекающиеся циклы показывает, что достаточно решить эту задачу для одного цикла (потому что разные циклы можно обрабатывать независимо). Остаётся представить один цикл, скажем, из n элементов, в качестве композиции двух однодневных перестановок. При $n = 1$ и $n = 2$ это уже так, и делать ничего не надо. Но как быть с бóльшими значениями n? Тут могут помочь геометрические соображения: композиция двух симметрий относительно показанных на рисунке осей как раз задаёт поворот, а осевая симметрия всегда является однодневным преобразованием (оставляет точки на месте или меняет местами попарно).

Ещё один вопрос, касающийся циклов, понадобится нам при дальнейшем анализе игры в «15» (и сам по себе важен). Вспомним, что всякая перестановка разлагается в произведение транспозиций (циклов длины 2 — не обязательно непересекающихся).

30 Всякая ли перестановка разлагается в произведение циклов длины 3?

Другими словами, у нас есть n объектов (скажем, букв слова). За один шаг можно их переставить по циклу длины 3. Всякую ли перестановку можно получить за несколько шагов?

Мы уже знаем достаточно, чтобы сразу сказать, что не всякую. Цикл длины 3 является чётной перестановкой (раскладываясь в произведение двух транспозиций). Поэтому и произведение таких циклов, сколько их ни взять, будет чётной перестановкой, и нечётные так не получатся. Следующее утверждение показывает, что это — единственное препятствие.

Теорема. *Всякая чётная перестановка раскладывается в произведение циклов длины 3.*

Доказательство. Вначале можно рассуждать так же, как при разложении перестановки в произведение транспозиций. На первом шаге поставим один из переставляемых объектов на место и больше не будем его трогать. Раньше мы это делали с помощью транспозиции, а теперь сделаем это с помощью цикла длины 3. Для этого цикла, правда, понадобится дополнительный элемент, который тоже куда-то переставится. Ну и ладно — мы поставили нужный элемент на место, а больше нас ничего не интересует. Осталось переставить $n-1$ элементов (если вначале было n), мы тоже можем взять один из них, поставить на место с помощью цикла длины 3, и свести дело к $n-2$ элементам. Всё это можно повторять, пока у нас есть ещё один дополнительный элемент, который можно включить в цикл. При $n = 3$ это ещё получается, но после этого, поставив один элемент на место, мы оставим только два. И если эти два будут в неправильном порядке, то мы не будем знать, что делать. Но в неправильном порядке они не окажутся. Почему?

Потому что в таком случае мы представили бы исходную перестановку в виде произведения циклов длины 3 и одной транспозиции (той самой, которую мы не смогли реализовать в виде цикла длины 3 на последнем шаге).

Теорема доказана. □

Вот ещё одно применение разложения на циклы. Мы когда-то спрашивали, какое максимальное число транспозиций может понадобиться, когда мы разлагаем какую-то перестановку n элементов в произведение транспозиций. Как мы видели, цикл из k элементов можно представить в виде произведения $k-1$ транспозиции (на одну меньше, чем элементов в цикле). В частности, если перестановка n элементов представляет собой один длинный цикл, то её можно представить в виде произведения $n-1$ транспозиций. Если циклов несколько, то каждый из них можно представлять по отдельности, и понадобится меньшее количество транспозиций (на каждом цикле мы экономим одну). Так что $n-1$ транспозиций всегда достаточно.

Но, может быть, всегда можно обойтись меньшим числом транспозиций и $n-2$ тоже достаточно? На самом деле нет.

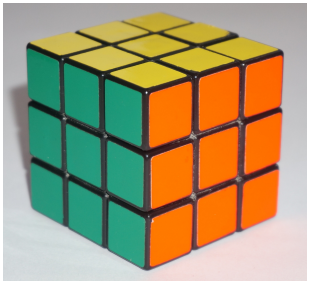
31 Докажите, что цикл длины n нельзя представить как произведение $n-2$ или менее транспозиций.

При $n=2$ или $n=3$ это очевидно (при $n=2$ нуля транспозиций не хватает по очевидным причинам, при $n=3$ не хватает одной транспозиции: цикл — не транспозиция). Хотелось бы доказывать это по индукции, сведя цикл длины n к циклу длины $n-2$. Однако так просто это не получается — переставив два элемента в цикле (выделив одну транспозицию), мы можем из одного цикла получить два. Однако можно доказать по индукции более сильное утверждение: *если перестановка разлагается на непересекающиеся циклы длиной $c_1, c_2, \ldots, c_m$, то для её разложения нужно не меньше*

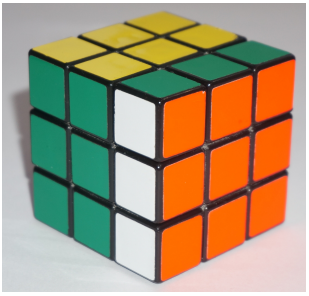
$$(c_1-1)+(c_2-1)+\ldots+(c_m-1)$$

транспозиций. Попробуйте сделать это, поняв, что происходит при выделении одной транспозиции. Тут придётся разобрать два случая: когда переставляемые элементы в одном цикле (тогда он разбивается на 2) и когда в разных (тогда из двух циклов получается один).

10. Порядок перестановки



Есть другая головоломка, даже более известная, чем игра «15» — кубик Рубика. В своей классической форме это кубик $3\times3\times3$, состоящий из маленьких кубиков $1\times1\times1$. Внешние стороны этих маленьких кубиков раскрашены в шесть цветов (обычно там цветные наклейки). Каждую грань можно поворачивать. Если повернуть её на 90°, то снова получается куб $3\times3\times3$, только цвета переставились.



Изначально каждая грань кубика раскрашена в свой цвет, но если сделать несколько поворотов, то цвета перепутываются, и совсем не просто вернуться в исходное положение (по этому делу проводятся даже специальные соревнования на скорость)

Но нас интересует другой вопрос. Если четыре раза повернуть одну и ту же грань, то она вернётся в исходное положение (естественно). Можно сказать, что если F — перестановка наклеек на кубиках, соответствующая повороту грани, то $F^4 = F \circ F \circ F \circ F$ будет тождественной перестановкой на множестве наклеек.[9]

Давайте повернём правую грань на 90°, а сразу после этого повернём верхнюю, тоже на 90°. Если обозначить поворот первой грани за F, а второй — за G, то их комбинация будет соответствовать перестановке $H = G \circ F$. Теперь снова повернём первую грань, и потом снова вторую. Получится перестановка $H^2 = G \circ F \circ G \circ F$. И так далее: будет H^3, H^4,... — и если хватит терпения, то странным образом через какое-то количество шагов все цвета чудесным образом возвратятся на свои места.

32 Сколько шагов для этого понадобится?

(Эту задачу удобно решать, имея в руках кубик. Можно написать и компьютерную программу, конечно.)

На самом деле тут никакого чуда нет, и это общий факт: если вместо H взять любую другую перестановку (скажем, последовательный пово-

[9]На каждой грани $9 = 3 \times 3$ наклеек, всего 54 наклейки, так что можно говорить о перестановках 54-элементного множества. Впрочем, центральные наклейки на каждой грани остаются на местах при поворотах, так что их можно не рассматривать, тогда будет перестановка 48-элементного множества.

рот вокруг трёх граней), то будет то же самое: после некоторого числа повторений кубик вернётся в исходное положение. И даже более общее утверждение: то же самое верно для перестановок любого множества.

Теорема. *Пусть F — произвольная перестановка конечного множества. Тогда найдётся такое n, что $F^n = F \circ F \circ ... \circ F$ (n раз) будет тождественной перестановкой.*

Доказательство. У нас есть последовательность перестановок $F, F^2, F^3, ...$ и надо доказать, что на каком-то шаге снова появится тождественная перестановка. Можно добавить в начало этой последовательности тождественную перестановку I, обозначив её F^0: будет последовательность $F^0 = I, F^1 = F, F^2, F^3, ...$, в которой каждая следующая перестановка получается из предыдущей композицией с F. Рано или поздно в последовательности должна снова появиться перестановка, которая уже была, потому что перестановок конечное число. Другими словами, $F^m = F^k$ для некоторых k, m, причём $k < m$. (Перестановка F^m оказалась не новой и совпала с одной из предыдущих F^k.) На самом деле $k = 0$, то есть первой повторится тождественная перестановка. Почему? Если $F^m = F^k$ и $k > 0$, то перестановки F^{m-1} и F^{k-1} становятся одинаковыми после композиции с перестановкой F. Значит, они и так одинаковые: $F^{m-1} = F^{k-1}$, то есть совпадение было уже и раньше.

Это можно сказать более формально: если $F^m = F^k$, то равенство сохранится и после композиции с обратной перестановкой F^{-1}:

$$F^{-1} \circ F^m = F^{-1} \circ F^k$$

Но

$$F^{-1} \circ F^m = F^{-1} \circ F \circ F^{m-1} = (F^{-1} \circ F) \circ F^{m-1} = I \circ F^{m-1} = F^{m-1}$$

и аналогично для k, так что $F^{m-1} = F^{k-1}$, и совпадение уже было. □

Минимальное натуральное число $n > 0$, при котором $F^n = I$, называется *порядком* перестановки I.

33 Каков порядок у перестановки, состоящей из одного цикла?

34 Перестановка F имеет порядок n, то есть в последовательности $F^0, F_1, F^2, ...$ тождественная перестановка второй раз (после F^0) встречается как F^n. Когда она встретится в третий раз?

Есть и другое доказательство теоремы, основанное на разложении на циклы. Пусть перестановка F разлагается на циклы длиной $c_1, ..., c_m$.

Для одного цикла утверждение понятно: если сдвинуться по циклу столько раз, какова длина этого цикла, то мы вернёмся в исходное положение. Если циклов много, то возьмём n, кратное всем длинам (скажем, $n = c_1 c_2 \ldots c_m$). Тогда в перестановке F^n мы проходим по каждому циклу несколько оборотов и возвращаемся в исходное положение, то есть F^n — тождественная перестановка.

Из этого рассуждения видно, что порядок перестановки F равен наименьшему общему кратному длин её циклов.

35 Докажите, что для любой перестановки F найдётся такое $n \geqslant 0$, что $F^n = F^{-1}$.

36 Каков максимальный возможный порядок перестановки множества из 10 элементов?

Вспоминая про разложение на циклы, мы можем переформулировать эту задачу так: представить число 10 в виде суммы слагаемых, у которых наименьшее общее кратное минимально. Ответом будет разложение $5 + 3 + 2$, дающее перестановку порядка 30, но чтобы доказать, что это наибольший возможный порядок, нужен небольшой перебор.

11. Игра «15»: классов только два

Вернёмся к игре «15». Как и с перестановками (которые делятся на чётные и нечётные), конфигурации делятся всего лишь на два класса.

Теорема. *Любую конфигурацию можно привести либо к стандартной конфигурации, либо к конфигурации с переставленными «14» и «15».*

Доказательство. Будем рассуждать с конца (чего было бы достаточно для доказательства теоремы). Первое (очевидное) замечание: пустую клетку можно перевести в любое место. Поэтому *достаточно доказать теорему для «приведённых» позиций* — так мы будем называть позиции игры, где пустая клетка в правом нижнем углу. (В самом деле, любую позицию можно перевести в приведённую.)

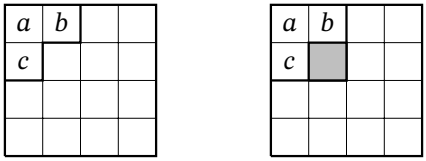
Приведённая позиция отличается от начальной некоторой перестановкой занятых клеток (кроме правой нижней). Достаточно доказать, что *если эта перестановка чётна, то позицию можно перевести в начальную, а если нечётна — то в позицию с переставленными «14» и «15».*

Оба эти утверждения вытекают из такой леммы: *приведённые конфигурации, отличающиеся чётной перестановкой, можно перевести одна*

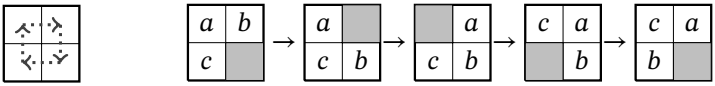
в другую. (Если какая-то приведённая конфигурация отличается от стандартной нечётной перестановкой, то после дополнительного обмена «14» и «15» перестановка станет чётной.)

Теперь мы воспользуемся утверждением, доказанным в разделе 9: всякая чётная перестановка представляет собой произведение циклов длины 3. Из этого следует, что *если мы научимся реализовывать любой цикл длины* 3 *в приведённой конфигурации, то сможем реализовать любую чётную перестановку.* Это первый существенный шаг в доказательстве (до этого, в общем, мы ограничивались тривиальными замечаниям). Реализация цикла длины 3 использует другую важную идею, которая в теории групп называется «сопряжёнными элементами».

Давайте поймём, что *достаточно доказать, что любые три фишки* a, b, c *можно поставить в левый верхний угол*. Почему? Во-первых, после этого можно поставить пустую клетку рядом с ними:



Теперь внутри получившегося квадрата 2×2 можно переставлять фишки по циклу:

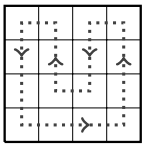


А теперь нужно выполнить все те же действия, которые привели фишки a, b, c в левый верхний угол, а пустую клетку рядом с ними, но в обратном порядке. Мы вернёмся почти к той же конфигурации, с которой начали, только сдвинемся по циклу: там, где раньше было a, теперь будет c, где раньше было b, теперь будет a, а где раньше c — теперь b. (Можно представить себе, что вместо перемещения по циклу в верхнем левом квадрате мы просто наклеили на фишки новые имена.)

Это можно объяснить и так: пусть F — перестановка, переводящая фишки a, b, c в исходной конфигурации в левый верхний угол и помещающая рядом с ними пустую фишку. Пусть G — перестановка с последнего рисунка (цикл длины 3 внутри левого верхнего квадрата). И F, и G можно реализовать по правилам игры. Поэтому и F^{-1} можно реализовать по правилам игры (делая ходы в обратном порядке). Теперь $F^{-1} \circ G \circ F$ будет

циклом длины 3, применённым к исходной конфигурации. Перестановку $F^{-1} \circ G \circ F$ математики называют «сопряжением G с помощью F».[10]

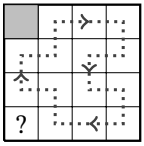
Итак, почему же любые три фишки можно поставить в левый верхний квадрат 2×2? Всякий игравший хоть немного в игру «15» скажет, что это совсем легко — если нас интересуют только три фишки, то свободы в перемещениях ещё очень много, и ничего не стоит поместить эти три фишки в нужное место. Но всё-таки нужно это доказать, а не просто ссылаться на опыт игроков. (На этом доказательство теоремы завершится.) Для доказательства достаточно нарисовать несколько картинок.

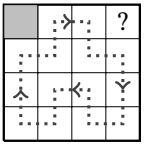


Первая картинка показывает, что любую фишку можно перевести в верхний угол. На ней нарисована «змейка», которая проходит по всем клеткам доски. Одна из этих клеток пустая и находится, так сказать, между «головой» и «хвостом» змейки.

Змейка может продвинуть голову в пустую клетку и постепенно подтягивать к ней хвост фишка за фишкой, пока она снова не воссоединится (а перед головой окажется пустая клетка, с которой только что уползёт хвост). Похожее действие мы выполняли, когда перемещали три фишки по циклу в верхнем левом квадрате, теперь просто змейка длиннее. Такое движение по циклу можно продолжать, пока в угловой (левой верхней) клетке не окажется нужная нам фишка.

Следующая картинка показывает, что можно поставить любые две фишки в угловую (верхнюю левую) клетку и в клетку сразу под ней.





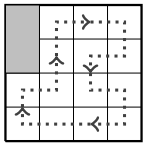
Сначала поставим в угловую клетку нужную фишку (это мы уже умеем) и больше не будем её трогать. А остальные клетки (кроме одной, помеченной вопросительным знаком) снова объединим в цикл, по которому будет двигаться змейка. Так можно поставить под угловую клетку любую

[10]Когда-то давно мне рассказывали (уж не знаю, насколько реальную) историю, иллюстрирующую понятие сопряжения. Два известных математика (А. А. Кириллов-старший и Д. Б. Фукс, если я не перепутал) поднимали в квартиру буфет — тяжёлый и большой параллелепипед. В лифт он не влезал, да и по лестнице проходил только по тщательно выбранной траектории, едва помещаясь. С трудом прошёл он и в дверь квартиры и был поставлен на место. Правда, оказалось, что он стоит дверцами к стенке, и развернуть его в комнате не получается. Что делать? Пришлось спустить его вниз, там перевернуть и снова поднять наверх.

фишку, кроме той, что стоит в клетке с вопросительным знаком. Как быть с этим исключительным случаем? Можно рассмотреть симметричную змейку, где исключительная клетка другая — и по крайней мере одна из этих двух змеек подойдёт.

37 Конечно, было бы лучше объединить все клетки, кроме левой верхней, в один цикл, чтобы не рассматривать эти два случая. Но это невозможно. Почему?

Теперь уже ничего не стоит привести и третью фишку в нужную позицию, не трогая первые две:



Это наблюдение завершает доказательство: умея приводить любые три фишки в левый верхний угол, мы можем их там провернуть по циклу и потом вернуть на место (сопряжение), тем самым реализовав любую цикл длины 3 в любой приведённой конфигурации. Перемножая такие циклы, можно реализовать любую чётную перестановку — и таким образом привести заданную конфигурацию либо к стандартной, либо к стандартной с переставленными фишками «14» и «15». Теорема доказана. □

12. Разное

12.1. Симметрии и перестановки

В геометрии рассматривают *симметрии* фигур, то есть варианты наложения фигуры на себя. Скажем, у равнобедренного треугольника (не равностороннего) имеется единственная ось симметрии: отражение относительно этой оси переводит его в себя, то есть является симметрией треугольника. Эта симметрия переставляет две вершины треугольника (концы основания), оставляя третью неподвижной.

Вообще, любая симметрия многоугольника как-то переставляет его вершины, то есть задаёт перестановку множества его вершин. В случае правильного треугольника так получаются все 6 перестановок его вершин (тождественная, два поворота на 120° и три осевые симметрии). А в случае квадрата или правильного пятиугольника — уже не все.

38 Сколько перестановок вершин квадрата получаются из его движений? Тот же вопрос для правильного пятиугольника.

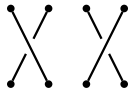
Иногда соответствие между движениями и перестановками более сложное. Например, у куба имеется 24 собственных (не разрешается отражение относительно плоскости) движения: заданную вершину куба можно перевести в любую из 8 других, и затем ещё три случая, отличающихся поворотами. Ровно столько же перестановок у четырёхэлементного множества.

39 Покажите, что каждое движение куба задаёт перестановку на множестве четырёх его больших диагоналей, и так получаются все перестановки по одному разу.

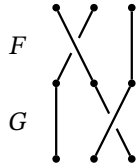
12.2. Группа кос

Мы изображали перестановки картинками из переплетающихся линий. Вот транспозиция:

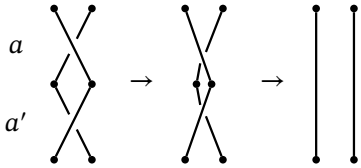
Но если мы захотим сделать такое из настоящих шнурков, а не на бумаге, то будет два варианта — какой шнурок проходит сверху:



Такие схемы переплетения можно умножать, как и перестановки:



Среди них есть и обратные друг другу: если умножить a на a', то получится по существу тождественная картинка (мы не различаем схемы, которые можно непрерывно деформировать одну в другую).



Но a^2 будет не тождественной (а дважды перекрученной).

Такие схемы переплетения математики называют *косами* (по-английски *braids*); рассматриваемые с операцией умножения, они образуют *группу кос*.

40 Вот фотография реальной косы из шнурков; как получить эту косу в виде произведения кос F, G, F^{-1}, G^{-1}?

12.3. Другие доказательства основной теоремы

Базовое утверждение, делающее теорию перестановок (а также определителей, возникающих при анализе систем линейных уравнений) возможной, состоит в том, что произведение нечётного числа транспозиций не может быть тождественной перестановкой. Мы доказали это, и даже по существу двумя способами. Первое доказательство сводит задачу к частному случаю транспозиции соседних элементов (а затем считает отдельно обмены для каждой пары). Второе доказательство (которое мы не проговорили явно) вытекает из сделанного нами в разделе 8 наблюдения: при транспозиции (точнее, при умножении на транспозицию) чётность

числа беспорядков меняется, поэтому после нечётного числа транспозиций мы не можем вернуться к нулю беспорядков.

Как ещё это можно доказывать? В классическом учебнике С. Ленга (*Алгебра*, М.: Мир, 1968) в упражнении 9 на с. 70 предлагается заметить, что при умножении на транспозицию число циклов в разложении перестановки на циклы меняется на 1 (два цикла сливаются в один или наоборот) и потому требуется чётное число действий, чтобы вернуться к прежнему числу циклов. А. И. Кострикин (*Введение в алгебру. Основы алгебры*. М.: Физматлит, 1994, доказательство теоремы 2 на с. 65) показывает, что если произведение m транспозиций равно тождественной перестановке при $m > 0$, то можно найти и произведение $m - 2$ транспозиций с этим свойством. Это рассуждение (довольно длинное и запутанное, по правде говоря) позволяет уменьшать m, оставляя его нечётным, пока не получится противоречия с одной транспозицией.

Совсем простое рассуждение, безо всякого разбора случаев, предлагается в учебнике Б. Л. ван дер Вардена (*Алгебра*, М.: Наука, 1976, с. 36). Там предложено назвать чётной перестановку, которая, будучи применена к переменным $x_1, \ldots, x_n$, переводит функцию

$$\Delta = \prod_{i<k} (x_i - x_k)$$

в себя (без изменения знака). Вроде бы понятно, что перестановка двух переменных меняет знак, и потому нечётное число транспозиций приведёт к изменению знака и не может быть тождественной перестановкой. Но рассуждение это выглядит настолько просто, что закрадывается сомнение: не используем ли мы неявно какое-то утверждение, равносильное доказываемому, или не пропустили ли какую-то необходимую проверку? На самом деле нет, и чтобы в этом убедиться, полезно пересказать это рассуждение немного подробнее.

Функция $(x_1, \ldots, x_n) \mapsto F(x_1, \ldots, x_n)$ с аргументами из какого-то множества M и числовыми значениями называется *кососимметрической*, если она меняет знак при перестановке любых двух своих аргументов:

$$F(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, \ldots, x_{j-1}, x_j, x_{j+1}, \ldots, x_n) = \\ = -F(x_1, \ldots, x_{i-1}, x_j, x_{i+1}, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n)$$

(Отсюда следует, в частности, что если хотя бы 2 из аргументов равны, то значение функции равно нулю.) Тождественно нулевая функция обладает этим свойством, но существуют ли другие?

Наблюдение: из их существования (с n аргументами) следует интересующий нас факт: произведение нечётного числа транспозиций не может быть тождественной перестановкой (n-элементного множества). В самом деле, возьмём набор аргументов с ненулевым значением и будем применять к нему эти транспозиции. Каждый раз будет меняться знак ненулевого числа, и через нечётное число раз он не может вернуться в исходное положение.

Остаётся построить кососимметрическую функцию с n аргументами $x_1, \dots, x_n$. Рассмотрим все пары $\{i, j\}$ различных чисел от 1 до n и перемножим скобки $(x_j - x_i)$ для всех этих пар, получив функцию

$$\prod_{\{i,j\}\subset\{1,\dots,n\}, i\neq j} (x_i - x_j).$$

Правда, мы должны сначала для каждой пары выбрать одно из двух направлений вычитания. Так что более точно можно сказать так: нарисуем полный граф с n вершинами $\{x_1, \dots, x_n\}$; на каждом ребре выберем и фиксируем ориентацию, после чего перемножим разности между концами и началами рёбер. Для каждого выбора ориентацией получится своя функция — но любые две такие функции отличаются только знаком (замена ориентации на одном ребре умножает функцию на -1). Функция не равна нулю, когда все числа x_i различны.

Остаётся понять, почему эта функция (точнее: любая из двух этих функций) кососимметрична. Что происходит, если x_i и x_j меняются местами? Скобка $(x_i - x_j)$ меняет знак, так что надо показать, что изменения знака в остальных компенсируются (то, что остаётся произведение попарных разностей, понятно, так что может измениться разве что знак). Поскольку изменение ориентаций рёбер может лишь умножить функцию на -1, и при этом кососимметричность сохраняется, то можно выбрать ориентации так, как нам удобно. (Мы используем одну и ту же ориентацию и до, и после перестановки x_i и x_j.) Будем считать. что обе вершины x_i и x_j являются началами всех своих рёбер (кроме $x_i - x_j$). Тогда ясно, что знаки при перестановке вообще не изменятся.

41 Как связана функция, определённая нами с помощью произведения, с числом беспорядков? [*Ответ.* Её знак будет равен (-1) в степени числа беспорядков, если в графе ориентировать рёбра от меньшим к большим.]

То же рассуждение можно пересказать и без кососимметрических функций, измеряя чётность перестановки с помощью беспорядков. Ориентируем как-нибудь все рёбра, соединяющие вершины $1, \dots, n$. Положим

$s(i,j)=1$, если ребро идёт от i к j, и $s(i,j)=-1$ в противном случае. Пусть F — некоторая перестановка множества $\{1,\dots,n\}$. Определим её знак $\sigma(F)$ как произведение $s(F(i),F(j))/s(i,j)$ по всем двухэлементным подмножествам $\{i,j\}\subset\{1,\dots,n\}$. (Дробь определена корректно, так как при перестановке i и j и числитель, и знаменатель меняют знак.) Заметим, что это произведение не зависит от выбора ориентации на рёбрах, так как при изменении ориентации одного ребра один сомножитель в числителе и один в знаменателе меняют знак. Для транспозиции F, меняющей местами i и j, знак равен 1 (что удобно проверить, выбрав исходящую ориентацию на всех рёбрах с началом i или j, кроме соединяющего их ребра). А для композиции перестановок знак равен произведению знаков:

$$\prod_{i\ne j}\frac{s(G(F(i)),G(F(j)))}{s(i,j)}=\prod_{i\ne j}\frac{s(G(F(i)),G(F(j)))}{s(F(i),F(j))}\cdot\prod_{i\ne j}\frac{s(F(i),F(j))}{s(i,j)}$$

Второй сомножитель равен $\sigma(F)$ по определению, а первый превращается в $\sigma(G)$, если заметить, что суммирование по всем парам $F(i),F(j)$ равносильно суммированию по всем двухэлементным подмножествам.[11]

12.4. Ещё одна задача о перестановках

Эта задача отчасти напоминает задачу о переездах в два дня, но сложнее.

42 Докажите, что любую перестановку объектов, стоящих в клетках прямоугольной таблицы, можно представить в виде композиции трёх перестановок: первая и третья переставляют элементы внутри строк (каждый объект остаётся в той же строке, где был, но может сменить столбец), а вторая — внутри столбцов.

Тут полезно такое вспомогательное утверждение: если n школьниц решали n задач, и каждая школьница решила k задач, а каждую задачу решили k школьниц, то можно так организовать разбор задач, чтобы каждая школьница рассказала одну из решённых ей задач, и все задачи были бы рассказаны (по одному разу). Для $k=2$ это доказывается сравнительно просто (это соответствует таблицам из двух столбцов).

[11]Примерно такое доказательство приводится в книжке Александрова «Введение в теорию групп» (Библиотечка Квант, выпуск 7,М.:Наука, 1980), но там используется только стандартный порядок на $\{1,\dots,n\}$.

Научно-популярное издание

Александр Шень

Перестановки

Подписано в печать 25.06.2018 г. Формат $60 \times 90\ ^1/_{16}$. Бумага офсетная.
Печать офсетная. Печ. л. 3,5. Тираж 2000 экз. Заказ №

Издательство Московского центра непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241-08-04.

Отпечатано в типографии ООО «Принт сервис групп»,
тел./факс: (499) 785-05-18, e-mail: 3565264@mail.ru, www.printsg.ru
105187, г. Москва, Борисовская ул., д. 14, стр. 6.

ISBN 978-5-4439-2775-6