Росошек Семен Константинович

ГРУППЫ: ВЗГЛЯД СО СТОРОНЫ КОМПЬЮТЕРНОЙ ПРОГРАММЫ VISAL

ВВЕДЕНИЕ

В информационном обществе абстрактные алгебраические структуры играют все более заметную роль для обработки и защиты информационных потоков. В частности, для современной криптографии базовыми структурами представления данных являются кольца классов вычетов, конечные поля и группы. Поэтому изучение этих алгебраических структур становится важной составляющей математического образования.

1. НЕКОТОРЫЕ ПРИМЕРЫ ИЗ КРИПТОГРАФИИ

Предположим, что мы хотим передать некоторую конфиденциальную информацию по компьютерной сети, например, ALGEBRA IS POWERFUL THING. Занумеруем позиции букв в исходном тексте, предварительно разбив его на блоки длины n, скажем, $n = 10$ в нашем примере. Получаем, рассматривая пробел как отдельный символ «_»:

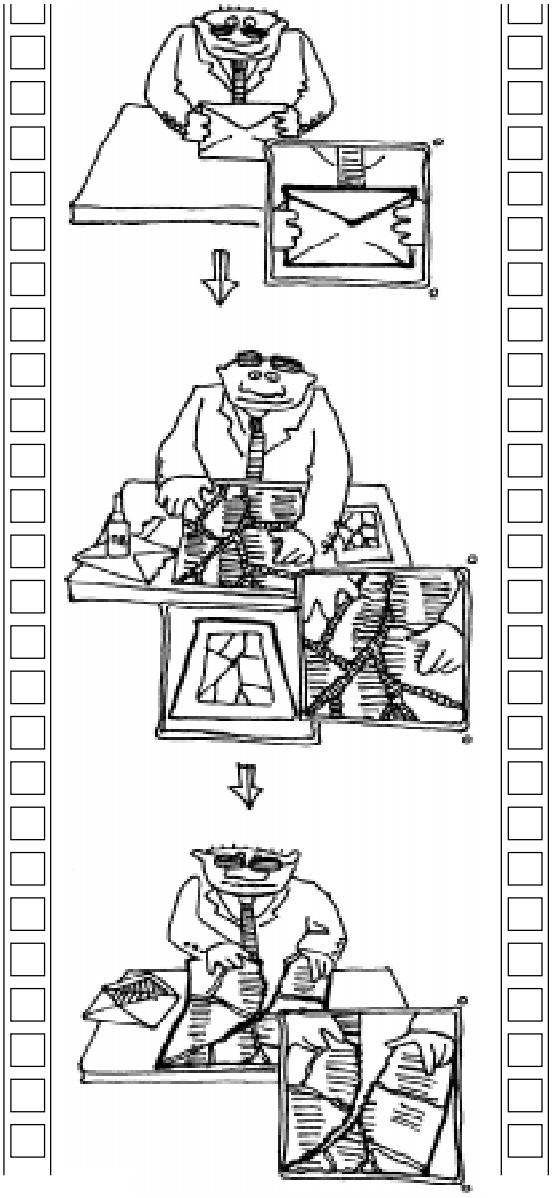
A L G E B R A _ I S
1 2 3 4 5 6 7 8 9 10

_ P O W E R F U L _
1 2 3 4 5 6 7 8 9 10

T H I N G A L G E B
1 2 3 4 5 6 7 8 9 10

(здесь в третьем блоке добавлены недостающие пять символов до полного блока посредством первых пяти символов из первого блока). Каждый блок шифруется отдельно. Запишем теперь таблицу из двух строк, где верхняя строка содержит номера символов при первоначальном их расположении, а нижняя строка – номера символов при некоторой их перестановке, например: 10, 6, 3, 9, 1, 5, 2, 7, 4, 8.

Предположим, что мы хотим передать некоторую конфиденциальную информацию...



Эта перестановка осуществляет дешифровку криптограммы...

Таблицу из двух строк, в которой одна из строк упорядочена, а вторая является перестановкой чисел первой строки, будем также называть перестановкой.[1] Например:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 10 & 6 & 3 & 9 & 1 & 5 & 2 & 7 & 4 & 8 \end{pmatrix}$$

Будем интерпретировать стрелки в этой таблице следующим образом: 1 переходит в 10, 2 переходит в 6, 3 переходит в 3 и т.д. Это означает, что символ *A*, находящийся на первой позиции в блоке, будет занимать теперь десятую позицию, символ L, находящийся на второй позиции в блоке, будет занимать теперь шестую позицию и т. д. Таким образом, получим первый блок криптограммы: BAGIRL_SEA. Применяя ко второму и третьему блокам исходного текста такую же перестановку, что и в первом блоке, получим второй и третий блоки криптограммы: EFOLRPU_W_ и GLIEAHGBNT. Таким образом, криптограмма имеет вид: BAGIRL_SEAEFOLRPU_W_GLIEAHGBNT. Приведенная выше перестановка представляет собой секретный ключ использованного шифра (здесь и далее стрелки в перестановках опускаются). Покажем теперь, как, зная секретный ключ, расшифровать криптограмму.

Сначала расшифруем первый блок криптограммы. Для этого поменяем местами верхнюю и нижнюю строки перестановки-ключа, получим перестановку

$$\begin{pmatrix} 10 & 6 & 3 & 9 & 1 & 5 & 2 & 7 & 4 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix},$$

а после перестановки столбцов этой таблицы так, чтобы верхняя строка была упорядочена, получим

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 7 & 3 & 9 & 6 & 2 & 8 & 10 & 4 & 1 \end{pmatrix}.$$

Эта перестановка осуществляет дешифровку криптограммы. В частности, применяя ее к первому блоку криптограммы, получим первый блок исходного текста: ALGEBRA_IS. Аналогично расшифровываются остальные блоки криптограммы.

Для повышения надежности шифра можно пытаться применить различные методы, например, повторное шифрование посредством другой перестановки. Последовательное выполнение двух перестановок также является перестановкой, которая называется их произведением. На-

[1] Автор статьи здесь и далее использует термин «перестановка» вместо принятого в литературе термина «подстановка».

пример, пусть даны перестановки

$$X=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\10&6&3&9&1&5&2&7&4&8\end{pmatrix}$$

и

$$Y=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\3&8&1&5&2&4&10&6&9&7\end{pmatrix}.$$

Их произведение находится так: в перестановке X число 1 переходит в число 10, а в перестановке Y число 10 переходит в число 7, тогда в перестановке XY число 1 переходит в число 7 и т. д. Следовательно, перестановка XY имеет вид:

$$X\cdot Y=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\7&4&1&9&3&2&8&10&5&6\end{pmatrix}$$

Замечание. Повышение надежности шифра связано с тем, что «периоды» первой и второй шифровки могут быть различными. Например, если первая шифровка связана с перестановкой десяти элементов, а вторая – одиннадцати, то «перемножать» придется перестановки из 110 символов.

Найдем теперь произведение перестановок, осуществлявших шифрование и дешифрование в приведенном выше примере:

$$\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\10&6&3&9&1&5&2&7&4&8\end{pmatrix}\cdot$$

$$\cdot\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\5&7&3&9&6&2&8&10&4&1\end{pmatrix}=$$

$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\1&2&3&4&5&6&7&8&9&10\end{pmatrix}$$

Перестановка, полученная в результате этого произведения, называется *тождественной перестановкой*. Перестановка, произведение которой с данной перестановкой A равно тождественной перестановке, называется *обратной перестановкой* к перестановке A и обозначается A^{-1}. Таким образом, если перестановка A является ключом шифрования, то перестановка A^{-1} является ключом дешифрования. Отметим также, что если применяется тройное шифрование посредством трех перестановок A, B и C, то, как легко проверить, результат не зависит от расстановки скобок: $A(BC) = (AB)C$.

Соберем теперь вместе те сведения о перестановках на n элементах, которыми мы располагаем. Во-первых, для любых двух таких перестановок их произведение также будет перестановкой на n элементах. Во-вторых, произведение перестановок ассоциативно, то есть для любых трех перестановок A, B, C имеет место равенство $(AB)C = A(BC)$. В-третьих, существует нейтральный элемент E такой, что $AE = EA = A$. В-четвертых, для любой перестановки A существует обратная перестановка A^{-1} такая, что $AA^{-1} = A^{-1}A = E$.

Дадим теперь определение группы.

Определение. Множество G называется группой, если на множестве G задана алгебраическая операция, то есть указано соответствие, по которому любой упорядоченной паре элементов из множества G однозначным образом сопоставляется некоторый третий элемент из множества G. При этом выполняются условия:

1) операция является ассоциативной;

2) существует нейтральный элемент относительно заданной алгебраической операции;

3) для любого элемента множества G существует обратный элемент из этого же множества G.

Наиболее распространенные обозначения для групповой алгебраической операции – это «·» (произведение) и «+» (сложение).

Относительно произведения имеем так называемую мультипликативную запись:

1) для любых элементов x, y, z множества G

$$(x\cdot y)\cdot z = x\,(y\cdot z);$$

2) существует элемент $e \in G$ такой, что для любого элемента $x \in G$

$$e\cdot x = x\cdot e = x$$

(такой элемент e называется нейтральным элементом и обозначается 1_G);

3) для любого элемента $x \in G$ существует элемент $y \in G$ такой, что $x\cdot y = y\cdot x = e$ (такой элемент y называется обратным к элементу x и обозначается x^{-1}).

Обычно в мультипликативной записи групповой операции знак операции «·» не указывают, и мы в дальнейшем будем придерживаться этого соглашения.

Относительно сложения имеем так называемую аддитивную запись:

1) для любых элементов x, y, z множества G

$$x + (y + z) = (x + y) + z;$$

2) существует элемент $e \in G$ такой, что для любого элемента $x \in G$

$$e + x = x + e = x$$

(такой элемент e называется нейтральным и обозначается 0_G или просто 0);

3) для любого элемента $x \in G$ существует элемент $y \in G$ такой, что

$$x + y = y + x = 0$$

(такой элемент y называется обратным к элементу x и обозначается $-x$).

Удивительно, что каждый школьник умеет работать с некоторыми группами, не подозревая об этом.

Пример 1. Рассмотрим множество Z всех целых чисел относительно алгебраической операции сложения. Тогда имеем ассоциативность этой операции, нейтральный элемент 0, и для любого целого числа a есть обратный по сложению элемент $-a$ (который обычно называют противоположным к элементу a). Следовательно, Z является группой по сложению.

Пример 2. Аналогично примеру 1, проверяется, что множество Q всех рациональных чисел и множество R всех действительных чисел являются группами по сложению.

Пример 3. Рассмотрим множество Q^* всех ненулевых действительных чисел относительно алгебраической операции умножения. Эта операция ассоциативна, есть нейтральный элемент 1, и для любого ненулевого действительного элемента a есть обратный элемент $1/a$. Следовательно, Q^* является группой по умножению.

Пример 4. Множество $Z[x]$ целочисленных многочленов от одной переменной x является группой по сложению. Аналогично этому множества $Q[x]$ и $R[x]$ многочленов от одной переменной x с рациональными и действительными коэффициентами, соответственно, являются группами по сложению.

Пример 5. Множества ненулевых алгебраических дробей с рациональными или действительными коэффициентами, являются группами по умножению.

В примерах 1–5 групповые операции коммутативны, то есть $x + y = y + x$ – в аддитивной записи и $xy = yx$ – в мультипликативной записи.

Все указанные выше примеры групп являются бесконечными и не могут быть реализованы на компьютере. Подходящими для компьютерной реализации являются группы перестановок, о которых шла речь выше. На конечных множествах алгебраические операции задаются посредством таблицы Кэли, которая заполняется следующим образом. В строках и столбцах этой таблицы произвольным образом записываются элементы данного конечного множества. На пересечении строки, относящейся к элементу x, и столбца, относящегося к элементу y, записывается элемент данного множества, который равен результату алгебраической операции для элементов x и y.

Рассмотрим теперь, как создавать различные алгебраические операции, в том числе и групповые, посредством компьютерной программы VISAL. Множества с заданными на них алгебраическими операциями (одной или несколькими) называются алгебраическими структурами.

2. СОЗДАНИЕ АЛГЕБРАИЧЕСКИХ СТРУКТУР В ПРОГРАММЕ VISAL

Предположим, что мы хотим создать некоторую алгебраическую структуру посредством VISAL. Для этого необходимо зайти в меню File/New. Затем необходимо выбрать тип создаваемого объекта (Type of structure). Пусть мы выбрали Abstract group – абстрактную группу с именем Simple и числом элементов 5. Для ее задания необходимо заполнить таблицу Кэли. В программе VISAL предусмотрены два способа заполнения таблицы Кэли.

Первый способ состоит в последовательном заполнении всех клеточек таб-

лицы Кэли для всех упорядоченных пар элементов данного множества. Поскольку мы уже выбрали тип создаваемого объекта – абстрактную группу (Abstract group), то для задания параметров (Parameters) необходимо указать имя операции (Name of operation). Пусть это будет, скажем, Operation∗. Теперь остается заполнить таблицу Кэли (см. 3-ю страницу обложки) по следующей схеме. Пусть a_0, a_1, ..., a_{n-1} – элементы данного множества, тогда над таблицей и слева от таблицы Кэли выписываются индексы элементов множества, то есть 0, 1, ..., $n - 1$. Мы хотим определить результат операции ∗ для элементов a_i и a_j как элемент a_k, где $i, j, k \in \{0, 1, ..., n - 1\}$, то есть $a_i * a_j = a_k$. Тогда в клетке таблицы на пересечении i-ой строки (то есть строки, у которой слева от таблицы находится число i) и j-го столбца (то есть столбца, у которого сверху над таблицей находится число j), вместо *none,* записываем число k. Контроль правильности задания алгебраической операции осуществляется в поле Warnings в нижней части экрана. Если групповая алгебраическая операция задана, то в этом поле выдается сообщение No warnings. В случае ошибки, а именно, если нарушается ассоциативность операции либо существование нейтрального или обратных элементов, то в поле Warnings выдается соответствующее предупреждение.

3. РАБОТА С ГРУППАМИ ПЕРЕСТАНОВОК

Можно пытаться создавать группы, заполняя таблицы Кэли описанным выше способом. Однако вероятность получения группы посредством такого случайного поиска очень мала. Кроме того, после заполнения таблицы Кэли автоматически выдается информация о выполнении ассоциативности (Assoc.), наличии нейтрального элемента (Neutr.), обратных элементов (Revrs.), коммутативности (Commut.). По этой информации можно сразу определить, является созданная алгебраическая операция группой или нет. Большое число неудачных попыток построить группу может негативно сказаться на эффективности работы учащихся с компьютерной программой Visal. Чтобы избежать такой ситуации, предусмотрены специальные средства создания групп на некоторых подмножествах групп перестановок. Рассмотрим их подробнее.

Для работы с группами перестановок в программе VISAL есть пункт меню Tools\Exploration of Permutation Group, который предусматривает (см. 3-ю страницу обложки):

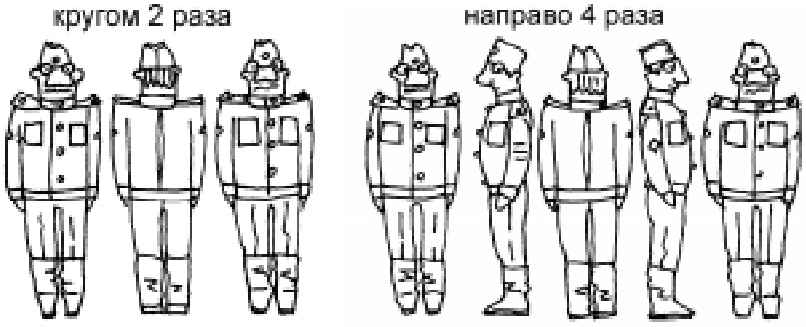
- создание подгруппы в группе перестановок через задание образующих элементов;
- определение порядков образующих элементов подгруппы;
- определение порядка самой подгруппы;
- просмотр всех элементов получившейся подгруппы;
- разложение перестановки в произведение независимых циклов;
- просмотр двумерной и трехмерной визуализации подгруппы.

Поясним термины, указанные выше.

Подгруппа – подмножество группы, которое само является группой относительно той же операции, которая задана в группе.

Система образующих элементов группы – совокупность элементов $a, b, c...$ группы таких, что любой элемент группы можно представить в виде произведения некоторых элементов группы, каждый из которых имеет вид $a, a^{-1}, b, b^{-1}, c, c^{-1}, ...$

Работа с группами перестановок...



...совокупность перестановок ... является циклической группой...

Если система образующих элементов группы состоит из одного элемента, то такая группа называется *циклической*.

Пример. Рассмотрим перестановку

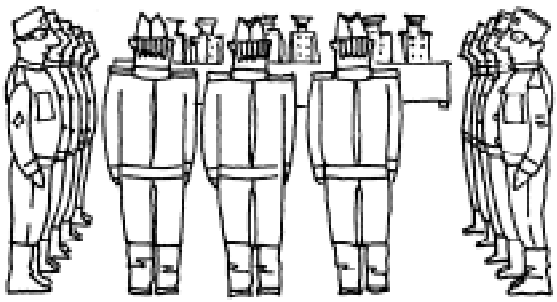
$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}.$$

Найдем степени этой перестановки:

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

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

Тогда совокупность перестановок $\{A, A^2, A^3\}$ является циклической группой с образующим элементом A. Действительно, произведение любых двух элементов из вышеуказанной совокупности является элементом из этой совокупности. Перестановка A^3 является нейтральным элементом, для перестановки A обратным элементом является A^2, а для перестановки A^2 – обратным будет A. Так как умножение перестановок ассоциативно, то мы действительно имеем группу, и поскольку любой элемент этой группы является степенью перестановки A, то данная группа – циклическая с образующим элементом A.



Порядок группы – это число ее элементов...

Порядок группы – это число ее элементов.

Порядок элемента x – это наименьшее натуральное число n такое, что $x^n = e$, где e – нейтральный элемент группы (если такое n существует). Если же такого числа n не существует, то x имеет бесконечный порядок.

Цикл – это перестановка на некотором множестве элементов, последовательно переходящих друг в друга, причем последний элемент переходит в первый.

Предположим, что мы хотим построить группу с двумя образующими. Назовем этот объект *examp*5, после этого выберем пункт меню Tools\Exploration of Permutation Group и получим окно (рисунок 1), в котором нам предлагается ввести от 1 до 4 образующих элемента в пустые поля (соответственно: *a, b, c,* и *d*). В данном случае внесем два образующих элемента (поля «*c*» и «*d*» – пустые, и в них записано «none»). Далее (см. 3-ю страницу обложки) можно увидеть следующую информацию о созданной подгруппе

Рисунок 1

...двумерная визуализация...

(Subgroup 1): ее образующие, порядки образующих (order of permutation), порядок подгруппы (order of subgroup) – в данном случае он равен 12. Для более детального исследования имеются кнопки «Detail» и «View of Subgroup». При нажатии кнопки «Detail» получаем разложение образующих элементов *a, b* в виде произведения непересекающихся циклов, а также перестановку *ab* (см. 3-ю страницу обложки).

Например, перестановка

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

может быть записана как (1 5) (2 4), а перестановка

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

как (2 3).

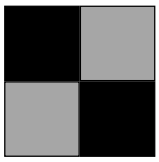
При нажатии кнопки «View of Subgroup» (см. 3-ю страницу обложки) можно увидеть все элементы созданной подгруппы (для этого надо воспользоваться полосой прокрутки).

Для *a* и *b*, показанных на рисунке 1, получим 12 перестановок, которые можно представить в виде произведения образующих *a*, *b* и их обратных, в общем случае (в данном примере $a^{-1} = a$, $b^{-1} = b$).

4. ВИЗУАЛИЗАЦИЯ АЛГЕБРАИЧЕСКИХ СТРУКТУР

Для осуществления двумерной визуализации алгебраического объекта нужно сначала создать этот объект, либо открыть объект, который сохранен на диске в директории Examples (File\New либо File\Open). Затем нужно выбрать пункт меню Visualization\2-dimensional. Покажем это на примере сохраненного на диске объекта examp1.

Заходим в меню Visualization\2-dimensional, после этого на экране появится изображение прямоугольной области, разделенной на 4 квадрата, причем каждый квадрат имеет свой собственный оттенок:

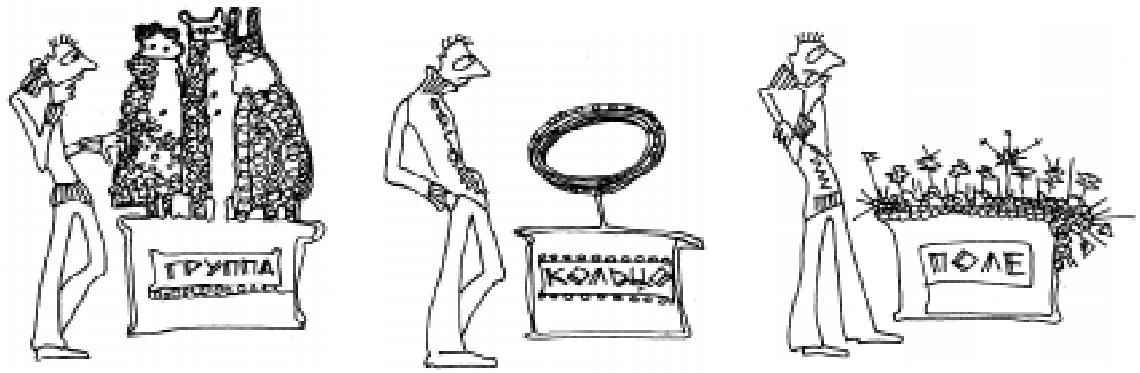


(другие примеры см. на 3-ей странице обложки). Как же получается это изображение? Рассмотрим таблицу Кэли данной группы. Элементы нашей группы – это перестановки $\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} = e$, $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = a$;

таблица Кэли группы имеет вид:

*	*e*	*a*
e	*e*	*a*
a	*a*	*e*

Двумерная визуализация по таблице Кэли осуществляется следующим образом: нейтральный элемент *e* соответствует самому темному оттенку синего цвета (почти черному), а элемент *a* соответствует оттенку чуть посветлей. Аналогично осуществляется двумерная визуализация по таблице Кэли для различных алгебраических операций таких абстрактрых структур, как группы, кольца, поля. Пусть a_1, ..., a_n – элементы множества *A*, на кото-



...трехмерная визуализация...

ром задана алгебраическая операция «∗». Ставим в соответствие каждому элементу a_i определенный оттенок фиксированного цвета (например, синего) так, чтобы оттенок, соответствующий a_{i+1}, был чуть светлее оттенка, соответствующего a_i. Далее в таблице Кэли заполним клеточки, в которых находятся элементы a_1, ..., a_n, цветом соответствующих этим элементам оттенков. Полученная таблица с клеточками, раскрашенными разными оттенками одного цвета, и будет двумерной визуализацией алгебраической операции «∗».

Для реализации трехмерной визуализации алгебраического объекта нужно сначала создать этот объект либо открыть объект, который сохранен на диске в директории Examples (File\New либо File\Open), а затем выбрать пункт меню Visualization\3-dimensional. Рассмотрим идею трехмерной визуализации алгебраической операции на простом примере.

Пусть дана группа перестановок с операцией «∗», например, рассмотренный ранее объект examp1. Элементы этой группы – $e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ и $a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$, а таблица Кэли имеет вид:

*	e	a
e	e	a
a	a	e

Теперь рассмотрим трехмерную визуализацию операции «∗» (рисунок 2). В трехмерном пространстве изображены 4 точки со следующими координатами (0, 0, 0), (1, 1, 0), (1, 0, 1) и (0, 1, 1). Эти точки получаются из таблицы Кэли следующим образом. Занумеруем элементы данной группы так: $e = a_0$ и $a = a_1$, после чего заменим в таблице Кэли элементы группы их номерами. Тогда таблица Кэли примет вид:

*	0	1
0	0	1
1	1	0

Далее, для каждой упорядоченной пары x, y элементов группы и соответствующего результата операции $x*y$ составим упорядоченную тройку, состоящую из номеров элементов x, y и $x*y$. Например, в нашем случае для пары e, e и результата операции $e*e = e$ (взятого из таблицы Кэли) получаем тройку номеров (0, 0, 0), для пары e, a и результата операции $e*a = a$ получаем тройку (0, 1, 1), для пары a, e и результата операции $a*e = a$ получаем тройку (1, 0, 1) и для пары a, a и результата операции $a*a = e$ получаем тройку (1, 1, 0). В итоге получается набор из 4 точек трехмерного пространства. В общем случае для множества X, состоящего из n элементов, трехмерная визуализация алгебраической операции, задан-

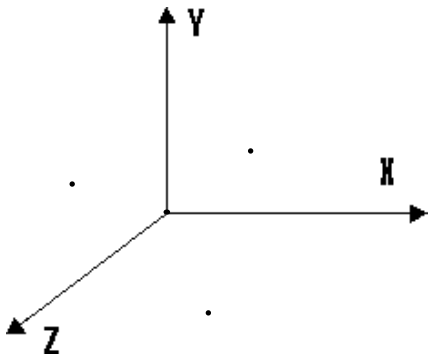


Рисунок 2

ной на этом множестве, есть набор из n^2 точек трехмерного пространства.

Для удобства работы с полученным объектом в Visal предусмотрены кнопки управления объектом (Object Controls) и камерой (Camera controls). Они позволяют вращать, приближать и удалять наш объект (см. 3-ю страницу обложки).

Приведем теперь примеры применения визуализации для некоторых понятий из теории групп. Две группы G и H называются изоморфными, если существует биекция (то есть взаимно-однозначное соответствие) φ: $G \to H$, которая «сохраняет операции» в G и H, а именно, для любых элементов x, y группы G, если $x \cdot y = z$ в группе G, то $\varphi(x) \cdot \varphi(y) = \varphi(z)$ в группе H. Для конечных множеств G и H наличие биекции между ними равносильно тому, что G и H имеют одинаковое число элементов. Тогда, если g_1, g_2, ..., g_n – элементы группы G и φ – произвольная биекция множества G на множество H, то $\varphi(g_1) = h_{i_1}$, $\varphi(g_2) = h_{i_2}$, ..., $\varphi(g_n) = h_{i_n}$ – элементы группы H. Поскольку при заполнении таблиц Кэли в программе Visal учитываются только индексы элементов, а не сами элементы, то можем считать, что биекция φ является некоторой перестановкой чисел 1, 2 ,...n, (в таблицах Кэли в VISAL нумерация ведется от 0 до n–1, что не меняет сути дела). Следовательно, можем считать, что изоморфизм φ групп G и H есть некоторая перестановка чисел 1, 2, ..., n, которая «сохраняет операции», то есть если на пересечении i-ой строки и j-го столбца в таблице Кэли группы G находится число k, то на пересечении $\varphi(i)$-ой строки и $\varphi(j)$-го столбца в таблице Кэли группы H находится число $\varphi(k)$. Таким образом, если группа H изоморфна группе G, то можем считать в нашем случае, что с точностью до перенумерации элементов группа H совпадает с группой G. Это означает, что двумерные визуальные образы изоморфных групп совпадают при некоторой перестановке строк и такой же перестановке столбцов, а трехмерные визуальные образы получаются друг из друга посредством некоторого преобразования. Это дает возможность решать вопрос об изоморфизме групп посредством сравнения их визуальных образов.

Еще одно возможное применение визуализации – строение подгрупп. Если подгруппа H группы G порождается несколькими элементами, то иногда может случиться так, что найдется система образующих подгруппы H, состоящая из одного элемента (то есть подгруппа H является циклической группой). Такие ситуации могут распознаваться визуально, так как двумерный визуальный образ циклической группы имеет специфический вид.

5. ИСПОЛЬЗОВАНИЕ VISAL ДЛЯ ОБУЧЕНИЯ

После ознакомления с описанными выше возможностями VISAL возникает естественный вопрос: как использовать этот инструмент для обучения школьников?

Можно предложить следующую схему изучения групп школьниками:

1) построение некоторого набора алгебраических операций;

2) изучение двумерных и трехмерных визуальных образов этих алгебраических операций с целью выявления сходства и различия их визуальных образов;

3) детализация пункта 2) относительно каждого из трех групповых свойств и коммутативности, а также некоторого набора этих свойств;

4) решение обратных задач типа: по некоторой паре визуальных образов (один – двумерный, другой – трехмерный) создать алгебраическую операцию, пара визуальных образов которой совпадает (или достаточно близка в некотором смысле) к первоначальной паре визуальных образов.

В результате использования VISAL по этой схеме понятие группы приобретает для школьников личностный смысл, поскольку каждый из них приходит к этому понятию не столько через определение, данное учителем или прочитанное в

книге, сколько в результате экспериментальной исследовательской деятельности с конкретными визуальными образами, созданными им самим. Из опыта работы с учениками 7–8 классов школы № 49 г. Томска, которые не отличались особыми математическими способностями, можно утверждать, что подобное знакомство с понятием группы вполне доступно, а главное, интересно среднему школьнику. Более того, часть из них обязательно захочет глубже познакомиться с группами и тогда учитель должен быть готов порекомендовать почитать литературу по теории групп (см.[1]–[4]). Таким учащимся можно порекомендовать следующую схему дальнейшей работы с использованием VISAL :

1) построение некоторого набора групп как подгрупп групп перестановок, порожденных некоторыми системами образующих;

2) изучение двумерных или трехмерных визуальных образов этих групп с целью выявления их сходства и различия;

3) детализация пункта 2) в плане выявления изоморфных групп;

4) решение обратных задач типа: по некоторой паре визуальных образов (один – двумерный, другой – трехмерный) групповой алгебраической операции построить различные группы, которые были бы изоморфны (или не изоморфны) исходной группе.

Можно также предложить следующие исследовательские задачи:

а) исследовать экспериментально с помощью VISAL связь между порядком конечной группы и порядком ее подгруппы; желательно, чтобы учащиеся вышли на теорему Лагранжа (порядок подгруппы конечной группы есть делитель порядка группы);

б) исследовать экспериментально с помощью VISAL связь между порядком произведения двух элементов и порядками сомножителей (нужно рассмотреть два случая в зависимости от того, коммутируют ли сомножители или нет, то есть $ab = ba$ или нет);

в) для заданной циклической группы экспериментально с помощью VISAL найти все ее подгруппы;

г) для заданной циклической группы экспериментально с помощью VISAL найти все ее порождающие элементы (то есть системы образующих, состоящие из одного элемента);

д) для заданной группы с фиксированной системой образующих найти экспериментально с помощью VISAL какие-то другие системы образующих;

е) исследовать экспериментально с помощью VISAL силовские p-подгруппы (то есть максимальные p-подгруппы) конечной группы перестановок (p-подгруппа конечной группы состоит из некоторого числа элементов, порядки которых являются какими-то степенями числа p).

В заключение хочу отметить, что математическая деятельность, принятая в современной школе, комфортна только для детей с логическим складом ума, которые составляют меньшую часть детей (по некоторым оценкам, 10–20%). В то же время дети-визуалы составляют большую часть детей, и они, чувствуя себя некомфортно на уроках математики в школе, редко выбирают математику в качестве своей профессиональной деятельности, хотя по своему интеллектуальному потенциалу вполне могли бы быть успешными в этой области деятельности. Хотелось бы надеяться, что компьютерная программа VISAL может помочь детям-визуалам поверить в свои силы, в то, что и они могут быть успешны в экспериментально-исследовательской, а затем и в формально-логической математической деятельности.

Литература.

1. Калужнин Л. А., Сущанский В. И. Преобразования и перестановки. М.: Наука, 1979.
2. Александров П.С. Введение в теорию групп. М.: Наука, 1980.
3. Кострикин А. И. Введение в алгебру. М.: Наука, 1977.
4. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. М.: Наука, 1977.

ВОСЬМАЯ МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ
МАТЕМАТИКА. КОМПЬЮТЕР. ОБРАЗОВАНИЕ
г. Пущино, 31 января – 5 февраля 2001 г.

Адрес Оргкомитета в Москве:
119899, Москва, Воробьевы Горы, МГУ, биологический ф-т, кафедра Биофизики,
Тел.: (095)939-02-89, факс: (095)939-11-15 E-mail: MCE@mars.biophys.msu.ru,
http://mars.biophys.msu.ru/awse

Место проведения конференции:
г. Пущино Моск. обл., пр–т Науки 3, Институт теоретической и экспериментальной биофизики РАН (ИТЭБ) и Институт биофизики клетки РАН (ИБК).
http://www.iteb.serpukhov.su/rus

План конференции

31 ЯНВ. СР.
Открытие. Доклады о Пущинском научном центре, обзорные доклады. Формирование секций. Круглый стол “Культурное пространство России: книги, журналы, конференции, Интернет".

1 ФВР. ЧТ.
Пленарное заседание: “Компьютеры в науке и образовании”. Выставка-ярмарка компьютерных образовательных программ.

2 ФВР. ПТ.
Пленарное заседание. Работа секций “Компьютеры в науке и образовании”, “Вычислительные методы и математическое моделирование”, “Математические модели в химии, биологии, экологии и медицине”, “Математические модели живых систем”, “Математические методы в экономике”, “Гуманитарное и естественно-научное образование”. Лекция “Россия в истории цивилизации”. Открытое заседание Ассоциации Женщины в науке и образовании.

3 ФВР. СБ.
Лекция 1 “Физика хаоса”. Пленарное заседание. Лекция “Наука и власть”

4 ФВР. ВС.
Лекция 2 “Физика хаоса”. Пленарное заседание. Обсуждение стендовой сессии и вручение призов за лучшие стендовые доклады. Лекция “Язык и Время Иосифа Бродского”.

5 ФВР. ПН.
Общая дискуссия и закрытие конференции.

Во время конференции редакционно-издательский совет **сборника научных трудов** “Математика. Компьютер. Образование” (8 том) начнет прием статей. По окончании конференции прием будет продолжаться в оргкомитете конференции до 1 марта 2001 года.

КОНФЕРЕНЦИЯ
ИНФОРМАТИЗАЦИЯ ОБРАЗОВАНИЯ'2001
г. Екатеринбург, 13–16 февраля 2001 г.

Конференция является ежегодным подведением итогов деятельности Института информатизации образования МО РФ и его филиалов в области развития информационных технологий и их применения в системе образования.

Конференция проводится при поддержке:
• Уральского государственного педагогического университета;
• Института информатизации образования Минобразования РФ;
• Академии информатизации образования;
• Журнала "Информатика и образование".

Программа конференции

1. Концепция разработки электронных учебников.
2. Использование информационных технологий в учебном процессе школы и педагогического вуза.
3. Технология и содержание дистанционного обучения.
4. Информационные технологии в управлении учебным заведением.
5. Методические аспекты преподавания информатики в школе и педагогическом вузе.
6. Информационные технологии во внеклассной работе с учащимися.

К участию в конференции приглашаются работники региональных управлений и департаментов образования, администраторы, научные работники и преподаватели вузов, сотрудники научно-исследовательских институтов, учителя школ, профтехучилищ, преподаватели техникумов и других учреждений образования.

Предполагается:
• издание сборника трудов конференции;
• предоставление возможностей для демонстрации программных разработок;
• выставка-продажа учебной и учебно-методической литературы и программных продуктов, представленных участниками.

Заявки на участие в конференции направлять по адресу:
620151, г. Екатеринбург, ул. К. Либкнехта, 9,
Центр информационных технологий УрГПУ
(с пометкой "конференция")
или по электронной почте: conference@uspu.ru
Телефоны для справок (3432) 51-52-55, 51-10-15

Наш комментарий:

ГРУППА ПОВОРОТОВ ТЕТРАЭДРА

В начале статьи, посвященной программе VISAL, описан простой пример конечной группы – перестановки букв слова при шифровке. Нам кажется, что читателям будет интересно познакомиться и с другим популярным примером конечной группы – группой поворотов тетраэдра. С помощью описанного программного продукта можно исследовать особенности строения этой группы, а «геометричность» этого примера позволяет легко связать наглядные представления с найденными характеристиками. Мы попробуем еще раз «пройтись» по всем основным терминам теории групп, описанным в предыдущей статье и посмотреть, что они означают на новом примере. Если приведенный пример покажется вам «недостойным» программы, попробуйте проделать то же для группы вращений куба.

Рассмотрим правильный тетраэдр – треугольную пирамиду, грани которой – одинаковые правильные треугольники. Поставим тетраэдр на лист бумаги и обведем основание. Теперь поднимем тетраэдр и поставим его снова какой-либо гранью на начерченный треугольник. При этом тетраэдр займет то же место в пространстве, но его положение изменится (говорят, что мы сделали преобразование тетраэдра, переводящее его в себя).

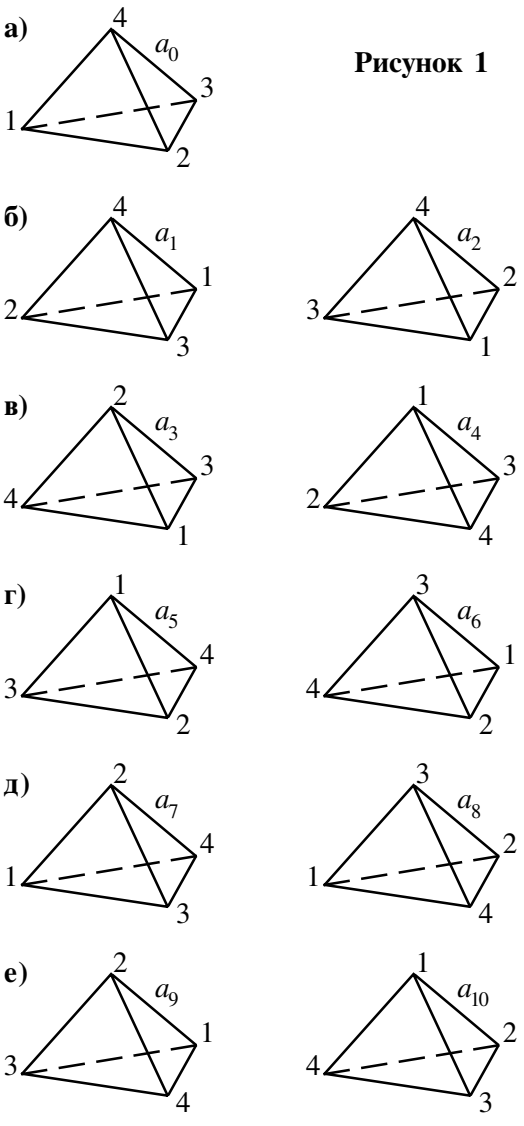


Рисунок 1

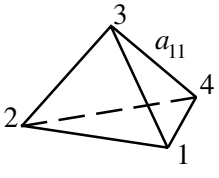
Сколько же можно сделать различных преобразований – поворотов тетраэдра, при которых тетраэдр «переходит в себя»?

Считать можно по-разному. Например, перебрать все варианты «вручную» (рисунок 1). Другой способ – применить какие-нибудь комбинаторные соображения, упорядочивающие перебор вариантов. Например, сначала перебрать преобразования, сохраняющие положение верхней вершины (повороты вокруг вертикальной оси – рисунок 1б). Затем – преобразования, сохраняющие какую-нибудь вершину при основании (рисунки 1в, 1г, 1д).

Можно поставить задачу формально. Обозначим начальные положения вершин тетраэдра цифрами 1, 2, 3, 4 (рисунок 1а). А преобразование тетраэдра запишем в виде подстановки.

Например,

$$a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$



$$a_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

описывают повороты тетраэдра относительно вершины 4.

«Читать» такую запись, например, для a_1, можно так: вершина 1 переходит на место вершины 3, вершина 2 – на место вершины 1 и т.д.

Подстановочная запись очень удобна, если необходимо узнать результат нескольких последовательных преобразований.

Например, как будет выглядеть положение тетраэдра после поворота

$$a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$

за которым следует поворот

$$a_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}.$$

Проследим за перемещением вершин тетраэдра:

$1 \to 3$ (после a_1)	$3 \to 3$ (после a_4)
$2 \to 1$ (после a_1)	$1 \to 4$ (после a_4)
$3 \to 2$ (после a_1)	$2 \to 1$ (после a_4)
$4 \to 4$ (после a_1)	$4 \to 2$ (после a_4)

Эти перемещения тоже описываются подстановкой, которая является произведением подстановок a_1, a_4 и обозначается $a_1 \cdot a_4$. Можно дать этой подстановке свое название, например, a_9, тогда

$$a_9 = a_1 \cdot a_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Посмотрите, какое интересное преобразование получилось: вершины 1, 3 и 2, 4 попарно меняются местами (рисунок 1е)! А сможете ли Вы так повернуть тетраэдр руками?!

Подсказка. Возьмите тетраэдр большим и указательным пальцами за середины противоположных ребер и поверните на 180^0.

Обратите внимание, что если выполнить преобразования a_1 и a_4 в другом порядке, то получится другой результат:

$$a_4 \cdot a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

который, впрочем, тоже переставляет пары вершин.

Получившаяся подстановка подсказывает другой (более экономный) способ ее записи, приведенный в предыдущей статье, который называется записью в виде произведения непересекающихся циклов.

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

Так же можно записать и другие подстановки, например,

$$a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (1\ 3\ 2)\,(4)$$

Это будет означать, что 1, 3, 2, как говорят, «циклически», то есть «по кругу» переходят друг в друга (рисунок 2), а 4 остается на месте (или «переходит» в себя).

Попробуем рассмотреть как можно больше различных произведений подстановок, сохраняющих одну из вершин. При этом найдутся еще два новых преобразования тетраэдра (рисунок 1е). Кроме того, обнаружится много новых закономерностей, например:

$$a_1 \cdot a_3 = a_6,\ a_1^2 = a_1 \cdot a_1 = a_2,\ a_9^2 = a_0$$

Обратим внимание на примеры, которые в результате дают преобразование a_0, то есть возвращают тетраэдр в исходное состояние, например,

$$a_1 \cdot a_2 = a_0,\ a_3 \cdot a_4 = a_0 \ldots$$

и более экзотические

$$a_0^2 = a_0,\ a_9^2 = a_0.$$

Геометрически это означает, что a_2 является обратным преобразованием к a_1.

Аналогично, a_4 является обратным к a_3, a_0 – к a_0 и a_9 – к a_9 (!).

Это обозначается следующим образом:

$$a_2 = a_1^{-1},\ a_4 = a_3^{-1},\ a_0 = a_0^{-1},\ a_9 = a_9^{-1}.$$

Обратим внимание на свойства полученного множества подстановок:

– есть нейтральный элемент

$$a_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix},$$

не меняющий положения тетраэдра;
– у каждого элемента (некоторого преобразования тетраэдра) из полученного множества есть обратный (возвращающий тетраэдр в исходное состояние);
– произведением двух подстановок множества является подстановка, соответствующая двум последовательным преобразованиям тетраэдра;
– произведение подстановок (преобразований тетраэдра) обладает свойством ассоциативности, но не обладает, вообще говоря, свойством коммутативности.

Таким образом, полученное множество подстановок, а следовательно, и преобразований тетраэдра образует некоммутативную группу. Порядок этой группы (число ее элементов) равен 12.

Поставим теперь такую задачу: можно ли получить все положения тетраэдра, используя не все, а одно или несколько различных преобразований, если при этом их можно осуществлять любое количество раз в любых комбинациях (перемножая и обращая).

Например, если мы возьмем преобразование

$$a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$

то можно получить преобразование a_2 повторным выполнением преобразования a_1:

$$a_2 = a_1 \cdot a_1 = a_1^2$$

или обращением преобразования a_1:

$$a_2 = a_1^{-1}$$

Далее, если умножить a_1 на себя трижды или, что то же самое, умножить a_1 на уже полученное a_2, то результатом будет a_0:

$$a_1^3 = a_1 \cdot a_2 = a_0$$

Как бы мы ни старались комбинировать эти подстановки, больше ничего нового не получим.

Мы построили группу G_1 меньшего размера, являющуюся частью группы всех поворотов: $G_1 = \{a_0, a_1, a_2\}$.

Аналогично, можно построить группы $G_2 = \{a_0, a_3, a_4\}$, $G_3 = \{a_0, a_5, a_6\}$ и пр., которые называются подгруппами исходной группы G. Порядок каждой из подгрупп G_1, G_2, G_3 равен 3.

Построение этих групп показывает, что подгруппу можно задать своими образующими. Так, подгруппу G_1 задали одним образующим элементом a_1:

$$a_2 = a_1^2, \; a_0 = a_1^3$$

Обратите внимание, что когда образующий элемент один, то порядок p подгруппы G_1 равен порядку элемента. В нашем примере $p = 3$. Если в качестве образующих взять элементы a_1 и a_3, то мы получим все элементы группы поворотов тетраэдра (покажите, как они получаются!).

Упражнение.

Попробуйте в качестве образующих использовать другие элементы, например,

$$a_9 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ и } a_{10} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Все ли повороты тетраэдра будут порождаться этими элементами?

Упражнение.

1) Найдите другие подгруппы G. Обратите внимание, что порядок группы всегда делится без остатка на порядок подгруппы.
2) Существуют ли у группы поворотов тетраэдра подгруппы порядка 1, 4, 6? Если да, то постройте их.

Подгруппу можно описать и по-другому – таблицей умножения, которая называется здесь таблицей Кэли.

Так для подгрупп G_1 и G_2 таблицы Кэли имеют вид:

G_1	a_0	a_1	a_2
a_0	a_0	a_1	a_2
a_1	a_1	a_2	a_0
a_2	a_2	a_0	a_1

G_2	a_0	a_3	a_4
a_0	a_0	a_3	a_4
a_3	a_3	a_4	a_0
a_4	a_4	a_0	a_3

Подгруппы G_1, G_2 и G_3 – это группы поворотов тетраэдра «вокруг вершин».

Перечисленные три группы являются изоморфными друг другу. Это означает, что мы можем переименовать элементы одной группы так, что таблица умножения одной группы перейдет в таблицу умножения другой. В нашем примере это достигается таким переименованием:

$$a_1 \to a_3,\ a_2 \to a_4$$

Наконец, поставим вопрос, а сколько же всего подстановок можно сделать на множестве из четырех элементов?

Ответ можно получить прямым перебором, а можно следующим комбинаторным рассуждением.

Первый элемент можно переместить в любое из четырех положений, второй – в любое из трех оставшихся, третий – в любое из двух оставшихся, четвертый же поставить на единственно свободное место.

Тогда с каждым из четырех способов перемещения первого элемента комбинируется три способа перемещения второго и два способа перемещения третьего, что дает 4·3·2=24 комбинации.

Из них 12 подстановок соответствуют поворотам тетраэдра. Что же означают оставшиеся 12? Возьмем, например, такую подстановку:

$$a_{12} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}.$$

Она означает такое преобразование тетраэдра, при котором две вершины поменяются местами, а две другие останутся в прежнем положении. Нетрудно увидеть, что такой поворот невозможен. Однако, если зеркально отобразить тетраэдр (рисунок 2), то после этого такое совмещение вершин станет возможным.

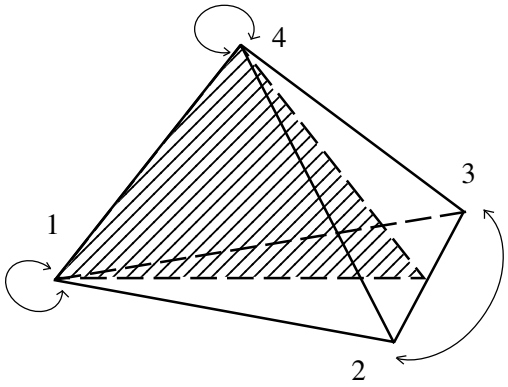


Рисунок 2

Таким образом, если к преобразованиям поворота добавить преобразования «зеркального отражения» (относительно сечений тетраэдра, каждое из которых проходит через ребро и высоту, опущенную из любого конца этого ребра на противоположную грань), то все подстановки будут соответствовать некоторым преобразованиям тетраэдра. Порядок этой «самой большой» группы преобразований будет 24, а группа поворотов станет подгруппой этой группы (обратите внимание на связь их порядков: 24 делится на 12!).

А теперь попробуйте проделать все действия, связанные с описанием групп и подгрупп (таблицами, непересекающимися циклами, образующими элементами), используя программу VISAL.

Постройте визуальные образы всех построенных групп и подгрупп и попробуйте разглядеть на них те или иные свойства. Например, как отражается на картинках изоморфизм групп? Коммутативность? Сможете ли Вы увидеть на картинке группы ее подгруппы меньшего порядка?

Думайте, пробуйте, исследуйте!

Росошек Семен Константинович, кандидат физ.-мат. наук, доцент кафедры алгебры Томского государственного университета.

Комментарий:
Поздняков Сергей Николаевич.