1. Множества и отображения

Множества. Традиционное построение почти всей современной математики, в том числе, и алгебры, является теоретико-множественным. Мы не станем излагать здесь теорию множеств; скажем только, что основным отношением в ней является отношение принадлежности $\in$. Запись $a \in A$ означает, что a является элементом множества A. То же самое часто выражается и другими словами: "a принадлежит A", "элемент a входит в множество A", и т.п. Отрицание утверждения $a \in A$ записывается так: $a \notin A$.

Напомним, что если множества A и B состоят из одних и тех же элементов (т.е. всякий элемент множества A является элементом множества B и, наоборот, всякий элемент множества B является элементом множества A), то эти множества совпадают: $A = B$. Если же выполняется только первая часть предыдущего условия (т.е. всякий элемент множества A является элементом множества B), а относительно его второй части ничего не известно, то говорят, что A – подмножество множества B, и записывают это следующим образом: $A \subseteq B$, или $B \supseteq A$ (A содержится в B, или B содержит A). Сопоставляя приведенные выше определения, мы получаем: если $A \subseteq B$, $B \subseteq A$, то $A = B$.

Если A, B – множества, то определены их объединение $A \cup B$ и пересечение $A \cap B$; c является элементом $A \cup B$ тогда и только тогда, когда c принадлежит хотя бы одному из множеств A, B, и $c \in A \cap B$ тогда и только тогда, когда $c \in A$ и $c \in B$. Аналогично определяются объединение и пересечение произвольных семейств множеств. Пусть I – некоторое множество индексов, и для каждого $i \in I$ задано множество X_i. Тогда определены их объединение $\bigcup\limits_{i \in I} X_i$ и пересечение $\bigcap\limits_{i \in I} X_i$; при этом $x \in \bigcup\limits_{i \in I} X_i$ тогда и только тогда, когда $x \in X_i$ хотя бы для одного индекса $i \in I$, а $x \in \bigcap\limits_{i \in I} X_i$ тогда и только тогда, когда $x \in X_i$ для всех $i \in I$.

Множество X, состоящее из конечного числа элементов $x_1, \ldots, x_n$ обозначается при помощи фигурных скобок: $X = \{x_1, \ldots, x_n\}$. Аналогично, если множество состоит из элементов x_i, занумерованных индексами, пробегающими множество I, то для него применяется обозначение $\{x_i\}_{i \in I}$ или $\{x_i \,|\, i \in I\}$. Пусть теперь X – некоторое множество, и пусть $P(x)$ – некоторое свойство элементов этого множества. Тогда определено множество всех элементов из X, обладающих этим свойством; оно обозначается через $\{x \in X \,|\, P(x)\}$. Например, если A, B – подмножества множества X, то

$$A \cup B = \{x \in X \,|\, x \in A \text{ или } x \in B\}, \quad A \cap B = \{x \in X \,|\, x \in A \text{ и } x \in B\}.$$

В качестве еще одного примера дадим определение теоретико-множественной разности $A \setminus B$ двух множеств A и B:

$$A \setminus B = \{a \in A \,|\, a \in A, a \notin B\}.$$

Удобно, а зачастую и необходимо, включить в рассмотрение множество, в котором нет ни одного элемента; оно называется пустым и обозначается $\emptyset$.

Отображения. Мы не будем давать строгое определение отображения, хотя это и можно сделать на языке теории множеств. Пусть A и B – два множества; отображение $f : A \to B$ ставит в соответствие каждому элементу $a \in A$ некоторый однозначно определенный элемент $f(a) \in B$, причем отображение полностью определяется этим соответствием: если $g : A \to B$ – другое отображение, и $f(a) = g(a)$ для всех $a \in A$, то $f = g$. Иначе отображения называются функциями. Подчеркнем, что отображение не обязательно задается какой-то формулой или алгорифмом. Часто, особенно если рассматриваются одновременно несколько отображений, удобно вместо $f : A \to B$ изображать отображение в виде $A \xrightarrow{f} B$.

Пусть $f : A \to B$, $g : B \to C$ – два отображения; их произведением, или композицией, называется отображение $g \circ f : A \to C$, заданное правилом: $(g \circ f)(a) = g(f(a))$ для каждого $a \in A$. Легко проверить, что, если $h : C \to D$ – еще одно отображение, то $(h \circ g) \circ f = h \circ (g \circ f)$. Действительно, для любого $a \in A$ мы имеем:

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a))) = h((g \circ f)(a)) = (h \circ (g \circ f))(a).$$

Пусть A – произвольное множество; отображение $\mathrm{id}_A : A \to A$, определенное правилом $\mathrm{id}_A(a) = a$ для всех $a \in A$, называется тождественным отображением множества A на себя. Для любого отображения $f : A \to B$ выполнены соотношения $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$, так как

$$(f \circ \mathrm{id}_A)(a) = f(\mathrm{id}_A(a)) = f(a), \qquad (\mathrm{id}_B \circ f)(a) = \mathrm{id}_B(f(a)) = f(a)$$

для каждого $a \in A$.

Если $f : A \to B$ – отображение, то отображение $g : B \to A$ называется обратным к f, если $f \circ g = \mathrm{id}_B$, $g \circ f = \mathrm{id}_A$. Если обратное отображение существует, то оно единственно. Действительно, пусть $g' : B \to A$ – еще одно отображение, обратное к f; тогда

$$g' = g' \circ \mathrm{id}_B = g' \circ (f \circ g) = (g' \circ f) \circ g = \mathrm{id}_A \circ g = g.$$

Единственное обратное к f отображение (если оно существует) обозначается f^{-1}.

Для того, чтобы выяснить, когда для отображения есть обратное, дадим еще несколько определений. Отображение $f : A \to B$ называется *инъективным*, если из того, что $f(a_1) = f(a_2)$ для некоторых $a_1, a_2 \in A$, следует, что $a_1 = a_2$. Отображение f называется *сюръективным*, если для каждого $b \in B$ найдется элемент $a \in A$, такой что $f(a) = b$. Наконец, отображение f называется *биективным*, если оно одновременно инъективно и сюръективно.

Предложение. *Для отображения $f : A \to B$ обратное отображение существует тогда и только тогда, когда f – биективное отображение.*

Доказательство. Пусть сначала обратное отображение f^{-1} существует. Если $a_1, a_2 \in A$ и $f(a_1) = f(a_2)$, то

$$a_1 = \mathrm{id}_A(a_1) = (f^{-1} \circ f)(a_1) = f^{-1}(f(a_1)) = f^{-1}(f(a_2)) = (f^{-1} \circ f)(a_2) = \mathrm{id}_A(a_2) = a_2.$$

Таким образом, отображение f инъективно. Далее, для любого $b \in B$ имеем: $b = \mathrm{id}_B(b) = (f \circ f^{-1})(b) = f(a)$, где $a = f^{-1}(b) \in A$, т.е. f и сюръективно.

Обратно, пусть $f : A \to B$ – биективное отображение; для всякого $b \in B$ существует элемент $a \in A$, такой что $f(a) = b$ (потому что f сюръективно). Более того, этот элемент единственный, так как из инъективности f следует, что если $f(a') = f(a) = b$, то $a' = a$. Определим теперь отображение $g : B \to A$, взяв для каждого $b \in B$ в качестве $g(b)$ единственный элемент из A, для которого $f(g(b)) = b$. Из самого определения отображения g получаем, что $(f \circ g)(b) = f(g(b)) = b = \mathrm{id}_B(b)$ для всех $b \in B$, т.е. $f \circ g = \mathrm{id}_B$. Далее, для каждого $a \in A$

$$f((g \circ f)(a)) = (f \circ (g \circ f))(a) = ((f \circ g) \circ f)(a) = \mathrm{id}_B(f(a)) = f(a) = f(\mathrm{id}_A(a));$$

поскольку f инъективно, отсюда следует, что $(g \circ f)(a) = \mathrm{id}_A(a)$ для всех $a \in A$, а это значит, что $g \circ f = \mathrm{id}_A$. Таким образом, g – обратное к f отображение.

Декартово произведение. Пусть A, B – множества. Рассмотрим множество всех таких функций $f : \{1, 2\} \to A \cup B$, что $f(1) \in A$, $f(2) \in B$. Это множество и называется декартовым произведением множеств A и B и обозначается $A \times B$. Функция $f \in A \times B$ полностью определяется своими значениями на единственных элементах 1, 2 множества $\{1, 2\}$. Пусть $a \in A$, $b \in B$; через (a, b) будем обозначать функцию $f \in A \times B$, для которой $f(1) = a$, $f(2) = b$. Таким образом, множество $A \times B$ состоит из всех упорядоченных пар (a, b), где $a \in A$, $b \in B$. Отметим, что

$(a, b) = (a', b')$ тогда и только тогда, когда $a = a'$, $b = b'$. Заметим еще, что даже если множество B совпадает с множеством A, пары (a_1, a_2) и (a_2, a_1) представляют собой, вообще говоря, различные элементы декартова произведения.

Бинарные алгебраические операции. Пусть A – некоторое множество. Бинарной алгебраической операцией на A называется любое отображение $f : A \times A \to A$. Обычно для результата применения бинарной операции f к элементам $a, b \in A$ вместо $f((a, b))$ пишут afb; в этом случае для обозначения операции вместо латинской буквы используется какой-то символ $*$. Чаще всего используются знаки $+$ (тогда говорят, что операция записана аддитивно, а сама она называется сложением) и $\times$ (в этом случае операцию называют умножением и говорят, что она записана мультипликативно). Впрочем, знаком для умножения часто бывает точка $\cdot$, а во многих случаях он вообще опускается.

2. Группы. Симметрическая группа

Группы: определение и простейшие примеры. Множество G, на котором задана бинарная алгебраическая операция умножения $*$, называется группой, если выполняются следующие условия:

(1) $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ для всех $g_1, g_2, g_3 \in G$ (это условие называется ассоциативностью умножения);
(2) существует такой элемент $e \in G$, называемый единицей группы G, что $e * g = g * e = g$ для каждого $g \in G$;
(3) для всякого элемента $g \in G$ существует элемент $g^{-1} \in G$, называемый обратным к g, такой что $g^{-1} * g = g * g^{-1} = e$.

В дальнейшем мы увидим, что единица группы и обратный элемент определены однозначно. Если операция умножения в группе удовлетворяет еще и условию

(4) $g_1 * g_2 = g_2 * g_1$ для всех $g_1, g_2 \in G$,

то группа G называется абелевой группой. Условие (4) называется коммутативностью умножения.

Обычно знак умножения в группе опускается, так что произведение элементов $g, h \in G$ обозначается gh. Однако, если группа абелева, то часто операция в группе обозначается знаком $+$; в этом случае говорят, что группа записана аддитивно, операция в ней называется сложением, единичный элемент в ней обозначается знаком 0, а обратный к элементу $g \in G$ обозначается $-g$ и называется противоположным к g элементом. Таким образом, аксиомы аддитивно записанной абелевой группы A приобретают следуюший вид:

(1) $a + (b + c) = (a + b) + c$ для всех $a, b, c \in A$ (ассоциативность сложения);
(2) существует такой элемент $0 \in A$, называемый нулем группы A, что $0+a = a$ для каждого $a \in A$;
(3) для всякого элемента $a \in A$ существует элемент $-a \in A$, называемый противоположным к , такой что $(-a) + a = 0$;
(4) $a + b = b + a$ для всех $a, b \in A$ (коммутативность сложения).

Как хорошо известно из школьного курса, сложение в множествах целых чисел $\mathbb{Z}$, рациональных чисел $\mathbb{Q}$ и вещественных чисел $\mathbb{R}$ обладает всеми этими свойствами. Таким образом, относительно операции сложения $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ представляют собой аддитивно записанные абелевы группы. Для того, чтобы подчеркнуть, что мы рассматриваем эти множества только относительно сложения, забывая об умножении, эти группы обозначаются соответственно $\mathbb{Z}^+$, $\mathbb{Q}^+$, $\mathbb{R}^+$.

Умножение чисел тоже ассоциативно и коммутативно, и во всех множествах $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ есть единичный элемент 1. Однако, обратный элемент не всегда существует, так что $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ не являются группами относительно умножения. Но множества

$\mathbb{Q}^*$, $\mathbb{R}^*$, полученные из $\mathbb{Q}$, $\mathbb{R}$ выбрасыванием 0, уже являются (мультипликативно записанными) абелевыми группами относительно умножения.

Группы преобразований. Пусть X – некоторое множество; преобразованием множества X называется любое биективное отображение X на себя. Обозначим через S_X множество всех преобразований $f : X \to X$ множества X. Если $f, g : X \to X$ – два преобразования из S_X, то определена их композиция $f \circ g$, которая тоже отображает X в X, и нетрудно видеть, что отображение $f \circ g$ биективно. Таким образом, для любых $f, g \in S_X$ их композиция $f \circ g$ принадлежит S_X. Выше было показано, что композиция любых отображений (а не только преобразований) ассоциативна. Далее, тождественное отображение id_X биективно и потому оно принадлежит S_X. Поскольку любое преобразование $f \in S_X$ биективно, для него, как показано выше, существует обратное отображение $f^{-1} : X \to X$, и очевидно, что оно биективно, т.е. $f^{-1} \in S_X$, Таким образом, множество S_X является группой относительно операции композиции преобразований. Эта группа называется группой преобразований множества X.

Преобразования конечного множества называются подстановками этого множества. В случае, когда $X = \{1, 2, \ldots, n\}$, группа S_X обозначается через S_n и называется симметрической группой порядка n. Элемент $\sigma \in S_n$ полностью задается таблицей значений функции σ. Такую таблицу, а значит, и саму подстановку σ, удобно записывать в виде двухстрочной таблицы, в верхней строке которой стоят элементы множества $\{1, 2, \ldots, n\}$ (не обязательно в возрастающем порядке), а под каждым элементом i из этого множества стоит элемент, в который подстановка σ переводит i. Приведем несколько примеров подстановок из S_5:

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

Отметим, что первые две таблицы задают на самом деле одну и ту же подстановку, а подстановка, описываемая третьей таблицей, обратна к подстановке, задаваемой первыми двумя таблицами.

Нетрудно сосчитать, сколько элементов содержится в группе S_n; их столько же, сколько таблиц вида

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix},$$

в которых $i_1, i_2, \ldots, i_n$ – попарно различные числа из множества $\{1, 2, \ldots, n\}$. В качестве i_1 мы можем взять любое из n чисел $1, 2, \ldots, n$. В каждом из этих n случаев в качестве i_2 можно взять любое из $n-1$ чисел ряда $1, 2, \ldots, n$, отличных от i_1. Таким образом, для пары i_1, i_2 есть $n(n-1)$ возможностей. Точно так же, для элемента i_3 остается $n-2$ возможности, $\ldots$, для элемента i_{n-1} – 2 возможности, а последний элемент i_n уже определяется однозначно. Итак, группа S_n состоит из $n(n-1)(n-2) \cdot \cdots \cdot 2 \cdot 1$ элементов. Принято обозначать произведение всех целых чисел от 1 до n через $n!$ (словами: n-факториал). Значит, число элементов группы S_n равно $n!$

При записи умножения подстановок знак умножения $\circ$ обычно не пишется. Отметим, что для обращения подстановки, заданной своей таблицей значений, достаточно поменять местами строки таблицы. Напомним еще, что при умножении подстановок сначала сначала действует правый сомножитель, а затем левый. Приведем несколько примеров вычислений в группе подстановок.

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

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

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

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

Сравнивая первые два из этих примеров, замечаем, что уже при $n = 3$ перестановка сомножителей из группы S_n, вообще говоря, меняет произведение. Таким образом, группа S_n неабелева (за исключением случаев $n = 1$ и $n = 2$).

О группе подстановок

Пусть X – конечное множество, и пусть x_1, x_2,..., x_r – попарно различные элементы множества X. Подстановка, переводящая x_1 в x_2, x_2 в x_3, ..., x_{r-1} в x_r, x_r в x_1, и оставляющая на месте все остальные элементы множества X, называется циклом и обозначается $(x_1, x_2, \ldots, x_r)$. Число r называется длиной цикла. Цикл (x) длины 1 оставляет все элементы множества X на месте.

Теорема 1. *Всякая подстановка конечного множества X может быть представлена в виде произведения нескольких циклов, никакие два из которых не содержат одинаковых элементов, причем каждый элемент множества X принадлежит некоторому циклу. Это представление единственно с точностью до порядка сомножителей.*

Доказательство. Прежде, чем начать доказательство, проиллюстрируем теорему примером, который сделает ясным, как ее доказывать. Пусть

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

Подстановка σ переводит 1 в 3, 3 в 7, 7 в 4, а 4 – опять в 1; таким образом, из подстановки выделяется цикл $(1, 3, 7, 4)$. Элемент 2 множества $\{1, 2, \ldots, 8\}$ не принадлежит этому циклу, и он переводится подстановкой σ в себя, так что мы выделили еще один цикл (2). Элемент 5 не содержится ни в одном из уже выбранных циклов, и $\sigma(5) = 8$, $\sigma(8) = 6$, $\sigma(6) = 5$. Итак, выделился еще один цикл $(5, 8, 6)$, и каждый элемент множества $\{1, 2, \ldots, 8\}$ принадлежит одному из циклов, так что $\sigma = (1, 3, 7, 4)(2)(5, 8, 6)$.

Обобщим это рассуждение на случай произвольной подстановки. Пусть $X = \{x_1, \ldots, x_n\}$ – конечное множество, и $\sigma \in S_X$; доказательство существования разложения в произведение циклов будем вести индукцией по количеству $a(\sigma)$ таких элементов $x \in X$, что $\sigma(x) \neq x$. Если $a(\sigma) = 0$, то σ не двигает ни один из элементов множества X, и $\sigma = (x_1)(x_2)\ldots(x_n)$. Пусть теорема уже доказана для всех подстановок σ', для которых $a(\sigma') < a(\sigma)$. Выберем произвольный элемент $y \in X$ и положим

$$y_1 = y,\ y_2 = \sigma(y_1),\ y_3 = \sigma(y_2),\ \ldots\ ,\ y_{i+1} = \sigma(y_i),\ \ldots\ .$$

Поскольку множество X конечно, среди элементов y_i будут повторяющиеся. Пусть y_{r+1} – первый из элементов y_i, совпадающий с одним из предшествующих элементов ($r \geq 1$); покажем, что $y_{r+1} = y_1$. Действительно, если $y_{r+1} = y_l$, $l \geq 2$, то $\sigma(y_{l-1}) = y_l = y_{r+1} = \sigma(y_r)$, и, поскольку σ – инъективное отображение, y_r совпадает с предшествующим ему элементом y_{l-1}, а это противоречит тому, что y_{r+1} был первым из элементов y_i, совпадающих с каким-то из предшествующих элементов. Таким образом, мы выделили в подстановке σ цикл $\alpha_1 = (y_1, \ldots, y_r)$.

Пусть $\sigma' = \alpha_1^{-1}\sigma$; подстановка σ' оставляет неподвижными элементы $y_1, \dots, y_r$, а другие элементы из X подстановка σ' двигает тогда и только тогда, когда их двигает подстановка σ. Поэтому $a(\sigma') = a(\sigma) - r < a(\sigma)$, и мы можем применить предположение индукции. Учитывая, что $\sigma'(y_1) = y_1, \dots, \sigma'(y_r) = y_r$, получаем разложение σ' в произведение попарно не пересекающихся циклов $\sigma' = (y_1) \dots (y_r)\alpha_2 \dots \alpha_k$, причем любой элемент из X принадлежит одному из этих циклов. Но тогда $\sigma = \alpha_1\sigma' = \alpha_1\alpha_2 \dots \alpha_k$.

Единственность разложения очевидна. Действительно, пусть $\sigma = \alpha_1 \dots \alpha_k = \beta_1 \dots \beta_l$ – разложения σ в произведения циклов, удовлетворяющие требованиям теоремы, и элемент $x \in X$ содержится в циклах $\alpha_i = (x, y_2, \dots, y_r)$, $\beta_j = (x, z_2, \dots, z_p)$, причем $r \leq p$ (ясно, что запись цикла можно начинать с любого входящего в него элемента). Тогда $y_2 = \sigma(x) = z_2$, $y_3 = \sigma(y_2) = \sigma(z_2) = z_3, \dots, y_r = \sigma(y_{r-1}) = \sigma(z_{r-1}) = z_r$, $x = \sigma(y_r) = \sigma(z_r)$. Таким образом, z_r – последний элемент цикла β_j, и $\alpha_i = (x, y_2, \dots, y_r) = (x, z_2, \dots, z_r) = \beta_j$.

Теорема 1 полностью доказана.

Транспозицией называется подстановка, переставляющая два различных элемента x, y множества X и оставляющая на месте все остальные элементы множества X. Таким образом, транспозиция – это цикл (x, y) длины 2.

Теорема 2. *Всякая подстановка раскладывается в произведение конечного числа транспозиций.*

Замечание. *Удобно считать, что произведением пустого множества сомножителей является единичный элемент, и поэтому тождественная подстановка может рассматриваться как произведение 0 транспозиций.*

Доказательство. По теореме 1, достаточно доказать, что любой цикл раскладывается в произведение транспозиций. Как мы только что отметили, цикл (x) – произведение пустого множества транспозиций, а при $k \geq 2$ мы имеем следующее разложение цикла длины k в произведение транспозиций:

$$(x_1, x_2, \dots, x_{k-1}, x_k) = (x_1, x_2)(x_2, x_3) \dots (x_{k-2}, x_{k-1})(x_{k-1}, x_k).$$

Отметим, что в отличие от разложения подстановки в произведение непересекающихся циклов, разложение подстановки в произведение транспозиций неоднозначно; например, $(1, 2)(1, 3) = (2, 3)(1, 2) = (2, 4)(3, 4)(1, 2)(1, 4)$. Как мы видим, даже число сомножителей может быть различным.

Пусть опять X – конечное множество, и пусть n – число его элементов. По теореме 1, всякая подстановка $\sigma \in S_X$ представляется в виде произведения попарно неперересекающихся циклов, причем каждый элемент из X принадлежит одному из циклов; обозначим через $k(\sigma)$ количество этих циклов. Знаком подстановки σ называется число $\operatorname{sgn}(\sigma) = (-1)^{n+k(\sigma)}$.

Теорема 3. *Пусть X – конечное множество. Для любых подстановок $\sigma, \tau \in S_X$ справедливо соотношение* $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

Лемма 1. *Если τ – транспозиция, то* $\operatorname{sgn}(\tau) = -1$.

Доказательство. Пусть $\tau = (x, y)$, и пусть $z_2, \dots, z_{n-2}$ – все элементы из X, отличные от x, y. Тогда $\tau = (x, y)(z_1) \dots (z_{n-2})$. Таким образом, $k(\tau) = n - 1$ и $\operatorname{sgn}(\tau) = (-1)^{n+(n-1)} = -1$.

Лемма 2. *Если τ – транспозиция, то для любой подстановки $\sigma \in S_X$ справедливо соотношение* $\operatorname{sgn}(\sigma\tau) = -\operatorname{sgn}(\sigma)$.

Доказательство. Очевидно, достаточно доказать, что $k(\sigma\tau) = k(\sigma) \pm 1$. Пусть $\tau = (x, y)$, $\sigma = \alpha_1\alpha_2 \dots \alpha_k$, где $\alpha_1, \dots, \alpha_k$ – попарно не пересекающиеся циклы, объединение которых совпадает со всем множеством X (так что $k = k(\sigma)$). Возможны два случая.

Случай 1. Элементы x, y принадлежат одному циклу. Меняя, если нужно, нумерацию циклов, мы можем считать, что x и y принадлежат циклу α_k, т.е. что $\alpha_k = (x, z_1, \dots, z_r, y, u_1, \dots, u_l)$. Тогда

$$\begin{aligned}\sigma\tau &= \alpha_1 \dots \alpha_{k-1}(x, z_1, \dots, z_r, y, u_1, \dots, u_l)(x, y) = \\ &= \alpha_1 \dots \alpha_{k-1}(x, u_1, \dots, u_l)(y, z_1, \dots, z_r).\end{aligned}$$

В последнем произведении все циклы попарно не пересекаются, и каждый элемент из X принадлежит какому-то из циклов; поэтому $k(\sigma\tau) = k + 1 = k(\sigma) + 1$.

Случай 2. Элементы x, y принадлежат разным циклам. Меняя, если необходимо, нумерацию циклов, мы можем считать, что элемент x принадлежит циклу $\alpha_{k-1} = (x, u_1, \dots, u_l)$, а элемент y – циклу $\alpha_k = (y, z_1, \dots, z_r)$. Тогда

$$\begin{aligned}\sigma\tau &= \alpha_1 \dots \alpha_{k-2}(x, u_1, \dots, u_l)(y, z_1, \dots, z_r)(x, y) = \\ &= \alpha_1 \dots \alpha_{k-2}(x, z_1, \dots, z_r, y, u_1, \dots, u_l).\end{aligned}$$

В последнем произведении все циклы попарно не пересекаются, и каждый элемент из X принадлежит какому-то из циклов; поэтому $k(\sigma\tau) = k - 1 = k(\sigma) - 1$.

Лемма 3. *Если $\sigma \in S_X$ – произведение r транспозиций (не обязательно попарно не пересекающихся), то $\operatorname{sgn}(\sigma) = (-1)^r$.*

Доказательство. Индукция по r; при $r = 1$ наше утверждение совпадает с леммой 1. Пусть $\sigma = \tau_1 \dots \tau_r$, где $r > 1$ и $\tau_1, \dots, \tau_r$ – транспозиции, и пусть уже доказано, что $\operatorname{sgn}(\tau_1 \dots \tau_{r-1}) = (-1)^{r-1}$. По лемме 2

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1 \dots \tau_{r-1}\tau_r) = -\operatorname{sgn}(\tau_1 \dots \tau_{r-1}) = -(-1)^{r-1} = (-1)^r.$$

Доказательство теоремы 3. По теореме 2, подстановки σ и τ раскладываются в произведения транспозиций. Пусть σ – произведение l транспозиций, а τ – произведение r транспозиций; тогда $\sigma\tau$ – произведение $l + r$ транспозиций. По лемме 3,

$$\operatorname{sgn}(\sigma\tau) = (-1)^{l+r} = (-1)^l(-1)^r = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau).$$

Следствие. *Если одна и та же подстановка σ представлена в виде произведения r транспозиций и l транспозиций, то числа r и l имеют одинаковую четность.*

Доказательство. По лемме 3, $(-1)^r = \operatorname{sgn}(\sigma) = (-1)^l$.

До сих пор множество X, на котором действуют подстановки из S_X, было произвольным. Теперь мы будем считать, что $X = \{1, 2, \dots, n\}$; напомним, что в этом случае мы обозначаем группу подстановок через S_n. На множестве $\{1, 2, \dots, n\}$ есть естественный порядок, и это позволяет дать другой способ вычисления знака подстановки, не требующий предварительного разложения подстановки в произведение циклов или транспозиций. Упорядоченная последовательность целых чисел $i_1, \dots, i_n$ называется перестановкой множества $\{1, 2, \dots, n\}$, если все эти числа различны и заключены между 1 и n. Таким образом, среди чисел $i_1, \dots, i_n$ встречаются все числа $1, \dots, n$, причем каждое ровно по одному разу. Мы говорим, что элементы i_s, i_t образуют инверсию в перестановке $i_1, i_2, \dots, i_n$, если числа $s-t$, $i_s - i_t$ разных знаков, т.е. большее число предшествует меньшему. Общее количество инверсий в перестановке $i_1, \dots, i_n$ обозначается через $I(i_1, \dots, i_n)$. Например, $I(3, 5, 1, 4, 2) = 6$: 3 образует инверсии с 1 и 2, 5 образует инверсии с 1, 2 и 4, 4 образует инверсию с 2.

Теорема 4. *Пусть $\sigma \in S_n$; тогда $\operatorname{sgn}(\sigma) = (-1)^{I(\sigma(1), \sigma(2), \dots, \sigma(n))}$.*

Доказательство. Докажем сначала две леммы.

Лемма 4. *Всякая подстановка $\sigma \in S_n$ может быть представлена в виде произведения транспозиций соседних элементов множества $\{1, 2, \ldots, n\}$ (т.е. транспозиций вида $(i, i+1)$, $1 \leq i < n$).*

Доказательство. По теореме 2 достаточно доказать, что любая транспозиция представляется в виде произведения транспозиций соседних элементов. Но это так: если $i < j$, то

$$(j,i)=(i,j)=(i,i+1)(i+1,i+2)\ldots(j-2,j-1)(j-1,j)(j-2,j-1)\ldots(i+1,i+2)(i,i+1).$$

Лемма 5. *Если $\sigma \in S_n$, а τ – транспозиция соседних элементов, то*

$$I(\sigma\tau(1), \sigma\tau(2), \ldots, \sigma\tau(n)) = I(\sigma(1), \sigma(2), \ldots, \sigma(n)) \pm 1.$$

Доказательство. Пусть $\tau = (s, s+1)$; для любого t обозначим число $\sigma(t)$ через i_t; тогда $\sigma\tau(t) = i_t$, если $t \neq s, s+1$, $\sigma\tau(s+1) = i_s$, $\sigma\tau(s) = i_{s+1}$. Таким образом, нам надо сравнить перестановки

$$i_1, i_2, \ldots, i_s, i_{s+1}, \ldots, i_n \qquad \text{и} \qquad i_1, i_2, \ldots, i_{s+1}, i_s, \ldots, i_n.$$

Если хотя бы один из индексов t, u не равен s или $s+1$, то элементы i_t, i_u одновременно образуют или не образуют инверсию в обеих подстановках, а если элементы i_s, i_{s+1} образуют инверсию в одной из перестановок, то они не образуют инверсию в другой, и наоборот. Итак, количества инверсий в наших перестановках отличаются на 1, т.е.

$$I(\sigma\tau(1), \sigma\tau(2), \ldots, \sigma\tau(n)) - I(\sigma(1), \sigma(2), \ldots, \sigma(n)) =$$
$$= I(i_1, i_2, \ldots, i_s, i_{s+1}, \ldots, i_n) - I(i_1, i_2, \ldots, i_{s+1}, i_s, \ldots, i_n) = \pm 1.$$

Теперь легко завершить доказательство теоремы. По лемме 4 подстановка σ раскладывается в произведение $\tau_1\tau_2\ldots\tau_r$, каждый сомножитель τ_i которого – транспозиция соседних элементов. Положим $\sigma_p = \tau_1\tau_2\ldots\tau_p$ $(0 \leq p \leq r)$, так что $\sigma = \sigma_r$. При этом, конечно, мы считаем, что σ_0 – тождественная подстановка. Ясно, что $I(\sigma_0(1), \sigma_0(2), \ldots, \sigma_0(n)) = I(1, 2, \ldots, n) = 0$, а из леммы 5 следует, что для любого $p \geq 1$ разность

$$\varepsilon_p = I(\sigma_p(1), \sigma_p(2), \ldots, \sigma_p(n)) - I(\sigma_{p-1}(1), \sigma_{p-1}(2), \ldots, \sigma_{p-1}(n))$$

равна 1 или -1. Поэтому $I(\sigma(1), \sigma(2), \ldots, \sigma(n)) = \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_r = r - 2l$, где l – количество тех ε_p, которые равны -1. Воспользовавшись леммой 3, получаем желаемый результат:

$$\operatorname{sgn}(\sigma) = (-1)^r = (-1)^{r-2l} = (-1)^{I(\sigma(1), \sigma(2), \ldots, \sigma(n))}.$$