Э. Белага

АЛГЕБРА — ДРЕВНЯЯ И СОВРЕМЕННАЯ

Вы уже прочли статьи А. Колмогорова «Группы преобразований» и Л. Садовского и М. Аршинова «Группы», в которых вводятся понятия бинарной операции и группы. Чтобы привыкнуть к этим новым для вас понятиям, надо разобрать несколько примеров «с карандашом в руке». В этом вам и поможет помещаемая ниже статья. В ней рассказывается об умножении слов, самосовмещений правильных многогранников, узлов и подстановок, о применении абстрактной теории к решению конкретных задач. Внимательный и терпеливый читатель сможет самостоятельно вывести много замечательных свойств операций над этими объектами, разбирая условия и отыскивая решения задач (они служат продолжением основного текста). Наиболее интересные и, как правило, при этом довольно трудные задачи отмечены звездочкой.

I. ВСЕ ПРОЧЕЕ — ДЕЛО РУК ЧЕЛОВЕЧЕСКИХ...

У первобытных племен названия чисел были неотделимы от названия перечисляемых предметов. Не «два» или «три», а лишь «две реки» или «три воина». С появлением отвлеченного понятия о числе родилась математика. Возможно, поэтому выдающийся немецкий математик Леопольд Кронекер произнес когда-то свою столь же парадоксальную, сколь и знаменитую фразу: «Целое число создал господь бог, все прочее — дело рук человеческих».

Потребовалось несколько тысячелетий, чтобы человечество научилось представлять решения задач в виде формул. Потом в этих формулах вместо чисел появились буквы. Новая «буквенная» арифметика стала называться алгеброй. А затем алгебраическая символика и алгебраические действия были распространены на самые разнообразные объекты неарифметической природы — подстановки, матрицы, геометрические преобразования и др., а числовая прямая (или комплексная плоскость) оказалась всего лишь одной из многих, очень многих алгебраических структур, изучаемых в новой алгебре.

II. О «ВЕЩАХ», КОТОРЫЕ МОЖНО «ПЕРЕМНОЖАТЬ», А ИНОГДА И ДЕЛИТЬ, ХОТЯ ОНИ И НЕ ЧИСЛА

К тому, что числа можно складывать, умножать, вычитать и делить, нас приучают очень рано. Удивительно — и к этому тоже нужно привыкать,— что «складывать» (или «умножать») можно и «вещи» не числовой природы.

Пример первый: слова

Алфавитом будем называть любую совокупность символов. Мы ограничимся конечными алфавитами (в алгебре и математической логике поль-

зуются и бесконечными). Вот два примера алфавитов:

A_1. *Алфавит, состоящий из двух греческих букв*: α *и* β.

A_2. *Арифметический алфавит: цифры от* 0 *до* 9, *символы арифметических действий, знак равенства и круглые скобки*:

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ +,\ -,\ :,\ \times,\ =,\ ),(\}.$$

Словом над алфавитом A мы будем называть *любую конечную последовательность символов из* A. Вот примеры слов над двумя описанными выше алфавитами (чтобы отделить запись слова от окружающего текста, мы «упаковываем» его в угловые скобки):

(A_1): $\langle\alpha\alpha\beta\rangle$, $\langle\alpha\beta\alpha\beta\alpha\beta\rangle$, $\langle\rangle$;
(A_2): $\langle 1976\rangle$, $\langle 2+2=4\rangle$, $\langle -)+)\,:\,(3)\rangle$.

Слово может быть и «пустым», то есть вовсе не содержать символов (последнее «слово» в первом примере), такое слово обозначают буквой λ: $\lambda = \langle\rangle$. Множество слов над данным алфавитом A обозначим через $C(A)$. Его элементы, то есть слова, мы будем обозначать малыми латинскими буквами (они не принадлежат алфавитам, которые нам здесь приходится рассматривать).

Произведением, или *композицией*, двух слов a и b из $C(A)$ мы будем называть *слово* c (и писать: $c = a \otimes b$), *полученное приписыванием к слову* a *справа от него слова* b. Вот примеры композиции слов:

(A_1): $a = \langle\alpha\rangle$, $b = \langle\alpha\beta\rangle$, $c = a \otimes b = \langle\alpha\alpha\beta\rangle$;
(A_2): $a = \langle 2+2\rangle$, $b = \langle =4\rangle$, $c = a \otimes b = \langle 2+2=4\rangle$.

Пустое слово не содержит символов, поэтому $a \otimes \lambda = \lambda \otimes a = a$ для любого слова a из $C(A)$, то есть пустое слово λ при перемножении слов ведет себя как единица при перемножении чисел.

Если продолжить поиски сходства и различий между умножением слов и умножением чисел, то можно заметить, что операция «$\otimes$» ассоциативна:

$$(a \otimes b) \otimes c = a \otimes (b \otimes c),$$

поэтому имеет смысл запись $a \otimes b \otimes c$.

Задача 1. Для любого слова a из $C(A)$ определим его неотрицательные степени, положив $a^0 = \lambda$, $a^1 = a$, $a^2 = a \otimes a$, вообще $a^{n+1} = a \otimes a^n$. Докажите, что для любых целых неотрицательных чисел выполняется равенство

$$a^m \otimes a^n = a^{m+n}.$$

Справедливость последнего равенства позволяет нам сокращать запись некоторых слов: вместо $a = \langle\alpha\alpha\alpha\beta\beta\beta\alpha\alpha\alpha\alpha\rangle$ мы можем написать $a = \langle\alpha\rangle^3 \otimes \langle\beta\rangle^3 \otimes \langle\alpha\rangle^4$ или, допуская некоторую вольность записи, $a = \langle\alpha^3\beta^3\alpha^4\rangle$. Но менять порядок букв в слове, вообще говоря, нельзя, потому что операция «$\otimes$» может быть не коммутативной, то есть $a \otimes b$ может не совпадать с $b \otimes a$.

Задача 2. а) Над каким алфавитом операция «$\otimes$» коммутативна, то есть для любых слов a и b будет $a \otimes b = b \otimes a$?

б)* Как должны быть устроены два слова a и b над алфавитом A, содержащим два или более символов, чтобы композиция этих слов не зависела от их порядка?

Пример второй: самосовмещения

Как известно, *конгруэнтность* (раньше говорили «равенство») фигур и тел в геометрии устанавливается перемещением: *если существует перемещение плоскости* (или пространства), *при котором одна фигура отображается на другую, то эти фигуры конгруэнтны*. Перемещение, при котором некоторая фигура отображается на себя, будем называть ее *самосовмещением*.

Для куба, например, найдется всего 48 различных самосовмещений. Действительно, закрасим одну грань куба и отметим направление на одном из ребер, ограничивающих эту грань (рис. 1). Тогда самосовмещение куба определяется тем, в какую грань куба отображается окрашенная грань, в какое ребро этой грани переходит отмеченное ребро и в какой конец этого ребра направлена стрелка (по этим данным однозначно опре-

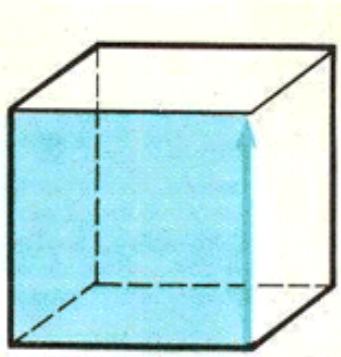


Рис. 1.

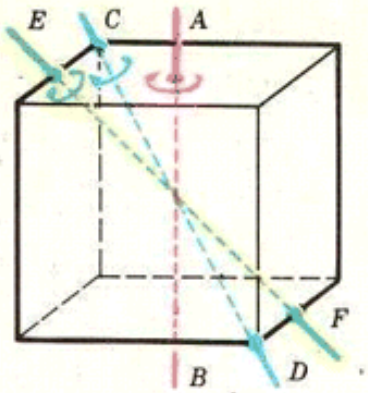


Рис. 2.

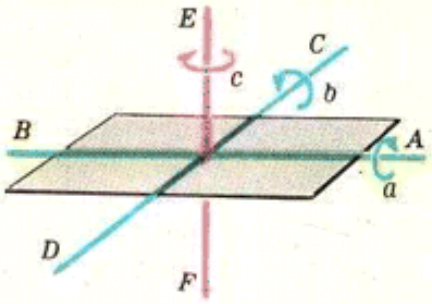


Рис. 3.

деляется положение куба). У куба 6 граней, у каждой грани 4 ребра, у каждого ребра 2 конца, итого $6 \times 4 \times 2 = 48$ способов.

Произведение $c = a \circ b$ *самосовмещений* a и b правильного многогранника Δ определяется как обычная композиция перемещений: сначала выполняется b, а затем a *). Проверьте, что $(a \circ b) \circ c = a \circ (b \circ c)$ для любых трех самосовмещений a, b, c из множества $\Gamma(\Delta)$ всех самосовмещений тела Δ (ассоциативность; сравните с описанием группы на с. 8 и аксиомой III группы там же).

Задача 3. Докажите, что последовательное выполнение двух поворотов куба: сначала вокруг оси AB (рис. 2) на угол 90°, а затем вокруг оси CD на угол 120°, — можно записать одним поворотом вокруг оси EF на 180°, что и является произведением двух первых поворотов. Зависит ли это произведение от порядка выполнения поворотов?

*) Такой порядок записи удобен тем, что образ $(a \circ b)(M)$ точки M при отображении $a \circ b$ будет $a(b(M))$.

Задача 4. Докажите, что существует всего четыре различных самосовмещения прямоугольника в пространстве (рис. 3): тождественное e, поворот a вокруг AB, b — вокруг CD, c — вокруг EF, причем $a^2 = b^2 = c^2 = e$, $a \circ b = b \circ a = c$, $b \circ c = c \circ b = a$, $a \circ c = c \circ a = b$.

Последние равенства задачи 4 можно записать в виде следующей таблицы умножения:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Очевидно, что всякому самосовмещению a фигуры или тела Δ соответствует единственное «обратное» a^{-1}, возвращающее тело в начальное положение (a^{-1} может и совпадать с a, как в задаче 4). При этом, если a^{-1} обратно a, то a обратно a^{-1}:

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

ТЕТРАЭДР *ОКТАЭДР* *ИКОСАЭДР*

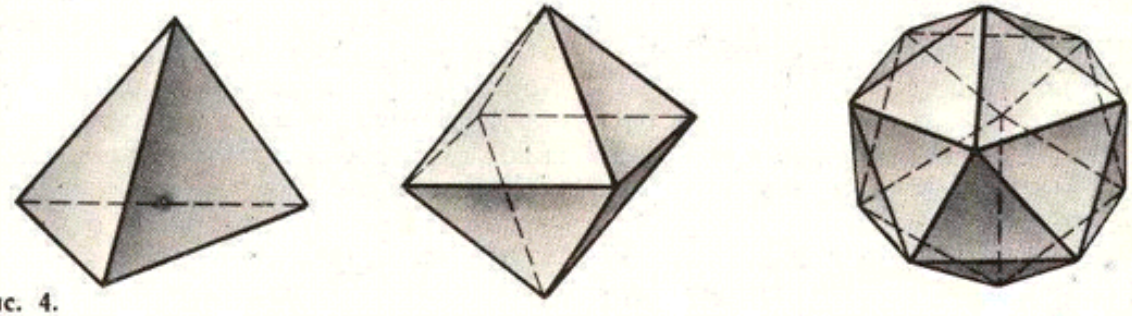


Рис. 4.

Рис. 5.

Теперь можно определить любую целую степень a^k самосовмещения a:

$$a^0 = e,\quad a^1 = a,\quad a^2 = a\circ a,\ \ldots$$
$$\ldots,\quad a^{k+1} = a\circ a^k,\quad a^{-k-1} = a^{-1}\circ a^{-k}.$$

Легко проверить, что $a^k\circ a^l = a^{k+l}$ для любого a из $\Gamma(\Delta)$ и любых целых k и l; в частности, a^k и a^{-k} взаимно обратны. (Сравните с описанием группы на с. 8 и аксиомой II.)

Задача 5. Найдите все самосовмещения правильного тетраэдра, октаэдра и икосаэдра (рис. 4). Какие из них удовлетворяют равенству $a^2 = e$? Равенству $a^3 = e$? Равенству $a^5 = e$? Составьте таблицу умножения для самосовмещений тетраэдра и куба.

Задача 6. Докажите, что любое самосовмещение икосаэдра можно получить «умножениями» из некоторых двух поворотов (на 72°) вокруг двух соседних вершин; точнее, если обозначить эти повороты буквами a, b, то любое самосовмещение икосаэдра можно записать в виде произведения нескольких самосовмещений, каждое из которых есть либо a, либо b.

Пример третий: подстановки

Генетика, как, вероятно, известно читателю, началась с гороха. Теория групп началась с подстановок — именно они были первым «нечисловым» объектом и инструментом новой алгебры для Жозефа-Луи Лагранжа, Паоло Руффини и Эвариста Галуа.

Основное свойство подстановки — переставлять, менять местами числа или буквы из некоторой последовательности. На рисунке 5 изображены подстановки букв в словах-анаграммах, меняющие смысл этих слов; рядом записаны обычные «двухэтажные» числовые записи этих подстановок.

О подстановках рассказано в статье «Группы», мы лишь напомним, что две подстановки b, a одного и того же набора элементов, выполненные одна за другой, дают третью подстановку $c = a\circ b$, называемую их *произведением*. Рисунок 6 иллюстрирует это краткое определение. Множество всех подстановок набора (1, 2, 3, ..., n) образует группу, которая называется «*симметрической группой степени n*» и обозначается через S_n. Эта группа содержит $n!$ подстановок.

Задача 7. Пусть a — некоторая подстановка. Докажите, что если k — наименьшее целое положительное число, для которого $a^k = e$, то из равенства $a^l = e$ следует, что k делит l. Далее докажите, что k делит $n!$ и не превосходит числа $3^{n/3}$*).

Задача 8*. Докажите, что любая подстановка из S_n может быть получена последовательным выполнением некоторого

*)Эта задача уже предлагалась читателям «Кванта» (см. «Квант», 1975, № 11, М355, а также «Квант», 1976, № 8, с. 39).

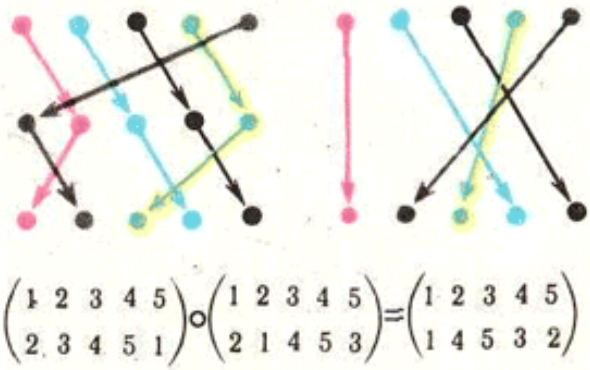
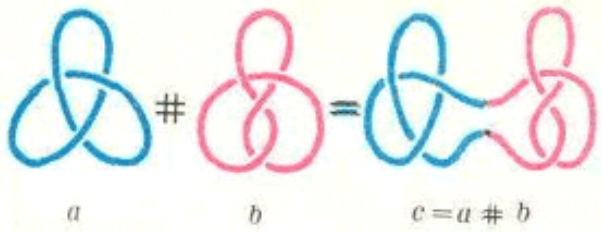


Рис. 6.



a b $c = a \# b$

Рис. 7.

m n

Рис. 8.

числа (и в подходящем порядке) подстановок

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix}$$

и

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

Пример четвертый и последний: узлы

Узел — это замкнутая пространственная кривая, не имеющая точек самопересечения. Узлы изучают в топологии, но алгебраические методы играют при этом решающую роль как в описании отдельных узлов, так и в изучении множества Y всех узлов. Мы рассмотрим здесь свойства композиции узлов. Определение композиции $c = a \# b$ двух узлов a и b ясно из рисунка 7.

Задача 9. Докажите, что композиция — ассоциативная и коммутативная (что несколько неожиданно) операция. Какой узел играет при этом роль единицы?

Можно доказать еще три замечательных свойства операции композиции узлов.

а) *Любой «неединичный»* (то есть не развязываемый без разрывов) *узел необратим*. Иными словами: нельзя развязать узел, завязав рядом с ним другой; или еще иначе: узлы можно умножать, но не делить друг на друга.

б) *Существуют «простые» узлы* — их нельзя представить в виде произведения двух других узлов, каждый из которых отличен от «единичного» (так, узлы a, b на рисунке 7 и m, n на рисунке 8 — простые).

в) *Любой узел либо сам является простым, либо есть композиция простых, причем такое представление единственно.* Какое поразительное сходство со свойствами целых чисел! (Подробно об узлах рассказано в «Кванте», 1975, № 7).

Что увидел алгебраист в наших примерах

Алгебраист подобен топографу — он смотрит на математические объекты «с высоты птичьего полета» и замечает и исследует лишь самые общие связи и закономерности. Зато и результаты его имеют наиболее общий и универсальный характер. (Неизбежны, конечно, и потери — так топографу недоступна красота ландшафтов страны, карту которой он составляет по аэрофотоснимкам.)

То общее, что сближает столь непохожие «вещи», как слова, узлы, подстановки и самосовмещения, может быть выражено на языке определений и аксиом, сформулированных в статье «Группы» (см. с. 7—8). В каждом из этих примеров возникает множество, на котором задана бинарная операция. Не всегда эта операция имеет обратную, но во всех примерах эта операция ассоциативна. Множество с ассоциативной бинарной операцией (аксиома III группы) называется *полугруппой*. Как видите, существование единицы и обратимость элементов (аксиомы I и II группы) в полугруппе не предполагается.

Все рассмотренные нами примеры — полугруппы, а самосовмещения и подстановки образуют даже группы — в них выполняются и аксиомы I и II.

Хорошо знакомые читателю множество N всех натуральных чисел с операцией умножения, множество всех

целых неотрицательных чисел с операцией сложения — также полугруппы, но не группы. Заметим, что в этих двух примерах единица полугруппы существует (1 в первом случае, 0 во втором) и единственна. Впрочем, это не случайно — можно доказать, что если в полугруппе существует единица, то она единственна: если $a * e_1 = e_1 * a = a$ и $a * e_2 = e_2 * a = a$ для любого элемента a из полугруппы, то, в частности, $e_1 * e_2 = e_1$ и $e_1 * e_2 = e_2$, так что $e_1 = e_2$.

Задача 10. Образует ли полугруппу
а) множество натуральных нечетных чисел с операцией умножения;
б) множество неотрицательных четных целых чисел с операцией сложения?

III. СНОВА О ГРУППАХ

Ранее при решении задач нам постоянно приходилось пользоваться специальными свойствами рассматриваемых объектов: тем, что слова состоят из букв, подстановки меняют местами, узлы развязываются и т. п. Методы абстрактной алгебры тем и сильны, что избавляют нас от необходимости вникать в свойства тех «вещей», которые фигурируют в наших операциях.

Теперь мы покажем, как легко и изящно могут быть получены многие свойства наших «вещей» с помощью одних только аксиом I—III.

Порядок элемента группы

Для произвольного элемента a группы G можно определить любую его целую степень: $a^0 = e$, $a^1 = a$, $a^2 = a * a$, ..., $a^{k+1} = a * a^k$, a^{-1} (обратный элемент), $a^{-2} = a^{-1} * a^{-1}$, ..., $a^{-k-1} = a^{-1} * a^{-k}$. При этом выполняются равенства $a^k * a^l = a^{k+l}$, $(a^k)^l = a^{kl}$.

Определение. Группу (полугруппу), число элементов которой конечно, называют *конечной группой* (полугруппой).

Теорема (о порядке элемента конечной группы). *Пусть G — конечная группа и a — произвольный элемент из G. Тогда найдется такое натуральное число k, что все элементы $a^0 = e$, a, ..., a^{k-1} попарно различны, $a^k = e$, и если $a^l = e$, то k делит l.* Число k называют *порядком элемента a.*

Доказательство. Рассмотрим последовательность степеней элемента a ($a \neq e$):

$$a^0 \quad e,\ a,\ a^2,\ a^3,\ \ldots,\ a^q,\ \ldots$$

Группа G конечна, поэтому в этой (бесконечной) последовательности найдутся два равных элемента: $a^p = a^q$ $(0 \leqslant p < q)$. Тогда $a^{q-p} = a^q * a^{-p} = a^p * a^{-p} = e$, то есть существует по крайней мере одно такое натуральное число $t = q - p$, что $a^t = e$. Пусть k — наименьшее число среди всех таких t, тогда равенство $a^p = a^q$ $(0 \leqslant p < q)$ может выполняться только при $q - p \geqslant k$ и поэтому все элементы e, a, a^2, ..., a^{k-1} попарно различны. Нам осталось доказать, что если $a^l = e$, то k делит l. Пусть r — остаток от деления l на k, то есть $l = k \cdot s + r$ $(0 \leqslant r < k)$, тогда $a^k = e$, $a^{ks} = e$, так что из $a^l = e$ следует, что $a^l * a^{-ks} = a^{l-ks} = a^r = e$, откуда $r = 0$.

Читатель, решивший задачу 7, возможно, разочарован нашим «абстрактным» вариантом ее решения. «Но уж доказательство делимости $n!$ на k (см. задачу 7) наверняка потребует использования особых свойств подстановок!» — мог бы воскликнуть заинтересованный читатель,— и был бы неправ.

Теорема (Жозеф-Луи Лагранж). *Порядок k любого элемента конечной группы G делит число $r(G)$ элементов этой группы.*

Число $r(G)$ называют *порядком* конечной группы G.

Вот другие удобные формулировки теоремы Лагранжа.

а) *В конечной группе G порядка r для любого элемента a справедливо равенство $a^r = e$.*

б) *Порядок конечной группы делится на наименьшее общее кратное порядков ее элементов.*

Теперь для решения второй части задачи 7 достаточно заметить, что порядок группы S_n равен $n!$.

Вокруг теоремы Лагранжа

Не приводя доказательства теоремы Лагранжа (его можно найти в учебниках по теории групп), проиллюстрируем на примерах, как «работает» эта теорема.

Иллюстрация 1 (алгебраическая). Если в конечной группе G найдется элемент g, порядок k которого равен порядку $r(G)$ группы G, то любой элемент a из G является некоторой степенью g: $a = g^m$ ($0 \leqslant m \leqslant k-1$). Такая группа G называется *циклической*; она всегда коммутативна.

Примером циклической группы является группа самосовмещений правильного n-угольника (см. с. 9), в ней элемент g, «порождающий» всю группу,— поворот на угол $360°/n$.

Задача 11. Докажите, что в циклической группе число решений уравнения $x^n = e$ равно наибольшему общему делителю чисел n и $r(G)$.

Задача 12*. Докажите, что если порядок $r(G)$ конечной группы G — простое число, то группа G — циклическая.

Иллюстрация 2 (геометрическая). Порядок группы $\Gamma(Д)$ самосовмещений додекаэдра $Д$ (группы симметрии додекаэдра) делится на 30. Этот факт можно вывести из теоремы Лагранжа без всяких подсчетов — просто из существования трех типов самосовмещений додекаэдра (см. рис. 9): поворотов вокруг вершины «на одну грань» (на 120°), поворотов вокруг середины ребра на 180° и поворотов вокруг центра грани на 72°. Порядки этих элементов из группы $\Gamma(Д)$, очевидно, равны 3, 2 и 5 соответственно, поэтому порядок группы $\Gamma(Д)$ делится на $3 \cdot 2 \cdot 5 = 30$

Иллюстрация 3 (арифметическая). Задачи на делимость чисел часто очень красивы; попробуйте, например, доказать, что числа 7^8-1, 11^8-1, 13^8-1, 17^8-1, 19^8-1, 23^8-1, 29^8-1 делятся на 30. После того как вы найдете решение, вам будет приятно узнать, что этот факт — одно из следствий теоремы Лагранжа.

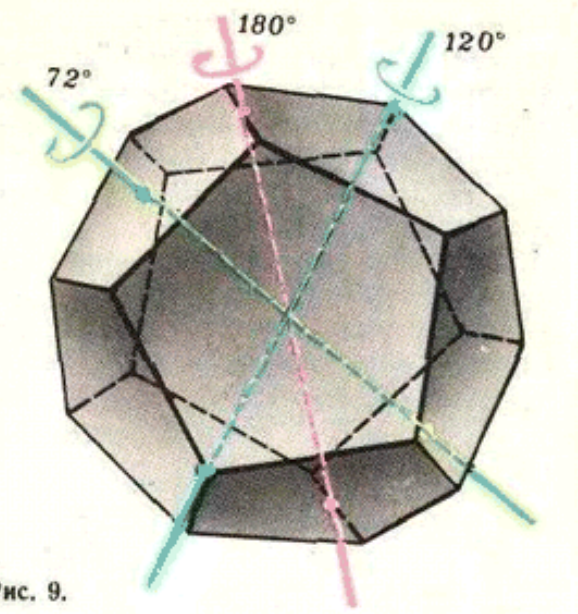


Рис. 9.

Обозначим через $\Phi(m)$ множество натуральных чисел, меньших m и взаимно простых с m. Введем на множестве $\Phi(m)$ операцию «$*$» умножения по модулю m: *$a * b$ равно остатку от деления обычного произведения $a \cdot b$ чисел a и b на m* (например, если $m = 30$, то $7 * 17 = 29$, так как $7 \cdot 17 = 119 = 3 \cdot 30 + 29$).

Задача 13. Докажите, что $\Phi(m)$ образует абелеву группу, то есть

а) $a * b$ принадлежит $\Phi(m)$, причем $a * b = b * a$;

б) число 1 всегда принадлежит $\Phi(m)$, и $a * 1 = a$ для любого a из $\Phi(m)$;

в) для любого a из $\Phi(m)$ найдется такое b, что $a * b = 1$.

Итак, $\Phi(m)$ — группа. Обозначим через $\varphi(m)$ ее порядок, тогда для любого a из $\Phi(m)$ будет $a^{\varphi(m)} = 1$ (теорема Лагранжа во второй формулировке!). Здесь возведение в степень $\varphi(m)$ производится в группе $\Phi(m)$, а для обычных степеней целых чисел это означает, что $a^{\varphi(m)}$ дает при делении на m остаток 1, то есть что $a^{\varphi(m)} - 1$ делится на m. Если $m = 30$, то $\Phi(m) = \{1, 7, 11, 13, 17, 19, 23, 29\}$, $\varphi(m) = 8$, и мы сразу получаем, что числа 7^8-1, 11^8-1, ... делятся на 30.

Темы для размышлений

О словах. Построим по алфавиту A алфавит $\hat{A}$ символов и «антисимволов»: если в A входит символ a, то в $\hat{A}$ входят a и $\overline{a}$.

Условимся, что после образования слова над алфавитом $\hat{A}$ в нем «аннигилируют» (удаляются) все соседние пары «символ — антисимвол» (например: $\langle ab\bar{c}c\bar{b}a\rangle \to \langle ab\bar{b}a\rangle \to \langle aa\rangle$).

Задача 14. Докажите, что результат полной «аннигиляции» не зависит от порядка «аннигиляции» отдельных пар «символ - антисимвол».

Условимся *композицией «*» двух слов* (в которых уже нет пар символ - антисимвол) над алфавитом $\hat{A}$ считать результат полной «аннигиляции» обычной композиции этих слов.

Задача 15 *. Докажите, что множество слов алфавита $\hat{A}$ с операцией «*» есть группа.

О самосовмещениях и подстановках.

Задача 16. Дан треугольник. Надо построить тетраэдр, все грани которого конгруэнтны этому треугольнику.

а) Для каких треугольников это возможно?

б) Найдите группу самосовмещений такого тетраэдра.

Задача 17. Выше мы доказали, что число самосовмещений куба, то есть порядок группы симметрии куба Г ($К$), равен 48. Попытайтесь аналогичным образом подсчитать порядок группы Г ($Д$) самосовмещений додекаэдра.

Задача 18. Постройте таблицу умножения для группы самосовмещений правильного пятиугольника.

Самосовмещения куба разбиваются на два класса: те, которые могут быть выполнены непрерывным движением куба в пространстве (повороты), будем называть их *движениями*, и те, которые движением в пространстве не выполняются (отражения). Множество движений куба с операцией композиции перемещений образует группу, в ней 24 элемента.

Задача 19. Опишите все элементы этой группы, то есть укажите оси и углы всех поворотов, входящих в эту группу.

Читатель, возможно, заметил, что группа S_4 содержит столько же элементов (24), сколько и группа движений куба. Более того, оказывается, что эти две группы *изоморфны* (об этом понятии рассказано в статье «Группы»): *каждому движению куба можно сопоставить подстановку из S_4 так, что композиции движений отвечает произведение соответствующих этим движениям подстановок.*

Задача 20 *. Установите изоморфизм между группой движений куба и группой S_4, указав 4 геометрических объекта в кубе таких, что произвольная их подстановка задает единственное движение куба (и, наоборот, каждому движению куба отвечает подстановка этих объектов).

Пусть a — подстановка последовательности $(1, 2, 3, \ldots, n)$. Назовем *орбитой числа p относительно подстановки a* множество чисел, на месте которых может оказаться p при действии подстановки a или ее степеней (a^2, a^3, ...).

Задача 21. Докажите, что множество $\{1, 2, 3, \ldots, n\}$ разбивается на орбиты, внутри каждой из которых любое число переводится на место любого другого под действием подстановки a или ее степеней.

Задача 22. Докажите, что порядок подстановки (как элемента группы S_n) равен наименьшему общему кратному длин ее орбит.

Очевидно, что всякая подстановка полностью определяется своими орбитами и порядком перехода от элемента к элементу внутри орбиты. Например, подстановка

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

полностью восстанавливается по такой записи:

$$a = (1\ 4\ 3)\ (2\ 6\ 5)\ (7),$$

если условиться, что из двух соседних элементов одной орбиты левый переводится подстановкой a в правый.

Задача 23. Как, зная «орбитальную» запись подстановки a, построить обратную к ней подстановку a^{-1}?

Задача 24 *. Опишите все пары подстановок a и b, удовлетворяющих равенству $a \circ b = b \circ a$.