GROUP CALCULUS

A. Yu. OL'SHANSKII

An axiomatic approach to the group definition, one of the most important in mathematics, is given. The definitions are accompanied by clear examples and exercises that are useful for optional classes at high school. A new proof of the Cauchy theorem is found not to be beyond the scope of the high-school mathematical programs.

Представлен аксиоматический подход к понятию группы – одному из важнейших в математике. Приводимые определения сопровождаются простыми примерами и упражнениями, полезными для факультативных занятий в школе. Чтобы сделать материал не выходящим за рамки школьной программы, для теоремы Коши найдено элементарное доказательство.

ГРУППОВЫЕ ИСЧИСЛЕНИЯ

А. Ю. ОЛЬШАНСКИЙ

Московский государственный университет им. М.В. Ломоносова

1. ВВЕДЕНИЕ

Используемые в математике алгебраические операции разнообразны и часто непохожи на арифметические действия с числами. В статье [1] мы обратили внимание на важную роль умножения симметрий геометрических фигур или многочленов от нескольких переменных. Такого рода произведения естественно изучать в контексте групп преобразований. Теперь мы переходим к общему понятию группы, которое оказалось одним из центральных в современной математике. На этот раз основной акцент делается на аксиоматическом подходе и его возможностях. Не забывая о примерах, мы коротко напоминаем в разделе 2 некоторые определения, чтобы читатель мог знакомиться с настоящей статьей независимо от предыдущей. По-прежнему не предполагаем никаких знаний вне рамок школьной программы.

2. ПРОИЗВЕДЕНИЕ СИММЕТРИЙ

Начнем с примера. Сколько существует различных поворотов в трехмерном пространстве, совмещающих куб (рис. 1) с самим собой? Перечислим типы таких поворотов. Во-первых, мы всегда учитываем *тождественное преобразование*, при котором каждая точка остается на своем месте. Во-вторых, проводя ось AB через середины противоположных граней, находим три различных нетождественных поворота около этой оси на углы 90°, 180° и 270°. (У куба три такие оси.) В-третьих, около диагонали $1–7$ куб можно поворачивать на 120° и 240°. (Имеются еще три такие диагонали: $2–8$, $3–5$ и $4–6$.) Наконец, около оси CD, проходящей через середины противоположных ребер, куб можно повернуть на

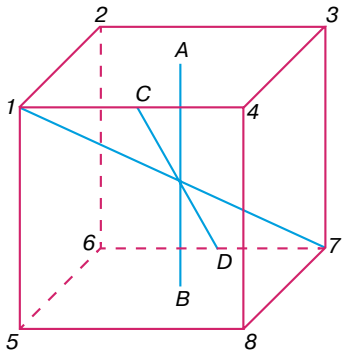


Рис. 1.

180°. (Имеются шесть таких осей.) В итоге число поворотов, самосовмещающих куб, составляет $1 + 3 \times \times 3 + 2 \cdot 4 + 6 = 24$ (то есть *порядок группы* поворотов куба равен 24).

Что получится, если последовательно выполнить два каких-либо поворота, например поворот α около *AB* на 90° (при котором вершина *1* переходит в вершину *2*, *2* переходит в *3* и т.д.), а затем поворот β на 120° около диагонали *1*–*7* (когда вершина *2* переходит в вершину *4*, *4* переходит в *5* и т.д.)? Для ответа достаточно проследить за судьбой каждой вершины. К примеру, под действием поворота α вершина *1* переходит в вершину *2*, а затем вершина *2* под действием поворота β перейдет в *4*. Таким образом, при выполнении поворота β вслед за α вершина *1* перейдет в *4*. Аналогично в результате последовательного выполнения α и β вершины *3* и *5*, *2* и *8*, *4* и *6* поменяются местами. Значит, результатом оказался поворот γ куба вокруг оси *CD* на 180°.

Читатель может найти итог выполнения сначала поворота β, а затем уже α и убедиться, что результирующий поворот отличен от полученного выше преобразования γ. Точно так же можно вычислить "произведение", то есть результат последовательного выполнения, любых двух поворотов.

Формально для определения *произведения* $h = fg$ двух каких-либо преобразований f и g какой-то фигуры или вообще какого-то множества X (например, поворотов куба) нужно для любой точки x определить ее *образ* y (то есть точку, в которую x переходит) по правилу $y = h(x) = f(g(x))$: сначала к x применяется преобразование g, а к полученной точке – f. Точка x является *прообразом* точки y при преобразовании h.

В приведенном примере образом вершины *1* для преобразования α будет вершина *2*, то есть $\alpha(1) = 2$. Далее $\beta(2) = 4$, а в итоге $\gamma(1) = \beta(\alpha(1)) = \beta(2) = 4$ для преобразования $\gamma = \beta\alpha$. В то же время $(\alpha\beta)(1) = \alpha(\beta(1)) = \alpha(1) = 2$ (так как $\beta(1) = 1$), откуда следует, в частности, что $\alpha\beta \neq \beta\alpha$.

Нетрудно заметить, что умножение симметрий (и любых преобразований) ассоциативно. Это значит, что для любых трех преобразований f, g, h обязательно $(fg)h = f(gh)$ (ввиду этого равенства скобки, указывающие на порядок выполнения умножений, далее не пишутся). Проверка состоит в повторном использовании определения произведения

$$((fg)h)(x) = (fg)(h(x)) = f(g(h(x))) = f((gh))(x)) = \\ = (f(gh))(x)$$

для любой точки x.

Среди всех симметрий фигуры или преобразований какого-либо множества X выделяется *тождественное преобразование* e, оставляющее каждую точку из X на месте: $e(x) = x$. Обозначение e используется в связи с тем, что это преобразование играет роль единицы при умножении: $ef = fe = f$ для всякого преобразования f, так как всегда $e(f(x)) = f(x)$ и $f(e(x)) = f(x)$ по определению преобразования e.

Отметим наконец, что для любого преобразования f имеется *обратное преобразование* g со свойством $fg = gf = e$. Для него используется обозначение $g = f^{-1}$. Преобразование g задается правилом $g(y) = x$, если $f(x) = y$. Это правило основано на определяющем свойстве преобразования *f:* для каждой точки y множества X существует, причем единственный, ее прообраз x. В разобранном выше примере преобразование α^{-1} переводит вершину *2* в вершину *1*, *1* – в *4*, *6* – в *5* и т.д.

3. ОБЩЕЕ ПОНЯТИЕ ГРУППЫ

Перечисленные свойства умножения преобразований позволяют сформулировать общее определение группы. Пусть задано некоторое множество (совокупность) G, состоящее из каких-то "элементов". (Выше в примере и статье [1] в качестве элементов рассматривались отдельные преобразования, а в качестве G – группа симметрий или преобразований.)

Пусть еще задана некоторая операция на множестве G, которую для определенности будем называть умножением. Это означает, что для любых двух элементов a и b из G, данных в определенном порядке, однозначно находится третий элемент d, равный произведению ab.

Тогда G называется *группой*, если:

а) умножение *ассоциативно*: $(ab)c = a(bc)$ для любых элементов a, b, c из G;

б) в G существует *единичный* (или "нейтральный") элемент e, такой, что $ae = ea = a$ для всякого элемента a из G;

в) для всякого элемента a в G существует *обратный* элемент b, то есть такой, что $ab = ba = e$.

Понятие группы не является столь однозначным, как, скажем, понятие целого числа. В частности, бывают *бесконечные* группы, то есть состоящие из бесконечного множества элементов (скажем, группа всех поворотов прямого кругового конуса), и *конечные* группы. Число различных элементов в конечной группе называют ее *порядком*, например группа вращений куба имеет порядок 24.

Несмотря на такую широту содержания, заключенного в определении, уже из общих аксиом а) – в) можно извлечь ряд следствий.

Из аксиомы б) следует единственность нейтрального элемента. Действительно, если теми же свойствами обладает еще какой-то элемент e', то $ee' = e'$ (так как e единичный) и в то же время $ee' = e$ (так как e' единичный). Отсюда $e' = e$.

Нетрудно объяснить и единственность обратного для каждого элемента a. А именно если b и b' – обратные для него, то на основании аксиом а) – в) получаем $b = be = b(ab') = (ba)b' = eb' = b'$, то есть

$b = b'$. Поэтому однозначный смысл приобретает обозначение для обратного элемента: $b = a^{-1}$.

Другими следствиями аксиом группы являются *законы сокращения*. Из равенства вида $ac = ad$ всегда следует, что $c = d$. Для обоснования достаточно элемент ac, совпадающий с ad, умножить слева на a^{-1}. Получаем $a^{-1}ac = a^{-1}ad$, то есть $ec = ed$ и $c = d$. Ввиду возможной некоммутативности умножения мы получили закон *левого* сокращения. Закон *правого* сокращения состоит в том, что из равенства $ca = da$ следует $c = d$. Он выводится с помощью умножения равенства $ca = da$ справа на a^{-1}.

Точно тем же приемом в любой группе G находится единственное решение линейного относительно x уравнения

$$ax = b \qquad (1)$$

для всяких коэффициентов a, b из G. Достаточно умножить левую и правую части в (1) слева на a^{-1}: $a^{-1}ax = a^{-1}b$, $ex = a^{-1}b$ и $x = a^{-1}b$. Проверкой является подстановка произведения $a^{-1}b$ в (1) вместо x.

Например, решая уравнение (1) в группе вращений куба при $a = \alpha$, $b = \beta$, в качестве ответа получим последовательное выполнение поворотов β, а затем α^{-1}. Значит, $x(1) = (\alpha^{-1}\beta)(1) = \alpha^{-1}(1) = 4$. Вычисляя аналогично $x(2)$ и т.д., читатель может убедиться, что решением x оказывается поворот на 90° около оси, проходящей через середины граней *1–4–8–5* и *2–3–7–6*.

Аналогично решением линейного уравнения $xa = b$ во всякой группе будет $x = ba^{-1}$, что в предыдущем примере совпадает с поворотом на 90° около оси, проходящей через середины граней *1–2–6–5* и *4–3–7–8*, при котором вершина *2* переходит в вершину *1* и т.д. (Проверьте!)

В качестве упражнений мы предлагаем решить в произвольной группе уравнение $axb = c$, а также решить уравнение $xa = b$ в группе всех симметрий квадрата (а не только его поворотов), если a – поворот по часовой стрелке на 90°, а b – зеркальная симметрия относительно диагонали.

А сколько решений в конечной группе G порядка n имеет следующее уравнение с двумя неизвестными:

$$xy = b\,? \qquad (2)$$

Для ответа нужно прежде всего иметь в виду, что решением уравнения с двумя неизвестными должна быть упорядоченная пара (x_0, y_0) элементов x_0 и y_0 из группы G, превращающая (2) в верное равенство $x_0y_0 = b$. Если мы выберем x_0 из G произвольно, то после подстановки в (2) получим линейное уравнение $x_0y = b$ относительно y, которое, как мы уже знаем, имеет единственное решение $y = x_0^{-1}b$. Ввиду полной свободы при выборе значения x_0 среди n элементов группы G общее число решений уравнения (2) в группе порядка n равно n.

Для перечисления всех решений (x_0, y_0, z_0) уравнения $xyz = b$ мы аналогично можем произвольно фиксировать x_0 и y_0, сводя его к линейному уравнению $az = b$, где $a = x_0y_0$, а затем однозначно находить z_0. Число всевозможных пар (x_0, y_0), где x_0, y_0 независимо принимают любые значения из G, равно n^2, если n – порядок группы G. (Все эти пары можно свести в квадратную таблицу размера $n \times n$, если ее строки отвечают выбору x_0, а столбцы – выбору y_0.) Значит, уравнение $xyz = b$ с тремя неизвестными имеет в группе порядка n ровно n^2 различных решений. Аналогично уравнение $x_1x_2...x_n = b$ с неизвестными $x_1, x_2, ..., x_p$ имеет n^{p-1} решений в группе G.

4. СВЯЗЬ С ГРУППАМИ ПРЕОБРАЗОВАНИЙ

Понятно уже, что непосредственно из аксиом можно извлечь ряд полезных свойств “абстрактной” группы. Мы говорим здесь об абстрактных группах потому, что есть группы, состоящие из чисел или элементов другой природы, а не только из преобразований. Например, если G обозначает множество всех ненулевых вещественных чисел с обычной операцией умножения, то все аксиомы а) – в) выполнены. (Здесь $e = 1$ – обычная единица.)

К тому же в аксиомах а) – в) заложены по существу все общие свойства умножения преобразований, что подтверждается теоремой Кэли о возможности реализации всякой абстрактной группы в виде некоторой группы преобразований. Для ее иллюстрации возьмем в качестве примера группу G всех вещественных чисел, отличных от 0, с обычной операцией умножения чисел и отождествим ее с некоторой группой преобразований.

Эти преобразования можно задать уже на множестве G ненулевых вещественных чисел. В самом деле, для каждого числа $k \neq 0$ обозначим: F_k – преобразование множества G, состоящее в умножении каждого числа x из G на k ; иначе говоря, $F_k(x) = kx$. К примеру, при $k = 3$ получаем, что $F_3(x) = 3x$, то есть преобразование F_3 – это растяжение вещественной оси в 3 раза. Умножаются такие преобразования так же, как и числа: $F_kF_l = F_{kl}$, поскольку при последовательном выполнении преобразований F_l и F_l результатом является умножение каждого числа x из G на kl, то есть преобразование F_{kl}.

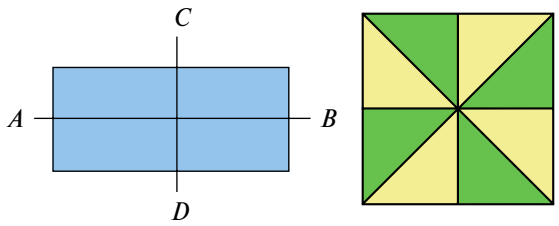
Читатель может убедиться, что тот же прием годится для представления преобразованиями всякой абстрактной группы G. Разница лишь в том, что для некоммутативной группы G нужно уточнить, что рассматриваются ее преобразования F_k, состоящие в умножении *слева* на данный элемент k группы G.

Таким образом, в зависимости от необходимости или удобства можно выбирать между аксиоматическим подходом к группам и их представлением преобразованиями. Исчисление преобразований оказалось на первом плане в статье [1], а ниже преобладает аксиоматический подход.

5. ТАБЛИЦЫ УМНОЖЕНИЯ

Наиболее прямым способом задания операции в группе, состоящей из элементов произвольной природы, является предъявление полной таблицы умножения. Найдем сначала эту таблицу для группы (обозначим ее *G)* симметрий прямоугольника, показанного на рис. 2*а*. Для этой цели обозначим тождественную симметрию буквой *e*, зеркальные отражения относительно средних линий *AB* и *CD* – буквами *a* и *b* соответственно, а поворот на 180° около центра – буквой *c*.

Вычисляя произведение *ab* (например, прослеживая образы вершин при последовательном выполнении сначала преобразования *b*, а потом *a*), получаем, что *ab* = *c*. Аналогично *ac* = *b*, *aa* = *e* и т.д. В полной таблице умножения (табл. 1*а*) на пересечении строки, помеченной буквой *a,* и столбца, помеченного буквой *b,* будет стоять *c* и т. д.



а *б*

Рис. 2.

Группа поворотов фигуры на рис. 2*б* (обозначим ее *H*) около ее центра по часовой стрелке на углы 0° (тождественное преобразование *e*), 90° (обозначим *a*), 180° (*b*) и 270° (*c*) тоже имеет таблицу умножения размера 4 × 4 (табл. 1*б*), но здесь уже *ac* = *e*, *aa* = *b* и т.д., то есть табл. 1*а* и 1*б* различны.

Можно спросить, не связано ли это отличие с обозначениями (можно было обозначить буквой *a* поворот не на 90°, а на 180° и т. п.). Но никакие переобозначения не могут устранить следующего различия: у первой таблицы на диагонали, идущей из левого верхнего угла в правый нижний, стоит одна и та же буква, а во второй таблице на той же диагонали – разные элементы. Это обстоятельство выражают словами “группы *G* и *H* неизоморфны между собой”.

Таблица 1

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*	*e*	*c*	*b*
b	*b*	*c*	*e*	*a*
c	*c*	*b*	*a*	*e*

а

	e	*a*	*b*	*c*
e	*e*	*a*	*b*	*c*
a	*a*	*b*	*c*	*e*
b	*b*	*c*	*e*	*a*
c	*c*	*e*	*a*	*b*

б

Напротив, в разделе 4 был установлен изоморфизм между двумя бесконечными группами: одной, состоящей из чисел и другой, состоящей из преобразований (когда числу 3 сопоставили растяжение прямой в 3 раза и т.д.). Правда, в этом случае пришлось бы говорить о бесконечных таблицах умножения...

Поскольку новый выбор обозначений для элементов не должен приводить к новой группе, изоморфные группы считаются одинаковыми с алгебраической точки зрения, подобно тому как в евклидовой геометрии равными считаются все квадраты со стороной 1, или в химии – одинаковыми свойства всех молекул H_2O.

С помощью аксиом группы и составления таблиц умножения читателю нетрудно проверить, что две группы изоморфны, если каждая из них имеет порядок 2 (то есть состоит из двух элементов) или каждая имеет порядок 3. Но для групп порядка 4 это уже неверно, как мы видели в табл. 1.

Конечно, если порядки групп разные, то таблицы умножения имеют разные размеры и группы неизоморфны между собой. Обратное же не всегда верно (см. табл. 1 для групп порядка 4). Таким образом, порядок группы является более грубой ее характеристикой, чем изоморфный тип. Другими словами, закон умножения в группе симметрий тоньше характеризует симметричность данной конфигурации, чем чисто количественное ее описание с помощью порядка этой группы.

6. ПОРЯДКИ СИММЕТРИЙ И ЭЛЕМЕНТОВ ГРУППЫ

Другой важной характеристикой абстрактной группы являются порядки ее элементов.

Поворот тетраэдра около одной из осей на угол 120° является симметрией третьего порядка, то есть после троекратного применения этого преобразования каждая точка переходит в себя же. Другими словами, тройное произведение *fff* для данного преобразования *f* равно тождественному преобразованию *e*, что сокращенно записывают как $f^3 = e$. Вообще запись f^n (*f* в степени *n*) заменяет *n*-кратное повторение *f* в виде сомножителя.

Аналогично поворот на 90° есть симметрия квадрата 4-го порядка, а поворот на 180° или зеркальное отражение – его симметрии 2-го порядка.

Заметим, что порядки симметрий делят порядки групп симметрий. Например, группа симметрий квадрата состоит из 8 элементов, и ее порядок 8 делится на 4 и на 2, то есть на порядки приведенных выше симметрий. С помощью группового исчисления,

основанного только на аксиомах группы, можно продемонстрировать справедливость нашего наблюдения для любых конечных групп, что мы и сделаем, доказав два утверждения, восходящих к Лагранжу и Коши.

Для этого выберем произвольный элемент a конечной группы G и выпишем ряд его степеней, в котором удобно по определению считать, что $a^0 = e$:

$$a^0 = e, \quad a^1 = a, \quad a^2, a^3, \quad \ldots \qquad (3)$$

Имеют смысл и степени с целыми отрицательными показателями: a^{-1} – обратный для a элемент, а далее, по определению, $a^{-2} = a^{-1}a^{-1} = (a^{-1})^2$, ..., $a^{-m} = (a^{-1})^m$ для всякого положительного целого m. Читателю предлагаем самостоятельно вывести из определения степеней обычные правила $a^k a^l = a^{k+l}$ и $(a^k)^l = a^{kl}$ для любых целых (не только положительных) показателей k и l.

Ввиду конечности группы G в бесконечной последовательности (3) неизбежны повторения, то есть найдутся различные положительные показатели k и l со свойством $a^k = a^l$. Пусть для определенности $k > l$. Тогда после сокращения справа на a^l равенство $a^k = ea^l$ превращается в $a^{k-l} = e$, где $k - l > 0$. Поэтому для каждого элемента a можно определить его *порядок* как наименьший положительный показатель n, такой, что $a^n = e$.

Если n – порядок элемента a, то среди n его степеней

$$e = a^0, a, a^2, \ldots, a^{n-1} \qquad (4)$$

повторений уже быть не может, так как равенство вида $a^k = a^l$ при условии, что $0 \le l < k \le n - 1$ приводит, как и выше, к равенству $a^{k-l} = e$, где уже $0 < k - l < n$, вопреки определению порядка n как *наименьшего* целого положительного числа со свойством $a^n = e$.

Любая другая степень a^m совпадает с одной из перечисленных в списке (4), например $a^n = e$, $a^{n+1} = a^n \cdot a = ea = a$, ... Далее ввиду единственности обратного элемента $a^{-1} = a^{n-1}$, так как $a^{n-1}a = aa^{n-1} = a^n = e$, аналогично $a^{-2} = a^{n-2}$ и т.д.

Таким образом, среди всех степеней элемента a имеется ровно n различных, если n – порядок элемента a.

7. ДВА СВОЙСТВА ПОРЯДКОВ

Теорема 1. *Порядок любого элемента произвольной конечной группы G является делителем порядка группы G.*

Сформулированная теорема позволяет по локальной информации о порядке отдельного элемента получить некоторую глобальную – о порядке всей группы. Например, порядок группы симметрий тетраэдра заведомо кратен трем, так как была указана его симметрия третьего порядка. Кстати, в качестве упражнения можно порекомендовать убедиться, что группа всех симметрий (а не только вращений) тетраэдра (куба) имеет порядок 24 (соответственно 48), и найти возможные порядки различных элементов этой группы.

Доказательство теоремы 1. Обозначим буквой n порядок произвольно выбранного элемента a из G. Если выбрать еще какой-нибудь элемент b, не входящий в список (4), то будут различны все n произведений из следующей "a-орбиты":

$$b = be, ba, ba^2, \ldots, ba^{n-1}. \qquad (5)$$

В самом деле, равенство вида $ba^k = ba^l$ после левого сокращения на b влекло бы уже разобранное в конце раздела 6 равенство $a^k = a^l$.

Предположим, что в G есть еще какой-нибудь элемент c, не входящий в списки (4) и (5). С его помощью можно построить еще одну a-орбиту:

$$c, ca, ca^2, \ldots, ca^{n-1}, \qquad (6)$$

состоящую, как и (6), из n различных элементов.

Проверим, что в списках (5) и (6) нет ни одного общего элемента. В противном случае выполнялось бы равенство $ba^s = ca^t$ для каких-нибудь целых s и t. После умножения обеих частей этого равенства справа на a^{-t} получилось бы, что $c = ba^{s-t}$. Но всякая степень элемента a, в том числе и a^{s-t}, совпадает с одним из элементов списка (4) (см. конец раздела 6). Поэтому равенство $c = ba^{s-t}$ означало бы, что элемент c содержится в списке (5) вопреки выбору для c.

Точно так же нет общих элементов в списках (4) и (5) или (4) и (6).

Если списками (4) – (6) не исчерпывается вся группа G, то, выбрав еще один элемент d из G, не перечисленный в них, получим еще один список d, da, da^2, ..., da^{n-1} и т.д. Ввиду конечности группы G она будет рано или поздно полностью исчерпана без повторений списками, каждый из которых содержит n различных элементов. Это означает, что общее число элементов в G кратно n и теорема 1 доказана.

Нельзя, однако, утверждать, что для любого делителя p порядка группы G в G найдется элемент порядка p. Например, в группе вращений куба порядка 24 нет элементов порядка 6, 8 или 12, а в группе порядка 4 с таблицей умножения (табл. 1a) нет элементов порядка 4. (И то и другое проверяется простым перебором элементов.) Но для некоторых значений делителя p порядка группы такого рода обращение теоремы 3 оказывается верным.

Рассмотрим случай, когда $p = 2$ и порядок n группы G делится на $p = 2$, то есть n является четным числом. Нам пригодится следующее вспомогательное уравнение от двух переменных в G:

$$xy = e. \qquad (7)$$

Оно является частным случаем уравнения (2) при $b = e$, а значит, имеет n различных решений.

Если $x_0y_0 = e$, то после умножения этого равенства слева на x_0^{-1}, а справа на x_0 получим, что $x_0^{-1}x_0y_0x_0 = x_0^{-1}ex_0$, а после упрощения последнего равенства

на основании аксиом группы имеем $y_0x_0 = e$. Поэтому если пара (y_0, x_0) – решение уравнения (7), то и пара (y_0, x_0) тоже решение.

Вторая пара отличается от первой при условии $x_0 \neq y_0$. То есть при условии, что значения неизвестных не совпадают, получаем четное число таких решений, учитывая их все попарно. Поскольку общее число решений n уравнения (7) тоже четно, четным должно быть и число оставшихся решений вида (x_0, x_0) с совпадающими значениями неизвестных, то есть четно число N элементов x_0 группы G со свойством $x_0^2 = e$. Среди таких элементов, очевидно, содержится единичный: $e^2 = e$. Отсюда $N > 0$, а тогда из четности числа N следует, что $N > 1$. Значит, имеется еще хотя бы один элемент $x_0 \neq e$, такой, что $x_0^2 = e$.

Мы доказали, что в любой группе четного порядка есть элемент порядка 2. Повторим аналогичное рассуждение для $p = 3$, то есть когда n делится на 3.

Теперь вспомогательным уравнением служит $xyz = e$ с числом решений n^2 (см. раздел 3), которое, как и n, делится на 3.

Каждое решение (x_0, y_0, z_0) приводит еще к решениям (y_0, z_0, x_0) и (z_0, x_0, y_0), что объясняется так же, как и в случае $p = 2$. Если какие-то два из этих трех решений совпадают, к примеру $(x_0, y_0, z_0) = (y_0, z_0, x_0)$, то есть $x_0 = y_0, y_0 = z_0, z_0 = x_0$, то получаем, что $x_0^3 = e$. Поэтому, группируя (теперь уже по три) те решения, у которых не все значения неизвестных совпадают, получаем, что делится на 3 число элементов x_0 группы G со свойством $x_0^3 = e$. Следовательно, среди них найдется и неединичный элемент x_0. Его порядок равен трем, а не меньше, ибо если $x_0^2 = e$, то вместе с $x_0^3 = e$ получили бы, что и $x_0 = e$.

Итак, если порядок группы делится на 3, то в ней есть элемент порядка 3.

На самом деле в приведенных рассуждениях важно лишь, что p – простое число, то есть не имеет делителей, больших 1 и меньших p одновременно.

Теорема 2. *Если p – простой делитель порядка n конечной группы G, то в G найдется хотя бы один элемент порядка p.*

Мы оставляем читателю возможность доказать теорему на основании разобранных случаев $p = 2, 3$. Очевидно, что теперь пригодится уравнение $x_1x_2...x_p = e$ с неизвестными $x_1, x_2, ..., x_p$, у которого n^{p-1} решений (см. раздел 3). Каким образом нужно использовать простоту числа p? Если общий случай вызывает затруднения, разберите сначала случай $p = 5$. В чем состоят пробелы аналогичного доказательства при $p = 4$?

ЛИТЕРАТУРА

1. *Ольшанский А.Ю.* Умножение симметрий и преобразований // Соросовский Образовательный Журнал. 1996. № 5. С. 115 – 120.

* * *

Александр Юрьевич Ольшанский, доктор физико-математических наук, профессор кафедры высшей алгебры механико-математического факультета Московского государственного университета им. М.В. Ломоносова, входит в состав редколлегий нескольких международных математических журналов. Область научных интересов: теория групп. Автор более 50 научных работ.