поэтому к системе применимо правило Крамера. Числителями для неизвестных будут определители

$$d_1=\begin{vmatrix}0 & -1 & 1\\ 1 & 2 & -5\\ 4 & 3 & -2\end{vmatrix}=13,\quad d_2=\begin{vmatrix}2 & 0 & 1\\ 3 & 1 & -5\\ 1 & 4 & -2\end{vmatrix}=47,$$

$$d_3=\begin{vmatrix}2 & -1 & 0\\ 3 & 2 & 1\\ 1 & 3 & 4\end{vmatrix}=21,$$

т. е. решением системы служит система чисел

$$x_1=\frac{13}{28},\quad x_2=\frac{47}{28},\quad x_3=\frac{21}{28}=\frac{3}{4}.$$

§ 3. Перестановки и подстановки

Для определения и изучения определителей порядка n нам будут нужны некоторые понятия и факты, относящиеся к конечным множествам. Пусть дано некоторое конечное множество M, состоящее из n элементов. Эти элементы могут быть перенумерованы при помощи первых n натуральных чисел $1, 2, \ldots, n$, и так как в интересующих нас вопросах индивидуальные свойства элементов множества M не будут играть никакой роли, то мы просто примем, что элементами M служат сами эти числа $1, 2, \ldots, n$.

Помимо употребляющегося нами расположения чисел $1, 2, \ldots, n$ в их нормальном порядке, их можно упорядочить и многими другими способами. Так, числа 1, 2, 3, 4 можно расположить также следующими способами: 3, 1, 2, 4 или 2, 4, 1, 3 и т. д. Всякое расположение чисел $1, 2, \ldots, n$ в некотором определенном порядке называется *перестановкой* из n чисел (или из n символов).

Число различных перестановок из n символов равно произведению $1\cdot 2\ldots n$, обозначаемому $n!$ (читается: «эн-факториал»). Действительно, общий вид перестановки из n символов есть $i_1, i_2, \ldots, i_n$, где каждое из i_s есть одно из чисел $1, 2, \ldots, n$, причем ни одно из этих чисел не встречается дважды. В качестве i_1 можно взять любое из чисел $1, 2, \ldots, n$; это дает n различных возможностей. Если, однако, i_1 уже выбрано, то в качестве i_2 можно взять лишь одно из оставшихся $n-1$ чисел, т. е. число различных способов выбрать символы i_1 и i_2 равно произведению $n(n-1)$ и т. д.

Таким образом, число перестановок из n символов при $n=2$ равно $2!=2$ (перестановки 12 и 21; мы не будем в примерах, где $n\leqslant 9$, разделять переставляемые символы запятыми); при $n=3$ это число равно $3!=6$, при $n=4$ оно равно $4!=24$. Далее, с ростом n число перестановок чрезвычайно быстро возрастает; так, при $n=5$ оно равно $5!=120$, а при $n=10$ — уже 3 628 800.

Если в некоторой перестановке мы поменяем местами какие-либо два символа (не обязательно стоящие рядом), а все остальные сим-

волы оставим на месте, то получим, очевидно, новую перестановку. Это преобразование перестановки называется *транспозицией*.

Все $n!$ перестановок из n символов можно расположить в таком порядке, что каждая следующая будет получаться из предыдущей одной транспозицией, причем начинать можно с любой перестановки.

Это утверждение справедливо при $n=2$: если требуется начинать с перестановки 12, то искомое расположение будет 12, 21; если же мы должны начать с перестановки 21, то это будет расположение 21, 12. Предположим, что наше утверждение уже доказано для $n-1$, и докажем его для n. Пусть мы должны начать с перестановки

$$i_1, i_2, \ldots, i_n. \tag{1}$$

Рассмотрим все перестановки из n символов, у которых на первом месте стоит i_1. Таких перестановок $(n-1)!$ и их можно упорядочить в согласии с требованиями теоремы, притом начиная с перестановки (1), так как это сводится на самом деле к упорядочению всех перестановок из $n-1$ символов, которое, по индуктивному предположению, можно начать с любой перестановки, в частности с перестановки $i_2, \ldots, i_n$. В последней из полученных таким путем перестановок из n символов совершаем транспозицию символа i_1 с любым другим символом, например с i_2, и, начиная с вновь полученной перестановки, упорядочиваем нужным образом все те перестановки, у которых на первом месте стоит i_2, и т. д. Этим путем можно, очевидно, перебрать все перестановки из n символов.

Из этой теоремы вытекает, что *от любой перестановки из n символов можно перейти к любой другой перестановке из тех же символов при помощи нескольких транспозиций.*

Говорят, что в данной перестановке числа i и j составляют *инверсию*, если $i>j$, но i стоит в этой перестановке раньше j. Перестановка называется *четной*, если ее символы составляют четное число инверсий, и *нечетной*—в противоположном случае. Так, перестановка $1, 2, \ldots, n$ будет четной при любом n, так как число инверсий в ней равно нулю. Перестановка 451362 ($n=6$) содержит 8 инверсий и поэтому четная. Перестановка 38524671 ($n=8$) содержит 15 инверсий и поэтому нечетная.

Всякая транспозиция меняет четность перестановки.

Для доказательства этой важной теоремы рассмотрим сначала случай, когда транспонируемые символы i и j стоят рядом, т. е. перестановка имеет вид $\ldots, i, j, \ldots$, где многоточия заменяют те символы, которые не затрагиваются транспозицией. Транспозиция превращает нашу перестановку в перестановку $\ldots, j, i, \ldots$, причем, понятно, в обеих перестановках каждый из символов i, j составляет одни и те же инверсии с символами, остающимися на месте. Если символы i и j раньше не составляли инверсии, то

в новой перестановке появляется одна новая инверсия, т. е. число инверсий увеличивается на единицу; если же они раньше составляли инверсию, то теперь она пропадает, т. е. число инверсий на единицу уменьшается. В обоих случаях четность перестановки меняется.

Пусть теперь между транспонируемыми символами i и j расположены s символов, $s>0$, т. е. перестановка имеет вид

$$\ldots,\ i,\ k_1,\ k_2,\ \ldots,\ k_s,\ j,\ \ldots \tag{2}$$

Транспозицию символов i и j можно получить в результате последовательного выполнения $2s+1$ транспозиций соседних элементов. А именно, это будут транспозиции, переставляющие символы i и k_1, затем i (уже стоящие на месте символа k_1) и k_2 и т. д., пока i не займет место символа k_s. За этими s транспозициями следует транспозиция, перемещающая символы i и j, а затем s транспозиций символа j со всеми k, после чего j занимает место символа i, а символы k возвращаются на свои старые места. Таким образом, мы нечетное число раз меняли четность перестановки, а поэтому перестановки (2) и

$$\ldots,\ j,\ k_1,\ k_2,\ \ldots,\ k_s,\ i,\ \ldots \tag{3}$$

имеют противоположные четности.

При $n\geqslant 2$ *число четных перестановок из n символов равно числу нечетных, т. е. равно* $\frac{1}{2}n!$.

В самом деле, упорядочим, на основании доказанного ранее, все перестановки из n символов так, что каждая получается из предыдущей одной транспозицией. Соседние перестановки будут иметь противоположные четности, т. е. перестановки расположены так, что четные и нечетные чередуются. Наше утверждение вытекает теперь из очевидного замечания, что при $n\geqslant 2$ число $n!$ четно.

Определим теперь одно новое понятие, а именно понятие *подстановки n-й степени*. Запишем одну под другой две перестановки из n символов, беря полученные две строки в скобки; например, при $n=5$:

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

В этом примере[1]) под числом 3 стоит число 5, под числом 5 — число 2 и т. д. Мы скажем, что число 3 *переходит* в 5, число 5 переходит в 2, число 1 переходит в 3, число 4 переходит в 4 (или *остается на месте*) и, наконец, число 2 переходит в 1. Таким образом, две перестановки, записанные друг под другом в виде (4), определяют некоторое *взаимно однозначное отображение* множества из первых пяти натуральных чисел на себя, т. е. отображе-

[1]) Внешне он напоминает матрицу из двух строк и 5 столбцов, но имеет совсем иной смысл.

ние, которое каждому из натуральных чисел 1, 2, 3, 4, 5 ставит в соответствие одно из этих же натуральных чисел, причем разным числам ставятся в соответствие различные же числа. При этом, так как чисел всего пять, т. е. конечное множество, каждое из этих пяти чисел будет соответствовать одному из чисел 1, 2, 3, 4, 5, а именно числу, которое в него «переходит».

Ясно, что то взаимно однозначное отображение множества из первых пяти натуральных чисел, которое мы получили при помощи (4), можно было бы получить, записывая одну под другой и некоторые другие пары перестановок из пяти символов. Эти записи получаются из (4) путем нескольких транспозиций столбиков; таковы, например,

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

Во всех этих записях 3 переходит в 5, 5 в 2, и т. д.

Аналогичным путем две перестановки из n символов, записанные одна под другой, определяют некоторое взаимно однозначное отображение множества первых n натуральных чисел на себя. Всякое взаимно однозначное отображение A множества первых n натуральных чисел на себя называется *подстановкой n-й степени*, причем, очевидно, всякая подстановка A может быть записана при помощи двух перестановок, подписанных одна под другой

$$A = \begin{pmatrix} i_1, & i_2, & \ldots, & i_n \\ \alpha_{i_1}, & \alpha_{i_2}, & \ldots, & \alpha_{i_n} \end{pmatrix}; \tag{6}$$

через α_i здесь обозначается то число, в которое при подстановке A переходит число i, $i = 1, 2, \ldots, n$.

Подстановка A обладает многими различными записями вида (6). Так, (4) и (5) являются различными записями одной и той же подстановки 5-й степени.

От одной записи подстановки A к другой можно перейти при помощи нескольких транспозиций столбиков. При этом можно получить такую запись вида (6), в верхней (или нижней) строке которой стоит любая наперед заданная перестановка из n символов. В частности, всякая подстановка n-й степени A может быть записана в виде

$$A = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \end{pmatrix}, \tag{7}$$

т. е. с натуральным расположением чисел в верхней строке. При такой записи различные подстановки отличаются друг от друга перестановками, стоящими в нижней строке, и поэтому *число подстановок n-й степени равно числу перестановок из n символов, т. е. равно $n!$*

Примером подстановки n-й степени служит *тождественная подстановка*

$$E=\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix},$$

при которой на месте остаются все символы.

Следует заметить, что верхняя и нижняя строки в записи (6) подстановки A играют разные роли и, переставив их, мы, вообще говоря, получаем другую подстановку. Так, подстановки 4-й степени

$$\begin{pmatrix}2 & 1 & 4 & 3\\ 4 & 3 & 1 & 2\end{pmatrix} \text{ и } \begin{pmatrix}4 & 3 & 1 & 2\\ 2 & 1 & 4 & 3\end{pmatrix}$$

различны: при первой число 2 переходит в 4, при второй — в 3.

Возьмем произвольную запись (6) некоторой подстановки n-й степени A. Перестановки, составляющие верхнюю и нижнюю строки этой записи, могут иметь или одинаковые, или противоположные четности. Переход к любой другой записи подстановки A можно осуществить, как мы знаем, путем последовательного выполнения нескольких транспозиций в верхней строке и соответствующих им транспозиций в нижней строке. Однако, совершая одну транспозицию в верхней строке записи (6) и одну транспозицию соответствующих элементов в нижней строке, мы одновременно меняем четности обеих перестановок и поэтому сохраняем совпадение или противоположность этих четностей. Отсюда следует, что *либо при всех записях подстановки A четности верхней и нижней строк совпадают, либо же при всех записях они противоположны.* В первом случае подстановка A будет называться *четной*, во втором — *нечетной*. В частности, тождественная подстановка будет четной.

Если подстановка A записана в виде (7), т. е. в верхней строке стоит четная перестановка $1, 2, \dots, n$, то четность подстановки A будет определяться четностью перестановки $\alpha_1, \alpha_2, \dots, \alpha_n$, стоящей в нижней строке. Отсюда следует, что *число четных подстановок n-й степени равно числу нечетных, т. е. равно $\frac{1}{2}n!$.*

Определению четности подстановок можно дать следующую несколько измененную форму. Если в записи (6) четности обеих строк совпадают, то число инверсий или в обеих строках четное, или в обеих нечетное, т. е. общее число инверсий в двух строках записи (6) будет четным; если же четности строк записи (6) противоположны, то общее число инверсий в этих двух строках нечетно. Таким образом, *подстановка A будет четной, если общее число инверсий в двух строках любой ее записи четно, и нечетной — в противоположном случае.*

Пример. Пусть дана подстановка пятой степени

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

В ее верхней строке 4 инверсии, в нижней 7 инверсий. Общее число инверсий в двух строках есть 11, и поэтому подстановка нечетна.

Перепишем эту подстановку в виде

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

Число инверсий в верхней строке есть 0, в нижней 5, т. е. общее число снова нечетно. Мы видим, что при разных записях подстановки сохраняется четность общего числа инверсий, но не само это число.

Мы хотим указать теперь другие формы определения четности подстановок, эквивалентные приведенным выше[1]). Для этой цели определим *умножение подстановок*, представляющее и само по себе очень большой интерес. Подстановка n-й степени есть, как мы знаем, взаимно однозначное отображение множества чисел $1, 2, \ldots, n$ на себя. Результат последовательного выполнения двух взаимно однозначных отображений множества $1, 2, \ldots, n$ на себя снова будет, очевидно, некоторым взаимно однозначным отображением этого множества на себя, т. е. последовательное выполнение двух подстановок n-й степени приводит к некоторой вполне определенной третьей подстановке n-й степени, называемой *произведением* первой из заданных подстановок на вторую. Так, если даны подстановки четвертой степени

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix},$$

то

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

Действительно, при подстановке A символ 1 переходит в 3, но при B символ 3 переходит в 4, поэтому при AB символ 1 переходит в 4, и т. д.

Можно перемножить лишь подстановки одинаковой степени. *Умножение подстановок n-й степени при $n \geqslant 3$ некоммутативно.* Действительно, для рассмотренных выше подстановок A и B произведение BA имеет вид

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

т. е. подстановка BA отлична от подстановки AB. Такие примеры можно подобрать для всех n при $n \geqslant 3$, хотя для некоторых пар подстановок закон коммутативности случайно может выполняться.

---

[1]) Они потребуются нам лишь в главе 14, и поэтому при первом чтении этот материал можно опустить.

Умножение подстановок ассоциативно, т. е. можно говорить о произведении любого конечного числа подстановок n-й степени, взятых (ввиду некоммутативности) в определенном порядке. В самом деле, пусть даны подстановки A, B и C и пусть символ i_1, $1 \leqslant i_1 \leqslant n$, переходит при подстановке A в символ i_2, i_2 при подстановке B переходит в символ i_3, а последний при подстановке C — в символ i_4. Тогда при подстановке AB символ i_1 переходит в i_3, при подстановке BC символ i_2 переходит в i_4, а поэтому как при $(AB)C$, так и при $A(BC)$ символ i_1 будет переходить в символ i_4.

Очевидно, что *произведение любой подстановки A на тождественную подстановку E, а также произведение E на A, равно A*:

$$AE = EA = A.$$

Назовем, наконец, *обратной* для подстановки A такую подстановку A^{-1} той же степени, что

$$AA^{-1} = A^{-1}A = E.$$

Легко видеть, что обратной для подстановки

$$A = \begin{pmatrix} 1 & 2 & \dots & n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$$

служит подстановка

$$A^{-1} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ 1 & 2 & \dots & n \end{pmatrix},$$

получающаяся из A переменой мест верхней и нижней строк.

Рассмотрим теперь подстановки специального вида, получающиеся из тождественной подстановки E при помощи одной транспозиции, производимой в ее нижней строке. Такие подстановки нечетны: они называются *транспозициями* и имеют вид

$$\begin{pmatrix} \dots & i & \dots & j & \dots \\ \dots & j & \dots & i & \dots \end{pmatrix}, \tag{8}$$

где многоточиями заменены символы, остающиеся на месте. Условимся обозначать эту транспозицию символом (i, j). Применение транспозиции символов i, j к нижней строке записи (7) произвольной подстановки A равносильно умножению подстановки A справа на подстановку (8), т. е. на (i, j). Мы знаем, что все перестановки из n символов можно получить из одной из них, например из $1, 2, \dots, n$, последовательным выполнением транспозиций; поэтому всякая подстановка может быть получена из тождественной подстановки путем последовательного выполнения нескольких транспозиций в нижней строке, т. е. путем последовательного умножения на подстановки вида (8). Можно утверждать, следовательно (опуская множитель E), что *всякая подстановка представима в виде произведения транспозиций.*

Всякую подстановку можно многими разными способами разложить в произведение транспозиций. Всегда можно, например, добавить два одинаковых множителя вида (i, j) (i, j), которые дают в произведении подстановку E, т. е. взаимно уничтожаются. Укажем менее тривиальный пример:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} = (12)\,(15)\,(34) = (14)\,(24)\,(45)\,(34)\,(13).$$

Новый способ определения четности подстановки основан на следующей теореме:

При всех разложениях подстановки в произведение транспозиций четность числа этих транспозиций будет одна и та же, причем она совпадает с четностью самой подстановки.

Так, подстановка в рассмотренном выше примере будет нечетной, как можно проверить и подсчетом числа инверсий.

Эта теорема будет доказана, если мы покажем, что *произведение любых k транспозиций есть подстановка, четность которой совпадает с четностью числа k.* При $k=1$ это верно, так как транспозиция есть нечетная подстановка. Пусть наше утверждение уже доказано для случая $k-1$ множителей. Тогда его справедливость для k множителей вытекает из того, что числа $k-1$ и k имеют противоположные четности, а умножение подстановки (в данном случае — произведения первых $k-1$ множителей) на транспозицию равносильно выполнению этой транспозиции в нижней строке подстановки, т. е. меняет ее четность.

Удобным способом записи подстановок, позволяющим легко находить их четность, является *разложение в циклы.* Всякая подстановка n-й степени может некоторые из символов 1, 2, ..., n оставлять на месте, другие же действительно перемещать. *Циклической подстановкой* или *циклом* называется такая подстановка, что при повторении ее достаточное число раз всякий из действительно перемещаемых ею символов может быть переведен в любой другой из этих символов. Такова, например, подстановка восьмой степени

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

она действительно перемещает символы 2, 3, 6 и 8, причем переводит символ 2 в 8, символ 8 в 3, символ 3 в 6, а символ 6 снова в 2.

К числу циклов принадлежат все транспозиции. По аналогии с употребленной выше сокращенной записью транспозиций, для циклов употребляется следующая запись: действительно переставляемые символы записываются в круглых скобках друг за другом в том порядке, в каком они друг в друга переходят при повторении подстановки; начинается запись с любого из действительно перемещаемых символов, а последний символ считается переходящим в первый. Так, для указанного выше примера эта запись имеет вид

$$(2\ 8\ 3\ 6).$$

Число символов, действительно перемещаемых циклом, называется *длиной* цикла.

Два цикла n-й степени называются *независимыми*, если они не имеют общих действительно переставляемых символов. Понятно, что при перемножении независимых циклов порядок множителей не влияет на результат.

Всякая подстановка может быть единственным способом разложена в произведение попарно независимых циклов. Доказательство этого утверждения не представляет затруднений, и мы его опускаем. Практически разложение осуществляется следующим образом: начинаем с любого из действительно перемещаемых символов и выписываем за ним те символы, в которые он переходит при повторении подстановки, пока не вернемся к исходному символу. После этого «закрытия» цикла начинаем с одного из оставшихся действительно перемещаемых символов, получаем второй цикл и т. д.

Примеры.

1) $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix} = (13)\,(254).$$

2) $$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 8 & 7 & 6 & 1 & 4 & 3 \end{pmatrix} = (156)\,(38)\,(47).$$

Обратно, для всякой подстановки, заданной разложением в независимые циклы, можно найти запись в обычной форме (при условии, что степень этой подстановки известна). Например,

3) $$(1372)\,(45) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 7 & 5 & 4 & 6 & 2 \end{pmatrix},$$

если известно, что степень этой подстановки есть 7.

Пусть дана подстановка n-й степени и пусть s есть число независимых циклов в ее разложении плюс число символов, оставляемых ею на месте[1]). Разность $n-s$ называется *декрементом* этой подстановки. Декремент равен, очевидно, числу действительно перемещаемых символов, уменьшенному на число независимых циклов, входящих в разложение подстановки. Для рассмотренных выше примеров 1), 2) и 3) декремент будет равен соответственно 3, 4 и 4.

Четность подстановки совпадает с четностью декремента этой подстановки.

Действительно, всякий цикл длины k можно следующим образом представить в виде произведения $k-1$ транспозиций:

$$(i_1, i_2, \ldots, i_k) = (i_1, i_2)\,(i_1, i_3)\ldots(i_1, i_k).$$

Предположим теперь, что дано разложение подстановки A в независимые циклы. Если каждый из циклов будет разложен указанным сейчас способом в произведение транспозиций, то мы получим представление подстановки A в виде произведения транспозиций. Число этих транспозиций будет, очевидно, меньше числа символов, действительно перемещаемых подстановкой A, на число, равное числу независимых циклов в разложении этой подстановки. Отсюда следует, что подстановку A можно разложить в произведение транспозиций, число которых равно декременту, а поэтому четность подстановки определяется четностью декремента.

---

[1]) Всякому символу, оставляемому подстановкой на месте, можно было бы поставить в соответствие «цикл» длины 1, т. е., например, в указанном выше примере 2) писать: (156) (38) (47) (2). Мы не будем, однако, этого делать.