

MULTIPLICATION
OF SYMMETRIES
AND TRANSFORMATIONS

A. Yu. OL'SHANSKII

This paper introduces the group theoretical point of view of symmetries and transformations. Symmetries of polynomials are used as a definition for permutation's sign, which is applied afterwards to a puzzle. Multiplication of symmetries is quite different from usual numerical operations. Therefore a "calculus" arises which leads to general notions of the group theory.

Статья знакомит с теоретико-групповой точкой зрения на симметрии и преобразования. С помощью симметрий многочленов вводится понятие четности перестановки, используемое для объяснения одной известной игры. Умножение симметрий совсем не похоже на привычные числовые операции. Возникает исчисление, которое в следующей статье приведет к общим понятиям теории групп.

УМНОЖЕНИЕ СИММЕТРИЙ
И ПРЕОБРАЗОВАНИЙ

А. Ю. ОЛЬШАНСКИЙ

Московский государственный университет
им. М.В. Ломоносова

1. ВВЕДЕНИЕ

Изошренная громоздкость алгебраических выражений, приводимых порою в учебниках и задачаниках, их отпугивающий вид в некоторых экзаменационных заданиях при поступлении в высшие учебные заведения могут создать впечатление, что математическое искусство должно совершенствоваться именно в исследовании все более запутанных нагромождений формул и уравнений. К счастью, такое представление далеко от реальностей математики, развитие которой связано как с решением известных старых проблем, так и с появлением новых точек зрения, новых понятий, диктуемых и внутренней логикой науки, и ее приложениями.

Исчисление, об элементах которого мы поведем речь, не является числовым и возникло в связи с фундаментальными для математики и естествознания свойствами симметрий и с необходимостью "умножать" преобразования.

Группы преобразований (и просто "группы") лежат в основании современной алгебры и определяют лицо многих разделов математики и теоретической физики, где симметрия проявляется не всегда столь наглядно, как, скажем, симметрия молекул в строении составленных из них кристаллов.

Цель настоящей статьи, адресованной преимущественно старшеклассникам, — дать представление о преобразованиях множеств и их умножении, свойства которого далеки от привычных свойств операций над числами. Правило четности для произведения перестановок иллюстрируется одной игрой. Каких-либо знаний за пределами школьной программы от читателя не требуется. В следующей статье, следуя истории возникновения "групповых исчислений", мы предполагаем перейти к общему понятию группы.

2. СИММЕТРИИ

Та или иная группа преобразований часто возникает как группа симметрий некоторого объекта. Например, квадрат симметричнее произвольного прямоугольника, потому что число симметрий квадрата равно восьми, а у прямоугольника их всего четыре. В самом деле, квадрат преобразуется в себя же при зеркальных отражениях относительно любой из двух средних линий AB или CD (рис. 1а), при отражениях относительно диагоналей $1-3$ и $2-4$ и при

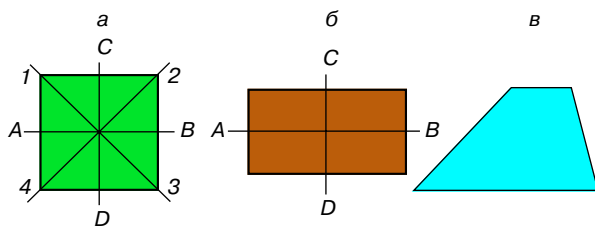


Рис. 1.

поворотах по часовой стрелке на углы 0° , 90° , 180° и 270° вокруг его центра.

Среди этих 8 преобразований “поворот” на 0° называется *тождественным преобразованием* (которое также полезно учитывать, как мы увидим позже). Оно состоит в том, что каждая точка остается неподвижной, то есть отображается в себя. В этом смысле поворот на 360° является тем же тождественным преобразованием, а поворот на 90° совпадает с поворотом на 450° : важен результат, а не пройденный той или иной точкой путь при динамической интерпретации движения.

У прямоугольника (рис. 1б) кроме тождественной есть еще 3 симметрии: поворот вокруг центра на 180° и зеркальные отражения относительно AB и CD . У трапеции (рис. 1в) группа симметрий включает в себя лишь одно тождественное преобразование. Читатель может сосчитать число симметрий у тетраэдра, куба и других правильных многогранников.

К фигурам с бесконечной группой симметрий (то есть состоящей из бесконечного множества различных преобразований) относятся, например, прямой круговой конус (рис. 2а) (любой поворот пространства около его оси есть симметрия), а также бесконечная трехцветная раскраска плоскости (рис. 2б), для которой симметриями будут параллельные переносы на векторы $3\vec{a}$, $3\vec{b}$, $6\vec{a}$, $6\vec{b}$, ... и вообще на любой вектор $k\vec{a} + l\vec{b}$, если разность $k - l$ целых чисел k и l делится на 3.

Многочлен $xy + xz + yz$ кажется симметричнее, чем многочлен $xy^2 + yz^2 + zx^2$, который в свою оче-

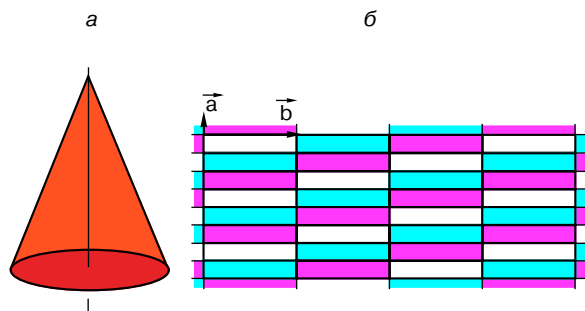


Рис. 2.

редь выглядит симметричнее, чем $x + 2y + 5z$. Однако, чтобы “измерить” симметрию многочленов, зависящих от трех переменных, нужно ввести в рассмотрение всевозможные перестановки переменных x , y и z между собой. К примеру, первый и второй многочлены, в отличие от третьего, не меняются при замене переменных $x \mapsto y, y \mapsto z, z \mapsto x$.

Запишем все возможные перестановки трех переменных вместе с тождественной в таблицу 1. Они и составляют группу симметрий первого многочлена, в то время как симметриями второго многочлена оказываются лишь перестановки из второго ряда таблицы 1 (проверьте!), а группа симметрий третьего содержит в себе лишь последнюю, тождественную перестановку переменных.

Таблица 1

$x \ y \ z$	$x \ y \ z$	$x \ y \ z$
$\downarrow \downarrow \downarrow$	$\downarrow \downarrow \downarrow$	$\downarrow \downarrow \downarrow$
$y \ x \ z$	$z \ y \ x$	$x \ z \ y$
$x \ y \ z$	$x \ y \ z$	$x \ y \ z$
$\downarrow \downarrow \downarrow$	$\downarrow \downarrow \downarrow$	$\downarrow \downarrow \downarrow$
$y \ z \ x$	$z \ x \ y$	$x \ y \ z$

Как мы видим, первой важной характеристикой и мерой симметричности фигуры, многочлена и т.д. является число различных симметрий в группе симметрий, которое называется *порядком* группы. Так, первый из трех рассмотренных многочленов имеет группу симметрии порядка 6, а квадрат имеет группу симметрии порядка 8. Но еще важнее понять, как устроена в таких группах операция умножения, к которой мы теперь и переходим.

3. ПРЕОБРАЗОВАНИЯ

Каждая симметрия является преобразованием какого-то “множества” (множества, состоящего в рассмотренных примерах из всех точек плоскости, пространства или из всех многочленов от трех переменных с вещественными коэффициентами).

Что такое произвольное преобразование f произвольного множества X ? Пусть X состоит из каких-то *точек*. (Вообще нужно говорить о так называемых “точках”. В одном из примеров у нас в качестве точек выступают многочлены от трех переменных!) Говорят, что задано *преобразование* (или взаимно однозначное отображение, соответствие, обратимая функция) f множества X , если для каждой точки a из X ($a \in X$) однозначно задана другая точка из X , которую называют *образом* точки a и обозначают $f(a)$; при этом требуется дополнительно, чтобы каждая точка b из X ($b \in X$) была также образом некоторой, причем единственной, точки $a \in X$. В этом случае точку a называют *прообразом* точки b .

Приведем несколько примеров.

1. Пусть X — плоскость, а f — ее поворот по часовой стрелке на 90° около начала координат. Тогда образом точки $(1, 0)$ будет точка $(0, -1)$, а образом точки $(0, -1)$ будет точка $(-1, 0)$. Проверьте, что вообще образом произвольной точки (x, y) является точка $(y, -x)$, а прообразом для (x, y) служит $(-y, x)$.

2. Пусть опять X — это координатная плоскость, но f — ее параллельный перенос на вектор \mathbf{v} с координатами (v_1, v_2) . Образом произвольной точки A с координатами (a_1, a_2) будет точка $(a_1 + v_1, a_2 + v_2)$, а прообраз точки A — точка с координатами $(a_1 - v_1, a_2 - v_2)$.

3. Пусть теперь X — множество всех вещественных чисел. Тогда формула $y = f(x)$ задает преобразование множества X , если в качестве образа y произвольной точки x выбрать $f(x) = 2x - 6$ или $f(x) = x^3$. Однако функция $f(x) = x^2$ уже не будет преобразованием вещественной прямой, так как, например, у точки 4 (то есть числа 4 в данном случае) два прообраза: 2 и -2, а у точки -1 нет ни одного прообраза.

4. Рассмотрим все преобразования какого-нибудь конечного множества X , то есть множества, в котором конечно число “точек”. Пусть, например, X состоит из трех букв x, y, z . Тогда преобразование f , для которого $f(x) = y, f(y) = z$ и $f(z) = x$, является просто четвертой перестановкой из таблицы 1, а число всевозможных преобразований множества X равно 6, как видно из той же таблицы.

При обобщении этого примера на произвольное конечное множество X , состоящее из n точек, поступают следующим образом. Все точки этого множества нумеруют целыми числами от 1 до n . (В примере выше можно считать, скажем, что x имеет номер 1, y — номер 2, а z — номер 3.) В таком случае всякая перестановка f (то есть преобразование конечного множества X) может быть задана двумя строками: в первой мы приводим все точки множества X (а значит, после нумерации — просто числа 1, ..., n), а во второй пишем соответственно их образы при преобразовании f . Так, преобразование f из предыдущего абзаца запишется как $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, а таблица 1 переписывается в виде таблицы 2.

Таблица 2

$$f_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad f_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$$f_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad f_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad f_6 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Понятно, что каждая перестановка f полностью определяется указанием образов всех точек конечного множества X , то есть f задается второй строкой

своей стандартной записи. Такая строка всего одна: (1) при $n = 1$, их две: (1, 2) и (2, 1) при $n = 2$ и их шесть: (2, 1, 3), (3, 2, 1), (1, 3, 2), (2, 3, 1), (3, 1, 2), (1, 2, 3) для $n = 3$.

Естественно предположить, что для всякого n число всех различных перестановок на множестве X , состоящем из n точек, равно $1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n = n!$. (Правая часть читается “ n факториал”.) Такое предположение оказывается верным, так как оно подтверждается каждый раз при переходе к следующему значению для n . В самом деле, из любой данной строки, заполненной числами от 1 до n , можно получить $n + 1$ строку, заполненную числами от 1 до $n + 1$, если вставлять число $n + 1$ на любое из возможных мест: в самом начале строки или после первого числа строки, или после второго, ..., или после n -го. Поэтому число всех строк, заполненных числами от 1 до $n + 1$, в $n + 1$ раз больше, чем число строк, составленных из чисел от 1 до n , а значит, оно равно $n!(n + 1) = (n + 1)!$.

4. ПРОИЗВЕДЕНИЕ ПРЕОБРАЗОВАНИЙ

Мы придем к “исчислению” симметрий и преобразований после того, как зададим следующую, присущую преобразованиям операцию, называемую их суперпозицией, или просто умножением.

Пусть f и g — два произвольных преобразования какого-то определенного множества X . Тогда их произведение fg , обозначаемое сейчас буквой h , определяется так: для всякой точки x из X по определению $h(x) = f(g(x))$. Другими словами, для вычисления $h(x)$ нужно сначала вычислить $y = g(x)$, а потом найти образ $z = f(y)$ точки y при преобразовании f . Пользуясь определениями, читатель без особого труда может убедиться, что h — также преобразование множества X . Мы ограничимся только следующими примерами.

1. Пусть преобразование f вещественной прямой задается функцией $f(x) = 2x + 6$ вещественного переменного x . Пусть также по определению $g(x) = x^3$. Тогда преобразование $h = fg$ является функцией, вычисляемой по правилу

$$h(x) = f(g(x)) = f(x^3) = 2x^3 + 6,$$

поскольку для получения последнего равенства h заменяется на x^3 в формуле, задающей функцию f . Заметим, что функция $h' = gf$ должна находиться по правилу

$$h'(x) = g(f(x)) = g(2x + 6) = (2x + 6)^3.$$

Этот пример показывает, что умножение преобразований вполне может быть некоммутативным, то есть результат может существенно зависеть от порядка множителей и преобразование fg не обязано совпадать с gf .

2. Найдем произведение каких-нибудь двух перестановок из таблицы 2, например $f_1 f_2$. Здесь множество X состоит из трех чисел: $X = \{1, 2, 3\}$. Значит,

для вычисления $h = f_1 f_2$ мы должны сначала найти $h(1) = f_1(f_2(1))$. Из таблицы 2 видим, что $f_2(1) = 3$, а $f_1(3) = 3$, откуда $h(1) = 3$. Аналогично находим последовательно: $h(2) = 1$ и $h(3) = 2$. Это означает, что произведение $f_1 f_2$ преобразует числа точно так же, как перестановка f_5 из таблицы 2, то есть, $f_1 f_2 = f_5$. Читатель тем же способом подсчитает, что $f_2 f_1 = f_4$, то есть f_1 и f_2 не коммутируют, а, к примеру, f_4 и f_5 коммутируют: $f_4 f_5 = f_5 f_4$.

3. Проверьте, пожалуйста, самостоятельно, что произведение зеркальных симметрий квадрата относительно прямых 2 – 4 и AB (рис. 1а) есть поворот на 90° вокруг его центра по часовой стрелке, а произведение тех же преобразований в обратном порядке – поворот на 270° по часовой стрелке. Для такой проверки достаточно проследить за образами только вершин квадрата. В качестве упражнения можно порекомендовать провести умножения для выбранных каким-либо образом симметрий других правильных многоугольников: тетраэдра, куба и т.д.

5. ГРУППЫ ПРЕОБРАЗОВАНИЙ

Выделим теперь общие свойства групп симметрий. Во-первых, симметрии выбираются среди преобразований какого-то множества X . При этом уже заранее к рассмотрению могут допускаться не обязательно все преобразования множества X . Так, при определении группы симметрий квадрата мы с самого начала ограничивались только движениями плоскости, то есть преобразованиями, сохраняющими длины отрезков (хотя допускали как “собственные” движения, при которых сохраняется еще и ориентация, так и “несобственные” движения, меняющие ориентацию, такие, как зеркальные симметрии). Затем среди движений плоскости выбирались симметрии квадрата, то есть те преобразования, при которых каждая его точка отображается в некоторую точку того же квадрата.

Во-вторых, определено произведение преобразований, которое опять-таки является преобразованием. Произведение симметрий – симметрия: если, например, преобразования f и g каждое переводят некоторую фигуру в себя, то и произведение fg , конечно же, переводит эту фигуру в себя, так как оно сводится к последовательному выполнению g и f . Следовательно, для симметрий фигуры всегда имеется операция умножения.

Отметим далее, что умножение преобразований (в том числе симметрий) ассоциативно. Это значит, что для любых трех (не обязательно различных) преобразований f, g, h произвольного множества X всегда $(fg)h = f(gh)$ (здесь скобки указывают на порядок выполнения умножений). Для проверки убедитесь просто, пользуясь определением умножения преобразований, что как произведение, стоящее в левой части этого равенства, так и произведение из правой части, отображают произвольную точку x из X в точку $f(g(h(x)))$. Это наблюдение позволяет далее

опускать скобки, то есть писать fgh , так как результат не зависит от их расстановки.

Нами было замечено также, что среди преобразований и симметрий всегда можно выделить тождественное преобразование e . Оно оставляет каждую точку x на месте: $e(x) = x$, а выбранное для него обозначение обусловлено тем, что e является “единичным” (или нейтральным) сомножителем при умножении преобразований: $ef = fe = f$ для любого преобразования f , так как всегда $e(f(x)) = f(x)$ и $f(e(x)) = f(x)$ по определению преобразования e . В таблице 2 $e = f_6$.

Наконец для каждого преобразования f имеется обратное преобразование g со свойством: $fg = gf = e$; для него используется обозначение $g = f^{-1}$. Чтобы задать преобразование f^{-1} , нужно его определить правилом $f^{-1}(b) = a$, если $f(a) = b$, то есть образ и прообраз меняются ролями при переходе от f к f^{-1} . Очевидно, что $(f^{-1})^{-1} = f$. Проверьте, что в таблице 2

$$f_1^{-1} = f_1, \quad f_2^{-1} = f_2, \quad f_3^{-1} = f_3, \quad f_4^{-1} = f_5, \quad f_5^{-1} = f_4, \quad f_6^{-1} = f_6.$$

Обратными в этом смысле к функциям вещественного переменного $f(x) = x^3$ и $f(x) = 2x + 6$ являются соответственно $g(x) = \sqrt[3]{x}$ и $g(x) = \frac{x}{2} - 3$. (Проверьте!)

Полезно заметить, что если некоторое преобразование f рассматривается как симметрия (преобразует некоторую фигуру в себя), то и f^{-1} – тоже симметрия.

6. ЧЕТНОСТЬ ПЕРЕСТАНОВОК

Обобщим сначала пример из раздела 2, рассматривая теперь многочлены с вещественными коэффициентами от n переменных x_1, x_2, \dots, x_n , где n – любое целое положительное число. Обозначим S_n группу всех перестановок на символах $1, 2, \dots, n$, порядок которой равен $n!$ (см. раздел 3). Группу S_n будем также считать группой преобразований множества всех многочленов от n переменных. Точнее, если перестановка f переводит 1 в какое-то число i_1 ,

2 – в i_2, \dots, n – в i_n (то есть $f = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$), то переменная x_1 заменяется на x_{i_1}, x_2 – на x_{i_2}, \dots, x_n – на x_{i_n} . Например, многочлен $x_1 - 2x_2 + 5x_3x_4$ под действием преобразования, заданного перестановкой $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$, меняется на $x_2 - 2x_4 + 5x_1x_3$.

При $n = 3$ многочлены второй и третьей степени от трех переменных $x_1^2 + x_2^2 + x_3^2$ и $(x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$ (читатель может сам раскрыть скобки) симметричны, то есть не меняются при любых перестановках переменных. А что можно сказать о многочлене $d_3(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$? Каждый из его трех множителей под действием любой перестановки, выбранной из таблицы 2,

заменяется на другой множитель из этого произведения, но с возможной заменой знака перед ним. (Проверьте!) Поэтому их произведение $d_3(x_1, x_2, x_3)$ либо не меняется, либо меняет свой знак на противоположный. Группу симметрий многочлена $d_3(x_1, x_2, x_3)$ составляют те перестановки, которые его не меняют. Проверьте, что к ним относятся f_4, f_5 и f_6 из таблицы 2. Такие перестановки называют четными, а f_1, f_2, f_3 — нечетными перестановками.

Чтобы определить четность произвольной перестановки

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

на числах от 1 до n , нужно ввести многочлен от n переменных x_1, x_2, \dots, x_n :

$$d_n(x_1, x_2, \dots, x_n) = (x_1 - x_2)(x_1 - x_3) \dots (x_1 - x_n)(x_2 - x_3) \dots (x_2 - x_n)(x_3 - x_4) \dots (x_3 - x_n) \dots (x_{n-1} - x_n). \quad (1)$$

По определению разность $x_k - x_l$ включается множителем в многочлен $d_n(x_1, \dots, x_n)$ тогда и только тогда, когда $k < l$.

Под действием перестановки f сомножитель $x_k - x_l$ заменяется на $x_{i_k} - x_{i_l}$, то есть либо на другой множитель произведения (1), либо на двучлен, противоположный по знаку одному из множителей в (1) (если $k < l$, но $i_k > i_l$). Значит, многочлен (1) преобразуется в $\pm d_n(x_1, \dots, x_n)$.

Те перестановки из группы всех перестановок S_n , которые составляют группу симметрий многочлена $d_n(x_1, \dots, x_n)$, то есть не меняющие произведения (1), называются четными, а меняющие его знак на противоположный называются нечетными.

Для примера рассмотрим элементарную транспозицию, которая меняет местами только два каких-либо соседних числа k и $k+1$ в ряду $1, \dots, n$:

$$f = \begin{pmatrix} 1 & 2 & \dots & k-1 & k & k+1 & k+2 & \dots & n \\ 1 & 2 & \dots & k-1 & k+1 & k & k+2 & \dots & n \end{pmatrix}. \quad (2)$$

Преобразование, заданное перестановкой (2), заменяет множитель $x_k - x_{k+1}$ на $x_{k+1} - x_k = -(x_k - x_{k+1})$. Все же остальные сомножители в (2) могут только остаться без изменения или поменяться местами с другими множителями, не меняя знак. Например, если $k+1 < l$, то $x_{k+1} - x_l$ превращается в $x_k - x_l$, где опять-таки $k < l$, и т.д. Поэтому перестановка (2) поменяет знак перед многочленом (1), то есть

всякая элементарная транспозиция является нечетной перестановкой.

7. ПРАВИЛО ЧЕТНОСТИ ДЛЯ ПРОИЗВЕДЕНИЯ ПЕРЕСТАНОВОК

Из свойств произвольной группы симметрий, в частности группы четных перестановок, заключаем, что произведение четных перестановок есть чет-

ная перестановка. Впрочем, это видно и непосредственно, поскольку результат действия на какой-либо многочлен произведения fg двух перестановок будет таким же, как и при последовательном применении к нему сначала g , а потом f . Отсюда видно также, что произведение нечетной перестановки на четную (или четной на нечетную) есть нечетная перестановка, так как если g не меняет многочлена (1), а f заменяет $d_n(x_1, \dots, x_n)$ на $-d_n(x_1, \dots, x_n)$, то произведение fg (то есть последовательное применение сначала g , а затем f) преобразует $d_n(x_1, \dots, x_n)$ в $-d_n(x_1, \dots, x_n)$. Точно так же произведение двух нечетных перестановок будет четной перестановкой. Все эти возможности объединяются одним правилом четности произведения:

При умножении перестановок их четности "складываются". В частности, произведение двух четных или двух нечетных перестановок является четной перестановкой, а произведение четной на нечетную (или нечетной на четную) есть нечетная перестановка.

Найдем четность произведения произвольной транспозиции, то есть перестановки, меняющей местами только два различных (не обязательно соседних, как в случае элементарной транспозиции) числа k и l :

$$\begin{pmatrix} 1 & 2 & \dots & k & k+1 & \dots & l-1 & l & \dots & n \\ 1 & 2 & \dots & l & k+1 & \dots & l-1 & k & \dots & n \end{pmatrix}. \quad (3)$$

Для определенности считаем, что $k < l$, а также, что $k+1 < l$, так как иначе транспозиция (3) является элементарной и, как уже нам известно, нечетной.

Удобно ввести следующую вспомогательную перестановку g , переставляющую только числа $k+1$ и l :

$$g = \begin{pmatrix} 1 & 2 & \dots & k & k+1 & k+2 & \dots & l-1 & l & l+1 & \dots & n \\ 1 & 2 & \dots & k & l & k+2 & \dots & l-1 & k+1 & l+1 & \dots & n \end{pmatrix}.$$

Для этой перестановки g и элементарной транспозиции f , заданной формулой (2), составим произведение gfg . Оставим читателю его вычисление, которое убеждает, что gfg совпадает с транспозицией (3). (Например, k под действием g переходит в себя, затем под действием f отображается в число $k+1$, которое при применении g отображается в l . В итоге k преобразуется в l , как и при выполнении итоговой перестановки (3), и т.д.) Однако нам уже известно, что f — нечетная перестановка. Поэтому двукратное применение правила четности к произведению gfg приводит к выводу, что транспозиция (3) есть нечетная перестановка. Тем самым доказана

Теорема 1. *Всякая транспозиция является нечетной перестановкой.*

Подсчет числа четных или нечетных перестановок в группе S_n может быть при $n > 1$ проведен следующим образом. Предположим, что f_1, \dots, f_s — все различные четные перестановки из S_n , а g_1, \dots, g_r — все нечетные перестановки. Выберем среди последних

также какую-нибудь одну транспозицию и обозначим ее h (такая найдется, ибо $n > 1$). Тогда все перестановки hf_1, \dots, hf_s различны (равенство вида $hf_i = hf_j$ после умножения слева обеих его частей на h^{-1} привело бы к равенству $f_i = f_j$). Но по правилу четности произведения и теореме 1 все эти s перестановок должны быть нечетными, а значит, содержаться среди перестановок g_1, \dots, g_t . Такое возможно только, если $s \leq t$. Однако тем же способом, но рассматривая уже произведения hg_1, \dots, hg_t , получаем и обратное неравенство: $t \leq s$. Следовательно, $s = t$, а из раздела 3 мы уже знаем, что $s + t = n!$. Значит, доказана

Теорема 2. При $n > 1$ число четных перестановок в группе S_n совпадает с числом нечетных перестановок и равно $n!/2$.

8. ИГРА В “ПЯТНАДЦАТЬ” И ПЕРЕСТАНОВКИ

Покажем теперь, как свойства перестановок помогают объяснить одну давно известную головоломку. Это так называемая игра в “пятнадцать”. Для нее предназначена коробка, заполненная фишками с номерами от 1 до 15. При этом шестнадцатое место в четырех рядах и четырех колонках остается пустым (рис. 3а). За один ход разрешается передвинуть на пустое место любую из соседних фишек, находящихся слева, справа, выше или ниже пустого места (место, занимаемое фишкой ранее, наоборот, становится пустым). В позиции рисунка 3а, например, можно передвинуть только одну из фишек с номерами 2 (вправо), 11 (влево), 6 (вниз) или 15 (вверх).

Спрашивается, можно ли от произвольной позиции перейти за несколько ходов к другой, скажем, от показанной на рисунке 3б к рисунку 3в.

Для математического анализа игры можно считать, что на пустом месте как бы находится дополнительная фишка с номером 16, которую только и разрешается менять с соседними (слева, справа, сверху или снизу). В этом случае каждая позиция однозначно характеризуется перестановкой

$$f = \begin{pmatrix} 1 & 2 & \dots & 16 \\ i_1 & i_2 & \dots & i_{16} \end{pmatrix},$$

где i_1 — номер фишки, стоящей в левом верхнем углу, i_2 — номер фишки из первого ряда и второй колонки, ..., i_5 — из второго ряда и первой колонки и т. д.

3	14	6	8	1	2	3	4	1	2	3	4
5	2		11	5	6	7	8	5	6	7	8
13	4	15	10	9	10	11	12	9	10	11	12
9	7	1	12	13	15	14		13	14	15	
а				б				в			

Рис. 3.

Например, позиция рисунка 3а задается перестановкой

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3 & 14 & 6 & 8 & 5 & 2 & 16 & 11 & 13 & 4 & 15 & 10 & 9 & 7 & 1 & 12 \end{pmatrix},$$

позиция рисунка 3в — тождественной перестановкой, а позиция рисунка 3б — элементарной транспозицией, меняющей местами 14 и 15.

Делая один ход, игрок меняет позицию и перестановку, ее характеризующую. Так, если в позиции рисунка 3а фишку с номером 6 опустить на пустое место (то есть поменять ее местами с фиктивной фишкой 16), то в нижней строке выписанной выше перестановки f числа 6 и 16 поменяются местами. Но тот же результат достигается, если перестановку f умножить слева на такую транспозицию g , которая меняет местами числа 6 и 16. (Проверьте умножением, что перестановка gf задает новую позицию.) Точно так же при перемещении на пустое место фишки с номером 2 (с номером 11 или 15) перестановка f умножится слева на транспозицию, переставляющую 2 и 16 (11 и 16 или 15 и 16 соответственно).

В соответствии с теоремой 1 и правилом четности произведения можно заключить теперь, что каждый ход меняет четность перестановки, характеризующей определенную позицию, на противоположную.

Перестановки, задающие позиции рисунков 3б и 3в, имеют разные четности. Поэтому от позиции рисунка 3б к позиции рисунка 3в можно было бы перейти, только сделав нечетное число ходов.

С другой стороны, в позициях рисунков 3б и 3в “фишка” 16 занимает одно и то же место. Значит, при существовании какой-то последовательности ходов, ведущих от позиции рисунка 3б к 3в, она бы в итоге столько же раз поднялась вверх, сколько и опустилась вниз, и столько же раз передвинулась налево, сколько и направо. Но это значит, что число ходов при преобразовании позиции рисунка 3б в 3в может быть только четным.

Полученное противоречие показывает всю тщетность попыток прийти от позиции рисунка 3б к стандартной позиции рисунка 3в (если, конечно, играть по правилам!). Читателю, заинтересованному в объяснении других игр (таких, например, как “кубик Рубика”) с помощью групп перестановок, мы рекомендуем следующую элементарную книгу:

Калужнин Л.А., Суцанский В.И. Преобразования и перестановки. М.: Наука, 1985.

Александр Юрьевич Ольшанский, доктор физико-математических наук, профессор кафедры высшей алгебры Механико-математического факультета Московского государственного университета им. М.В. Ломоносова, входит в состав редколлегии нескольких международных математических журналов. Автор более 50 научных работ, им и его учениками найдены решения многих известных старых вопросов теории групп.