Конечные группы

А.СОСИНСКИЙ

ПОНЯТИЕ группы, в частности конечной группы, — одно из важнейших понятий математики. И вместе с тем *одно из самых* распространенных и наиболее полезных для приложений.

Без конечных групп нельзя, например, указать, какие алгебраические уравнения разрешимы в радикалах, а какие — нет, описать, как устроены кристаллы, создавать коды, *исправляющие ошибки*. Об этом, однако, мы здесь рассказывать не будем, а ограничимся простейшими примерами конечных групп.

Иллюстрации: группы действий

Непустой набор некоторых действий, которые можно последовательно выполнять, называют группой, если в этом наборе для каждого действия обязательно присутствует обратное к нему, а результат последовательного *выполнения* любых двух действий тоже является действием из этого набора.

В качестве *иллюстрации* рассмотрим действия солдата, выполняющего команды строевой подготовки

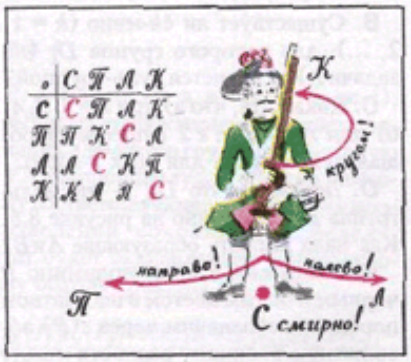


Рис. 1

(рис.1). Эти четыре действия составляют группу $R(\square) = \{С, П, Л, К; \circ\}$. Так, результат последовательного выполнения действий П и К (направо и кругом) будет совпадать с результатом действия Л (налево); *это* записывается в виде равенства $К \circ П = Л$. Точно так же $Л \circ Л = П \circ П = К$, $Л \circ П = П \circ Л = К \circ К = С$. Остальные соотношения в группе можно извлечь из ее *таблицы умножения*, показанной на рисунке 1. Особую роль играет *здесь действие* С, которое можно назвать «ничегонеделание». (Такое действие обязательно есть в любой группе: мы его получим, *выполнив* произвольное действие, а затем обратное к нему.) У нас действия П и Л обратны друг к другу, действие К — обратно к самому себе, и т.д.

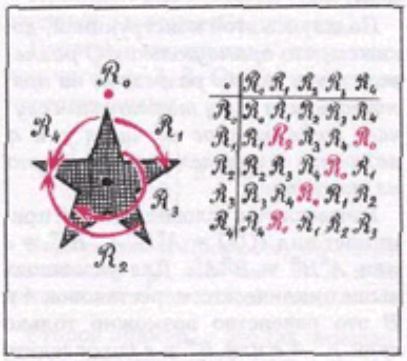


Рис. 2

Рассмотрим *другую группу*, тоже состоящую из поворотов. Именно — группу поворотов пятиконечной звезды $П(\bigstar)$ относительно ее центра (рис.2). «Ничегонеделание» (в этом случае — поворот на 0°) обозначено через R_0, а остальные повороты (на 72°, 144°, 216°, 288°) — через R_1, R_2, R_3, R_4. Здесь $R_2 \circ R_1 = R_1 \circ R_2 = R_3$, $R_3 \circ R_3 = R_1$, $R_1 \circ R_4 = R_0$ (последнее означает, что R_4 обратно к R_1) и т.д. Набор

$$П(\bigstar) = \{R_0, R_1, R_2, R_3, R_4; \circ\}$$

образует группу.

Рассмотрим, наконец, «группу надевания носка» (рис.3), состоящую из следующих действий:

О = «Оставь, как есть»,

П = «Сними и надень на другую ногу»,

В = «Сними, выверни и надень на ту же ногу»,

$П'$ = «Сними, выверни и надень на другую ногу».

Здесь «ничегонеделание» — это О, далее $П \circ В = П'$, $П \circ П = В \circ В = О$, $П' \circ П = В$ и т.д.

Снова получается группа $Н = \{О, П, В, П'; \circ\}$, *состоящая*, как и $R(\square)$, из четырех действий. Группы H и $R(\square)$, однако, принципиально разные: у них таблицы умножения отличаются не только обозначением элементов, но и своим строением. Так, по диагонали таблицы умножения H стоит одно и то же действие О, в то время *как на этой* диагонали у $R(\square)$ стоят разные элементы.

Подозреваю, что у самых серьезных читателей нарастает возмущение: какая-то там строевая подготовка, надевание носков — что за глупости такие, не научно это все! Спешу возразить: научно, даже очень. *Знаете*, как на самом деле называется набор действий солдата? *Циклическая группа 4-го порядка* или *группа вычетов по модулю 4*. А наше «надевание носков» — *группа Клейна*. Повороты же звезды — это одна из так называемых *простых конечных групп*.

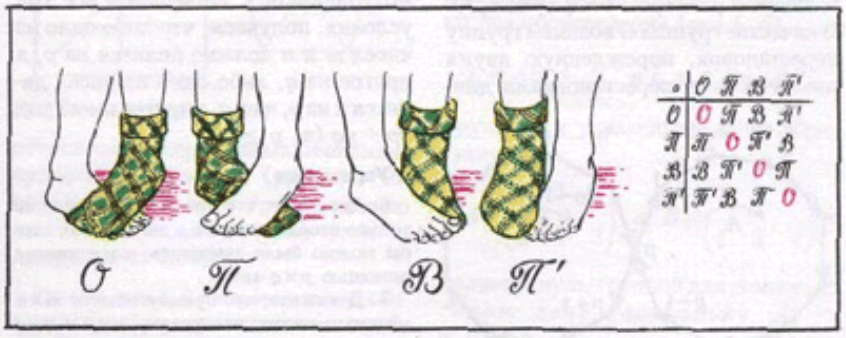
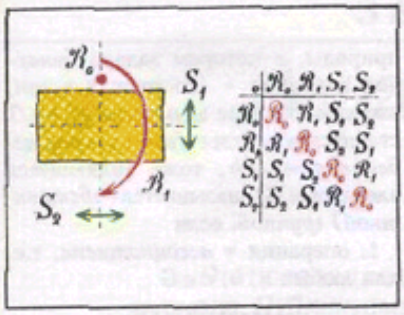


Рис.3

Эта статья была опубликована журнале «Квант» в №2 за 1987 год.



$\circ$	$\mathcal{R}_0$	$\mathcal{R}$	S_1	S_2
$\mathcal{R}_0$	$\mathcal{R}_0$	$\mathcal{R}$	S_1	S_2
$\mathcal{R}$	$\mathcal{R}$	$\mathcal{R}_0$	S_2	S_1
S_1	S_1	S_2	$\mathcal{R}_0$	$\mathcal{R}$
S_2	S_2	S_1	$\mathcal{R}$	$\mathcal{R}_0$

Рис. 4

Группы симметрий геометрических фигур

С каждой геометрической фигурой F *можно связать вполне* определенную группу $S(F)$, называемую *группой самосовмещений* или *группой симметрий* этой фигуры; по определению, ее набор действий состоит из всех перемещений, совмещающих фигуру F саму с собой. Например, $S(\square)$состоит из 8 действий: четырех поворотов квадрата (относительно его центра, в том числе на 0°) и четырех отражений (относительно двух диагоналей и двух «средних линий» квадрата).

В группе $S(\triangle)$ самосовмещений правильного треугольника — 6 действий, в группе $S(\square)$ прямоугольника — 4. Таблица умножения группы $S(\square)$ изображена на рисунке 4.

Если сравнить таблицу умножения для группы $S(\square)$ с таблицей умножения для группы H, можно заметить, что эти таблицы отличаются только обозначением действий. Если переименовать действия так:

$$O \to R_0,\ \Pi \to R_1,\ B \to S_1,\ \Pi' \to S_2,$$

то одна таблица превратится в другую. Группы с совпадающими (при подходящем переименовании действий) таблицами умножения называются *изоморфными*. Мы сейчас установили, что группы $S(\square)$ и H изоморфны (их обычно в честь Ф.Клейна обозначают буквой K), а ранее заметили, что эти группы не изоморфны группе $R(\square)$ действий солдата.

Читатель, возможно, догадался, почему мы обозначили группу действий солдата через $R(\square)$: она изоморфна *группе поворотов квадрата* относительно его центра на углы $2k\pi/4$, $k = 0, 1, 2, 3$. *Эта группа* — частный случай (при $n = 4$) *группы поворотов правильного n-угольника* (относительно его центра), которая еще называется *циклической группой n-го порядка* и обычно обозначается через Z_n.

В алгебре группы изучают «с точностью до изоморфизма», т.е. не различают изоморфные группы: алгебраисту не интересно, как называется группа и ее действия, ему важно знать структуру таблицы умножения группы.

Группы перестановок и их подгруппы

Рассмотрим конечный набор предметов — скажем, пять. Обозначим предметы цифрами, а весь набор через $N_5 = \{1, 2, 3, 4, 5\}$. *Перестановкой* $i \in S_5$ этих предметов называется любое взаимно однозначное *отображение* i: $N_5 \to N_5$, т.е., попросту говоря, перенумерация предметов. Новый номер $i(k)$ k-го *предмета* мы будем обозначать через i_k. Для наглядности перестановку i обычно *представляют в виде* таблицы:

$$i = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ i_1 & i_2 & i_3 & i_4 & i_5 \end{pmatrix}.$$

Это позволяет легко находить произведение *перестановок* i и j. Например, если

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

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

то $k(3) = (i \circ j)(3) = i(j(3)) = i(5) = 2$, так что

$$i \circ j = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

(обратите внимание, что при $k = i \circ j$ сначала *выполняется* j, *а потом* i, причем это не все равно: $i \circ j \neq j \circ i$ — проверьте!). Также легко находить *обратные перестановки* («чтением снизу вверх»):

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

Нетрудно проверить, что S_5 образует группу, состоящую из $5! = 120$ перестановок. Эта группа называется *группой перестановок пяти предметов* или *симметрической группой пятой степени*. Совершенно аналогично определяется *симметрическая группа* S_n *n-й степени* для любого натурального n.

Группы перестановок интересны в частности тем, что содержат много *подгрупп* (т.е. частей, которые сами являются группами). В группах перестановок содержатся подгруппы, изоморфные всем нашим ранее рассмотренным группам. Заинтересованный читатель может в этом убедиться, проштудировав рисунок 5.

Рассматривая этот рисунок, читатель наверняка обратит внимание на красивые числовые *закономерности*, которые на нем проявляются. В частности, если назвать *порядком группы* число *ее элементов*, а *порядком элемента* g — наименьшее число k, для которого $g^k = e$, то можно сформулировать *следующую* теорему.

Теорема Лагранжа. *Порядок любой подгруппы, также как порядок любого элемента группы, является делителем порядка группы.*

Доказательство (не очень сложное) мы здесь не приводим.

Взаимоотношения групп: гомоморфизмы

Группы изучают не каждую саму по себе, а в их взаимодействии. Назовем *гомоморфизмом* $\gamma: G \to H$ *группы* G в группу H всякое отображение, ставящее в соответствие каждому действию g из G *вполне определенное* действие $h = \gamma(g)$ из H, если для любых g и g' из G выполняется

$$\gamma(g \circ g') = \gamma(g) \circ \gamma(g').$$

(Коротко говорят так: гомоморфизм — это отображение, сохраняющее операцию $\circ$.)

Бестолковый солдат, который игнорирует команды «кругом» и «смирно», а в ответ на команды «налево» и «направо» поворачивается кругом, тем самым задает гомоморфизм

$$\beta: R(\square) \to \boldsymbol{Z}_2 = \{\text{С},\ \text{К};\ \circ\}$$

по правилу $\beta(\text{С}) = \beta(\text{К}) = \text{С}$, $\beta(\Pi) = \beta(\text{Л}) = \text{К}$. Задумавшийся солдат, не реагирующий *ни на какую* команду, определяет *тривиальный гомоморфизм* и *тривиальную группу*:

$$\alpha: R(\square) \to \{e\}.$$

Нетривиальные гомоморфизмы не всегда существуют. Например, лю-

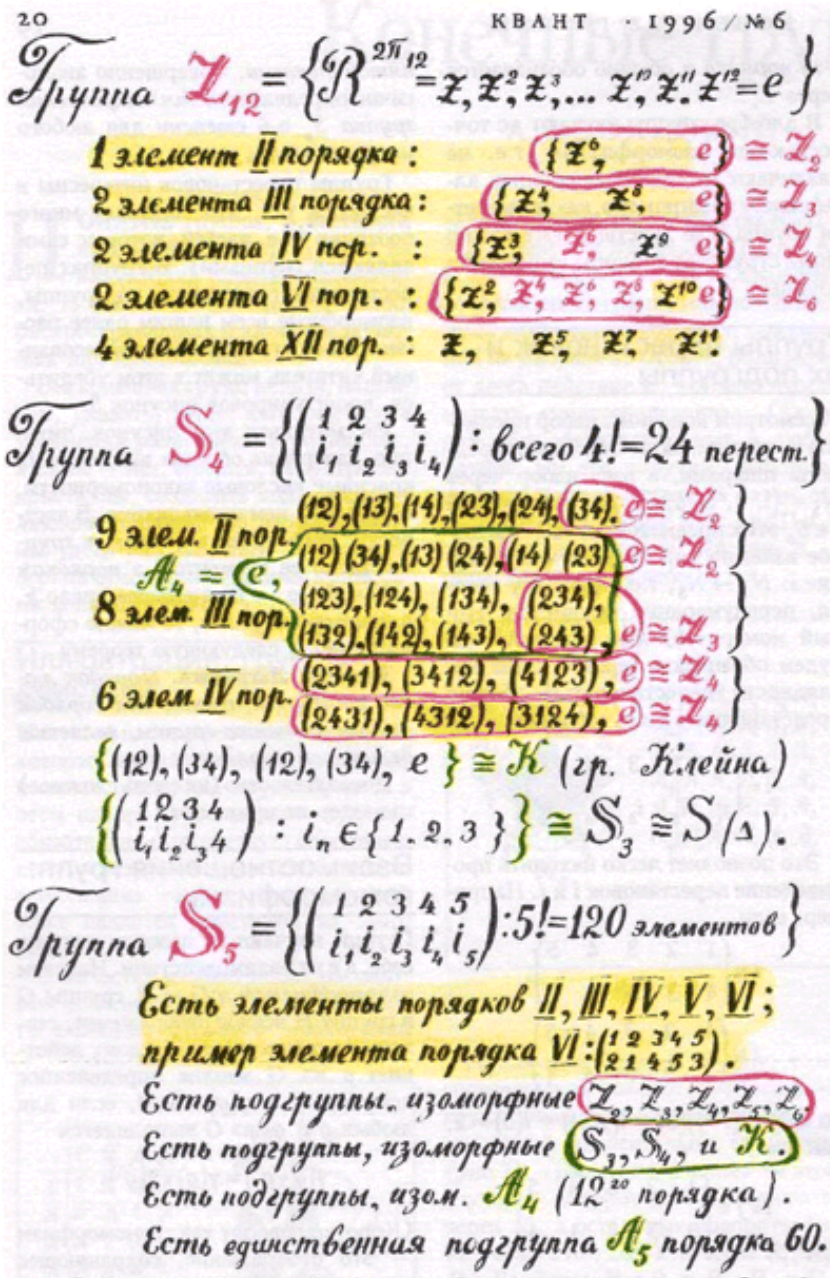


Рис. 5. Подгруппы циклической группы Z_{12} и групп перестановок S_4 и S_5. Красным выделены циклические подгруппы Z_k, зеленым — так называемые знакопеременные группы (A_4 и A_5). В описании группы S_4 цифры в круглых скобках обозначают циклы, т.е. перестановки, меняющие цифры по кругу, например $(123) = \begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$ (т.е. $1 \to 2 \to 3 \to 1$, $4 \to 4$) или $(24) = \begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$, $(13)(24) = \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$.

бой гомоморфизм $\alpha: \mathbf{Z}_5 \to \mathbf{Z}_2$ или $\beta: \mathbf{Z}_5 \to \mathbf{Z}_6$ — тривиален.

Абстрактные группы и теорема Кэли

До сих пор мы рассматривали вполне конкретные группы, состоящие из действий — поворотов, симметрий и других преобразований. Но к понятию группы можно походить с более формальных, общих позиций; группы тогда считаются состоящими из элементов произвольной природы, а умножение — тоже произвольная операция (не обязательно композиция действий). Получается следующее аксиоматическое определение. Множество G элементов произвольной природы, в котором задана *бинарная операция* $*$ (состоящая в том, что каждой паре элементов $a, b \in G$ ставится в соответствие их *произведение* $c = a*b$, тоже являющееся элементом G), называется *(абстрактной) группой*, если

1. операция $*$ *ассоциативна*, т.е. для любых $a, b, c \in G$

$$a*(b*c) = (a*b)*c;$$

2. в G имеется единственный *нейтральный* элемент $e \in G$, для которого

$$a*e = e*a = a$$

при любом $a \in G$;

3. для каждого $a \in G$ существует единственный *обратный элемент* $a^{-1} \in G$ такой, что

$$a^{-1}*a = a*a^{-1} = e.$$

Это общее определение позволяет сразу получить много новых примеров групп. Так, целые числа $\mathbf{Z}$ образуют группу (в качестве $*$ берем операцию $+$, нейтральный элемент — это 0, а обратным к $a \in G$ служит $(-a)$); ненулевые действительные числа $\mathbf{R}\{0\}$ образуют группу относительно умножения и т.д.

Однако по существу абстрактный подход ничего нового не дает: оказывается, что любая абстрактная группа изоморфна некоторой группе действий. Мы докажем это здесь лишь для конечных групп.

Теорема Кэли. *Всякая конечная группа G изоморфна некоторой подгруппе группы перестановок S_n.*

Доказательство. Пусть $G = \{e = g_1, g_2, \dots, g_n\}$. Каждому элементу $g_k \in G$ поставим в соответствие перестановку

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

где i_1 — номер элемента $g_k*g_1 = g_k*e$ (на самом деле $i_1 = k$), i_2 — номер элемента g_k*g_2, …, i_n — номер элемента g_k*g_n. Тогда все i_s различны (т.е. действительно получается перестановка) и соответствие

$$g_k \to \begin{pmatrix}1&2&\dots&n\\i_1&i_2&\dots&i_n\end{pmatrix}$$

задает *гомоморфизм* $h: G \to S_n$ (это следует из ассоциативности), притом h отображает G взаимно однозначно на подгруппу $h(G) \subset S_n$ (это следует из аксиом 2 и 3).