Л. Садовский,
М. Аршинов

ГРУППЫ

Математика двадцать первого века может сильно отличаться от нашей; возможно, школьник начнет изучение алгебры с теории групп подстановок, что он мог бы сделать сейчас, если бы не установившиеся традиции.

Саймон Ньюкомб, 1893 год

Алгебра изучает различные действия (операции) и законы, которым они подчиняются. Эти операции могут быть определены не только над числами, многочленами и векторами, что вам известно из школьного курса математики и физики, но и над элементами иной природы.

В статье А. Колмогорова вы познакомились с операцией композиции перемещений и понятием «группа преобразований». Здесь речь пойдет об абстрактной алгебраической конструкции, называемой группой.

Чтобы выработать понятие группы в его современной форме, математикам потребовалось почти сто лет. Двести лет назад знаменитый французский ученый Жозеф-Луи Лагранж (1736—1813), изучая решение алгебраических уравнений в радикалах, оперировал фактически с понятием группы, хотя и не пользовался самим этим термином. Им была сформулирована и доказана в 1771 году первая существенная теорема в теории групп.

Исследования Лагранжа продолжили норвежский математик Нильс Хенрик Абель и француз Эварист

Галуа*), которые впервые ввели термин «группа». Элементами рассматриваемых ими групп были подстановки корней алгебраического уравнения

$$a_n x^n + a_{n-1}x^{n-1} + \\ + \ldots + a_1 x + a_0 = 0.$$

Группы подстановок изучали также Огюстен-Луи Коши (1789—1857), Артур Кэли (1821—1903), Камилл Жордан (1838—1922) и другие известные математики. Принятое ныне определение группы было предложено Кэли в 1854 году.

С понятием группы тесно связано широко распространенное в природе *свойство симметрии.* Симметричны не только снежинки, пчелиные соты, кристаллы поваренной соли и кварца. Элементарные частицы тоже подчиняются «закону симметрии» — зарядовому сопряжению, согласно которому каждой частице соответствует античастица. Проявлением симметрии окружающего нас мира являются принцип относительности Галилея, законы сохранения энергии, количества движения, электрического заряда и др.

Изучение закономерностей симметрии, общих для самых различных ее проявлений, и привело к созданию специального математического аппарата, называемого *теорией групп*.

В основе определения группы лежит понятие *бинарной операции*.

Бинарная операция

Предположим, что каждой упорядоченной паре a и b элементов некоторого произвольного множества G поставлен в соответствие некоторый элемент c того же множества. Тогда говорят, что на множестве G определена *бинарная операция*. Результат применения этой операции к заданной паре элементов записывают в символическом виде

$$a * b = c.$$

Иногда для бинарной операции избирают привычный термин, именуя ее *сложением, умножением* или *композицией*. Примером бинарной операции является *композиция перемещений на плоскости*.

Произведения $a * b$ и $b * a$ могут оказаться одинаковыми или различными. В первом случае говорят, что a и b *коммутируют* (перестановочны), во втором — *не коммутируют*. Бинарная операция $*$ называется *коммутативной*, если для любых a, b будет $a * b = b * a$, и некоммутативной, если найдется хотя бы одна пара элементов a, b, для которых $a * b \neq b * a$.

З а д а ч а 1. Проверьте, что

а) обычное сложение является бинарной операцией на множестве Z всех целых чисел;

б) умножение также является бинарной операцией на множестве Z.

Таким образом, на одном и том же множестве можно, вообще говоря, определить различные бинарные операции.

З а д а ч а 2. Являются ли на множестве Z бинарными операциями

а) деление;

б) вычитание?

Коммутативны ли эти операции?

З а д а ч а 3. Являются ли сложение, вычитание, умножение и деление бинарными операциями на множестве всех нечетных чисел?

Есть лишь две возможности перемножить заданную тройку элементов a, b, c, не меняя их порядка: $(a*b)*c$ или $a*(b*c)$. Если

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

то тройка элементов a, b, c называется *ассоциирующей*; для нее вполне определенный смысл имеет символ $a * b * c$. Если же для операции $*$ к а ж д а я тройка элементов ассоциирует, то и сама операция $*$ называется *оциативной*.

З а д а ч а 4. Ассоциативны ли следующие операции:

а) композиция перемещений;

б) сложение и умножение действительных (комплексных) чисел;

в) деление и возведение чисел в степень ($a * n = a^n$)?

*) Об этих математиках см. «Квант», 1973, № 10 и 1976, № 5.

Определение группы

Множество G с определенной на нем бинарной операцией $*$ называется *группой*, если выполняются три аксиомы:

Аксиома I (существование единичного элемента). *Существует единичный элемент e множества G такой, что*

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

для любого элемента a из G.

Аксиома II (существование обратного элемента). *Для каждого элемента a множества G существует в G единственный элемент a^{-1} такой, что*

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

Аксиома III (ассоциативность бинарной операции). *Для любой тройки a, b, c элементов из G выполняется равенство*

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

Если бинарная операция коммутативна, то группа называется *абелевой* (в честь Абеля) или *коммутативной*, в противном случае — *неабелевой* или некоммутативной.

Итак, множество превращается в группу, как только на нем задается бинарная операция, подчиняющаяся трем указанным аксиомам. При этом ничего не предполагается относительно самих элементов этого множества: ими могут быть числа, многочлены, перемещения или объекты какой-либо иной природы.

Теперь, когда дано определение группы, каждый обнаружит, что с группами он, оказывается, давно знаком. В самом деле, многие числовые множества относительно обычных операций сложения и умножения образуют группу. Так, группой является множество целых чисел с операцией сложения, ее называют *аддитивной группой целых чисел*. Это абелева группа, ее «единичным» элементом служит число нуль: $0+c=c+0=c$, обратным для произвольного числа — ему противоположное: $c+(-c)=0$.

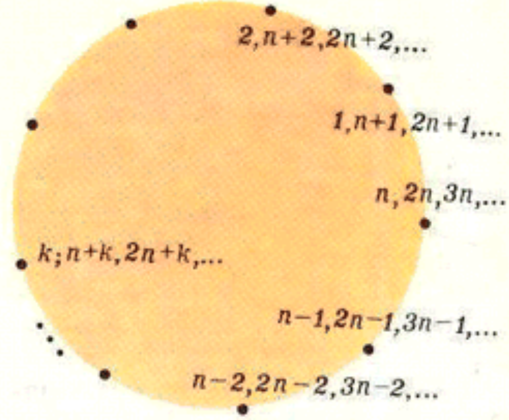

Рис. 1.

Группу образует также множество G всех перемещений, отображающих на себя некоторую фигуру (тело) F. Эта группа служит характеристикой симметричности фигуры F и называется группой симметрии фигуры F.

Задача 5. Проверьте, что множества рациональных и действительных чисел с операцией сложения являются группами (*аддитивные группы рациональных и действительных чисел*).

Задача 6. Докажите, что

а) положительные рациональные;

б) положительные действительные числа по умножению образуют группы (*мультипликативные группы положительных рациональных и положительных действительных чисел*).

Задача 7. Образуют ли группы множества рациональных и действительных чисел с операцией умножения?

Три лица одной группы

Лицо первое (арифметическое). Зафиксируем натуральное число n ($n \neq 1$) и рассмотрим множество (обозначаемое через T_n) остатков от деления каждого натурального числа на n. Ясно, что различных остатков ровно n, они равны соответственно $0, 1, 2, \ldots, n-1$. Всякие два числа k и l, которые при делении на n дают равные остатки, называют *сравнимыми по модулю n* и пишут

$$k \equiv l \pmod{n}.$$

Разобьем теперь множество N натуральных чисел на n классов по следующему принципу.

В нулевой класс (для его обозначения удобно пользоваться тем же числом 0) собираем все те числа, которые при делении на n дают в

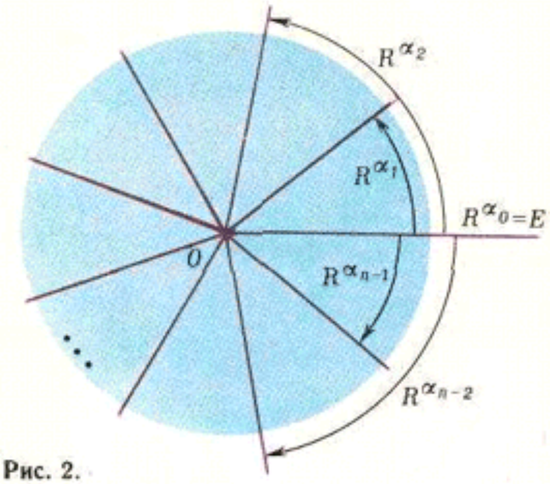

Рис. 2.

остатке 0, то есть все такие a, что $a \equiv 0 \pmod{n}$.

В первый класс собираем числа $a \equiv 1 \pmod{n}$, т. е. дающие остаток 1 при делении на n.

Вообще в k-й класс помещаем все числа $a \equiv k \pmod{n}$. Для обозначения этого класса используем то же число k (рис. 1).

Определим теперь бинарную операцию на множестве Z_n построенных классов. Пусть k и l — два любых класса. Выберем в каждом из них по любому числу, например, a и b:

$$a \equiv k \pmod{n}, \quad b \equiv l \pmod{n}.$$

Составим обычную сумму $a+b$ и разделим ее на n. Тогда в остатке получим либо $k+l$ (если $k+l<n$), либо $k+l-n$ (если $k+l \geqslant n$).

Значит, имеет смысл следующее определение операции $\oplus$ (назовем ее «сложением классов»):

$$k \oplus l = \begin{cases} k+l, & \text{если } k+l<n, \\ k+l-n, & \text{если } k+l \geqslant n. \end{cases} \quad (1)$$

Например, при $n=3$ имеется три класса: 0, 1, 2. Таблица сложения этих классов выглядит следующим образом:

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Множество Z_n относительно операции $\oplus$ образует группу, называемую *группой вычетов по модулю n*. В самом деле, все групповые аксиомы выполнены: нейтральным элементом служит нулевой класс; элементом, противоположным классу k ($k \neq 0$), является класс $n-k$ ($-0=0$). Наконец, операция $\oplus$ ассоциативна (проверьте!).

Лицо второе (геометрическое). Множество поворотов плоскости вокруг центра O правильного n-угольника на углы α, при которых этот n-угольник отображается на себя, также образует группу относительно операции $\circ$ композиции перемещений. Поворотом, обратным для R^α, является $R^{-\alpha}$:

$$R^\alpha \circ R^{-\alpha} = E.$$

В этой группе n элементов (повороты R^{α_k}, где $\alpha_k = k \cdot \frac{360°}{n}$, $k=0, 1, \ldots, n-1$; см. рис. 2), а правило композиции поворотов можно записать так:

$$R^{\alpha_k} \circ R^{\alpha_m} = \begin{cases} R^{\alpha_{k+m}}, & \text{если } k+m<n, \\ R^{\alpha_{k+m-n}}, & \text{если } k+m \geqslant n. \end{cases}$$

Это правило очень похоже на правило (1) сложения классов, используя его, мы могли бы написать

$$R^{\alpha_k} \circ R^{\alpha_m} = R^{\alpha_{k \oplus m}}. \quad (2)$$

Лицо третье (комплексное). Его смогут разглядеть те, кто знаком с комплексными числами и действиями над ними. Нас интересует сейчас множество всех комплексных корней степени n из единицы, то есть множество решений уравнения $z^n=1$.

Если $z=\cos\alpha + i\sin\alpha$ — тригонометрическая форма такого числа, то, согласно правилу умножения комплексных чисел, $z^n = \cos n\alpha + i \sin n\alpha$. Равенство $z^n=1$ выполняется при $n\alpha = 2\pi k$, где k — целое, поэтому все n различных корней из единицы задаются формулой

$$z_k = \cos\frac{2\pi}{n}k + i\sin\frac{2\pi}{n}k$$

($k=0, 1, \ldots, n-1$). Легко проверить, что множество всех этих корней образует группу со следующим правилом умножения:

$$z_k \cdot z_l = z_{k \oplus l}. \qquad (3)$$

Напомним, что каждое комплексное число $z=r(\cos\alpha+i\sin\alpha)$ с модулем r и аргументом α изображается в прямоугольной системе координат вектором длины r, составляющим с осью Ox угол α. Поэтому числа z_k изобразятся векторами длины 1 так, что каждые два соседних вектора составят между собой угол $2\pi/n$. Иными словами, концы этих векторов разместятся в вершинах правильного n-угольника (рис. 3).

Теперь ясно, что группа корней n-й степени из единицы и группа поворотов R^{α_k} по существу «не отличаются» и «схожи» с группой Z_n. Дабы уточнить последнюю фразу, следует ввести одно из важнейших понятий математики.

Понятие изоморфизма

Рассмотрим какие-либо две группы G и H. Предположим, что между элементами этих групп установлено взаимно однозначное соответствие (обозначим его буквой φ), то есть задано обратимое отображение φ множества G на множество H. Выберем в G произвольную пару элементов a, b; им соответствуют некоторые элементы $\varphi(a)$, $\varphi(b)$ в H. Так как G и H — группы, то определены произведения $ab \in G$, $\varphi(a)\,\varphi(b) \in H$, а также $\varphi(ab) \in H$.

Определение. Группы G и H называются *изоморфными*, если существует взаимно однозначное отображение φ группы G на группу H, сохраняющее произведение, то есть такое, что для любых $a, b \in G$ будет

$$\varphi(a)\,\varphi(b) = \varphi(ab). \qquad (4)$$

Это отображение называется *изоморфизмом*.

Изоморфизм двух групп означает, что законы, которым подчиняются операции в обеих группах, *идентичны*, и что всякое свойство, присущее операции в одной из групп, в равной

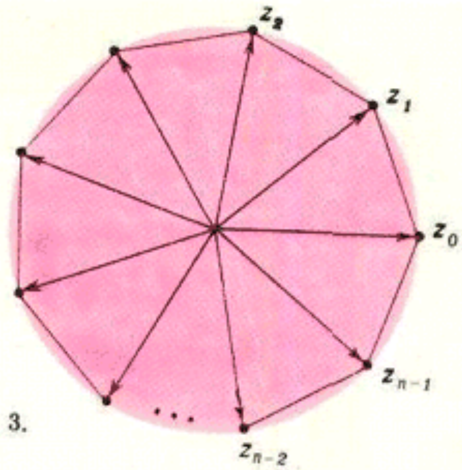

Рис. 3.

мере присуще операции в изоморфной ей группе. Поэтому изоморфные группы называют «абстрактно равными» и отождествляют между собой, что приводит к возникновению одной абстрактной группы: группы, относительно природы элементов которой не делается никаких конкретных предположений.

Примером изоморфных групп являются три только что рассмотренные группы: и группа вычетов, и группа поворотов, и группа корней из единицы в действительности — лишь три реализации одной и той же абстрактной группы.

Изоморфизмом ψ между группой поворотов и группой Z_n является отображение

$$\psi(R^{\alpha_k}) = k.$$

Ясно, что при этом произведению вращений будет соответствовать, как это следует из формулы (2), сумма вычетов.

Изоморфизм φ' между группой поворотов правильного n-угольника и группой корней n-й степени из единицы устанавливается соотношением

$$\varphi(R^{\alpha_k}) = z_k.$$

Правило (4), конечно, выполняется, оно вытекает из равенства (3).

Задача 8. Установите изоморфизм между группой корней n-й степени из единицы и группой Z_n вычетов по модулю n.

Задача 9. Постройте изоморфизм между аддитивной группой всех действительных чисел и мультипликативной группой положительных действительных чисел.

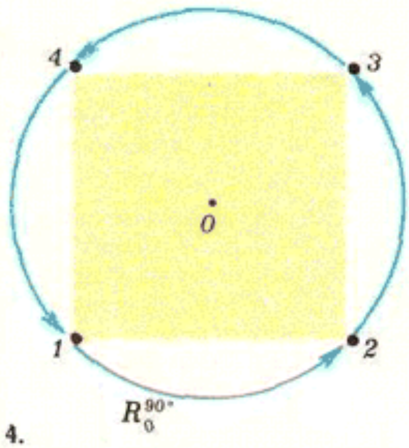

Рис. 4.

Группы симметрии

Отличить симметричную фигуру от несимметричной легко — в этом нам помогает интуиция. Она подсказывает нам, что квадрат симметричнее ромба, а окружность симметричнее эллипса. Но одной интуиции недостаточно. Соображения более обстоятельные возникают при рассмотрении *перемещений пространства* (или плоскости), *при которых данная фигура F отображется на себя*. Множество таких преобразований (с операцией композиции перемещений) образует группу, называемую *группой симметрии фигуры F*. Об этом вы уже знаете из статьи А. Колмогорова (см. с. 4.), да и мы уже приводили этот пример группы. Теперь мы изучим группы симметрии некоторых фигур.

Начнем с окружности, которая издревле представлялась людям воплощением совершенства и образцом симметрии. При любом повороте относительно центра и при зеркальном отражении относительно произвольного диаметра окружность самосовмещается. Таким образом, группа симметрии окружности состоит из всех поворотов R_O^α вокруг центра O окружности и всех осевых симметрий S_l с осями l, проходящими через точку O.

Значительно меньше группа симметрии эллипса — она состоит из двух осевых симметрий относительно взаимно перпендикулярных сопряженных диаметров эллипса (об эллипсе рассказано в «Кванте», 1975, № 1), поворота $R_O^{180°}$ (центральной симметрии) вокруг центра эллипса и, конечно, тождественного отображения E. Такой же будет группа симметрии ромба.

А вот у квадрата группа симметрии побольше, ее мы сейчас и рассмотрим.

Нарисуем на плоскости квадрат и обозначим его вершины цифрами 1, 2, 3, 4. При любом самосовмещении квадрата каждая его вершина оказывается на месте некоторой вершины. Так, например, при повороте $R_O^{90°}$ (O — центр квадрата) вершины 1, 2, 3, 4 перейдут соответственно в вершины 2, 3, 4, 1 (рис. 4): $R_O^{90°}(1) = 2$, $R_O^{90°}(2) = 3$, $R_O^{90°}(3) = 4$, $R_O^{90°}(4) = 1$. Это факт можно записать иначе:

$$1 \to 2,\ 2 \to 3,\ 3 \to 4,\ 4 \to 1.$$

Подобным же образом повороту $R_O^{180°}$ сопоставляется запись

$$1 \to 3,\ 2 \to 4,\ 3 \to 1,\ 4 \to 2.$$

Сказанное можно записать и в иной форме, смысл которой ясен из предыдущего:

$$R_O^{90°} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},\quad R_O^{180°} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Мы получили то, что математики называют *подстановкой*: обратимое отображение конечного множества M на себя (здесь — множества четырех точек — вершин квадрата). Занумеровав элементы этого конечного множества числами 1, 2, …, n, мы сможем записать каждую подстановку в виде таблицы

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ a_1 & a_2 & a_3 & a_4 & \ldots & a_n \end{pmatrix},$$

в нижней строке которой записаны те же числа, что и в верхней, но в ином порядке. Подстановка, следовательно, состоит в том, что каждому элементу a_k из M ставится в соответствие единственный элемент b_k из того же множества, и разным элементам a_k соответствуют разные b_k.

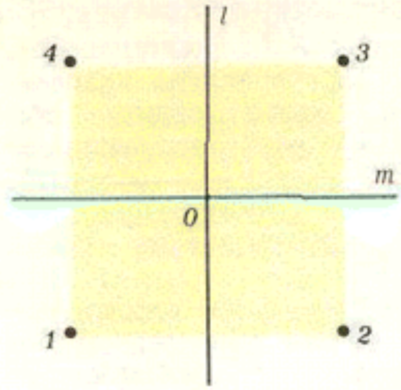

Рис. 5.

При такой точке зрения для одной и той же подстановки можно принять различные записи, например:

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

Обычно элементы верхней строки располагают в естественном порядке, и потому в общем виде подстановку из n элементов записывают в виде

$$\begin{pmatrix}1 & 2 & \ldots & n\\ a_1 & a_2 & \ldots & a_n\end{pmatrix}.$$

Пусть σ и τ — две подстановки множества M. Произведением $\tau\circ\sigma$ подстановки σ на τ назовем такую подстановку ω, которая возникает в результате последовательного выполнения сначала σ, а затем τ. Таким образом, если σ элементу a ставит в соответствие b, а τ элементу b ставит в соответствие c, то произведение $\tau\circ\sigma$ элементу a сопоставляет c. Произведение зависит от порядка сомножителей. Действительно, если τ сопоставляет элементу a элемент d, а σ элементу d сопоставляет f, то произведение $\sigma\circ\tau$ отображает a в f.

Тождественная подстановка

$$e=\begin{pmatrix}1 & 2 & \ldots & n\\ 1 & 2 & \ldots & n\end{pmatrix},$$

не изменяющая расположения элементов, играет роль единицы. Для каждой подстановки ω имеется единственная ей обратная ω^{-1} такая, что $\omega\circ\omega^{-1}=\omega^{-1}\circ\omega=e$.

Задача 10. Докажите, что определенное выше умножение подстановок ассоциативно.

Задача 11. Покажите, что подстановка ω^{-1} возникает из заданной, если поменять местами ее верхнюю и нижнюю строки.

Множество подстановок из n элементов образует группу (обратимых отображений конечного множества M на себя), ее называют «симметрической группой n-й степени» и обозначают через S_n.

Задача 12. Выпишите подстановки, соответствующие осевым симметриям квадрата (рис. 5) $S_{(24)}$, $S_{(13)}$, S_l, S_m и повороту $R_O^{270°}$ (здесь (24) — прямая, проходящая через точки 2, 4 и т. п.).

Задача 13. Докажите, что группа подстановок четырех элементов состоит из 24 элементов.

Задача 14. Убедитесь, что не каждой из этих подстановок можно поставить в соответствие самосовмещение квадрата.

Последняя задача показывает, что в группе симметрии квадрата меньше 24 элементов — каждому самосовмещению квадрата соответствует подстановка (4 вершин квадрата), но не каждой подстановке соответствует самосовмещение квадрата.

Этим квадрат отличается от треугольника: у треугольника группа симметрии состоит из шести элементов и подстановок 3 вершин треугольника тоже шесть, причем группа симметрии треугольника изоморфна группе подстановок 3 элементов.

Заметим, что группа симметрии квадрата (как и треугольника) *некоммутативна:*

$$S_{(13)}\circ S_l=R_O^{-90°}\neq R_O^{90°}=S_l\circ S_{(13)}.$$

Задача 15. Найдите все перемещения плоскости, отображающие квадрат на себя (их будет всего восемь).

Задача 16. Составьте таблицу композиций перемещений плоскости, отображающих квадрат на себя (подобно таблице умножения чисел от 1 до 9).

Задача 17. Докажите, что число различных подстановок множества из n элементов равно $n!$ ($n!=1\cdot 2\cdot 3\cdot \ldots \cdot n$).

В заключение заметим, что свойства и строение абстрактных и конкретных реализаций групп изучаются математической дисциплиной, называемой теорией групп, которая ныне нашла широкое применение во многих разделах математики, теоретической физики, химии, кристаллографии, теории связи и в других науках.