

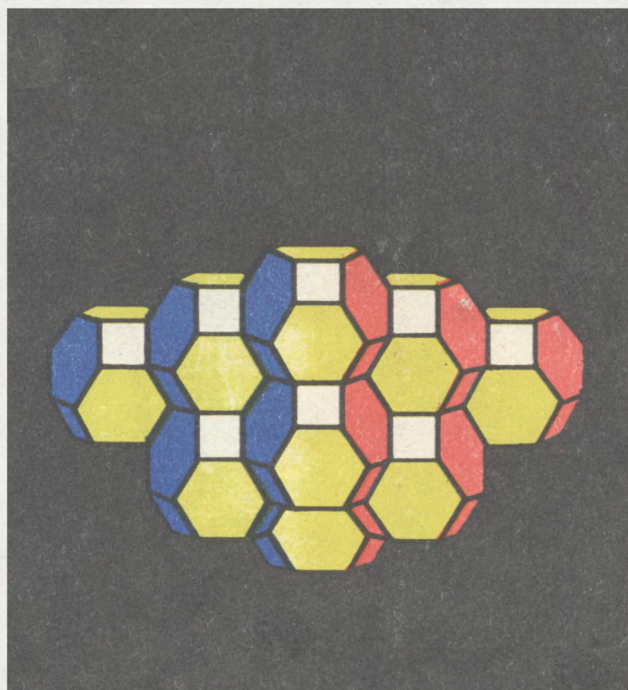


БИБЛИОТЕЧКА • КВАНТ •

выпуск 7

П. С. АЛЕКСАНДРОВ

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП





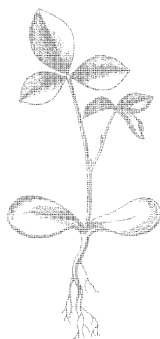
БИБЛИОТЕЧКА • КВАНТ •
выпуск 7

П. С. АЛЕКСАНДРОВ

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП



МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ
ЛИТЕРАТУРЫ
1980



Scan AAW

22.144

А 46

УДК 519.4

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

Академик **И. К. Киоин** (председатель), академик **А. Н. Колмогоров** (заместитель председателя), кандидат физ.-мат. наук **И. Ш. Слободский** (ученый секретарь), член-корреспондент АН СССР **А. А. Абрикосов**, академик **Б. К. Вайнштейн**, заслуженный учитель РСФСР **Б. В. Воздвиженский**, академик **В. М. Глушков**, академик **П. Л. Капица**, профессор **С. П. Капица**, член-корреспондент АН СССР **Ю. А. Осипьян**, член-корреспондент АН СССР **В. Г. Разумовский**, академик **Р. З. Сагдеев**, кандидат хим. наук **М. Л. Смолянский**, профессор **Я. А. Смородинский**, академик **С. Л. Соболев**, член-корреспондент АН СССР **Д. К. Фаддеев**, член-корреспондент АН СССР **И. С. Шкловский**.

Александров П. С.

А 46 Введение в теорию групп. — М.: Наука. Главная редакция физико-математической литературы, 1980, 144 с. — (Библиотечка «Квант». Вып. 7) — 25 коп.

Книга представляет собой введение в элементарную алгебру и теорию групп, которая находит широкое применение в современной математике и физике, кристаллографии, физике твердого тела и физике элементарных частиц. Все вводимые понятия подробно разбираются на простых геометрических примерах. В книгу включено дополнение, написанное Ю. П. Соловьевым.

Для школьников, преподавателей, студентов.

А $\frac{20203-106}{053(02)-80}$ 87-80. 1702030000

ББК 22.144
517.1

А $\frac{20203-106}{053(02)-80}$ 87-80. 1702030000

© Издательство «Наука»,
Главная редакция
физико-математической
литературы, 1980

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ	5
ВВЕДЕНИЕ	7
Глава I. ПОНЯТИЕ ГРУППЫ	10
§ 1. Простейшие понятия теории множеств	10
1. Сумма множеств (10). 2. Пересечение множеств (11). 3. Отображения или функции (11). 4. Разбиение множества на подмножества (14).	
§ 2. Вводные примеры	20
1. Действия над целыми числами (20). 2. Действия над рациональными числами (20). 3. Повороты правильного треугольника (21). 4. Клейновская группа четвертого порядка (23). 5. Повороты квадрата (24).	
§ 3. Определение группы	25
§ 4. Простейшие теоремы о группах	27
1. Произведение любого конечного числа элементов группы. Первое правило раскрытия скобок (27). 2. Нейтральный элемент (29). 3. Обратный элемент (30). 4. Замечания об аксиомах группы (32). 5. «Мультипликативная» и «аддитивная» терминология в теории групп (33).	
Глава II. ГРУППЫ ПОДСТАНОВОК	36
§ 1. Определение групп подстановок	36
§ 2. Понятие подгруппы	40
1. Примеры и определение (40). 2. Условие, чтобы подмножество группы было подгруппой (41).	
§ 3. Подстановки как отображения конечного множества на себя. Четные и нечетные подстановки	42
1. Подстановки как отображения (42). 2. Четные и нечетные подстановки (43).	
Глава III. ИЗОМОРФНЫЕ ГРУППЫ. ТЕОРЕМА КЭЛИ	48
§ 1. Изоморфные группы	48
§ 2. Теорема Кэли	52
Глава IV. ЦИКЛИЧЕСКИЕ ГРУППЫ	55
§ 1. Подгруппа, порожденная данным элементом данной группы. Определение циклической группы	55
§ 2. Конечные и бесконечные циклические группы	56
§ 3. Системы образующих	61
1*	3

Глава V. ПРОСТЕЙШИЕ ГРУППЫ САМОСОВМЕЩЕНИЙ	63
§ 1. Примеры и определение группы самосовмещений геометрических фигур	63
1. Самосовмещения правильных многоугольников в их плоскости (63). 2. Самосовмещения правильного многоугольника в трехмерном пространстве (64).	
3. Общее определение группы самосовмещений дан- ной фигуры в пространстве или на плоскости (65).	
§ 2. Группы самосовмещений прямой и окружности	65
§ 3. Группы поворотов правильной пирамиды и двойной пирамиды	67
1. Пирамида (67). 2. Двойная пирамида (диэдр) (68). 3. Случай вырождения: группы поворотов отрезка и ромба (70).	
§ 4. Группа поворотов правильного тетраэдра	72
§ 5. Группа поворотов куба и октаэдра	76
§ 6. Группа поворотов икосаэдра и додекаэдра. Общее замечание о группах поворотов правильных много- гранников	82
Глава VI. ИНВАРИАНТНЫЕ ПОДГРУППЫ	85
§ 1. Сопряженные элементы и подгруппы	85
1. Трансформация одного элемента группы при по- мощи другого (85). 2. Пример группы тетраэдра (87). 3. Сопряженные элементы (88). 4. Транс- формация подгруппы (89). 5. Примеры (92).	
§ 2. Инвариантные подгруппы (нормальные делители)	93
1. Определение (93). 2. Примеры (93).	
Глава VII. ГОМОМОРФНЫЕ ОТОБРАЖЕНИЯ	96
§ 1. Определение гомоморфного отображения и его ядра	96
§ 2. Примеры гомоморфных отображений	99
Глава VIII. РАЗБИЕНИЕ ГРУППЫ НА КЛАССЫ ПО ДАННОЙ ПОДГРУППЕ. ФАКТОРГРУППА	104
§ 1. Левосторонние и правосторонние классы	104
1. Левосторонние классы (104). 2. Случай конеч- ной группы G (105). 3. Правосторонние классы (106). 4. Совпадение правосторонних классов с левосторонними в случае инвариантных подгрупп (107). 5. Примеры (108).	
§ 2. Факторгруппа по данной инвариантной подгруппе	110
1. Определение (110). 2. Теорема о гомоморфных отображениях (112).	
Добавление. ГРУППЫ ПЕРЕМЕЩЕНИЙ ПЛОСКОСТИ И ПРОСТРАНСТВА И ИХ ПОДГРУППЫ. Ю. П. Соловьев	116
1. Группа перемещений плоскости (116). 2. Группа перемещений пространства (123). 3. Конечные под- группы группы перемещений пространства (134).	

ПРЕДИСЛОВИЕ

Эта книга написана на основе моей книги с таким же названием, вышедшей в 1938 году¹⁾. По-видимому, потребность в совершенно элементарном введении в теорию групп сохраняется и в настоящее время, несмотря на довольно обширную литературу по алгебре, в которой, в частности, не мало хороших и достаточно полных изложений теории групп. Поэтому я был очень обрадован представившейся теперь возможности опубликовать популярное изложение теории групп в серии «Библиотечка «Квант», тем более, что эта серия предназначена как раз тому кругу читателей, для которого я в основном и писал эту книжку.

Понятие группы приобретает в настоящее время все большее господство над самыми различными разделами математики и ее приложений и наряду с понятием функции относится к самым фундаментальным понятиям всей математики.

Понятие группы не труднее понятия функции; его можно освоить на самых первых ступенях математического образования, тем более, что сделать это можно на материале элементарной математики. Вместе с тем знакомство с этим понятием кажется мне одним из самых естественных способов первого ознакомления с современной математикой вообще.

Овладеть понятием группы может с интересом и пользой всякий любящий математику ученик старших клас-

¹⁾ П. С. Александров. Введение в теорию групп. — М.: Учпедгиз, 1938 г.

сов средней школы. Книжка эта и написана в первую очередь для интересующихся математикой учащихся старших классов средней школы, а также для лиц, преподающих математику в школе. Что касается характера изложения, то я старался не давать понятий, не разъяснив их на простых, в значительной части геометрических примерах.

Книга содержит написанное Юрием Петровичем Соловьевым добавление «Группы перемещений плоскости и пространства и их подгруппы». Это добавление представляется мне дающим одну из самых живых, важных и интересных иллюстраций общего понятия группы, фундаментальная важность которого для всей математики и ее приложений уже отмечалась выше.

Переработка моей прежней книги осуществлена Ю. П. Соловьевым, которому я выражаю искреннюю благодарность. Особенно же я благодарю Ю. П. Соловьева за то, что он написал уже упомянутое добавление к этой книге, существенно дополняющее и украшающее ее.

П. С. Александров

г. Москва
12 сентября 1979 года

ВВЕДЕНИЕ

В школе переход от арифметических задач к алгебраическим находит свое выражение в том, что в задачах численные данные заменяются буквенными. Обозначение чисел буквами отвлекает нас от специальных числовых данных, фигурирующих в той или иной задаче, и приучает решать задачи в общем виде, т. е. для любых числовых значений входящих в нее величин.

В соответствии с этим, в начальных, самых важных, главах школьного курса алгебры изучаются правила действий над буквенными выражениями, или, что то же самое, законы так называемых тождественных преобразований алгебраических выражений. Постараемся с самого начала пояснить это понятие.

Каждое алгебраическое выражение представляет собой совокупность букв, связанных между собой знаками алгебраических действий; при этом для простоты мы в настоящую минуту будем рассматривать лишь действия сложения, вычитания и умножения. Смысл каждого алгебраического выражения заключается в следующем: если буквы, участвующие в выражении, заменить числами, то выражение показывает, какие действия и в каком порядке надо выполнить над этими числами; другими словами, всякое алгебраическое выражение представляет собой некоторый, записанный в общем виде, рецепт для обыкновенного арифметического вычисления. Тождественное преобразование алгебраического выражения означает переход от одного выражения к другому, связанному с первым следующим соотношением: если мы в обоих выражениях каждой букве дадим совершенно произвольное числовое значение с одним условием, чтобы одна и та же буква, входящая в оба выражения, получила в обоих случаях одно и то же значение, и если после этого произведем

показанные действия, то оба выражения дадут один и тот же числовой результат. Тождественное преобразование записывается в виде равенства двух алгебраических выражений; равенства эти справедливы при любой замене входящих в них букв числами (как указано выше). Равенства этого вида называются, как известно, тождествами. Например:

$$a - a = 0, \quad (1)$$

$$(a + b)c = ac + bc. \quad (2)$$

Всякое тождество выражает некоторое свойство входящих в него действий. Так, например, тождество (1) говорит нам, что вычитая из какого-нибудь числа это самое число, мы всегда получим один и тот же результат, а именно нуль. Тождество (2) утверждает следующее свойство действий сложения и умножения: произведение суммы двух чисел на третье число равно сумме произведения каждого из слагаемых на это третье число.

Тождеств существует бесконечно много. Однако можно установить небольшое число основных тождеств, подобных вышенаписанным, таким образом, что любое тождество является следствием из этих основных тождеств.

Всякое алгебраическое вычисление, т. е. всякое сколь угодно сложное тождественное преобразование одного алгебраического выражения в другое, является, таким образом, комбинацией небольшого числа основных или элементарных тождественных преобразований, излагаемых в элементарной алгебре под названием правил раскрытия скобок, правил знаков и т. п. Совершая эти комбинации элементарных преобразований, обычно даже забывают о том, что каждая буква в алгебраическом выражении есть только символ, знак, обозначающий некоторое число: вычисления, как говорят, производят *механически*, забывая о реальном смысле производимого в каждый момент преобразования, а заботясь лишь о соблюдении правил этих преобразований. Так поступают обычно и опытные математики и начинающие учащиеся. Однако в последнем случае иногда, к сожалению, бывает, что этот реальный смысл производимых преобразований вообще ускользает из сознания.

В механическом осуществлении алгебраических операций есть и другая, более серьезная сторона. Она

заключается в том, что под буквами, входящими в алгебраическое выражение, во многих случаях можно понимать не число, а разнообразные другие объекты математического исследования: не только над числами, но и над другими объектами — примеры этому мы увидим — можно производить действия, которые имеют ряд общих основных свойств с алгебраическими действиями, и которые поэтому естественно назвать сложением, умножением и т. д. Например, силы в механике не являются числами: они являются так называемыми векторами, т. е. величинами, имеющими не только числовое значение, но и направление. Между тем силы можно складывать, и это сложение обладает основными свойствами обычного алгебраического сложения чисел. Это приводит к тому, что над силами можно производить вычисления по правилам алгебры. Таким образом, могущество алгебраических преобразований идет гораздо дальше, чем запись в общей форме действий над числами: *алгебра учит вычислениям с любыми объектами, для которых определены действия, удовлетворяющие основным алгебраическим аксиомам.*

ПОНЯТИЕ ГРУППЫ

§ 1. ПРОСТЕЙШИЕ ПОНЯТИЯ ТЕОРИИ МНОЖЕСТВ

В этом параграфе мы опишем вкратце те основные понятия из теории множеств, которые постоянно употребляются в теории групп. Большинство этих понятий хорошо известно читателю из курса математики средней школы.

Прежде всего, мы предполагаем известными понятия множества и его подмножеств. Напомним лишь, что если B является подмножеством множества A , то этот факт обозначается так: $B \subset A$ или $A \supset B$. Знак \subset называется знаком *включения*.

Множества, состоящие из конечного числа элементов, называются *конечными множествами*. Теория конечных множеств называется иногда комбинаторикой. Но бывают и *бесконечные множества*. Таковы, например: множество всех натуральных (т. е. целых положительных) чисел; множество всех прямых, проходящих через данную точку (в плоскости или в пространстве); множество всех окружностей, проходящих через две данные точки; множество всех плоскостей, проходящих через данную прямую в пространстве и т. д.

Заметим еще одно обстоятельство: в математике рассматривается и множество, обозначаемое символом \emptyset , вовсе не содержащее элементов (*пустое* множество). Пустое множество есть подмножество *всякого* множества. Пустое множество в этой книге нам почти не придется рассматривать, вообще же в математике оно часто является необходимым моментом в рассуждениях.

Напомним теперь определение операций над множествами.

1. Сумма множеств. *Суммой $A \cup B$ (или объединением) множеств A и B называется множество, состоя-*

ице из всех элементов множества A и всех элементов множества B .

Отметим, в частности, следующее: если множество B есть подмножество множества A , то сумма множеств B и A совпадает с A .

Совершенно аналогичным способом определяется сумма любого числа множеств. Можно определить и сумму бесконечного числа множеств. Все это содержится в следующем определении:

Пусть дана какая-нибудь конечная или бесконечная совокупность множеств. **Суммой множеств** данной совокупности называется множество всех элементов, принадлежащих хотя бы одному из множеств, входящих в данную совокупность.

2. Пересечение множеств. Под **пересечением множеств** A и B понимается множество элементов, принадлежащих и множеству A и множеству B . Пересечение множеств A и B обозначается $A \cap B$. Конечно, это множество может оказаться и пустым.

Заметим, что если $B \subset A$, то пересечение множеств A и B есть множество B .

Вообще **пересечением множеств** данной (конечной или бесконечной) совокупности множеств называется множество, состоящее из элементов, принадлежащих ко всем множествам данной совокупности.

3. Отображения или функции. Предположим, что некоторое количество людей идет, скажем, в театр. При входе в театр люди раздеваются и получают в гардеробе номер, под которым висит их пальто.

Что интересует нас с математической стороны в этом всем известном явлении? Интересующим нас обстоятельством является факт, который может быть сформулирован следующим образом.

Каждому зрителю театра *соответствует* (или *поставлен в соответствие*) некоторый предмет, а именно: тот номер, который этот зритель получил в гардеробе.

Если каким-нибудь образом каждому элементу a некоторого множества A поставлен в соответствие определенный элемент b некоторого множества B , то мы говорим, что множество A отображено **во** множество B , или что мы имеем **функцию**, **аргумент** которой пробегает множество A , а **значения** ее принадлежат

множеству B . Для того чтобы показать, что данный элемент b поставлен в соответствие элементу a , пишут: $b=f(a)$ и говорят, что b есть **образ** элемента a при данном отображении f (или что b есть значение функции для значения a аргумента).

При этом могут представиться различные случаи, которые мы сейчас и разберем. Может случиться, что на данный спектакль распроданы все билеты. Тогда и в гардеробе обычно не остается свободных мест: не только каждый зритель получит номер, но при этом все номера окажутся распределенными между зрителями. Этот факт с математической точки зрения означает, что:

каждому элементу множества A поставлен в соответствие элемент $b=f(a)$ множества B , *причем каждый элемент множества B оказывается поставленным в соответствие хотя бы одному элементу множества A .* (Выделенные слова выражают в применении к нашему частному примеру как раз то обстоятельство, что все номера оказались розданными.) В этом случае мы говорим, что имеем *отображение множества A на множество B .*

Почему мы пишем «каждый элемент множества B оказывается поставленным в соответствие *хотя бы* одному элементу множества A »? Потому что может случиться, что нескольким различным элементам множества A поставлен в соответствие один и тот же элемент множества B . В нашем частном случае это означает, что *несколько человек повесят свои пальто на один и тот же номер*. Наиболее важным случаем отображений является случай отображений одного множества *на* другое. К нему легко приводится и общий случай отображения одного множества *в* другое. В самом деле, пусть дано какое-нибудь отображение f множества A во множество B ; множество всех тех элементов множества B , которые в силу отображения f поставлены в соответствие хотя бы одному элементу множества A , назовем **образом множества A при отображении f** и обозначим через $f(A)$. Очевидно, что отображение f есть отображение множества A *на* множество $f(A)$.

Это замечание дает нам возможность в дальнейшем ограничиться рассмотрением отображений одного множества *на* другое.

В нашем примере посетителей театра A есть множество всех зрителей, пришедших на данный спектакль, а $f(A)$ есть множество всех номеров, оказавшихся занятыми в гардеробе.

Определение. Пусть дано отображение f множества A на множество B . Пусть b есть произвольный элемент множества B . Полным **прообразом** элемента b при отображении f называется *множество всех тех элементов множества A , которым при отображении f ставится в соответствие данный элемент b* . Это множество обозначается через $f^{-1}(b)$.

В нашем примере b есть какой-либо из номеров в гардеробе театра; полный прообраз элемента b есть множество всех тех посетителей театра, которые повесили свои пальто на этот номер b .

Рассмотрим теперь особый случай, когда *на каждый номер повешено только одно пальто*, т. е. когда полный прообраз $f^{-1}(b)$ каждого элемента b множества B состоит лишь из одного элемента множества A . В этом случае отображение множества A на множество B называется **взаимно однозначным**.

Дадим еще пример, иллюстрирующий понятие взаимно однозначного отображения. Вообразим кавалерийский отряд. На каждого всадника приходится одна лошадь, на каждой лошади сидит один всадник. Этим установлено взаимно однозначное отображение множества всех всадников на множество всех лошадей (данного отряда), а также взаимно однозначное отображение множества всех лошадей на множество всех всадников (речь все время идет о всадниках и лошадях данного отряда).

Этот пример показывает, что взаимно однозначное отображение множества A на множество B автоматически производит также взаимно однозначное отображение множества B на множество A : ведь если каждое множество $f^{-1}(b)$, где b — любой элемент B , состоит лишь из одного элемента a , то мы и получаем отображение f^{-1} множества B на множество A , ставящее в соответствие каждому элементу b множества B элемент $a = f^{-1}(b)$ множества A . **Отображение f^{-1} называется обратным отображением к отображению f .**

Итак, при взаимно однозначном отображении множества A на множество B происходит следующее: каждый элемент a множества A объединяется в пару

с некоторым вполне определенным элементом $f(a)$, и при этом оказывается, что каждый элемент b множества B находится в паре с единственным вполне определенным элементом a множества A . Ставя в соответствие каждому элементу b множества B находящийся с ним в паре элемент a множества A , мы получим взаимно однозначное отображение f^{-1} множества B на множество A , обратное к отображению f .

Таким образом, при взаимно однозначном отображении одного множества на другое оба множества занимают равноправное положение (так как *каждое* взаимно однозначно отображается на другое). Для того чтобы подчеркнуть это равноправие, часто говорят о *взаимно однозначном соответствии между двумя множествами*, разумея под этим совокупность обоих взаимно однозначных отображений каждого множества на другое.

4. Разбиение множества на подмножества. а) Множества множеств. Мы можем рассматривать множества, состоящие из самых различных элементов. В частности, можем рассматривать *множества множеств*, т. е. множества, элементы которых сами являются множествами. Мы уже встречались с ними, когда вводили определения суммы и пересечения множеств: ведь речь там шла о сумме и о пересечении некоторой (конечной или бесконечной) совокупности множеств, т. е. именно о множестве множеств. К приведенным по этому поводу примерам прибавим еще некоторые, взятые из повседневной жизни. Множеством множеств является, например, множество всех спортивных команд Москвы (каждая спортивная команда есть множество составляющих ее спортсменов); множество всех научных обществ данного города или данной страны, множество всех профессиональных союзов, множество всех воинских частей (дивизий, полков, рот, батальонов, взводов и т. д.) данной армии — также являются множествами множеств. Эти примеры показывают, что множества, являющиеся элементами данного множества множеств, могут в одних случаях пересекаться, в других случаях, наоборот, не иметь общих элементов. Так, например, множество всех профессиональных союзов СССР есть множество попарно непересекающихся множеств, так как гражданин СССР не может быть одновременно членом двух профессиональных союзов. С другой стороны, множество всех воинских частей какой-либо

армии дает пример множества множеств, некоторые элементы которого являются подмножествами других элементов: так, каждый взвод есть подмножество некоторого полка, полк есть подмножество дивизии и т. д.

Множество спортивных команд данного города состоит, вообще говоря, из пересекающихся множеств, так как одно и то же лицо может входить в несколько спортивных команд (например, в команду пловцов и в команду волейболистов или лыжников).

Замечание. Для облегчения речи мы будем иногда вместо термина «множество множеств» употреблять, как совершенно равнозначные, термины «система множеств» или «совокупность множеств».

б) Разбиение на классы. Очень важный класс систем множеств мы получим, если рассмотрим всевозможные *разбиения какого-нибудь множества на попарно непересекающиеся множества*. Другими словами, пусть дано множество M , представленное в виде суммы попарно непересекающихся подмножеств (в конечном или бесконечном числе). Эти подмножества (множества — слагаемые нашей суммы) и являются *элементами* данного разбиения множества M .

Пример 1. Пусть M есть множество всех учащихся какой-нибудь школы; школа разбита на классы, которые, очевидно, и образуют непересекающиеся подмножества, дающие в сумме все множество M .

Пример 2. M есть множество всех учащихся в средних школах Москвы. Множество M можно разбить на попарно непересекающиеся подмножества, например, следующими двумя способами: 1) мы объединяем в одно слагаемое всех учащихся одной и той же школы (т. е. разбиваем множество всех учащихся по школам); 2) мы объединяем в одно слагаемое всех учащихся одного и того же класса (хотя и разных школ).

Пример 3. Пусть M есть множество всех точек плоскости; возьмем на этой плоскости какую-нибудь прямую g и разобьем всю плоскость на прямые, параллельные прямой g . Множества точек каждой такой прямой и являются теми подмножествами, на которые мы разбиваем множество M .

Примечание 1. Те читатели, которые знают, что такое система координат, пусть представляют себе прямую g как одну из координатных осей (для определенности ось абсцисс) этой координатной системы.

Примечание 2. Если данное множество M разбито на попарно непересекающиеся подмножества, дающие в сумме множество M , то для краткости говорят просто о разбиении множества M на классы.

Теорема 1. Пусть дано отображение f множества A на множество B . Полные прообразы $f^{-1}(b)$ всевозможных точек b множества B образуют разбиение множества A на классы. Множество этих классов находится во взаимно однозначном соответствии с множеством B .

Эта теорема, в сущности, очевидна: каждому элементу a множества A соответствует в силу отображения f один и только один элемент $b = f(a)$ множества B , так что a входит в один полный прообраз $f^{-1}(b)$. А это и значит, что полные прообразы точек b , во-первых, дают в сумме все множество A , во-вторых, попарно не пересекаются.

Множество классов находится во взаимно однозначном соответствии с множеством B : каждому элементу b множества B соответствует класс $f^{-1}(b)$ и каждому классу $f^{-1}(b)$ соответствует элемент множества B ¹⁾.

Теорема 2. Пусть дано разбиение множества A на классы. Оно порождает отображение множества A на некоторое множество B , а именно, на множество всех классов данного разбиения. Это отображение получается, если поставить в соответствие каждому элементу множества A тот класс, к которому он принадлежит.

Доказательство теоремы уже заключено в самой ее формулировке.

Пример 4. Тем, что учащиеся Москвы распределены по школам, уже и установлено²⁾ отображение множества A всех учащихся на множество B всех школ: каждому учащемуся соответствует та школа, в которой он учится.

При всей самоочевидности наших двух теорем факты, устанавливаемые ими, не сразу получили в математике отчетливую формулировку; получив же эту формулировку, они сразу приобрели очень важное значение в логическом построении различных математических дисциплин и прежде всего алгебры.

¹⁾ Обратите внимание на то, что f отображает A на B . Для отображения A в B теорема, вообще говоря, не верна.

²⁾ В предположении, что каждый учащийся учится лишь в одной школе.

в) Отношение эквивалентности. Пусть дано разбиение множества M на классы. Введем следующее определение: назовем два элемента множества M **эквивалентными** по отношению к данному разбиению множества M на классы, если они *принадлежат к одному и тому же классу*.

Таким образом, если мы разобьем учащихся Москвы по школам, то двое учащихся будут «эквивалентны», если они учатся в одной и той же школе (хотя бы и в разных классах). Если же мы разобьем учащихся по классам, то двое учащихся будут «эквивалентны», если они учатся в одном и том же классе (хотя бы и различных школ).

Отношение эквивалентности, только что определенное нами, очевидно, обладает следующими свойствами.

Свойство **симметрии** (или **взаимности**). Если a и b эквивалентны, то эквивалентны также b и a .

Свойство **транзитивности** (или **переходности**). Если эквивалентны элементы a и b , а также b и c , то a и c эквивалентны (с учетом симметричности это свойство можно сформулировать так: «два элемента, a и c , эквивалентные третьему, b , эквивалентны между собой»).

Наконец, мы считаем *каждый элемент эквивалентным самому себе*; это свойство отношения эквивалентности называется свойством **рефлексивности**.

Итак, всякое разбиение данного множества на классы определяет между элементами этого множества некоторое отношение эквивалентности, обладающее свойствами симметрии, транзитивности и рефлексивности.

Предположим теперь, что нам удалось, — каким бы то ни было способом, — установить некоторый признак, дающий нам возможность о некоторых парах элементов множества M говорить как о парах эквивалентных элементов. При этом мы требуем от этой эквивалентности только, чтобы она обладала свойствами симметрии, транзитивности и рефлексивности.

Докажем, что это отношение эквивалентности определяет разбиение множества M на классы.

В самом деле, обозначим символом K_a множество всех элементов M , эквивалентных элементу a .

В силу того, что наше отношение эквивалентности, по предположению, обладает свойством рефлексивности, каждый элемент a содержится в своем классе K_a .

Докажем, что *если два класса пересекаются (т. е. имеют хоть один общий элемент), то они непременно совпадают* (т. е. каждый элемент одного класса является в то же время элементом другого).

В самом деле, пусть классы K_a и K_b имеют общий элемент c . Записывая эквивалентность двух каких-нибудь элементов x и y в виде $x \sim y$, имеем по определению классов:

$$a \sim c, \quad b \sim c.$$

Следовательно, из симметрии $c \sim b$ и транзитивности вытекает

$$a \sim b. \quad (1)$$

Пусть y — какой-нибудь элемент класса K_b , т. е.

$$b \sim y;$$

тогда в силу транзитивности и (1), получаем

$$a \sim y,$$

т. е. y есть элемент класса K_a .

Пусть теперь x — какой-нибудь элемент класса K_a . Имеем

$$a \sim x;$$

применяя свойство симметрии, получаем

$$x \sim a,$$

а из (1) и транзитивности вытекает

$$x \sim b.$$

Применяя опять свойство симметрии

$$b \sim x,$$

получаем, что x принадлежит к классу K_b .

Таким образом, два класса, K_a и K_b , имеющие общий элемент c , действительно совпадают между собой.

Мы доказали, что *различные классы K_a образуют систему попарно непересекающихся подмножеств множества M* . Далее, классы в сумме дают все множество M , так как каждый элемент множества M принадлежит к своему классу.

Повторим еще раз доказанные в этом пункте результаты, объединив их в следующее предложение.

Теорема 3. *Каждое разбиение на классы какого-нибудь множества M определяет между элементами множества M некоторое отношение эквивалентности,*

обладающее свойствами симметрии, транзитивности и рефлексивности. Обратно, каждое отношение эквивалентности, установленное между элементами множества M и обладающее свойствами симметрии, транзитивности и рефлексивности, определяет разбиение множества M на классы попарно эквивалентных между собой элементов.

Приведем теперь несколько геометрических примеров отношений эквивалентности и разбиений множеств на классы.

Пример 5. Пусть M — множество всех прямых на плоскости. Напомним, что две прямые, l_1 и l_2 , называются *параллельными*, если либо l_1 и l_2 совпадают, либо не имеют общих точек (символически: либо $l_1 = l_2$, либо $l_1 \cap l_2 = \emptyset$). Разобьем множество M на классы, относя прямые l_1 и l_2 к одному классу в том и только том случае, когда $l_1 \parallel l_2$. Параллельность прямых есть отношение эквивалентности на множестве M . Действительно, $l \parallel l$ и, если $l_1 \parallel l_2$, то $l_2 \parallel l_1$. Следовательно, отношение \parallel рефлексивно и симметрично. Далее, пусть $l_1 \parallel l_2$ и $l_2 \parallel l_3$. Если $l_1 = l_2$ и $l_2 = l_3$, то, очевидно, $l_1 = l_3$. Если $l_1 = l_2$, а $l_2 \cap l_3 = \emptyset$, то $l_1 \cap l_3 = \emptyset$; аналогично для случая $l_1 \cap l_2 = \emptyset$ и $l_2 = l_3$. Остается рассмотреть случай $l_1 \cap l_2 = \emptyset$ и $l_2 \cap l_3 = \emptyset$. Но тогда либо $l_1 \cap l_3 = \emptyset$, либо пересечение $l_1 \cap l_3$ содержит хотя бы одну точку A ; в последнем случае $l_1 = l_3$ в силу пятого постулата Евклида, т. е. отношение \parallel транзитивно. Таким образом, отношение \parallel есть отношение эквивалентности. Полученные классы эквивалентности называются *направлениями* на плоскости.

Пример 6. Назовем две плоские фигуры F_1 и F_2 эквивалентными, если они конгруэнтны ($F_1 \cong F_2$), т. е. если существует такое перемещение f плоскости, что $f(F_1) = F_2$. Конгруэнтность также есть отношение эквивалентности. Действительно, $F \cong F$, поскольку в этом случае в качестве перемещения можно взять тождественное перемещение плоскости. Далее, если $F_1 \cong F_2$, то существует такое перемещение f , что $f(F_1) = F_2$. Но тогда $f^{-1}(F_2) = f^{-1}(f(F_1)) = f^{-1} \cdot f(F_1) = F_1$, т. е. $F_2 \cong F_1$. И, наконец, если $F_1 \cong F_2$ и $F_2 \cong F_3$, то $f(F_1) = F_2$ и $g(F_2) = F_3$ для некоторых перемещений f и g . Поэтому $F_3 = g(F_2) = g(f(F_1)) = g \cdot f(F_1)$, т. е. $F_1 \cong F_3$. Итак, отношение \cong рефлексивно, симметрично и транзитивно, т. е. является отношением эквивалентности.

Упражнения. 1. Доказать, что отношение подобия фигур является отношением эквивалентности.

2. Доказать, что равенство векторов есть отношение эквивалентности.

§ 2. ВВОДНЫЕ ПРИМЕРЫ

1. Действия над целыми числами. Сложение целых чисел¹⁾ удовлетворяет следующим условиям, которые называются аксиомами сложения и которые для всего последующего будут иметь чрезвычайно большое значение:

I. Всякие два числа можно сложить (т. е. для любых двух чисел a и b существует вполне определенное число, называемое их суммой: $a + b$).

II. Условие сочетательности или ассоциативности:

Для любых трех чисел a, b, c имеет место тождество:
$$(a + b) + c = a + (b + c).$$

III. Среди чисел существует одно определенное число, нуль, удовлетворяющее для всякого числа a соотношению

$$a + 0 = a.$$

IV. Для каждого числа a существует так называемое противоположное ему число, $-a$, обладающее тем свойством, что сумма $a + (-a)$ равняется нулю:

$$a + (-a) = 0.$$

Наконец, занимающее несколько особое место условие

V. Условие переместительности или коммутативности:

$$a + b = b + a.$$

2. Действия над рациональными числами. Рассмотрим теперь множество \mathbf{Q} , состоящее из всех положительных и отрицательных рациональных чисел²⁾, т. е. из всех рациональных чисел, *отличных* от нуля. Умножение этих чисел удовлетворяет так называемым **аксиомам умножения**. Перечислим их.

I. *Всякие два числа из \mathbf{Q} можно перемножить* (т. е. для любых двух чисел a и b существует вполне определенное число, называемое их произведением: $a \cdot b$).

¹⁾ Под целыми числами всегда понимаются все положительные и все отрицательные целые числа и, кроме того, число нуль.

²⁾ Под рациональным числом понимается любое целое и любое дробное число.

II. Условие сочетательности или ассоциативности. Для любых трех чисел a, b, c из множества \mathbf{Q} имеет место тождество:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

III. Среди чисел множества \mathbf{Q} существует единственное число — единица, удовлетворяющее для всякого числа a соотношению

$$a \cdot 1 = a.$$

IV. Для каждого числа a из \mathbf{Q} существует обратное ему число a^{-1} , обладающее тем свойством, что произведение $a \cdot a^{-1}$ равняется единице:

$$a \cdot a^{-1} = 1.$$

V. Условие коммутативности:

$$a \cdot b = b \cdot a.$$

Сравнивая примеры пп. 1 и 2, нетрудно заметить полное сходство аксиом, которым удовлетворяет операция сложения для целых чисел и операция умножения для ненулевых рациональных чисел. Ниже мы увидим, что это сходство не случайно и проявляется при рассмотрении разнообразных конкретных операций.

3. Повороты правильного треугольника. Покажем, что не только числа, но и многие другие объекты можно перемножать и притом с соблюдением только что перечисленных условий.

Пример 1. Рассмотрим всевозможные повороты правильного треугольника вокруг его центра O (рис. 1). При этом мы будем считать два поворота совпадающими, если они отличаются друг от друга на целое число полных оборотов (т. е. на целочисленное кратное 360°)¹⁾. Легко видеть, что из всех возможных пово-

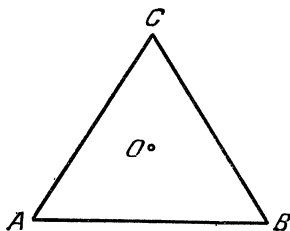


Рис. 1.

¹⁾ Так как поворот на целочисленное кратное 360° , очевидно, ставит каждую вершину на ее первоначальное место, то естественно объявить такой поворот совпадающим с нулевым и вообще считать совпадающими два поворота, отличающиеся друг от друга на целое число полных оборотов.

ровов треугольника лишь три поворота переводят треугольник в себя, а именно: повороты на 120° , на 240° и так называемый *нулевой* поворот, оставляющий все вершины, а следовательно, и все стороны треугольника на месте. Первый поворот переводит вершину A в вершину B , вершину B в вершину C , вершину C в вершину A (он перемещает, как говорят, вершины A, B, C в циклическом порядке). Вторым поворотом перемещает A в C , B в A , C в B (т. е. перемещает в циклическом порядке A, C, B).

Теперь мы, в соответствии со здравым смыслом, вводим следующее определение.

Умножить два поворота — значит, последовательно произвести их один за другим.

Таким образом, поворот на 120° , умноженный с самим собой, дает поворот на 240° , умноженный с поворотом на 240° дает поворот на 360° , т. е. нулевой поворот. Два поворота на 240° дают поворот на $480^\circ = 360^\circ + 120^\circ$, т. е. их произведение есть поворот на 120° .

Если мы нулевой поворот обозначим через a_0 , поворот на 120° через a_1 , поворот на 240° через a_2 , то получим следующие соотношения:

$$a_0 \cdot a_0 = a_0, \quad a_0 \cdot a_1 = a_1 \cdot a_0 = a_1,$$

$$a_0 \cdot a_2 = a_2 \cdot a_0 = a_2, \quad a_1 \cdot a_1 = a_2,$$

$$a_1 \cdot a_2 = a_2 \cdot a_1 = a_0, \quad a_2 \cdot a_2 = a_1.$$

Итак, для каждого из двух поворотов определено их произведение. Читатель легко проверит, что это умножение удовлетворяет сочетательному закону; очевидно также, что оно удовлетворяет переместительному закону. Далее, среди наших поворотов имеется также нулевой поворот a_0 , который удовлетворяет условию

$$a \cdot a_0 = a_0 \cdot a = a$$

для любого поворота a .

Наконец, каждый из наших трех поворотов имеет обратный ему поворот, дающий в произведении с данным поворотом нулевой поворот: нулевой поворот, очевидно, обратен самому себе, $a_0^{-1} = a_0$, так как $a_0 \cdot a_0 = a_0$, тогда как $a_1^{-1} = a_2$ и $a_2^{-1} = a_1$ (так как $a_1 \cdot a_2 = a_0$). Итак, умножение поворотов правильного треугольника, удовлетворяет всем перечисленным аксиомам умножения.

Запишем еще раз наше правило умножения поворотов более компактным образом в виде следующей *пифагоровой таблицы умножения*:

Т а б л и ц а 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

Произведение двух элементов в этой таблице находим в пересечении строки, отмеченной первым элементом, и столбца, отмеченного вторым элементом.

Читатель, который будет вычислять с нашими поворотами механически, возьмет просто три буквы: a_0 , a_1 , a_2 и будет умножать их, пользуясь только что выписанной таблицей умножения; при этом он может совершенно забыть, что именно эти буквы обозначали.

4. Клейновская группа четвертого порядка.

Пример 2. Рассмотрим совокупность четырех букв a_0 , a_1 , a_2 , a_3 , умножение которых определено следующей таблицей:

Т а б л и ц а 2

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

или в развернутом виде:

$$\begin{aligned}a_0 \cdot a_0 &= a_0, & a_0 \cdot a_1 &= a_1 \cdot a_0 = a_1, \\a_0 \cdot a_2 &= a_2 \cdot a_0 = a_2, & a_0 \cdot a_3 &= a_3 \cdot a_0 = a_3, \\a_1 \cdot a_1 &= a_0, & a_2 \cdot a_2 &= a_0, \\a_1 \cdot a_2 &= a_2 \cdot a_1 = a_3, & a_2 \cdot a_3 &= a_3 \cdot a_2 = a_1, \\a_1 \cdot a_3 &= a_3 \cdot a_1 = a_2, & a_3 \cdot a_3 &= a_0.\end{aligned}$$

Умножение определено для любых двух букв из числа наших четырех. Непосредственная проверка сразу показывает, что это умножение удовлетворяет условию ассоциативности и коммутативности.

Буква a_0 обладает основным свойством единицы: произведение двух сомножителей, из которых одно есть a_0 , равно другому сомножителю.

Таким образом, условия, аналогичные условиям I, II, III, V из пп. 1—2, оказываются выполненными в нашей «алгебре четырех букв». Для того чтобы убедиться, что условие IV также выполнено, достаточно заметить, что мы положили

$$a_0 \cdot a_0 = a_0, \quad a_1 \cdot a_1 = a_0, \quad a_2 \cdot a_2 = a_0, \quad a_3 \cdot a_3 = a_0,$$

т. е. каждая буква сама себе обратна (дает при умножении с самой собой единицу).

Наша «алгебра четырех букв» на первый взгляд может показаться своего рода математической игрой, забавой, лишенной реального содержания. В действительности законы этой алгебры, выраженные таблицей 2, имеют вполне реальный смысл, с которым мы вскоре познакомимся; замечу, более того, что эта «алгебра четырех букв» имеет серьезное значение и в высшей алгебре. Она называется *клеиновской группой четвертого порядка*.

5. Повороты квадрата.

Пример 3. Некоторую «алгебру четырех букв», отличную от предыдущей, можно построить в полной аналогии с тем, что мы делали в первом примере. Рассмотрим квадрат $ABCD$ и повороты вокруг его центра, переводящие фигуру в самое себя. Опять будем считать совпадающими всякие два поворота, отличающиеся друг от друга на целочисленное кратное 360° . Таким образом, будем иметь всего четыре поворота, а именно: нулевой, поворот на 90° , на 180° и на 270° .

Эти повороты обозначим соответственно через a_0, a_1, a_2, a_3 . Если под умножением двух поворотов понимать снова последовательное осуществление двух поворотов, то получим следующую таблицу умножения, вполне аналогичную второму примеру:

Таблица 3

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_2	a_3	a_0
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_0	a_1	a_2

Таким же точно образом как в этом и в первом примере, можно рассматривать повороты правильного пяти-, шести- и вообще n -угольника. Читателю предоставляется самому провести относящиеся сюда рассуждения и построить соответствующие таблицы умножения.

§ 3. ОПРЕДЕЛЕНИЕ ГРУППЫ

Прежде чем идти дальше в изучении отдельных примеров, подведем итог уже рассмотренным примерам, введя основное определение.

Пусть задано некоторое (конечное или бесконечное) множество G , на котором определена **операция умножения**, т. е. определен закон, сопоставляющий любой паре a, b элементов из G некий элемент из G называемый **произведением** a и b и обозначаемый символом $a \cdot b$. Предположим, что эта операция умножения удовлетворяет следующим условиям:

I. Условие ассоциативности. Для любых трех элементов a, b, c множества G справедливо соотношение:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Это значит следующее. Обозначим через d элемент множества G , являющийся произведением элементов a и b ; точно так же обозначим через e элемент $b \cdot c$ множества G . Тогда $d \cdot c$ и $a \cdot e$ являются одним и тем же элементом множества G .

II. Условие существования нейтрального элемента. Среди элементов множества G имеется некоторый определенный элемент, называемый **нейтральным** элементом и обозначаемый символом 1 , такой, что

$$a \cdot 1 = 1 \cdot a = a$$

при любом выборе элемента a .

III. Условие существования обратного элемента к каждому данному элементу. К каждому данному элементу a множества G можно подобрать такой элемент b того же множества G , что

$$a \cdot b = b \cdot a = 1.$$

Элемент b называется **обратным** к элементу a и обозначается a^{-1} .

Множество G с определенной в нем операцией умножения, удовлетворяющей только что перечисленным трем условиям, называется **группой**; сами эти условия называются **аксиомами группы**.

Операция умножения, удовлетворяющая аксиомам группы, иногда называется **групповой операцией** или **групповым законом**. Мы будем пользоваться всеми этими терминами, не оговаривая каждый раз их эквивалентность.

Пусть в группе G , кроме указанных выше трех аксиом, оказывается выполненным еще и следующее условие:

IV. Условие коммутативности:

$$a \cdot b = b \cdot a.$$

В этом случае группа G называется **коммутативной** или **абелевой группой**.

Группа называется **конечной**, если она состоит из конечного числа элементов; в противном случае она называется **бесконечной**.

Число элементов конечной группы называется ее **порядком**.

Познакомившись с определением группы, мы видим, что приведенные в первых двух параграфах этой главы

примеры являются примерами групп. Действительно, мы познакомились последовательно:

1) с группой целых чисел (групповая операция — обычное сложение целых чисел);

2) с группой отличных от нуля рациональных чисел (групповая операция — обычное умножение рациональных чисел);

3) с группой поворотов правильного треугольника (групповая операция — композиция поворотов);

4) с клейновской группой порядка 4 (групповая операция — умножение букв a_0, a_1, a_2, a_3 , задаваемое таблицей 2);

5) с группой поворотов правильного четырехугольника (групповая операция — композиция поворотов);

6) с группой поворотов правильного n -угольника.

Все эти группы коммутативны. Группа целых чисел и группа ненулевых рациональных чисел бесконечны; остальные — конечные группы.

§ 4. ПРОСТЕЙШИЕ ТЕОРЕМЫ О ГРУППАХ¹⁾

1. Произведение любого конечного числа элементов группы. Первое правило раскрытия скобок. Аксиома ассоциативности имеет в теории групп и, следовательно, во всей алгебре очень большое значение: она позволяет определить произведение не только двух, но и трех и вообще любого конечного числа элементов группы и пользоваться при рассмотрении этих произведений обычными правилами раскрытия скобок²⁾.

В самом деле, если даны, положим, три элемента a, b, c , то мы еще пока не знаем, что значит умножить эти *три* элемента: ведь аксиомы групп говорят лишь о произведениях *двух* элементов и выражения вида $a \cdot b \cdot c$ еще не определены. Однако условие ассоциативности гласит, что умножая, с одной стороны, элемент a на элемент $b \cdot c$ и, с другой стороны, элемент $a \cdot b$ на элемент c мы получим *один и тот же элемент в качестве произведения*. Вот этот элемент, являющийся произведением двух элементов a и $b \cdot c$,

¹⁾ Читатель, желающий сначала ознакомиться с дальнейшими примерами групп, может пропустить этот параграф и вернуться к нему только по прочтении глав II—IV.

²⁾ При этом надо только помнить, что в случае некоммукативных групп нельзя, вообще говоря, менять порядок сомножителей.

а также произведением двух элементов $a \cdot b$ и c , и представляется естественным *определить* в качестве произведения трех элементов a, b, c в том порядке, как только они здесь выписаны, и обозначить его просто через $a \cdot b \cdot c$. Таким образом, на равенство

$$a \cdot b \cdot c = a \cdot (b \cdot c) = (a \cdot b) c$$

надо смотреть, как на определение abc произведения трех элементов a, b, c (здесь знак умножения для удобства опущен).

Таким же точно образом можно определить произведение четырех элементов a, b, c, d , например, как $a \cdot (bcd)$. Докажем, что при этом

$$a(bcd) = (ab)(cd) = (abc)d.$$

По только что сказанному имеет прежде всего место равенство:

$$a(bcd) = a[b(cd)].$$

Но для трех элементов a, b, cd мы имеем:

$$a[b(cd)] = (ab)(cd).$$

С другой стороны, имеем для трех элементов ab, c, d :

$$(ab)(cd) = [(ab)c]d = (abc)d,$$

что и требовалось доказать.

Предположим, что произведение любых $n-1$ элементов уже определено. Определим произведение n элементов $a_1 a_2 \dots a_n$ как $a_1(a_2 \dots a_n)$. Таким образом, выражение $a_1 a_2 \dots a_n$ может считаться определенным методом математической (полной) индукции для любого n .

Теорема. Пусть n — любое натуральное число. Для любого натурального числа¹⁾ $m \leq n$ справедливо тождество (первое правило раскрытия скобок):

$$(a_1 \dots a_m)(a_{m+1} \dots a_n) = a_1 \dots a_n. \quad (2)$$

Доказательство. Доказательство будем вести методом полной индукции²⁾: для $n=1$ теорема выражает тождество $a_1 = a_1$. Предположим, что она спра-

¹⁾ Натуральное число — это целое положительное число.

²⁾ Читателю рекомендуется самому провести рассуждения, и только потом сверить их с приведенными в тексте.

ведлива для $n \leq k-1$ и докажем ее для $n=k$. Рассмотрим сначала случай $m=1$. Тогда формула (2) превращается в

$$a_1 (a_2 \dots a_k) = a_1 \dots a_k.$$

Но это есть *определение* выражения $a_1 \dots a_k$.

Итак, для данного $n=k$ и $m=1$ формула (2) справедлива.

Теперь, фиксируя $n=k$, предположим, что наша формула доказана для $m=q-1$; докажем ее для $m=q$. Так как при $m=n$ формула (2), очевидно, справедлива, можем предположить $q < k$. Тогда, так как теорема предположена справедливой для $n \leq k-1$, то

$$(a_1 \dots a_q) (a_{q+1} \dots a_k) = [(a_1 \dots a_{q-1}) a_q] (a_{q+1} \dots a_k).$$

Условие ассоциативности, примененное к трем элементам $(a_1 \dots a_{q-1})$, a_q , $(a_{q+1} \dots a_k)$, дает

$$[(a_1 \dots a_{q-1}) a_q] (a_{q+1} \dots a_k) = (a_1 \dots a_{q-1}) [a_q (a_{q+1} \dots a_k)].$$

Но выражение, стоящее справа в квадратных скобках, есть, по определению,

$$a_q a_{q+1} \dots a_k.$$

Итак, получаем:

$$(a_1 \dots a_q) (a_{q+1} \dots a_k) = (a_1 \dots a_{q-1}) (a_q \dots a_k),$$

но в силу предположенной справедливости формулы (2) для $n=k$ и $m=q-1$, правая часть последнего равенства есть $a_1 \dots a_k$. Отсюда следует равенство

$$(a_1 \dots a_q) (a_{q+1} \dots a_k) = a_1 \dots a_k,$$

что и требовалось доказать.

2. Нейтральный элемент. Условие существования нейтрального элемента гласит: *в группе существует некоторый элемент 1, такой, что для любого элемента a группы выполнено условие*

$$a \cdot 1 = 1 \cdot a = a. \quad (3)$$

В этом условии не содержится утверждения, что не может быть в данной группе второго элемента $1'$, отличного от 1, но обладающего тем же свойством

$$a \cdot 1' = 1' \cdot a = a \quad (4)$$

для любого a .

Отсутствие такого элемента $1'$ вытекает из следующей более сильной теоремы, которую иногда называют *теоремой об единственности нейтрального элемента*.

Теорема. Если для какого-нибудь определенного элемента a группы G найден элемент 1_a , удовлетворяющий одному из условий

$$a \cdot 1_a = a \quad \text{или} \quad 1_a \cdot a = a,$$

то непременно

$$1_a = 1.$$

Доказательство. Предположим сначала, что $a \cdot 1_a = a$. Заметим прежде всего, что для любого элемента b имеем

$$b \cdot 1_a = (b \cdot 1) \cdot 1_a,$$

что при замене 1 на $a^{-1} \cdot a$ дает

$$b \cdot 1_a = b \cdot a^{-1} \cdot a \cdot 1_a = b \cdot a^{-1} (a \cdot 1_a) = b \cdot a^{-1} a = b.$$

Точно так же имеем

$$1_a \cdot b = (1 \cdot 1_a) \cdot b = a^{-1} \cdot a \cdot 1_a \cdot b = a^{-1} (a \cdot 1_a) \cdot b = a^{-1} a \cdot b = b.$$

Итак, для любого b имеем

$$b \cdot 1_a = 1_a \cdot b = b.$$

Возьмем, в частности, $b = 1$. Получаем

$$1 \cdot 1_a = 1. \quad (5)$$

Но по определению элемента 1 имеем, с другой стороны,

$$1 \cdot 1_a = 1_a. \quad (6)$$

Из уравнений (5) и (6) следует $1_a = 1$, что и требовалось доказать.

Совершенно аналогичным образом можно вывести тождество $1_a = 1$ из предположения $1_a \cdot a = a$.

3. Обратный элемент. Условие существования обратного элемента гласит: для каждого элемента a существует определенный элемент a^{-1} такой, что

$$a^{-1} \cdot a = a \cdot a^{-1} = 1.$$

Здесь опять-таки утверждается лишь существование элемента a^{-1} , а никак не единственность его. Докажем эту единственность, т. е. докажем следующую теорему.

Теорема. Если для данного a имеем какой-нибудь элемент a' , удовлетворяющий одному из условий

$$a \cdot a' = 1 \quad \text{или} \quad a' \cdot a = 1,$$

то непременно

$$a' = a^{-1}.$$

Доказательство. Пусть

$$a \cdot a' = 1.$$

Отсюда следует, что

$$(a^{-1}) \cdot (a \cdot a') = a^{-1} \cdot 1 = a^{-1},$$

т. е.

$$(a^{-1} \cdot a) \cdot a' = a^{-1},$$

т. е.

$$1 \cdot a' = a^{-1},$$

т. е.

$$a' = a^{-1}.$$

Совершенно аналогичным образом можно из предположения $a' \cdot a = 1$ вывести $a' = a^{-1}$.

Итак, для данного a существует *единственный* элемент x , удовлетворяющий равенству $ax = 1$ или равенству $xa = 1$, а именно элемент $x = a^{-1}$.

Возьмем теперь элемент a^{-1} . Элемент a удовлетворяет равенству

$$a^{-1} \cdot a = 1,$$

т. е. является для элемента a^{-1} как раз тем элементом $x = (a^{-1})^{-1}$, о котором только что шла речь. Итак,

$$(a^{-1})^{-1} = a.$$

Пусть теперь a, b — некоторые элементы группы G . Рассмотрим в этой группе уравнение

$$xa = b. \tag{7}$$

Очевидно, что это уравнение имеет решение

$$x = ba^{-1}.$$

Это решение — единственно, так как если элемент c есть решение уравнения (7), то $ca = b$, значит,

$$c = caa^{-1} = ba^{-1}.$$

Точно так же уравнение

$$ax = b \quad (8)$$

имеет своим единственным решением элемент $a^{-1}b$.

Следствие. Если $ab = ac$, а также, если $ba = ca$, то $b = c$.

Докажем теперь следующее важное тождество:

$$(ab)^{-1} = b^{-1}a^{-1}. \quad (9)$$

В самом деле, элемент $(ab)^{-1}$ есть единственный элемент x группы, удовлетворяющий условию

$$ab \cdot x = 1; \quad (10)$$

но

$$ab \cdot (b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a \cdot 1 \cdot a^{-1} = aa^{-1} = 1.$$

Отсюда элемент $x = b^{-1}a^{-1}$ как раз удовлетворяет условию (10), значит, действительно,

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Методом математической индукции легко получаем общий результат

$$(a_1 \dots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \dots a_1^{-1}.$$

Отсюда, в частности, следует тождество

$$c(a_1 \dots a_n)^{-1} = ca_n^{-1}a_{n-1}^{-1} \dots a_1^{-1},$$

называемое вторым правилом раскрытия скобок.

4. Замечания об аксиомах группы. Мы не ставим себе задачей дать *наименьшее* число требований, достаточных для определения понятия группы. Действительно, мы потребовали, чтобы нейтральный элемент удовлетворял сразу условиям

$$a \cdot 1 = 1 \cdot a = a,$$

а обратный элемент a^{-1} к любому элементу a условиям

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Между тем на основании доказанного в пунктах 2 и 3 настоящего параграфа достаточно было бы потребовать выполнения *одного* какого-нибудь из условий

$$a \cdot 1 = a \quad \text{или} \quad 1 \cdot a = a,$$

а также одного какого-нибудь из условий

$$a \cdot a^{-1} = 1 \quad \text{или} \quad a^{-1} \cdot a = 1.$$

Наконец, заметим, что в определении группы (§ 3) аксиомы II и III, т. е. условие существования обратного элемента ко всякому данному, можно было бы заменить одной следующей аксиомой (*условие неограниченной возможности деления*):

Ко всяким двум элементам a и b можно найти элементы x и y такие, что $ax = b$ и $ya = b$.

Доказательство предлагаем привести самому читателю (или прочитать его, например, в книге А. Г. Куроша «Теория групп»).

5. «Мультипликативная» и «аддитивная» терминология в теории групп. Составными частями понятия группы являются:

а) множество тех предметов (числа, подстановки, повороты и т. д.), которые являются элементами группы;

б) определенная *операция* или *действие*, которое мы называли умножением и которое позволяет для каждого двух элементов a и b нашей группы найти третий элемент $a \cdot b$ той же группы.

Мы выбрали термин *умножение* для обозначения операции, имеющей место в каждой группе. Выбор того или иного термина на существо дела, конечно, влияния не оказывает; в применении к каждой группе можно было бы говорить о *сложении* ее элементов (а не об умножении их) и рассуждать не на *мультипликативном*, а на *аддитивном* языке. С мультипликативным языком, или, как говорят, с мультипликативной записью группы, мы уже познакомились. Теперь сообразим, какое выражение получают групповые аксиомы на аддитивном языке («в аддитивной записи»).

Прежде всего, мы требуем, чтобы для каждого двух элементов a и b нашего множества G (см. § 3) был однозначно определен элемент $a + b$ — сумма двух элементов a и b .

Собственно групповые аксиомы примут при этом следующий вид:

I. Условие ассоциативности. *Для любых трех элементов a , b , c множества G справедливо соотношение*

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

II. Условие существования нейтрального элемента. *Среди элементов множества G имеется некоторый определенный элемент, называемый нейтральным элементом*

и обозначаемый через 0, такой, что

$$a + 0 = 0 + a = a$$

при любом выборе элемента a .

III. Условие существования противоположного элемента. К каждому данному элементу a множества G можно подобрать такой элемент $-a$ того же множества G , что

$$a + (-a) = (-a) + a = 0.$$

Мы видим, что если операцию, определяющую данную группу, переименовать из умножения в сложение, то оказывается естественным нейтральный элемент переименовать из единицы в нуль и говорить о *противоположных* элементах $(-a)$ вместо обратных a^{-1} .

Условие коммутативности в аддитивной записи имеет вид

$$a + b = b + a.$$

Мультипликативная терминология является исторически первой и сейчас употребляется подавляющим большинством авторов. Наиболее удобно в одних случаях рассуждать о группах на мультипликативном, в других случаях на аддитивном языке. Наконец, имеется много случаев, когда оба языка оказываются одинаково удобными.

Как на пример, где, конечно, удобнее пользоваться аддитивным языком, укажем на группу целых чисел: групповой операцией является здесь обыкновенное арифметическое сложение, нейтральный элемент есть обыкновенный арифметический нуль, и понятие противоположных чисел имеет также свой обычный арифметический смысл.

Едва ли можно спорить о том, что непривычно и неудобно было бы обычное арифметическое сложение вдруг называть умножением, нуль единицей и т. д. Однако читатель должен хорошо понять, что, несмотря на все неудобства такого переименования, оно вполне возможно и не приведет ни к какому противоречию до тех пор, пока мы ограничиваемся изучением группы целых чисел, т. е. рассматриваем единственную операцию над целыми числами, а именно, арифметическое сложение.

Если мы наряду с арифметическим сложением стали бы рассматривать еще и умножение (также в элемен-

тарном, арифметическом смысле слова), то переименование сложения в умножение, о котором идет речь, конечно, совершенно запутало бы терминологию. Как пример группы, для которой мультипликативный язык более удобен, можно назвать группу \mathbf{Q} ненулевых рациональных чисел, которую мы рассмотрели в § 2, п. 2 настоящей главы.

Чтобы покончить с вопросами терминологии, отметим, что в настоящее время становится все более и более общепринятым говорить об общих группах на мультипликативном языке, а о *коммутативных группах* на аддитивном языке (хотя мы только что видели исключение из этого правила, когда упоминали о группе отличных от нуля рациональных чисел).

В этой книжке мы будем, в основном, придерживаться указанного соглашения.

ГРУППЫ ПОДСТАНОВОК

§ 1. ОПРЕДЕЛЕНИЕ ГРУПП ПОДСТАНОВОК

Если три человека Сидор, Иван и Петр сидят на скамейке, предположим, слева направо, то их можно пересадить шестью разными способами, а именно (считая все время слева направо):

- (1) Сидор, Иван, Петр;
- (2) Сидор, Петр, Иван;
- (3) Иван, Сидор, Петр;
- (4) Иван, Петр, Сидор;
- (5) Петр, Сидор, Иван;
- (6) Петр, Иван, Сидор.

Переход от одного какого-нибудь порядка, в котором они сидят, к любому другому порядку называется *подстановкой*. Подстановка записывается так:

$$\begin{pmatrix} \text{Сидор, Иван, Петр} \\ \text{Иван, Петр, Сидор} \end{pmatrix};$$

и означает, что Иван сел на место Сидора, Петр на место Ивана, Сидор — на место Петра.

В таком смысле можно говорить о подстановках любых предметов. Так как при этом природа представляемых предметов значения не имеет, то эти предметы обычно обозначаются числами, и речь идет о *подстановках чисел*. Из трех чисел 1, 2, 3 можно сделать следующие подстановки:

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

Каждая подстановка заключается в том, что на место числа, стоящего в верхней строчке, ставится подписанное под ним число из нижней строчки. Пер-

вая подстановка $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ называется *тождественной*, в ней каждое число остается на своем месте. Вторая подстановка $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ заключается в том, что число 1 остается на месте, число 3 ставится на место числа 2, а число 2 — на место числа 3 и т. д.

Общий вид подстановки из чисел $1, 2, \dots, n$ таков:

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

Здесь i_1, i_2, \dots, i_n — это те же числа $1, 2, \dots, n$, но только записанные в другом порядке. Например, пусть

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

тогда, очевидно, $n=5$, $i_1=3$, $i_2=1$, $i_3=4$, $i_4=5$, $i_5=2$.

Из n чисел можно сделать $n!$ различных подстановок. Докажем это. Каждая подстановка из чисел $1, 2, \dots, n$ имеет вид

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

где все i_1, \dots, i_n различны и каждое из них есть одно из чисел $1, 2, \dots, n$. Значит, i_1 принимает n возможных значений. После того как одно из них выбрано, мы имеем для выбора значения i_2 уже только $n-1$ возможностей. Остановившись на одной из них, имеем для выбора значения i_3 лишь $n-2$ возможностей. И так далее, пока для i_n останется лишь одна возможность. Всего таким образом имеется $n(n-1) \times \dots \times (n-2) \dots 2 \cdot 1 = n!$ возможностей, что и требовалось доказать.

Вернемся к подстановкам из трех цифр. По определению, будем считать, что *перемножить* две подстановки, значит последовательно произвести их одну за другой. В результате получится опять подстановка, называемая **произведением** двух данных подстановок.

Перемножим, например, подстановки

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ и } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

В силу первой подстановки единица заменится двойкой, в силу второй подстановки эта двойка оста-

нется на месте; итак, после последовательного совершения обеих подстановок *единица перейдет в двойку*. Точно так же после последовательного совершения обеих подстановок *двойка перейдет в тройку, тройка перейдет в единицу*:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \quad (1)$$

Таким же точно образом можно перемножить любые две подстановки. Для того чтобы удобно записать результаты всех этих перемножений, введем следующие обозначения:

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

P_0 — тождественная подстановка.

Тогда имеем следующую таблицу умножения:

Таблица 4

первый множитель	второй множитель					
	P_0	P_1	P_2	P_3	P_4	P_5
P_0	P_0	P_1	P_2	P_3	P_4	P_5
P_1	P_1	P_0	P_3	P_2	P_5	P_4
P_2	P_2	P_4	P_0	P_5	P_1	P_3
P_3	P_3	P_5	P_1	P_4	P_0	P_2
P_4	P_4	P_2	P_5	P_0	P_3	P_1
P_5	P_5	P_3	P_4	P_1	P_2	P_0

Для того чтобы найти произведение двух подстановок, например, $P_2 \cdot P_4$, надо взять строчку, в заголовке которой («первый сомножитель») стоит первая подстановка (в нашем случае P_2), и столбец, в заголовке которого («второй сомножитель») стоит вторая подстановка (в нашем случае P_4). В пересечении выбранной строки с выбранным столбцом и будет стоять искомое произведение: $P_2 \cdot P_4 = P_1$.

Проведем вычисление в развернутом виде; пусть

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix};$$

при помощи тех же рассуждений, что и в случае равенства (1), получаем

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

т. е. действительно:

$$P_2 \cdot P_4 = P_1.$$

Читателю рекомендуется проверить таким же образом всю таблицу умножения.

Непосредственной проверкой можно убедиться в том, что наше умножение удовлетворяет ассоциативному закону.

Тождественная подстановка P_0 есть единственная подстановка, удовлетворяющая условию

$$P_0 \cdot P_i = P_i \cdot P_0 = P_i$$

для любой подстановки P_i .

Наконец, к каждой подстановке имеется обратная к ней, дающая в произведении с данной тождественную подстановку: обратная подстановка к данной ставит все числа, смещенные подстановкой, на их прежние места. Так, например,

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

Чтобы в таблице умножения найти сразу подстановку, обратную к данной подстановке, надо в строчке, отмеченной слева данной подстановкой, найти элемент P_0 ; в заголовке столбца, в котором лежит этот элемент, и стоит подстановка, обратная данной. Имеем, как легко видеть:

$$P_0^{-1} = P_0, \quad P_3^{-1} = P_4,$$

$$P_1^{-1} = P_1, \quad P_4^{-1} = P_3,$$

$$P_2^{-1} = P_2, \quad P_5^{-1} = P_5.$$

Итак, умножение подстановок удовлетворяет всем групповым аксиомам и, следовательно, совокупность всех подстановок из трех элементов есть группа. Мы обозначим эту группу через S_3 . Группа S_3 конечна, ее порядок равен 6.

Заметим, что умножение подстановок, вообще говоря, не обладает свойством переместительности (коммутативности): произведение двух подстановок зависит, в общем случае, от порядка множителей. Так, мы имеем, например,

$$P_2 \cdot P_3 = P_5, \quad P_3 \cdot P_2 = P_1.$$

§ 2. ПОНЯТИЕ ПОДГРУППЫ

1. Примеры и определение. Естественно возникает вопрос: нельзя ли получить группу, взяв не все, а только некоторые из числа наших подстановок (из трех чисел) и сохранив для них, конечно, тот же закон умножения? Нетрудно убедиться, что ответ на этот вопрос утвердительный.

В самом деле, рассмотрим, например, пару элементов P_0 и P_1 . Наша таблица умножения дает нам непосредственно:

$$\begin{aligned} P_0 \cdot P_0 &= P_0, & P_0 \cdot P_1 &= P_1, \\ P_1 \cdot P_0 &= P_1, & P_1 \cdot P_1 &= P_0. \end{aligned}$$

Мы видим, что все групповые аксиомы выполнены (в частности, $P_0^{-1} = P_0$ и $P_1^{-1} = P_1$), значит, два элемента P_0 и P_1 образуют группу, составляющую часть группы всех подстановок из трех чисел.

Точно так же можно убедиться, что пара элементов P_0 и P_3 в свою очередь образует группу, как и пара P_0 и P_5 .

Что же касается пары P_0 и P_3 (и также пары P_0 и P_4), то она группы не образует, так как $P_3 \cdot P_3 = P_4$ (т. е. произведение элемента P_3 с самим собой не есть элемент нашей пары). Эти простые рассуждения оправдывают введение следующего общего определения.

О п р е д е л е н и е. Пусть задана какая-нибудь группа G ; тогда, если множество H , состоящее из некоторых элементов нашей группы G , образует (при законе умножения, заданном в G) группу, то группа H называется **подгруппой** группы G .

Таким образом, пары элементов (P_0, P_1) , (P_0, P_2) , (P_0, P_5) , каждая, являясь подгруппами порядка 2 группы S_3 . Других подгрупп порядка 2 группа S_3 не имеет: из определения подгруппы следует, что всякая подгруппа H группы G содержит нейтральный элемент

группы G , значит, всякая подгруппа порядка 2 группы S_3 имеет вид (P_0, P_i) , где i — одно из чисел 1, 2, 3, 4, 5; но мы видели, что i не может равняться ни 3, ни 4, значит, остаются только рассмотренные подгруппы

$$(P_0, P_1), (P_0, P_2), (P_0, P_5).$$

В группе S_3 имеется также подгруппа, состоящая из трех элементов (подгруппа порядка 3). Это будет подгруппа (P_0, P_3, P_4) . Читателю предлагается самому убедиться, что эта подгруппа есть единственная подгруппа порядка 3, содержащаяся в S_3 . Подгрупп порядка 4 и 5 в группе S_3 не имеется вовсе¹⁾.

Итак, подгруппы порядка S_3 суть: три подгруппы порядка 2, а именно: (P_0, P_1) , (P_0, P_2) , (P_0, P_5) , одна подгруппа порядка 3, а именно: (P_0, P_3, P_4) .

Таким же образом, как мы изучили группу S_3 , можно было бы изучить группу S_4 , состоящую из всех подстановок из четырех чисел.

Группа S_4 имеет порядок $1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Да и вообще, при любом n подстановки из n чисел образуют группу S_n порядка $1 \cdot 2 \cdot 3 \cdot \dots \cdot n = n!$

Закон умножения во всех этих группах один и тот же: умножить две подстановки из n чисел, значит, последовательно произвести эти подстановки одну за другой.

Отметим, наконец, что группа S_n всех подстановок из n элементов называется *симметрической группой* (подстановок из n элементов).

Любая подгруппа группы S_n называется *группой подстановок* из n элементов.

2. Условие, чтобы подмножество группы было подгруппой. При доказательстве того, что некоторое подмножество H группы G является подгруппой, удобнее всего бывает пользоваться следующей общей теоремой:

Подмножество H группы G тогда и только тогда является подгруппой группы G , когда выполнены следующие условия:

¹⁾ В этом можно убедиться, разобрав все 10 подмножеств группы S_3 , содержащих элемент P_0 и состоящих из четырех элементов, а также все 5 подмножеств, содержащих 5 элементов, включая непременно P_0 . Однако отсутствие подгрупп порядка 4 и 5 в группе вытекает непосредственно из следующей общей теоремы, которая будет доказана позже (гл. VIII): *порядок всякой подгруппы H конечной группы G есть делитель порядка G .*

1. Произведение двух элементов a и b из H (в смысле умножения, определенного в G) есть элемент множества H .

2. Нейтральный элемент группы G есть элемент множества H .

3. Элемент, обратный к какому-нибудь элементу множества H , есть элемент множества H .

Для доказательства достаточно заметить, что наши условия выражают в точности требования, чтобы операция умножения, определенная в G , но применяемая лишь к элементам множества H , удовлетворяла всем аксиомам группы (ассоциативности требовать не нужно: будучи выполнена при умножении любых элементов множества G , она тем более выполнена в частном случае, когда эти элементы являются элементами множества H).

§ 3.¹⁾ ПОДСТАНОВКИ КАК ОТОБРАЖЕНИЯ КОНЕЧНОГО МНОЖЕСТВА НА СЕБЯ. ЧЕТНЫЕ И НЕЧЕТНЫЕ ПОДСТАНОВКИ

1. Подстановки как отображения. Мы изложили понятие подстановки тем элементарным и несколько кустарным способом, каким это обычно и делается. Если не бояться общематематических терминов, то подстановку из n элементов следует определить просто как *взаимно однозначное отображение f множества данных n элементов на себя*.

Если наши элементы суть, положим, числа $1, 2, 3, \dots, n$, то подстановка

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$$

задается как функция

$$a_k = f(k), \quad k = 1, 2, \dots, n,$$

причем и значения аргумента и значения функции суть числа $1, 2, 3, \dots, n$.

Для двух данных значений аргумента значения функции всегда различны.

¹⁾ Читатель, которому этот параграф покажется трудным, может опустить его при первом чтении и вернуться к нему лишь перед гл. VI.

В частности, подстановка вполне определена, если для каждого k указано значение $f(k)$, т. е. a_k .

Отсюда следует, что совершенно несущественно, в каком порядке записаны числа в верхней строчке: важно только, чтобы под числом k было подписано именно a_k . Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}$$

представляют собой две записи одной и той же подстановки. Этому, в сущности, самоочевидному замечанию можно придать и такую форму.

Пусть дана подстановка

$$A = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}. \quad (2)$$

Если

$$P = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ p_1 & p_2 & p_3 & \dots & p_n \end{pmatrix} \quad (3)$$

есть какая-нибудь подстановка тех же чисел 1, 2, 3, ..., n , то подстановка (2) может быть записана в виде

$$\begin{pmatrix} p_1 & p_2 & \dots & p_n \\ a_{p_1} & a_{p_2} & \dots & a_{p_n} \end{pmatrix}.$$

2. Четные и нечетные подстановки. Пусть дана подстановка

$$A = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}.$$

Рассмотрим множество, состоящее из двух каких-нибудь чисел набора 1, 2, ..., n , положим для определенности из чисел i и k . Такое множество назовем *парой* чисел¹⁾, а именно парой, состоящей из элементов i и k ; обозначим его (i, k) .

Число всех пар, которые можно составить из данных n элементов, нетрудно подсчитать. Сначала вычислим, сколько различных *упорядоченных* подмножеств из двух элементов содержится в множестве из n эле-

¹⁾ Здесь с понятием пары не связано никакое предположение о порядке следования элементов пары: (i, k) и (k, i) суть две записи одной и той же пары. Такие пары элементов, взятые из числа данных n элементов, называются также *сочетаниями* из n элементов по 2.

ментов. Обозначим число таких подмножеств через A_n^2 и покажем, что

$$A_n^2 = n(n-1).$$

Действительно, для того чтобы распределить два элемента, взятых из данных n элементов, по двум местам, можно сначала выбрать какой-нибудь один элемент и поместить его на первое место. Это можно сделать n способами. На второе место теперь остается $n-1$ «кандидатов» и значит, $n-1$ способ выбора второго элемента. Следовательно, всего мы получим $n(n-1)$ способов размещения, что и требовалось.

Пусть C_n^2 — число всех пар, которые можно составить из n элементов. Покажем, что

$$C_n^2 = \frac{1}{2} A_n^2 = \frac{n(n-1)}{2},$$

или, что то же самое,

$$A_n^2 = 2C_n^2.$$

В самом деле, чтобы образовать упорядоченное множество, содержащее два элемента из данных n , надо выделить какие-либо два из этих n элементов, что можно сделать C_n^2 способами, а затем упорядочить выделенные два элемента, что можно сделать двумя способами. Итак,

$$A_n^2 = 2C_n^2,$$

что и требовалось доказать.

Пара, состоящая из элементов i и k , называется *правильной по отношению к подстановке A* , если разности $i-k$ и a_i-a_k имеют один и тот же знак; это значит: если $i < k$, то должно быть $a_i < a_k$; если же $i > k$, то должно быть $a_i > a_k$. В противном случае говорят, что наша пара *неправильна в подстановке A* или образует в ней *инверсию*. Следовательно, если пара (i, k) образует инверсию, то имеем либо $i < k$ и $a_i > a_k$ либо, наоборот, $i > k$ и $a_i < a_k$. Рассмотрим, как пример, подстановки группы S_3 .

В подстановке $P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ нет ни одной инверсии — все пары правильны.

В подстановке $P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ имеется единственная инверсия $(2, 3)$, так как при $i=2$, $k=3$ имеем $a_i=3$ и $a_k=2$.

В подстановке $P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ имеется единственная инверсия (1, 2).

В подстановке $P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ имеются две инверсии: (1, 3), (1, 2).

В подстановке $P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ имеются две инверсии: (1, 3), (2, 3).

В подстановке $P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ имеются три инверсии: (1, 2), (1, 3), (2, 3).

Определение. Подстановка, содержащая четное число инверсий, называется **четной** подстановкой; подстановка, содержащая нечетное число инверсий, **нечетной** подстановкой.

Мы видим, что в группе S_3 четные подстановки (P_0 , P_3 и P_4) образуют подгруппу. Наша задача — доказать, что это замечание справедливо для любой группы S_n .

Доказательство опирается на некоторые предварительные замечания, к которым мы и переходим.

Знаком подстановки A называется число $+1$, если подстановка A четная, и число -1 , если она нечетная.

Отвлекаясь от обычного словоупотребления, назовем теперь **знаком** рационального числа r число $+1$, если число r положительно, число -1 , если r отрицательно, и число 0, если $r = 0$. Знак числа r в только что установленном смысле обозначим так: $(\text{зн } r)$.

При этих обозначениях ясно, что знак подстановки A равен произведению знаков всех $\frac{n(n-1)}{2}$ чисел $\frac{i-k}{a_i - a_k}$, причем дробь $\frac{i-k}{a_i - a_k} = \frac{k-i}{a_k - a_i}$ строится по одному разу для каждой пары, взятой из чисел $1, 2, 3, \dots, n$.

Этим замечанием мы воспользуемся для доказательства следующей теоремы.

Теорема 1. *Знак произведения двух подстановок равен произведению знаков сомножителей.*

Доказательство. Пусть даны две подстановки:

$$A = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix}.$$

Их произведение есть, очевидно, подстановка

$$A \cdot B = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ b_{a_1} & b_{a_2} & b_{a_3} & \dots & b_{a_n} \end{pmatrix}. \quad (4)$$

Знаки A и B равны соответственно произведениям всех знаков

$$\frac{i-k}{a_i-a_k} \text{ и } \frac{i-k}{b_i-b_k}.$$

Но так как можно также написать

$$B = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_{a_1} & b_{a_2} & \dots & b_{a_n} \end{pmatrix},$$

то имеем:

знак B равен произведению всех знаков $\frac{a_i-a_k}{b_{a_i}-b_{a_k}}$.

Отсюда сразу следует:

$$\begin{aligned} (\text{зн } A) \cdot (\text{зн } B) &= \\ &= \text{произведению всех } \left(\text{зн } \frac{i-k}{a_i-a_k} \right) \cdot \left(\text{зн } \frac{a_i-a_k}{b_{a_i}-b_{a_k}} \right) = \\ &= \text{произведению всех } \left(\text{зн } \frac{i-k}{a_i-a_k} \cdot \frac{a_i-a_k}{b_{a_i}-b_{a_k}} \right) = \\ &= \text{произведению всех } \left(\text{зн } \frac{i-k}{b_{a_i}-b_{a_k}} \right). \end{aligned}$$

Но последнее произведение есть знак подстановки

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ b_{a_1} & b_{a_2} & b_{a_3} & \dots & b_{a_n} \end{pmatrix},$$

т. е. подстановки $A \cdot B$, что и требовалось доказать.

Из доказанной теоремы непосредственно следует: *произведение двух подстановок одинаковой четности¹⁾ есть четная, а произведение двух подстановок различной четности²⁾ есть нечетная подстановка.* Тождественная подстановка не содержит ни одной инверсии и, следовательно, есть четная подстановка. Далее,

$$A \cdot A^{-1} = E$$

(E — тождественная подстановка), т. е. произведение данной подстановки A и обратной ей подстановки есть четная подстановка; отсюда по только что доказанному следует, что любая подстановка имеет ту же четность, что и обратная ей.

Итак, *произведение двух четных подстановок есть четная подстановка; тождественная подстановка есть*

¹⁾ То есть произведение двух четных или двух нечетных подстановок.

²⁾ То есть произведение четной и нечетной или нечетной и четной подстановок.

четная подстановка, обратная четной подстановке есть четная подстановка.

Отсюда следует, что совокупность всех четных подстановок из n элементов есть подгруппа группы S_n всех вообще подстановок из n элементов. Группа четных подстановок из n элементов называется **знакопеременной** или **альтернирующей** группой подстановок из n элементов, и обозначается через A_n .

Теорема 2. *Порядок группы A_n равен $\frac{n!}{2}$.*

Другими словами, в группу A_n входит ровно половина всех подстановок из n элементов. Для того чтобы убедиться в этом, достаточно установить взаимно однозначное соответствие между множеством всех четных и множеством всех нечетных подстановок из n элементов. Такое соответствие устанавливается, если выбрать какую-нибудь определенную нечетную подстановку P и каждой четной подстановке A поставить в соответствие подстановку $P \cdot A$. Тогда:

1) каждой четной подстановке будет соответствовать нечетная подстановка;

2) двум различным четным подстановкам будут соответствовать различные нечетные подстановки;

3) каждая нечетная подстановка B окажется поставленной в соответствие одной (и только одной) четной подстановке, а именно: четной подстановке $P^{-1} \cdot B$.

Таким образом, наше соответствие есть взаимно однозначное соответствие между множеством всех четных и множеством всех нечетных подстановок.

ИЗОМОРФНЫЕ ГРУППЫ. ТЕОРЕМА КЭЛИ

§ 1. ИЗОМОРФНЫЕ ГРУППЫ

Рассмотрим, с одной стороны, группу поворотов R_3 правильного треугольника (гл. I, § 2), а с другой стороны, содержащуюся в группе всех подстановок из трех цифр подгруппу A_3 , состоящую из трех элементов P_0, P_3, P_4 (гл. II, § 2). Мы обозначили элементы группы R_3 через a_0, a_1, a_2 . Установим теперь между элементами группы R_3 и элементами группы A_3 следующее взаимно однозначное соответствие:

$$a_0 \leftrightarrow P_0,$$

$$a_1 \leftrightarrow P_3,$$

$$a_2 \leftrightarrow P_4.$$

Это соответствие сохраняет умножение в следующем смысле. Если какой-либо элемент в левом столбце может быть записан в виде произведения двух элементов (конечно, того же левого столбца), например, $a_0 a_1 = a_1$ или $a_1 a_1 = a_2$ или $a_1 a_2 = a_0$, и если мы каждый элемент полученного равенства заменим соответствующим элементом правого столбца, то равенство останется справедливым.

Мы видим, что группы R_3 и A_3 хотя и состоят из элементов различной природы (одна группа состоит из поворотов треугольника, а другая из подстановок цифр), но *устроены они одинаково*: таблицы умножения этих групп отличаются лишь обозначениями и, следовательно, заменой обозначений, т. е. переименованием элементов, они могут быть приведены к одинаковому виду.

Такие группы, которые при надлежащем выборе обозначений элементов таблицы умножения оказываются тождественными (одинаковыми), называются **изоморфными** группами.

Обыкновенно понятие изоморфизма высказывают в немного отличной форме. Дело в том, что «переименование» элементов в таблице умножения, о котором шла речь в нашем определении изоморфизма, по существу, сводится к установлению взаимно однозначного соответствия между элементами двух групп. Мы теперь дадим определение изоморфизма, непосредственно исходящее из понятия взаимно однозначного отображения.

Определение I. Пусть дано взаимно однозначное соответствие

$$g \leftrightarrow g'$$

между множеством всех элементов группы G и множеством всех элементов группы G' . Мы скажем, что это соответствие есть **изоморфное соответствие** (или **изоморфизм**) между двумя группами, если выполнено условие сохранения умножения, гласящее:

каково бы ни было соотношение вида

$$g_1 \cdot g_2 = g_3$$

между элементами одной группы, например, G , соотношение, получаемое при замене элементов g_1, g_2, g_3 группы G соответствующими им в группе G' элементами g'_1, g'_2, g'_3 также оказывается справедливым: $g'_1 \cdot g'_2 = g'_3$.

Определение II. Две группы называются **изоморфными**, если между ними возможно установить изоморфное соответствие.

Примечание. Если требовать, чтобы всегда из равенства

$$g_1 \cdot g_2 = g_3 \quad (\text{в группе } G)$$

следовало равенство

$$g'_1 \cdot g'_2 = g'_3$$

для элементов группы G' , соответствующих элементам g_1, g_2, g_3 , то имеет место и обратное, а именно:

если для каких-либо трех элементов g'_1, g'_2, g'_3 группы G' имеет место соотношение

$$g'_1 \cdot g'_2 = g'_3,$$

то для элементов g_1, g_2, g_3 группы G , соответствующих элементам g'_1, g'_2, g'_3 , также выполнено соотношение

$$g_1 \cdot g_2 = g_3. \tag{1}$$

В самом деле, если бы соотношение (1) не имело места, то было бы

$$g_1 \cdot g_2 = g_4 \neq g_3.$$

В силу взаимной однозначности соответствия между G и G' элементу группы g_4 соответствует в группе G' элемент $g'_4 \neq g'_3$ и в силу нашего предположения из

$$g_1 \cdot g_2 = g_4$$

должно вытекать

$$g'_1 \cdot g'_2 = g'_4,$$

вопреки тому, что

$$g'_1 \cdot g'_2 = g'_3.$$

Теорема. При изоморфном отображении

$$g \leftrightarrow g'$$

группы G на группу G' нейтральному элементу одной группы соответствует нейтральный элемент другой группы, и всякой паре взаимно обратных элементов одной группы соответствует пара взаимно обратных элементов другой группы.

В самом деле, пусть g_0 — нейтральный элемент группы G , и пусть ему при данном изоморфном соответствии между группами G и G' соответствует элемент g'_0 группы G' . Докажем, что g'_0 есть нейтральный элемент группы G' . В самом деле, так как g_0 — нейтральный элемент группы G , то имеем для произвольного элемента g той же группы

$$g \cdot g_0 = g;$$

в силу изоморфности отображения $g \leftrightarrow g'$ имеем:

$$g' \cdot g'_0 = g',$$

откуда и следует, что g'_0 есть нейтральный элемент группы G' .

Пусть g_1 и g_2 — пара обратных элементов в группе G :

$$g_1 \cdot g_2 = g_0$$

(где g_0 по-прежнему — нейтральный элемент группы G). Отсюда

$$g'_1 \cdot g'_2 = g'_0.$$

Так как g'_0 — нейтральный элемент группы G' , то g'_1 и g'_2 взаимно обратны.

Упражнения. 1) Показать, что группа, состоящая из двух элементов a_0 и a_1 с таблицей умножения

	a_0	a_1
a_0	a_0	a_1
a_1	a_1	a_0

изоморфна группе поворотов отрезка (вокруг его середины).

2) Доказать, что все группы порядка 2 изоморфны между собой.

3) Доказать, что все группы порядка 3 изоморфны между собой.

Решение. Пусть a_0, a_1, a_2 — элементы группы; пусть a_0 — единичный элемент. Тогда

$$a_0 \cdot a_0 = a_0; \quad a_0 \cdot a_1 = a_1; \quad a_0 \cdot a_2 = a_2.$$

Не может быть, чтобы $a_1 \cdot a_1 = a_1$, так как тогда $a_1 = a_0$. Итак,

$$a_1 \cdot a_1 = a_2.$$

Аналогично,

$$a_1 \cdot a_2 \neq a_2 \quad \text{и} \quad a_1 \cdot a_2 \neq a_1.$$

Следовательно,

$$a_1 \cdot a_2 = a_0.$$

Таким же точно образом заключаем, что

$$a_2 \cdot a_1 = a_0.$$

Наконец, поскольку

$$a_2 \cdot a_2 \neq a_2 \quad (\text{так как тогда имели бы } a_2 = a_0)$$

и

$$a_2 \cdot a_2 \neq a_0 \quad (\text{так как } a_1 \cdot a_2 = a_0),$$

то

$$a_2 \cdot a_2 = a_1.$$

Итак, для группы порядка 3 возможна лишь одна таблица умножения, а именно:

	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

4) Доказать, что всякая коммутативная группа порядка 4 изоморфна или клейновской группе, или группе поворотов правильного четырехугольника (две последние группы между собой неизоморфны; почему?).

5) Доказать, что группа всех положительных чисел (с арифметическим умножением в качестве групповой операции) изоморфна группе всех действительных чисел (с арифметическим сложением в качестве групповой операции).

У к а з а н и е: изоморфное отображение осуществляется логарифмированием.

§ 2¹⁾. ТЕОРЕМА КЭЛИ

В этом параграфе мы докажем следующее предложение, открытое Кэли²⁾.

Т е о р е м а. *Всякая конечная группа изоморфна некоторой группе подстановок.*

Д о к а з а т е л ь с т в о. Пусть G — конечная группа, n — ее порядок, a_1, a_2, \dots, a_n — ее элементы, среди них a_1 — нейтральный элемент.

Напишем для каждого $i = 1, 2, \dots, n$

$$a_1 \cdot a_i, \quad a_2 \cdot a_i, \quad \dots, \quad a_n \cdot a_i.$$

Все эти элементы различны; число их равно n ; значит, это суть те же элементы a_1, a_2, \dots, a_n , но только

¹⁾ Читатель, пропустивший § 3 предыдущей главы, должен пропустить и этот параграф.

²⁾ Кэли А. (Cauley) — английский математик (род. 1821, умер 1895) — один из основателей теории групп.

записанные в другом порядке, а именно: пусть

$$a_1 \cdot a_i = a_{i_1}, \quad a_2 \cdot a_i = a_{i_2}, \quad \dots, \quad a_n \cdot a_i = a_{i_n}.$$

Итак, элементу a_i соответствует подстановка

$$P_i = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 \cdot a_i & a_2 \cdot a_i & \dots & a_n \cdot a_i \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_{i_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix}$$

или подстановка

$$P'_i = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

отличающаяся от подстановки P_i только тем, что в P_i переставляются элементы группы G , а в P'_i — взаимно однозначно соответствующие этим элементам их номера.

Если $i \neq k$, то $P_i \neq P_k$, так как в подстановке P_i под элементом a_1 расположен $a_1 \cdot a_i = a_i$, а в подстановке P_k под элементом a_1 расположен $a_1 \cdot a_k = a_k$, $a_k \neq a_i$.

Итак, имеем взаимно однозначное соответствие между элементами a_1, a_2, \dots, a_n группы G и подстановками P_1, P_2, \dots, P_n .

Теперь нужно доказать, что во-первых, подстановки P_1, P_2, \dots, P_n образуют группу по отношению к обычному умножению подстановок и, во-вторых, что эта группа изоморфна группе G .

Заметим прежде всего:

1. Среди подстановок P_1, P_2, \dots, P_n содержится тождественная подстановка.

В самом деле, так как a_1 есть, по предположению, нейтральный элемент группы G , то подстановка

$$P_1 = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 \cdot a_1 & a_2 \cdot a_1 & \dots & a_n \cdot a_1 \end{pmatrix}$$

есть тождественная подстановка.

Далее докажем: если $a_h = a_i \cdot a_k$, то $P_h = P_i \cdot P_k$.

Сначала заметим, что

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 \cdot a_k & a_2 \cdot a_k & \dots & a_n \cdot a_k \end{pmatrix}$$

и

$$\begin{pmatrix} a_1 \cdot a_i & a_2 \cdot a_i & \dots & a_n \cdot a_i \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \dots & a_n \cdot a_i \cdot a_k \end{pmatrix}$$

представляют две записи одной и той же подстановки P_k ; в самом деле, обе записи означают, что каждому элементу a группы G ставится в соответствие элемент $a \cdot a_k$ той же группы.

Итак, мы можем записать

$$P_k = \begin{pmatrix} a_1 \cdot a_i & a_2 \cdot a_i & \dots & a_n \cdot a_i \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \dots & a_n \cdot a_i \cdot a_k \end{pmatrix}.$$

Заметив это, видим, что подстановка

$$P_i \cdot P_k = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 \cdot a_i & a_2 \cdot a_i & \dots & a_n \cdot a_i \end{pmatrix} \cdot \begin{pmatrix} a_1 \cdot a_i & a_2 \cdot a_i & \dots & a_n \cdot a_i \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \dots & a_n \cdot a_i \cdot a_k \end{pmatrix}$$

на основании общего определения умножения подстановок тождественна с подстановкой

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \dots & a_n \cdot a_i \cdot a_k \end{pmatrix}.$$

Но если $a_i \cdot a_k = a_h$, то

$$\begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 \cdot a_i \cdot a_k & a_2 \cdot a_i \cdot a_k & \dots & a_n \cdot a_i \cdot a_k \end{pmatrix} = P_h,$$

т. е.

$$P_i \cdot P_k = P_h.$$

Только что доказанное можно сформулировать так:

IIa. Произведению двух элементов группы G соответствует произведение подстановок, соответствующих этим элементам.

Отсюда следует:

IIb. Произведение любых двух из числа подстановок P_1, P_2, \dots, P_n есть одна из подстановок P_1, P_2, \dots, P_n .

Рассмотрим подстановку P_i , элемент a_i и элемент $a_i^{-1} = a_k$. Так как $a_i \cdot a_k = a_1$, то по только что доказанному $P_i \cdot P_k = P_1$; но P_1 есть, как мы видели, тождественная подстановка, поэтому $P_k = P_i^{-1}$.

Итак, мы доказали еще одно утверждение.

III. Подстановка P_i^{-1} для любого $i = 1, 2, \dots, n$ есть одна из подстановок P_1, P_2, \dots, P_n .

Из IIb, I и III следует, что совокупность подстановок P_1, P_2, \dots, P_n есть группа при обычном определении умножения подстановок. Из IIa следует, что эта группа изоморфна группе G .

Теорема Кэли, таким образом, доказана.

ЦИКЛИЧЕСКИЕ ГРУППЫ

§ 1. ПОДГРУППА, ПОРОЖДЕННАЯ ДАННЫМ ЭЛЕМЕНТОМ ДАННОЙ ГРУППЫ. ОПРЕДЕЛЕНИЕ ЦИКЛИЧЕСКОЙ ГРУППЫ

Пусть a — произвольный элемент группы G . Умножим его на себя, т. е. возьмем элемент $a \cdot a$. Этот элемент обозначим через a^2 . Точно так же обозначим $a \cdot a \cdot a$ через a^3 и вообще положим

$$\underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ раз}} = a^n.$$

Рассмотрим, далее, элемент a^{-1} и обозначим последовательно

$$\begin{aligned} a^{-1} \cdot a^{-1} & \text{ через } a^{-2}, \\ a^{-1} \cdot a^{-1} \cdot a^{-1} & \text{ через } a^{-3}, \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \dots \cdot a^{-1}}_{n \text{ раз}} & \text{ через } a^{-n}. \end{aligned}$$

Обозначения эти оправданы тем, что, действительно,

$$a^n \cdot a^{-n} = 1.$$

Для доказательства последнего утверждения заметим прежде всего, что в случае $n = 1$ оно очевидно (следует из самого определения a^{-1}). Предположим, что оно верно для $n - 1$ и докажем в этом предположении его справедливость для n . Имеем

$$a^n \cdot a^{-n} = (a \cdot a^{n-1}) (a^{-(n-1)} \cdot a^{-1}) = a \cdot \{a^{n-1} \cdot a^{-(n-1)}\} \cdot a^{-1}.$$

Но в силу нашего предположения фигурная скобка равна единице, значит,

$$a^n \cdot a^{-n} = a \cdot 1 \cdot a^{-1} = a \cdot a^{-1} = 1,$$

что и требовалось доказать.

Мы определили выражение a^n для любого положительного и для любого отрицательного значения n . Положим, наконец, что, по определению, $a^0 = 1$.

Пусть теперь p и q — два целых числа. Из наших определений следует, что для любых целых p и q имеем

$$a^p \cdot a^q = a^{p+q}.$$

Мы получаем следующий результат:

Множество $H(a)$ тех элементов группы G , которые могут быть представлены в виде a^n при целом n с той групповой операцией, которая задана в группе G , образует группу $H(a)$.

В самом деле: 1) произведение двух элементов, принадлежащих $H(a)$, есть опять элемент $H(a)$; 2) единица принадлежит $H(a)$; 3) к каждому элементу a^m из $H(a)$ найдется элемент a^{-m} , который также принадлежит $H(a)$.

Итак, $H(a)$ есть подгруппа G . Эта подгруппа называется **циклической подгруппой группы G , порожденной элементом a .**

Поскольку в группе $H(a)$

$$a^m \cdot a^n = a^{m+n} = a^{n+m} = a^n \cdot a^m,$$

то группа $H(a)$ коммутативна.

Мы определили понятие циклической подгруппы $H(a)$, порожденной некоторым элементом a данной группы G . Станем теперь на более абстрактную точку зрения и рассмотрим группу H такую, что каждый ее элемент имеет вид a^n для некоторого фиксированного элемента a из H и некоторого числа n . Такую группу мы назовем *циклической группой, порожденной элементом a* , и будем обозначать, как и ранее, $H(a)$. Теперь нет нужды считать, что группа $H = H(a)$ содержится в какой-либо объемлющей группе.

Так как группа $H(a)$ коммутативна, то ее групповую операцию принято записывать на аддитивном языке. Итак, операция в $H(a)$ теперь обозначается $+$, нейтральный элемент 0 , элемент $\underbrace{a + a + \dots + a}_{n \text{ раз}}$ через na и т. д.

§ 2. КОНЕЧНЫЕ И БЕСКОНЕЧНЫЕ ЦИКЛИЧЕСКИЕ ГРУППЫ

Группу $H(a)$ мы определили как состоящую из всех тех элементов, которые могут быть записаны в виде na . При этом мы не ставили вопроса: будут ли

две записи m_1a и m_2a при различных целых m_1 и m_2 всегда давать два различных элемента группы $H(a)$ или же может случиться, что $m_1a = m_2a$, хотя m_1 и m_2 различны?

Постараемся разобраться в этом. Пусть существуют два различных между собой целых числа m_1 и m_2 таких, что $m_1a = m_2a$. Прибавляя к обеим частям последнего равенства элемент $-m_1a$, получим

$$0 = (m_2 - m_1)a.$$

Следовательно, существуют такие целые числа m , что

$$ma = 0.$$

Так как из $ma = 0$ следует $-ma = 0$, то всегда можно предположить, что число m в равенстве $ma = 0$ положительно.

Возьмем теперь среди всех натуральных чисел, удовлетворяющих условию $ma = 0$, наименьшее и обозначим его через α . Имеем

$$a \neq 0, \quad 2a \neq 0, \dots, \quad (\alpha - 1)a \neq 0, \quad \alpha a = 0.$$

Докажем, что все элементы

$$0 = 0a, a, 2a, \dots, (\alpha - 1)a \quad (1)$$

различны между собой. В самом деле, если бы было

$$pa = qa \quad \text{при} \quad 0 \leq p < q \leq \alpha - 1,$$

то имели бы, прибавляя к обеим частям последнего равенства по $-pa$:

$$(q - p)a = 0,$$

а это противоречит определению числа α , так как в наших условиях заведомо

$$0 < q - p \leq \alpha - 1.$$

Итак, все элементы (1) различны между собой. Докажем, что вся группа $H(a)$ исчерпывается элементами (1), т. е., что для любого целочисленного m имеем

$$ma = ra, \quad \text{причем} \quad 0 \leq r \leq \alpha - 1.$$

Для этого разделим число m на число α с остатком (по правилу деления целых чисел), а именно — представим его в виде

$$m = q\alpha + r, \quad (2)$$

где q есть неполное частное, а r — остаток, удовлетворяющий условию ¹⁾

$$0 \leq r < \alpha.$$

Имеем

$$ma = (q\alpha + r) a = q\alpha \cdot a + ra,$$

HO

$$q\alpha \cdot a = q(\alpha a) = q \cdot 0 = 0,$$

значит,

$$ma = ra.$$

Итак, если существуют два такие числа m_1 и m_2 , что $m_1 a = m_2 a$, то существует натуральное число α , такое, что вся группа $H(a)$ исчерпывается α различными между собой элементами:

$$0, a, 2a, \dots, (\alpha - 1)a, \quad (3)$$

Тогда как $\alpha a = 0$.

Положение получается такое: весь ряд

$$\dots, -ma, \dots, -a, 0, a, \dots, ma, \dots$$

представляет собой бесконечное повторение (в обе стороны — направо и налево) своего «отрезка» (3).

В самом деле,

$$(\alpha + 1) a = \alpha a + a = a,$$

$$(\alpha + 2)a = \alpha a + 2a = 2a,$$

$$(2\alpha - 1) a = \alpha a + (\alpha - 1) a = (\alpha - 1) a,$$

$$2\alpha a = 0,$$

$$(2\alpha + 1) a = a \text{ и т. д.}$$

1) При отрицательном m остаток r при делении на $\alpha > 0$ все же берется положительным. В самом деле, пусть m отрицательно; тогда $-m$ положительно и может быть записано в виде

$$-m = q'\alpha + r', \quad 0 \leq r' < \alpha,$$

где q' и r' — неотрицательные. Тогда $m = -q'\alpha - r' = -(q' + 1)\alpha + (\alpha - r')$. В этих условиях число $-(q' + 1)$ называется неполным частным от деления отрицательного числа m на положительное число α , а неотрицательное число $r = \alpha - r' < \alpha$ называется остатком при этом делении. Более подробно см. об этом § 2 гл. VII.

И аналогично в левую сторону:

$$\begin{aligned} -a &= \alpha a - a = (\alpha - 1)a, \\ -2a &= \alpha a - 2a = (\alpha - 2)a, \\ &\dots\dots\dots \\ -(\alpha - 1)a &= \alpha a - (\alpha - 1)a = a, \\ -\alpha a &= 0 \text{ и т. д.} \end{aligned}$$

Чтобы найти, какой именно элемент группы $H(a)$ мы получаем, взяв сумму

$$\underbrace{a + a + \dots + a}_{m \text{ раз}} = ma$$

или

$$\underbrace{(-a) + (-a) + \dots + (-a)}_{m \text{ раз}} = -ma,$$

надо разделить m (или $-m$) на α . Неотрицательный остаток r , полученный при этом делении, $0 \leq r \leq \alpha - 1$ и дает нам ответ на наш вопрос:

$$ma = r\alpha.$$

Отсюда также ясно, как складываются элементы группы $H(a)$:

$$pa + qa = (p + q)a = ra,$$

где r есть остаток при делении $p + q$ на α .

Рассмотрим теперь правильный α -угольник; центральный угол, опирающийся на сторону нашего многоугольника, есть

$$\varphi = \frac{2\pi}{\alpha}.$$

Многоугольник переходит сам в себя при поворотах на углы:

0 («тождественный» поворот), φ , 2φ , ..., $(\alpha - 1)\varphi$.

Если считать тождественными повороты, отличающиеся друг от друга на целое число полных оборотов, то никакие другие повороты, кроме перечисленных α , не переводят наш многоугольник в самого себя. При этом композиция поворота на угол $p\varphi$ и поворота на угол $q\varphi$ есть поворот на угол $r\varphi$, где r есть остаток при делении $p + q$ на α .

Мы видим: если повороту нашего многоугольника на угол $m\varphi$ поставить в соответствие элемент ma груп-

пы $H(a)$, получается изоморфное отображение группы $H(a)$ на группу поворотов правильного α -угольника.

Группы, изоморфные группам поворотов правильных многоугольников, называются **конечными циклическими группами**.

Итак, если $m_1 a = m_2 a$ для некоторых m_1 и m_2 , то конечная группа $H(a)$ есть конечная циклическая группа.

Таблица сложения для циклической группы порядка m имеет вид

Т а б л и ц а 5

	a_0	a_1	a_2	a_3	\dots	a_{m-1}
a_0	a_0	a_1	a_2	a_3	\dots	a_{m-1}
a_1	a_1	a_2	a_3	a_4	\dots	a_0
a_2	a_2	a_3	a_4	a_5	\dots	a_1
a_3	a_3	a_4	a_5	a_6	\dots	a_2
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
a_{m-3}	a_{m-3}	a_{m-2}	a_{m-1}	a_0	\dots	a_{m-4}
a_{m-2}	a_{m-2}	a_{m-1}	a_0	a_1	\dots	a_{m-3}
a_{m-1}	a_{m-1}	a_0	a_1	a_2	\dots	a_{m-2}

Эта таблица сложения может служить вторым определением циклической группы порядка m .

* * *

Мы исследовали случай, когда для данного элемента a группы $H(a)$ имеются два таких целых числа m_1 и m_2 , что $m_1 a = m_2 a$.

Рассмотрим теперь случай, когда таких двух целых чисел нет, т. е. когда все элементы

$$\dots, -ta, -(m-1)a, \dots, \\ -3a, -2a, -a, 0, a, 2a, 3a, \dots, ta, \dots \quad (4)$$

различны. Элементы (4) находятся в этом случае во взаимно однозначном соответствии с целыми числами:

элементу ta соответствует целое число m и обратно. Если при этом

$$m_1a + m_2a = m_3a,$$

то

$$m_1 + m_2 = m_3.$$

Отсюда следует, что наше взаимно однозначное соответствие есть изоморфное соответствие между группой $H(a)$ и группой всех целых чисел.

Группы, изоморфные группе целых чисел, называются бесконечными циклическими группами.

Далее, так как две группы A и B , изоморфные одной и той же группе C , очевидно, изоморфны между собой, то все бесконечные циклические группы между собой изоморфны. Изоморфны между собой (по той же причине) и все конечные циклические группы одного и того же порядка m .

§ 3. СИСТЕМЫ ОБРАЗУЮЩИХ

Вернемся на время к циклической группе $H(a)$, порожденной элементом a группы G . Элемент a в том смысле порождает группу $H(a)$, что всякий ее элемент является произведением нескольких сомножителей¹⁾, каждый из которых есть или a или a^{-1} . Вместо того чтобы говорить: элемент a порождает группу $H(a)$, часто говорят: элемент a есть *образующий элемент* группы $H(a)$.

Однако не всякая группа есть циклическая, не всякая группа порождается одним элементом — нециклические группы порождаются не одним, а с необходимостью несколькими (иногда бесконечным числом) элементами; понятию одного образующего элемента приходит на смену понятие *системы образующих*²⁾.

О п р е д е л е н и е. Некоторое множество E элементов группы G называется *системой образующих* этой группы, если всякий элемент группы G есть произведение конечного числа сомножителей, каждый из которых либо есть элемент множества E , либо является обратным некоторому элементу множества E .

¹⁾ В «аддитивной» терминологии: суммой нескольких слагаемых.

²⁾ Очевидно, совокупность всех элементов какой-нибудь группы есть (тривиальная) система образующих этой группы. Итак, *всякая группа имеет систему образующих*.

Пример. Рассмотрим плоскость с выбранной на ней системой декартовых координат. Обозначим через G множество тех точек $P = (x, y)$, обе координаты которых x и y — суть целые числа. Установим следующее правило сложения точек: суммой двух точек $P_1 = (x_1, y_1)$ и $P_2 = (x_2, y_2)$ называется точка $P_3 = (x_3, y_3)$ с координатами $x_3 = x_1 + x_2$ и $y_3 = y_1 + y_2$. Читатель сам легко убедится, что это определение сложения превращает множество G в коммутативную группу и что точки $(0, 1)$ и $(1; 0)$ составляют систему образующих этой группы.

Замечание. Читатель, знакомый с понятием комплексного числа, сразу поймет, что только что построенная группа изоморфна группе целых комплексных чисел (со сложением в качестве групповой операции). При этом комплексное число $x + iy$ называется целым, если x и y суть целые числа.

Задача. Доказать, что всякая система натуральных чисел, наибольший общий делитель которых равен единице, есть система образующих группы всех целых чисел.

ПРОСТЕЙШИЕ ГРУППЫ САМОСОВМЕЩЕНИЙ

§ 1. ПРИМЕРЫ И ОПРЕДЕЛЕНИЕ ГРУПП САМОСОВМЕЩЕНИЙ ГЕОМЕТРИЧЕСКИХ ФИГУР

1. Самосовмещения правильных многоугольников в их плоскости. Обширный и очень важный класс разнообразных групп как конечных, так и бесконечных составляют группы «самосовмещений» геометрических фигур. Под *самосовмещением* данной геометрической фигуры F понимают такое *перемещение* фигуры F (в пространстве или на плоскости), которое *переводит* F в *самое себя*, т. е. совмещает фигуру F с самой собой.

Мы уже познакомились с простейшими группами самосовмещений, а именно: с группами поворотов правильных многоугольников.

Пусть дан в плоскости правильный многоугольник $A_0A_1 \dots A_n$ (рис. 2), например, правильный восьмиугольник $A_0A_1A_2A_3A_4A_5A_6A_7$ (вершины все перенумерованы подряд в одном направлении, например, против часовой стрелки).

Требуется найти те перемещения многоугольника в его плоскости, которые совмещают его с самим собой. При этом перемещении всякая вершина многоугольника должна перейти в вершину, всякая сторона — в сторону, а центр многоугольника — в самого себя. Пусть

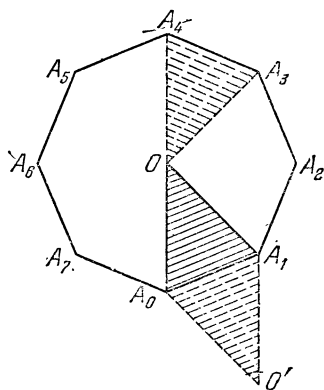


Рис. 2.

при некотором определенном перемещении вершина A_0 перейдет, положим, в A_k (на рисунке $k=4$).

Тогда сторона A_0A_1 должна перейти либо в сторону A_kA_{k+1} либо в сторону A_kA_{k-1} . Но если бы сторона A_0A_1 перешла в сторону A_kA_{k-1} , то треугольник A_0A_1O перешел бы в треугольник $A_kA_{k-1}O$. Этот последний треугольник можно было бы, передвигая его в плоскости, перевести в положение A_0A_1O' , являющееся зеркальным отражением треугольника A_0A_1O относительно стороны A_0A_1 . В результате оказалось бы, что мы треугольник A_0A_1O перемещением в его плоскости перевели в его зеркальное отражение, а это невозможно¹⁾.

Итак, сторона A_0A_1 должна перейти в сторону A_kA_{k+1} . Точно таким же образом мы убеждаемся в том, что сторона A_1A_2 переходит в $A_{k+1}A_{k+2}$, сторона A_2A_3 переходит в $A_{k+2}A_{k+3}$ и т. д. Другими словами, наше перемещение есть поворот многоугольника в его плоскости на угол $k \cdot \frac{2\pi}{n}$. Итак, мы показали, что:

а) всякое самосовмещение правильного n -угольника в его плоскости есть поворот многоугольника на угол $k \frac{2\pi}{n}$, где k — целое число;

б) таким образом, самосовмещений имеется n ;

в) эти самосовмещения, как мы знаем, образуют группу.

2. Самосовмещения правильного многоугольника в трехмерном пространстве. Предыдущее рассуждение существенно предполагало, что мы рассматриваем лишь самосовмещения многоугольника в его плоскости. Если бы мы рассматривали совмещения n -угольника с самим собой в пространстве, то к перечисленным поворотам прибавились бы еще «опрокидывания» многоугольника, т. е. повороты на угол 180° вокруг осей симметрии многоугольника. Осей симметрии правильный n -угольник имеет n : в случае четного n осями симметрии являются $\frac{n}{2}$ прямых, соединяющих пары противоположных вершин многоугольника, и $\frac{n}{2}$ прямых, соединяющих середины его противоположных сторон;

¹⁾ Строгое доказательство этой невозможности, являющейся одним из основных фактов геометрии плоскости, выходит за рамки этой книги.

в случае нечетного n оси симметрии суть прямые, соединяющие вершины с серединами противоположных сторон многоугольника. Доказательство того, что n поворотами и n «прокидываниями» правильного n -угольника исчерпываются все самосовмещения n -угольника, т. е. все перемещения его в пространстве, переводящие многоугольник в самого себя, по существу, содержится в рассуждениях § 3 этой главы. Читателю предлагается вернуться к этому вопросу по прочтении указанного параграфа и еще раз продумать все вопросы, связанные с самосовмещениями правильных многоугольников.

3. Общее определение группы самосовмещений данной фигуры в пространстве или на плоскости. Пусть в пространстве или на плоскости дана фигура F . Рассмотрим все самосовмещения этой фигуры, т. е. все перемещения ее (в пространстве или на плоскости), совмещающие эту фигуру с нею самой.

В качестве произведения $g_1 \cdot g_2$ двух самосовмещений g_1 и g_2 определим перемещение, возникающее в результате последовательного совершения сначала перемещения g_2 , а потом перемещения g_1 . Очевидно, что перемещение $g_1 \cdot g_2$ также является совмещением фигуры F с собой, в предположении, что перемещения g_1 и g_2 порознь являются таковыми.

Совокупность всех самосовмещений фигуры F с только что определенной операцией произведения образует *группу*. В самом деле, умножение перемещений удовлетворяет условию ассоциативности; далее, в совокупности самосовмещений имеется *единичное*, или *тождественное*, самосовмещение (именно, «покой», т. е. перемещение, оставляющее каждую точку фигуры на месте). Наконец, к каждому самосовмещению g имеется обратное ему самосовмещение g^{-1} (передвигающее каждую точку назад, в исходное положение, из положения, которое оно заняло после перемещения g).

§ 2. ГРУППЫ САМОСОВМЕЩЕНИЙ ПРЯМОЙ И ОКРУЖНОСТИ

Группы самосовмещений правильных многоугольников — *конечны*. В этой же главе мы познакомимся и с другими конечными группами самосовмещений, а именно, с группами самосовмещений некоторых

многогранников. А сейчас дадим несколько примеров бесконечных групп самосовмещений.

Первый пример — группа всех самосовмещений прямой в какой-либо проходящей через нее плоскости. Эта группа состоит: из *скольжений* прямой по себе (самосовмещения *первого рода*) и из поворотов прямой в выбранной плоскости на угол 180° вокруг любой из ее точек (самосовмещения *второго рода*).

Группа самосовмещений прямой некоммутативна.

Чтобы убедиться в этом, достаточно перемножить два самосовмещения, из которых одно первого, а другое — второго рода: результат этого перемножения изменится при изменении порядка сомножителей ¹⁾. Очевидно, *все самосовмещения второго рода можно получить, перемножая* (т. е. последовательно осуществляя) *всевозможные скольжения прямой с одним каким-нибудь поворотом на 180°* (т. е. поворотом на 180° вокруг одной определенной, но произвольно выбранной точки этой прямой).

Скольжения прямой по самой себе составляют подгруппу всех ее самосовмещений. Эти скольжения суть единственные перемещения прямой самой по себе. Каждому скольжению прямой самой по себе взаимно однозначным образом соответствует некоторое действительное число, указывающее, на какую длину и в каком из двух возможных направлений мы сдвинули прямую по ней самой. Отсюда легко заключить, что *группа всех скольжений прямой по самой себе изоморфна группе действительных чисел* (с операцией обыкновенного арифметического сложения в качестве групповой операции).

В качестве второго примера рассмотрим группу всех самосовмещений окружности в ее плоскости. Эта группа состоит из всевозможных поворотов окружности в ее плоскости вокруг ее центра, причем, как всегда, повороты на углы, кратные 2π , считаются тождественными. Каждому элементу нашей группы соответствует, таким образом, определенный угол φ . Измеряя этот угол в отвлеченной (радианной) мере, мы получим

¹⁾ Читателю рекомендуется фактически убедиться в этом, взяв два каких-нибудь определенных самосовмещения первого и второго рода и построив их произведение для одного и другого порядка сомножителей.

действительное число x . Но, так как углы, отличающиеся на целочисленные кратные 2π , определяют один и тот же поворот окружности, то каждому элементу группы поворотов окружности соответствует не только данное число x , но и все числа вида $x + 2\pi \cdot k$, где k — любое целое число.

С другой стороны, каждому действительному числу x соответствует единственный вполне определенный поворот окружности, а именно: поворот на угол, отвлеченная мера которого равна x . Таким образом, между поворотами окружности и действительными числами установлено следующее соответствие: *каждому действительному числу x соответствует один-единственный вполне определенный поворот, а именно поворот на угол x . Но при этом каждый поворот оказывается поставленным в соответствие не одному, а бесконечному множеству действительных чисел, которые все отличаются друг от друга на целочисленные кратные 2π .*

Группа поворотов окружности обозначается **SO (2)**.

Все только что рассмотренные группы, а именно: группы самосовмещений прямой и окружности, имеют следующие особенности: все эти группы состоят из перемещений соответствующей фигуры в себе. Другими словами, в течение каждого перемещения вся фигура — окружность, прямая — остается совмещенной с самой собой. Это свойство не имеет места при самосовмещениях правильных многоугольников: при этих последних конечное положение перемещающейся фигуры совмещено с начальным, но промежуточные положения, которые фигура занимает в процессе перемещения, отличаются от ее начального и конечного положений. Таково же положение вещей и при перемещениях многогранников, к которым мы сейчас переходим.

§ 3. ГРУППЫ ПОВОРОТОВ ПРАВИЛЬНОЙ ПИРАМИДЫ И ДВОЙНОЙ ПИРАМИДЫ

1. Пирамида. Группа поворотов правильной (рис. 3) n -угольной пирамиды (вокруг ее оси), очевидно изоморфна группе поворотов правильного n -угольника, лежащего в ее основании; эта группа есть, таким образом, циклическая группа порядка n . Легко убедиться, что поворотами пирамиды вокруг оси

(на углы $0, \frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}$) исчерпываются все перемещения, совмещающие пирамиду с самой собой.

2. Двойная пирамида (диэдр). Определим теперь группу самосовмещений тела, известного под названием «двойной правильной n -угольной пирамиды» или *n -угольного диэдра* (рис. 4).

Это тело состоит из правильной n -угольной пирамиды

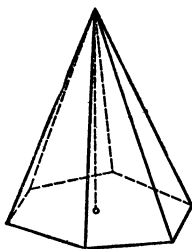


Рис. 3.

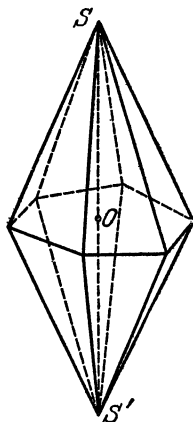


Рис. 4.

и ее зеркального отражения в плоскости основания. Мы сейчас докажем, что группа самосовмещений диэдра состоит из следующих элементов:

1) поворотов вокруг оси пирамиды (на углы $0, \frac{2\pi}{n}, \dots, (n-1)\frac{2\pi}{n}$);

2) так называемых опрокидываний, т. е. поворотов на угол π вокруг каждой из осей симметрии «основания диэдра», т. е. правильного многоугольника, являющегося общим основанием обеих пирамид, составляющих диэдр. Таких осей симметрии имеется, как мы видели, n , так что перемещений второго рода имеется тоже n .

Число всех полученных перемещений есть, таким образом, $2n$. Чтобы убедиться в том, что (за исключением случая $n=4$) не имеется никаких других перемещений, переводящих n -угольный диэдр в самого себя, заметим прежде всего, что в случае $n \neq 4$ всякое совмещение диэдра с самим собой должно либо оставлять на месте точки S и S' (самосовмещения первого рода), либо менять их местами (самосовмещения второго рода). Далее, основание диэдра должно переходить при таком

перемещении в самого себя. Заметим, наконец, что произведение (т. е. последовательное осуществление) двух самосовмещений первого рода дает самосовмещение первого рода, произведение самосовмещений первого рода с самосовмещениями второго рода дает самосовмещение второго рода, а произведение двух самосовмещений второго рода дает самосовмещение первого рода.

При этом произведение двух самосовмещений, из которых одно — первого, а другое — второго рода, зависит от порядка сомножителей: если a — самосовмещение первого, а b — самосовмещение второго рода, то $ab = ba^{-1}$.

Рассмотрим сначала самосовмещения первого рода. При таких самосовмещениях основание переходит в само себя, оставаясь в своей плоскости; оно испытывает, таким образом, поворот на один из углов:

$$0, \frac{2\pi}{n}, \dots, (n-1) \frac{2\pi}{n}.$$

Таким образом, и все перемещение диэдра оказывается поворотом вокруг оси диэдра на тот же угол.

Итак, самосовмещений первого рода имеется (включая тождественное самосовмещение, т. е. покой) ровно n . Эти самосовмещения суть не что иное, как повороты диэдра вокруг его оси на углы

$$0, \frac{2\pi}{n}, \dots, (n-1) \frac{2\pi}{n}.$$

Пусть дано некоторое вполне определенное самосовмещение второго рода, т. е. такое самосовмещение диэдра с самим собой, при котором вершины S и S' меняются местами.

Произведем после данного самосовмещения второго рода некоторое вполне определенное опрокидывание диэдра, т. е. перемещение, заключающееся в повороте диэдра на угол π вокруг *одной какой-нибудь, раз навсегда выбранной, оси симметрии основания*. Получим самосовмещение первого рода¹⁾, т. е. поворот диэдра вокруг его оси.

¹⁾ В самом деле, этот поворот есть самосовмещение второго рода, а произведение двух самосовмещений второго рода есть самосовмещение первого рода.

Итак, всякое самосовмещение второго рода переходит после одного и того же опрокидывания в некоторое самосовмещение первого рода. Отсюда следует легко: всякое самосовмещение второго рода можно получить, производя (до или после некоторого самосовмещения первого рода) одно и то же опрокидывание. Отсюда, далее следует, что число самосовмещений второго рода равно числу самосовмещений первого рода, т. е. n .

С другой стороны, ясно, что все опрокидывания являются самосовмещениями второго рода. Так как этих опрокидываний имеется ровно n , то ими, очевидно, и исчерпывается вся совокупность самосовмещений второго рода.

Итак, мы доказали следующее: *группа самосовмещений n -угольного диэдра есть некоммутативная группа порядка $2n$, состоящая из n поворотов вокруг оси диэдра SS' и из n опрокидываний, т. е. поворотов на угол π вокруг осей симметрии основания диэдра. Все n опрокидываний получаются умножением одного из них на n поворотов диэдра вокруг его оси SS' .*

Так как все повороты диэдра вокруг его оси получаются умножением с самим собой одного поворота — именно, поворота на угол $\frac{2\pi}{n}$, то группа всех самосовмещений имеет систему образующих из двух элементов: поворота на угол $\frac{2\pi}{n}$ и одного какого-нибудь опрокидывания.

Случай $n = 4$ является особым потому, что частным случаем четырехугольного диэдра является октаэдр, допускающий не 8, а как мы увидим ниже, 24 самосовмещения. Это объясняется тем, что при самосовмещении некоторых четырехугольных диэдров, а именно правильных октаэдров, вершина S может совмещаться не только с вершиной S' , но и с каждой из вершин основания. Одно из необходимых для этого условий — одинаковое число граней (а также и ребер), примыкающих к каждой вершине, выполнено, очевидно, в случае любого четырехугольного диэдра. В случае правильного октаэдра и все углы, телесные и плоские, при любых двух вершинах оказываются соответственно равными так же, как и сами грани и ребра.

3. Случай вырождения: группы поворотов отрезка и ромба. Наименьшее число вершин, которое может

иметь многоугольник, есть 3; в известном смысле, однако, отрезок может рассматриваться как случай «вырождения» многоугольника, или, если угодно, как «многоугольник с двумя вершинами».

Возможность такой точки зрения, в частности, подтверждается тем, что группа самосовмещений отрезка в какой-нибудь плоскости, содержащей его, есть циклическая группа, и притом порядка 2: она, очевидно, состоит из тождественного самосовмещения и из поворота отрезка на угол 180° .

Подобно этому равнобедренный треугольник будет случаем вырождения правильной пирамиды: группа самосовмещений равнобедренного треугольника в пространстве также есть группа порядка 2.

Далее, вырождением диэдра или двойной пирамиды будет, очевидно, ромб. Группа самосовмещений или поворотов ромба (в пространстве) состоит из четырех элементов: из тождественного преобразования a_0 , из поворотов a_1 и a_2 вокруг каждой из диагоналей ромба на 180° и из поворота a_3 ромба в его плоскости вокруг его центра на 180° (этот поворот есть произведение двух предыдущих)¹⁾. Таблица умножения для нашей группы имеет вид:

	a_0	a_1	a_2	a_3
a_0	a_0	a_1	a_2	a_3
a_1	a_1	a_0	a_3	a_2
a_2	a_2	a_3	a_0	a_1
a_3	a_3	a_2	a_1	a_0

Она совпадает с таблицей умножения клейновской группы порядка 4, приведенной нами в качестве второго

¹⁾ Рассматривая одну из диагоналей ромба как «основание», другую — как ось диэдра, мы получим эти четыре перемещения из поворотов вокруг «оси» (на угол π) и «опрокидывания» относительно основания.

примера в гл. I, § 2, п. 4. В этом легко убедиться непосредственно, а еще проще — рассматривая вместо группы самих поворотов ромба изоморфную ей группу подстановок его четырех вершин A, B, C, D : очевидно, поворотам a_0, a_1, a_2, a_3 соответствуют следующие подстановки вершин¹⁾:

$$\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ B & A & C & D \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ A & B & D & C \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}.$$

§ 4. ГРУППА ПОВОРОТОВ ПРАВИЛЬНОГО ТЕТРАЭДРА²⁾

Для определения всех самосовмещений тетраэдра $A_0A_1A_2A_3$ (рис. 5) рассмотрим сначала те из них, которые одну определенную вершину, пусть на-

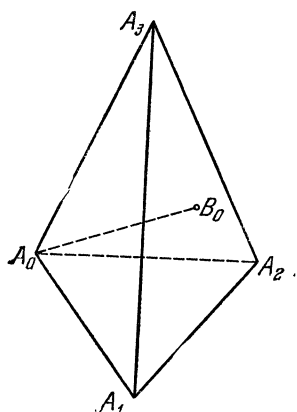


Рис. 5.

пример A_0 , оставляют неподвижной. Такие самосовмещения совмещают и треугольник $A_1A_2A_3$ с самим собою, поворачивая его вокруг его центра B_0 на один из углов $0, \frac{2\pi}{3}, \frac{4\pi}{3}$. Отсюда следует, что самосовмещений тетраэдра $A_0A_1A_2A_3$, оставляющих вершину A_0 на месте, имеется ровно три: тождественное самосовмещение a_0 , оставляющее на месте все элементы тетраэдра, и два поворота a_1 и a_2 вокруг оси A_0B_0 соответственно на углы $\frac{2\pi}{3}$

и $\frac{4\pi}{3}$. Обозначим теперь через x_i какое-нибудь определенное самосовмещение тетраэдра, переводящее верши-

¹⁾ Мы принимаем за a_1 поворот вокруг диагонали CD , за a_2 — поворот вокруг диагонали AB .

²⁾ Под тетраэдром здесь и везде дальше понимаем *правильный* тетраэдр.

ну A_0 в вершину $A_i, i=1, 2, 3$ ¹⁾; через x_0 обозначим снова тождественное самосовмещение.

Докажем, что всякое самосовмещение b тетраэдра может быть записано в виде

$$b = a_i \cdot x_k, \quad (1)$$

где $i=0, 1, 2$ и $k=0, 1, 2, 3$ являются однозначно определенными (последнее утверждение означает, что если $b = a_i \cdot x_k, b' = a_{i'} \cdot x_{k'}$ и по крайней мере одно из неравенств $i \neq i', k \neq k'$ имеет место, то непременно $b \neq b'$).

Итак, пусть дано какое-нибудь самосовмещение b ; оно переводит вершину A_0 в некоторую определенную вершину A_k , где $k=0, 1, 2, 3$; но тогда самосовмещение $b x_k^{-1}$ оставляет вершину A_0 на месте и есть следовательно, некоторое вполне определенное a_i , так что $b x_k^{-1} = a_i$ и $b = a_i x_k$, где i и k определены однозначно. Так как и обратной каждой паре (i, k) соответствует по записи (1) некоторое самосовмещение тетраэдра, то имеется взаимно однозначное соответствие между всеми самосовмещениями тетраэдра и всеми парами (i, k) , где i принимает значения 0, 1, 2, а k — значения 0, 1, 2, 3. Отсюда следует, что имеется ровно 12 самосовмещений тетраэдра.

Каждое самосовмещение тетраэдра означает некоторую подстановку его вершин, т. е. некоторую подстановку их номеров 0, 1, 2, 3. Но всех подстановок из четырех элементов имеется 24; из них, как мы сейчас видели, только 12 осуществляются перемещениями тетраэдра в пространстве. Посмотрим, какие это перемещения и какие подстановки.

Назовем для краткости *граневой медианой* тетраэдра прямую, проходящую через какую-нибудь вершину A_i тетраэдра и через центр B_i грани, противоположной этой вершине. *Реберной медианой* назовем прямую, проходящую через середины двух каких-нибудь взаимно противоположных ребер тетраэдра.

Каждой граневой медиане соответствует два нетождественных самосовмещения тетраэдра, именно: пово-

¹⁾ Вершина A_0 переводится в A_1 и A_3 , например, посредством поворотов вокруг оси $A_2 B_2$ (соединяющей вершину A_2 с центром противоположной грани); A_0 переводится в A_2 , например, посредством поворота вокруг оси $A_3 B_3$.

роты вокруг этой медианы на углы $\frac{2\pi}{3}$ и $\frac{4\pi}{3}$. Всего, таким образом, получаем восемь поворотов, которые в виде подстановок номеров записываются так:

$$\begin{aligned} a_1 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 1 & 2 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 1 & 3 & 0 \end{pmatrix}, \\ a_4 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 1 & 0 & 2 \end{pmatrix}, \quad a_5 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 3 & 2 & 0 \end{pmatrix}, \quad a_6 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 2 & 1 \end{pmatrix}, \quad (2) \\ a_7 &= \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 3 \end{pmatrix}, \quad a_8 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \end{pmatrix}. \end{aligned}$$

Вокруг каждой реберной медианы имеем один нетождественный поворот на угол π , что дает нам (так как реберных медиан имеется три) еще три поворота, записываемых в виде подстановок:

$$a_9 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}, \quad a_{10} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}, \quad a_{11} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \end{pmatrix}. \quad (3)$$

Эти 11 поворотов вместе с тождественным самосовмещением («тождественным поворотом») a_0 и дают нам все 12 самосовмещений тетраэдра. Каждое из них является поворотом вокруг одной из семи осей симметрии¹⁾ тетраэдра; поэтому группу самосовмещений и называют группой поворотов тетраэдра.

Легко проверить, что все подстановки (2) и (3) — четные; так как всех четных подстановок из четырех элементов (вершин тетраэдра) имеется 12, то перед нами взаимно однозначное и, очевидно, изоморфное соответствие между группой поворотов тетраэдра и знакопеременной группой подстановок из четырех элементов.

Посмотрим теперь, каковы подгруппы группы поворотов тетраэдра.

В ней, как и во всякой группе, имеются прежде всего две так называемые несобственные подгруппы: это, во-первых, вся рассматриваемая группа и, во-вто-

¹⁾ Эти семь осей симметрии суть четыре граневые и три реберные медианы тетраэдра. В широком смысле слова осью симметрии геометрической фигуры называется всякая прямая, вокруг которой фигуру можно повернуть на отличный от нуля угол таким образом, что она совместится сама с собой. Заметим в связи с этим, что всякое перемещение твердого тела в пространстве, оставляющее неподвижной какую-либо точку O этого тела, является поворотом этого тела вокруг некоторой оси, проходящей через точку O .

рых, подгруппа, состоящая из одного нейтрального элемента. Нас интересуют остальные, так называемые *собственные*¹⁾ подгруппы поворотов тетраэдра. Их имеется восемь. Прежде всего заметим, что произведение поворотов на угол π вокруг двух различных реберных медиан дает нам поворот на тот же угол π вокруг третьей реберной медианы (в этом можно убедиться как геометрически, так и непосредственным умножением двух каких-нибудь из подстановок (3)). Отсюда следует, что повороты на угол π вокруг всех трех реберных медиан образуют вместе с тождественным поворотом группу, очевидно, четвертого порядка; она изоморфна клейновской группе (т. е. группе всех поворотов ромба). Эту группу обозначим через H . Среди всех подгрупп группы поворотов тетраэдра она имеет наибольший порядок. В ней содержатся три подгруппы второго порядка, состоящие из поворотов на углы 0 и π вокруг каждой данной реберной медианы. Эти подгруппы обозначим через H_{01} , H_{02} , H_{03} . Кроме указанных групп имеются еще четыре подгруппы третьего порядка, именно: H_i , $i = 0, 1, 2, 3$, состоящие каждая из трех поворотов на углы 0 , $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ вокруг соответствующей граневой медианы.

Для того чтобы доказать, что никаких других подгрупп в группе поворотов тетраэдра нет, достаточно показать, что любые два отличных от нуля элемента, взятые из двух различных групп H_i или взятые один из какой-либо группы H_i , а другой из какой-либо группы H_{0k} , уже дают систему образующих всей группы поворотов тетраэдра. Для этого в свою очередь достаточно рассмотреть любые два элемента из числа элементов a_1, a_3, a_5, a_7 , например, a_1 и a_3 , а также какой-нибудь из элементов a_2, a_4, a_6, a_8 и какой-нибудь из элементов a_9, a_{10}, a_{11} . Читателю рекомендуется провести доказательство геометрически, а именно: показать, что каждый поворот тетраэдра может быть получен умножением любой упомянутой пары поворотов. Можно достигнуть того же результата и непосредственно вычислениями. Следующие тождества доказывают, например, что элементы a_1 и a_3 составляют систему обра-

1) Подгруппа H группы G называется *собственной*, если она содержит по крайней мере два элемента и $H \neq G$.

зующих группы поворотов тетраэдра:

$$\begin{aligned} a_0 &= a_1 a_1^{-1}, & a_7 &= a_1 a_3 a_1^{-1}, \\ a_2 &= a_1^3, & a_8 &= a_1^3 a_3, \\ a_4 &= a_3^3, & a_9 &= a_3^{-1} a_1 a_3^2, \\ a_5 &= a_3^{-1} a_1 a_3, & a_{10} &= a_1^{-1} a_3, \\ a_6 &= a_3^{-1} a_1^3 a_3, & a_{11} &= a_3 a_1. \end{aligned}$$

Не следует думать, что каждый элемент единственным образом выражается через образующие; например, $a_7 = a_1 a_3 a_1^{-1}$ и в то же время $a_7 = a_3^{-1} a_1^{-1} a_3 a_1 a_3$.

Группа поворотов тетраэдра некоммукативна. Например,

$$a_1 a_3 = a_{10}, \quad a_3 a_1 = a_{11}.$$

У п р а ж н е н и е. Читателю рекомендуется доказать следующую общую теорему: *некоторое множество E элементов группы G тогда и только тогда является системой образующих этой группы, когда не существует никакой собственной подгруппы группы G , которая содержала бы все элементы множества E .*

Пользуясь этой теоремой, найти все системы образующих группы поворотов тетраэдра (состоящие не более чем из трех элементов каждая).

Уже из этого примера будет видно, как много различных систем образующих может иметь конечная группа.

§ 5. ГРУППЫ ПОВОРОТОВ КУБА И ОКТАЭДРА ¹⁾

1. Для того чтобы установить все самосовмещения куба, поступим так же, как и в случае тетраэдра: рассмотрим сначала лишь те самосовмещения куба $ABCD A' B' C' D'$ (рис. 6), которые одну из вершин, — пусть A , — совмещают с самой собой.

При каждом самосовмещении куба вершина переходит в вершину, ребро в ребро, грань в грань; также и диагонали куба переходят в самих себя. Если данное самосовмещение оставляет вершину A неподвижной, то оно оставляет неподвижной и диагональ AC' (так как существует лишь одна диагональ куба,

¹⁾ Так же как и в случае тетраэдра, мы везде под октаэдром разумеем *правильный октаэдр*.

выходящая из вершины A). Итак, наше самосовмещение есть поворот куба вокруг диагонали AC' . Таких поворотов, кроме тождественного, имеется два: на угол $\frac{2\pi}{3}$ и на угол $\frac{4\pi}{3}$.

Итак, имеется всего три самосовмещения куба, переводящих вершину A в саму себя. Но вершину A надлежаще подобранным поворотом можно перевести в каждую из восьми вершин куба; отсюда, повторяя те же рассуждения, что и в случае тетраэдра, легко выводим, что всех самосовмещений куба имеется $3 \cdot 8 = 24$.

Постараемся определить каждое из этих самосовмещений. Заметим прежде всего, что у куба имеются следующие 13 осей симметрии: четыре диагонали, три прямые, соединяющие попарно середины граней куба, шесть прямых, соединяющих попарно середины противоположных ребер куба. Вокруг каждой из четырех диагоналей имеется два нетождественных поворота куба, совмещающих куб с самим собой, всего имеем восемь поворотов вокруг диагоналей.

Вокруг каждой из прямых, соединяющих центры противоположных граней куба, имеется три нетождественных поворота. Следовательно, всего таких поворотов 9.

Наконец, имеем один нетождественный поворот (на угол π) вокруг прямой, соединяющей середины двух противоположных ребер; общее число этих поворотов равно, следовательно, шести.

Итак, имеем $8 + 9 + 6 = 23$ нетождественных поворота, совмещающих куб с самим собой. Если присоединить к ним еще тождественный поворот, получим 24 самосовмещения, т. е. все самосовмещения куба, какие только имеются.

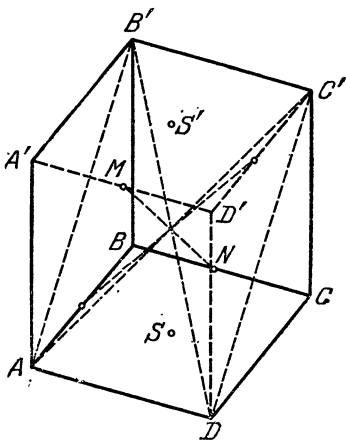


Рис. 6.

Итак,
поворотами куба вокруг его осей симметрии исчерпываются все его самосовмещения.

Поэтому, так же как и в случае тетраэдра, группа самосовмещений куба обычно называется **группой поворотов куба**.

Прежде чем идти дальше в изучении строения группы поворотов куба, докажем следующую лемму:

Лемма. Единственный поворот куба, переводящий каждую из его четырех диагоналей в самое себя, есть тождественный поворот ¹⁾.

В самом деле, заметим сначала, что всякий поворот, переводящий в себя какие-нибудь две диагонали куба, положим, AC' и DB' , — переводит в себя и диагональную плоскость $ADC'B'$ (см. рис. 6). Всякий нетождественный поворот, переводящий в себя некоторую плоскость, имеет своей осью либо прямую, лежащую в данной плоскости, — в этом случае угол поворота равен π , либо прямую, перпендикулярную к этой плоскости. Но поворот плоскости на угол π вокруг оси, лежащей в этой плоскости, переводит в самих себя, кроме оси поворота, лишь прямые, перпендикулярные к этой оси. Так как прямоугольник $ADC'B'$ не есть квадрат, то диагонали его, не будучи взаимно перпендикулярными, не могут переходить каждая в себя саму при повороте вокруг какой бы то ни было оси, лежащей в плоскости прямоугольника. Итак, AC' и DB' могут переходить в самих себя лишь при поворотах куба вокруг оси, перпендикулярной к плоскости $ADC'B'$. Такой осью является прямая MN , соединяющая середины сторон $A'D'$ и BC . Единственный нетождественный поворот куба вокруг прямой MN есть поворот на угол π . Значит, только при этом повороте каждая из диагоналей AC' и DB' переходит в саму себя. Но при этом повороте две другие диагонали BD' и CA' меняются местами, так что нетождественного поворота, переводящего в самих себя все четыре диагонали куба, вовсе нет.

¹⁾ Не следует упускать из виду следующее обстоятельство: если при данном повороте куба данная диагональ, положим AC' , переходит в самое себя, то это не значит, что вершины, определяющие эту диагональ (в нашем случае вершины A и C'), непременно остаются неподвижными: они могут поменяться местами (т. е. A может перейти в C' , а C' в A).

Таким образом, при каждом нетождественном повороте куба четыре его диагонали испытывают нетождественную подстановку. Отсюда следует: при двух различных поворотах a и b диагонали испытывают различные подстановки, так как если бы при поворотах a и b происходила та же самая подстановка диагоналей, то при повороте ab^{-1} все диагонали оставались бы на месте, и значит, ab^{-1} было бы тождественным поворотом, а потому повороты a и b совпадали бы между собой.

Итак, всем 24 различным поворотам куба соответствуют различные подстановки четырех диагоналей, производимые этими поворотами. Но всех различных подстановок из четырех элементов имеется, как известно, $1 \cdot 2 \cdot 3 \cdot 4 = 24$.

Отсюда следует: между группой всех поворотов куба и группой всех подстановок его четырех диагоналей имеется взаимно однозначное соответствие. Так как при установленном нами соответствии произведению поворотов соответствует, очевидно, произведение подстановок ¹⁾, то имеем следующую теорему:

Группа поворотов куба изоморфна группе всех подстановок из четырех элементов.

Среди подгрупп поворотов куба отметим прежде всего циклические подгруппы второго, третьего и четвертого порядков, состоящие соответственно из поворотов вокруг каждой из 13 осей симметрии куба. Циклических подгрупп второго порядка шесть (по числу осей, соединяющих середины двух противоположных ребер), циклических подгрупп третьего порядка четыре (по числу диагоналей), циклических подгрупп четвертого порядка имеется три (по числу соединяющих центры противоположных граней).

Значительно больший интерес представляют следующие перечисленные ниже подгруппы.

а) Подгруппа двенадцатого порядка, состоящая из поворотов переводящих в себя (одновременно) каждый

¹⁾ Ведь произведение двух поворотов состоит в последовательном осуществлении этих поворотов, произведение подстановок — в последовательном осуществлении этих подстановок, тогда как взаимно однозначное соответствие между поворотом и подстановкой диагоналей заключается в соответствии данного поворота с фактически производимой им подстановкой диагоналей.

из двух тетраэдров $ACB'D'$ и $BDA'C'$ (рис. 7), вписанных в куб. Эта подгруппа состоит из $2 \cdot 4 = 8$ нетождественных поворотов вокруг диагоналей куба, из трех поворотов, каждый на угол π , вокруг осей, соединяющих центры противоположных граней, и из тождественного поворота.

б) Три подгруппы восьмого порядка, изоморфные группе четырехугольной двойной пирамиды (диэдра). Каждая из этих подгрупп состоит из тех поворотов

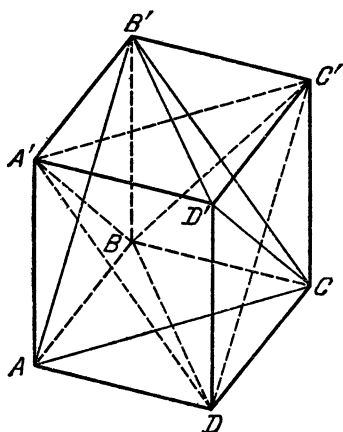


Рис. 7.

куба, которые переводят в самое себя одну из прямых, соединяющих центры двух противоположных граней, например, точки S и S' (октаэдр, вписанный в куб, является частным случаем четырехугольного диэдра; группа его поворотов, оставляющих неподвижными или меняющими местами две вершины его S и S' , и будет, очевидно, группой четырехугольного диэдра).

Эта подгруппа восьмого порядка получается из следующих восьми поворотов: четырех поворотов вокруг оси SS' (включая тождественный); двух поворотов на угол π вокруг осей, соединяющих соответственно середины ребер AA' и CC' , BB' и DD' ; двух поворотов на угол π вокруг осей, соединяющих соответственно центры граней $ABB'A'$ и $CDD'C'$, $ADD'A'$ и $BCC'B'$.

в) Подгруппа четвертого порядка, состоящая из тождественного преобразования и трех поворотов на угол π вокруг каждой из осей, соединяющих центры двух противоположных граней. Эта группа состоит из тех поворотов, которые входят в каждую из перечисленных в п. б) трех подгрупп восьмого порядка. Эта подгруппа четвертого порядка коммутативна и изоморфна группе поворотов ромба (т. е. клейновской группе порядка 4).

Кроме упомянутых, имеются еще подгруппы четвертого порядка, также изоморфные группе самосовмещений ромба.

2. *Группа самосовмещений или поворотов правильного октаэдра изоморфна группе поворотов куба.*

Чтобы убедиться в этом, достаточно описать куб вокруг правильного октаэдра (рис. 8) или вписать куб в правильный октаэдр (рис. 9). Каждое самосовмещение

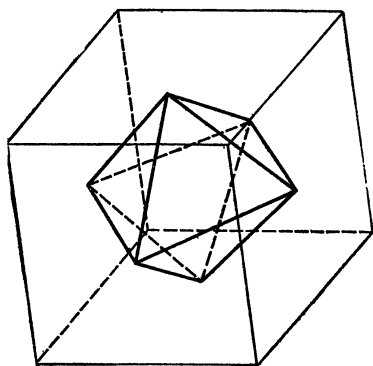


Рис. 8.

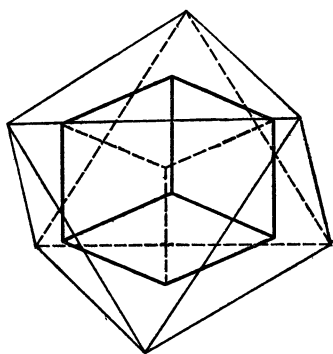


Рис. 9.

октаэдра соответствует некоторому самосовмещению куба, и наоборот.

Это положение вещей есть одно из проявлений отношения *двойственности*, имеющего место между кубом и октаэдром; его мы сейчас определим.

Прежде всего мы назовем два элемента (вершина, ребро, грань) какого-нибудь многогранника **инцидентными**, если один из этих двух элементов принадлежит другому (как его элемент). Таким образом, вершина и грань, имеющая эту вершину среди своих вершин, а также грань и ребро этой грани, наконец вершина и ребро, одним из концов которого является эта вершина — суть пары инцидентных элементов.

Два многогранника называются **двойственными**, если элементы одного могут быть таким образом поставлены во взаимно однозначное соответствие с элементами другого, что при этом пары инцидентных элементов одного многогранника соответствуют парам инцидентных элементов другого, и при этом:

вершины первого многогранника соответствуют граням второго, ребра первого многогранника соответствуют ребрам второго, грани первого многогранника соответствуют вершинам второго.

Нетрудно видеть, что куб и октаэдр в этом смысле двойственны друг другу, а тетраэдр двойствен самому себе.

§ 6. ГРУППА ПОВОРОТОВ ИКОСАЭДРА И ДОДЕКАЭДРА ¹⁾. ОБЩЕЕ ЗАМЕЧАНИЕ О ГРУППАХ ПОВОРОТОВ ПРАВИЛЬНЫХ МНОГОГРАННИКОВ

1. Среди всех пяти правильных многогранников нам осталось рассмотреть два: икосаэдр и додекаэдр (рис. 10, 11). Эти многогранники двойственны между собой и группы их самосовмещений изоморфны.

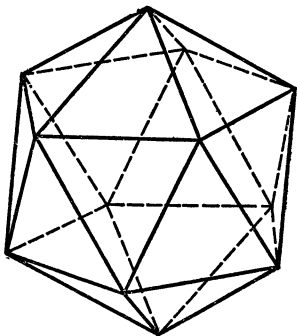


Рис. 10.

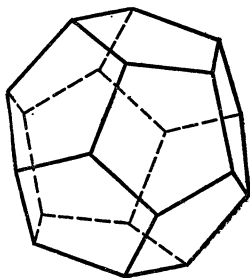


Рис. 11.

Для того чтобы убедиться в этом, достаточно вписать икосаэдр в додекаэдр (рис. 12) или додекаэдр в икосаэдр (рис. 13). Поэтому нам достаточно ознакомиться с группой самосовмещений икосаэдра. Чтобы определить число ее элементов, мы поступим так же, как и в случае тетраэдра и куба. Именно, мы сначала рассмотрим те самосовмещения икосаэдра, которые оставляют неподвижной одну какую-нибудь из его вершин. Таких самосовмещений имеется пять, а именно: пять поворотов вокруг оси, соединяющей данную

¹⁾ Имеем опять в виду правильный икосаэдр и правильный додекаэдр.

вершину с противоположной ей. Так как всех вершин 12, то число самосовмещений икосаэдра есть $5 \cdot 12 = 60$.

Все эти самосовмещения оказываются поворотами икосаэдра вокруг его осей симметрии. В самом деле, имеются следующие оси симметрии икосаэдра:

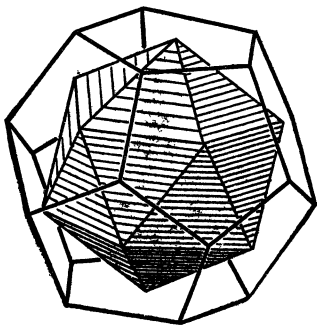


Рис. 12.

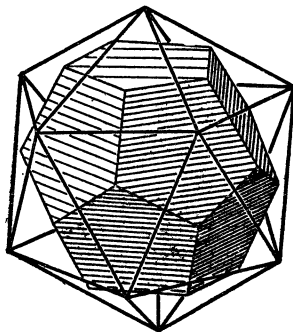


Рис. 13.

Шесть осей, соединяющих противоположные вершины: вокруг каждой из них имеем четыре нетождественных поворота (на углы $\frac{2\pi}{5}$, $\frac{4\pi}{5}$, $\frac{6\pi}{5}$, $\frac{8\pi}{5}$), совмещающих икосаэдр с самим собой; всего, значит, получаем $4 \cdot 6 = 24$ поворота;

10 осей, соединяющих центры противоположных граней; вокруг каждой из этих осей имеем два нетождественных поворота (на угол $\frac{2\pi}{3}$ и $\frac{4\pi}{3}$), а всего 20 поворотов;

15 осей, соединяющих середины противоположных ребер и дающих каждая по одному нетождественному повороту (на 180°);

итак, имеем $24 + 20 + 15$ нетождественных поворота и один тождественный поворот — всего 60 поворотов.

Как всегда, из этого рассуждения следует, что икосаэдр имеет 31 ось симметрии.

Ввиду достаточной сложности группы поворотов икосаэдра мы не будем здесь далее останавливаться на ее изучении. Заметим только, что эта группа изоморфна знакопеременной группе подстановок из пяти элементов.

2. Мы определяли группы поворотов многоугольников и многогранников как группы самосовмещений.

Рассмотрим как бы два экземпляра пространства, вложенных один в другой. Одно пространство представляем себе в виде бесконечно распространяющегося во все стороны твердого тела и назовем его *твердым пространством*. Другое пространство представляем себе в виде *пустого пространства*.

Твердое пространство помещаем в пустое, в котором оно может перемещаться. Наш многогранник представляем как часть твердого пространства, неподвижную в нем и способную перемещаться лишь вместе с ним. При такой точке зрения можно рассматривать повороты всего «*твердого*» пространства в «*пустом*» пространстве (вокруг тех или иных осей), которые совмещают данный многогранник с самим собой, т. е. производят самосовмещения его. Так как каждое самосовмещение рассмотренных нами многогранников оказывалось поворотом вокруг той или иной оси и каждый поворот многогранника вокруг оси можно представлять себе как порожденный поворотом всего пространства вокруг той же оси, то группа самосовмещений данного многогранника изоморфна группе поворотов пространства, совмещающих этот многогранник с самим собой. Эту последнюю группу обычно и имеют в виду, когда говорят о группе поворотов данного правильного многогранника. Часто ее даже называют просто «группой правильного многогранника».

Группы правильных пирамид (т. е. конечные циклические группы), группы диэдров и только что рассмотренные группы правильных многогранников суть единственные *конечные* подгруппы группы *всех перемещений* пространства.

ИНВАРИАНТНЫЕ ПОДГРУППЫ

§ 1. СОПРЯЖЕННЫЕ ЭЛЕМЕНТЫ И ПОДГРУППЫ

1. Трансформация одного элемента группы при помощи другого. Рассмотрим в группе G два каких-нибудь элемента a и b . Элемент

$$b^{-1}ab$$

называется **трансформацией** элемента a при помощи элемента b .

Посмотрим, при каких условиях имеет место равенство

$$b^{-1}ab = a. \quad (1)$$

Если равенство (1) выполнено, то умножая его части слева на b , получим

$$ab = ba. \quad (1')$$

Итак, если выполнено (1), то выполнено и (1'), т. е. элементы a и b переместительны. Обратно, если выполнено (1'), то умножая обе его части на b^{-1} слева, получим

$$b^{-1}ab = b^{-1}ba = a,$$

т. е. имеет место и равенство (1). Итак, мы видим, что для того, чтобы при данных a и b имело место равенство (1), т. е. чтобы трансформация элемента a посредством элемента b равнялась самому элементу a , необходимо и достаточно, чтобы элементы a и b были переместительны (удовлетворяли равенству (1')).

В частности, в коммутативных группах равенство (1) имеет место для любых элементов a и b .

В качестве иллюстрации понятия трансформации рассмотрим группу G всех подстановок из n элементов; пусть

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ b_1 & b_2 & b_3 & \dots & b_n \end{pmatrix}.$$

Тогда очевидно,

$$\begin{aligned} b^{-1} &= \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}, \\ b^{-1}a &= \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, \\ b^{-1}ab &= \begin{pmatrix} b_1 & b_2 & b_3 & \dots & b_n \\ b_{a_1} & b_{a_2} & b_{a_3} & \dots & b_{a_n} \end{pmatrix}. \end{aligned} \quad (2)$$

Формула (2) может быть записана в виде следующего правила:

пусть

$$a = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \text{ и } b = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix};$$

чтобы получить трансформацию подстановки a при помощи подстановки b , нужно в обеих строчках обычной записи подстановки a сделать подстановку b .

Поясним это правило еще частными примерами. Пусть, например, $n=3$ и

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Получаем

$$b^{-1}ab = \begin{pmatrix} 3 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq a.$$

Гораздо проще понять только что выведенное правило, пользуясь термином отображение или функция.

Подстановка a означает функцию $y=f(x)$, $x=1, 2, \dots, n$, $y=1, 2, 3, \dots, n$, где двум различным значениям x всегда соответствуют два различных значения y , так что f есть взаимно однозначное отображение множества $\{1, 2, \dots, n\}$ на себя.

Подстановка b есть функция $y=\varphi(x)$ той же природы, что и $f(x)$. Подстановка $b^{-1}ab$ есть функция $y=F(x)$, определенная формулой

$$F(x) = \varphi \{f[\varphi^{-1}(x)]\}. \quad (3)$$

Она получается, если элементу $\varphi(x)$ поставить в соответствие элемент $\varphi[f(x)]$; это непосредственно видно,

если в формуле (3) поставить $\varphi(x)$ вместо x и заметить, что

$$\varphi^{-1}[\varphi(x)] = x.$$

Так как x пробегает все числа $1, 2, 3, \dots, n$, то и $\varphi(x)$ пробегает все те же числа, только в другом порядке, и формулой

$$F[\varphi(x)] = \varphi[f(x)] \quad (4)$$

функция $F(x)$, т. е. подстановка $b^{-1}ab$, вполне определена. Формула (4) представляет собой только другую запись формулы (2). Наконец, если обозначить $f(x)$ через y , полученный результат можно сформулировать еще и так:

подстановка F заключается в том, что элемент $\varphi(x)$ заменяется элементом $\varphi(y)$.

Так как всякая конечная группа изоморфна некоторой группе подстановок, то формула (2) выясняет содержание понятия «трансформация», по крайней мере для всех конечных групп.

2. Пример группы тетраэдра. Рассмотрим в виде дальнейшего примера группу поворотов тетраэдра $ABCD$ (рис. 14).

Пусть a есть поворот тетраэдра вокруг оси MN (соединяющей середины ребер BC и AD) на угол π , пусть b есть поворот вокруг оси DO , переводящий A в C , B в A , C в B ; тогда $b^{-1}ab$ есть поворот на угол π вокруг оси PQ , соединяющей середины ребер AB и CD . В этом можно убедиться как непосредственно, так и замечая, что поворот a производит подстановку вершин $\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$, тогда как b производит подстановку $\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix}$.

Производя в каждой строке выражения $\begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}$ подстановку $\begin{pmatrix} A & B & C & D \\ C & A & B & D \end{pmatrix}$, получим $\begin{pmatrix} C & A & B & D \\ D & B & A & C \end{pmatrix}$, т. е.

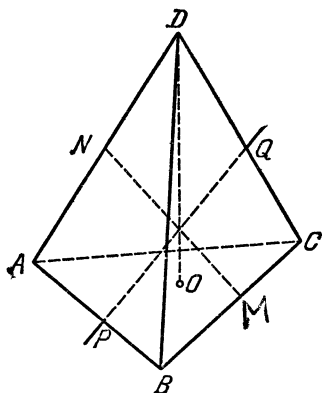


Рис. 14.

$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$, соответствующую повороту вокруг оси PQ на угол π .

Таким же точно образом убедимся, что

$$a^{-1}ba$$

есть поворот, переводящий B в C , C в D , D в B вокруг оси, соединяющей вершину A с центром грани BCD . Этому повороту соответствует подстановка $\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$.

3. Сопряженные элементы. Пусть G — какая-нибудь группа.

Лемма 1. *Если элемент b есть трансформация элемента a при помощи элемента c , то элемент a есть трансформация элемента b при помощи элемента c^{-1} .*

В самом деле, из соотношения

$$b = c^{-1}ac,$$

умножая обе части слева на c , а справа на c^{-1} , получаем

$$cbc^{-1} = a,$$

т. е.

$$a = (c^{-1})^{-1}bc^{-1},$$

что и требовалось доказать.

Определение. Два элемента группы называются **сопряженными элементами**, если один из них есть трансформация другого.

Лемма 2. *Если a сопряжен с b , b сопряжен с d , то a сопряжен с d .*

В самом деле, так как a сопряжен с b , то существует такой элемент c , что

$$b = c^{-1}ac. \quad (5)$$

Так как b сопряжен с d , то существует такой элемент e , что

$$b = e^{-1}de, \quad (5')$$

так что $c^{-1}ac = e^{-1}de$. Умножая обе части последнего равенства слева на c , а справа на c^{-1} , получим

$$a = (ce^{-1})d(ec^{-1}) = (ec^{-1})^{-1}d(ec^{-1}),$$

т. е. a есть трансформация элемента d при помощи элемента ec^{-1} , что и требовалось доказать.

Лемма 3. *Каждый элемент сопряжен самому себе.*

В самом деле, совершенно очевидно, что

$$a = 1^{-1}a \cdot 1.$$

Содержание лемм 1—3 заключается в том, что сопряженность двух элементов группы обладает свойствами симметрии, транзитивности и рефлексивности. Отсюда на основании теоремы 3 гл. I, § 1, п. 4 следует

Теорема 1. *Всякая группа G распадается на классы попарно сопряженных между собой элементов.*

При этом класс какого-нибудь элемента a группы G состоит из всех сопряженных с a элементов группы G , т. е. трансформаций элемента a при помощи всевозможных элементов группы G .

Заметим, что класс нейтрального элемента всякой группы G состоит из одного этого элемента (так как при любом a имеем $a^{-1} \cdot 1 \cdot a = 1$).

Задача. Требуется доказать, что группа поворотов тетраэдра распадается на следующие классы сопряженных элементов:

1) класс, состоящий из одного нейтрального элемента;

2) класс, состоящий из поворотов на угол $\frac{2}{3}\pi$ вокруг каждой из четырех осей, соединяющих вершину тетраэдра с центром противоположной грани;

3) класс, состоящий из четырех поворотов на угол $\frac{4}{3}\pi$ вокруг тех же осей (всюду по (или против) часовой стрелки, если смотреть из неподвижной вершины);

4) класс, состоящий из поворотов на угол π вокруг каждой из трех осей, соединяющих середины двух противоположных ребер тетраэдра.

Читателю рекомендуется также исследовать классы сопряженных элементов в других группах поворотов.

4. Трансформация подгруппы. Класс сопряженных элементов, к которому принадлежит данный элемент a группы G , состоит из трансформаций элемента a при помощи всевозможных элементов b группы G . Теперь возьмем какую-нибудь подгруппу H группы G и будем рассматривать трансформации всевозможных элементов x этой подгруппы при помощи одного и того же произвольно выбранного элемента b группы G . Полученное множество элементов, т. е. совокупность всех элементов вида

$$b^{-1}xb,$$

где b — выбранный нами определенный элемент группы G , а x пробегает множество всех элементов подгруппы H , называется **трансформацией подгруппы H** при помощи элемента b и обозначается через

$$b^{-1}Hb.$$

Докажем, что $b^{-1}Hb$ есть группа.

В самом деле: 1. Пусть имеем два элемента c_1 и c_2 , принадлежащие к $b^{-1}Hb$. Докажем, что c_1c_2 принадлежит к $b^{-1}Hb$. Имеем:

$$\left. \begin{aligned} c_1 &= b^{-1}x_1b, \\ c_2 &= b^{-1}x_2b, \end{aligned} \right\} \quad (6)$$

где x_1 и x_2 суть элементы группы H .

Из уравнений (6) следует непосредственно:

$$c_1c_2 = b^{-1}x_1x_2b; \quad (7)$$

итак, c_1c_2 есть трансформация элемента x_1x_2 при помощи b , а потому c_1c_2 принадлежит к $b^{-1}Hb$.

2. Докажем, что нейтральный элемент 1 группы G принадлежит к $b^{-1}Hb$. Так как 1 принадлежит к H , и так как

$$b^{-1} \cdot 1 \cdot b = 1,$$

то 1 принадлежит и к $b^{-1}Hb$.

3. Наконец, если a принадлежит к $b^{-1}Hb$, то и a^{-1} принадлежит $b^{-1}Hb$. В самом деле, если a принадлежит к $b^{-1}Hb$, то $a = b^{-1}xb$, где x есть некоторый элемент H . Но тогда элемент $a^{-1} = (b^{-1}xb)^{-1} = b^{-1}x^{-1}b$, т. е. a^{-1} есть трансформация элемента x^{-1} группы H при помощи b , следовательно, a^{-1} есть элемент множества $b^{-1}Hb$.

Итак, $b^{-1}Hb$ есть группа.

Каждому элементу x группы H соответствует вполне определенный элемент группы $b^{-1}Hb$, именно элемент $b^{-1}xb$ группы $b^{-1}Hb$. При этом двум различным элементам x_1 и x_2 соответствуют различные элементы $b^{-1}x_1b$ и $b^{-1}x_2b$, так как если x_1 и x_2 различны, то различны

и элементы x_1b и x_2b ¹⁾; а если различны элементы x_1b и x_2b , то различны и элементы $b^{-1}x_1b$ и $b^{-1}x_2b$ ²⁾. Итак, поставив в соответствие элементу x группы H элемент $b^{-1}xb$ группы $b^{-1}Nb$, мы получаем взаимно однозначное соответствие между H и $b^{-1}Nb$. В силу равенств (6) и (7) произведению двух элементов x_1 и x_2 соответствует при этом произведение элементов $b^{-1}x_1b$ и $b^{-1}x_2b$, т. е. наше соответствие есть изоморфное соответствие между группами H и $b^{-1}Nb$. Таким образом, нами доказана следующая

Теорема 2. *Трансформация подгруппы H группы G при помощи элемента b группы G есть подгруппа группы G , изоморфная группе H .*

З а м е ч а н и е. Непосредственно вытекают из определений следующие предложения:

1) Если G — коммутативная группа, а H — ее подгруппа, то трансформация подгруппы H при помощи любого элемента b группы G есть сама группа H (ведь в этом случае трансформация любого элемента x при посредстве b есть сам этот элемент x : $b^{-1}xb = x$).

2) Если G — любая группа, H — ее подгруппа, b — элемент H , то

$$b^{-1}Nb = H,$$

так как для всякого элемента x группы H при b , принадлежащем H , принадлежит H и элемент $b^{-1}xb$.

3) Если подгруппа H_2 есть трансформация подгруппы H_1 при посредстве элемента b , то H_1 есть трансформация подгруппы H_2 при посредстве элемента b^{-1} .

Доказательство непосредственно следует из леммы 1, п. 3.

О п р е д е л е н и е. Две подгруппы группы G , из которых одна является трансформацией другой, называются **сопряженными подгруппами**.

Так как $1^{-1} \cdot H \cdot 1 = H$, то каждая группа сопряжена с самой собой.

¹⁾ В самом деле, если

$$x_1b = x_2b = c,$$

то

$$x_1 = cb^{-1} \text{ и } x_2 = cb^{-1}.$$

²⁾ Так, если

$$b^{-1}x_1b = b^{-1}x_2b = c,$$

то

$$x_1b = bc \text{ и } x_2b = bc.$$

Из леммы 2 п. 4 следует, что две подгруппы, сопряженные третьей, сопряжены между собой, так что множество всех подгрупп группы G распадается на классы сопряженных между собой подгрупп.

Мы уже знаем (теорема 2 этого пункта), что *все сопряженные между собой подгруппы изоморфны между собой*.

5. Примеры. В группе поворотов правильного тетраэдра имеются, как мы видели, следующие подгруппы:

1. Две несобственные подгруппы: первая, состоящая из одного нейтрального элемента, и вторая, состоящая из всех двенадцати поворотов тетраэдра. Каждая из этих подгрупп, очевидно, сопряжена с самой собой.

2. Три подгруппы второго порядка: H_{01} , H_{02} , H_{03} , каждая из которых состоит из поворотов на углы 0 и π вокруг некоторой реберной медианы. *Все эти группы образуют один класс сопряженных подгрупп.*

3. Группа H четвертого порядка (клеиновская), являющаяся объединением (в смысле теории множеств) трех групп H_{01} , H_{02} , H_{03} (т. е. состоящая из тождественного поворота и из поворотов на угол π вокруг каждой из трех реберных медиан). Из определения группы H как объединения групп H_{01} , H_{02} , H_{03} и из того, что группы H_{01} , H_{02} , H_{03} образуют один класс сопряженных подгрупп, следует, что *группа H сопряжена лишь с самой собой*.

4. Четыре подгруппы третьего порядка: H_0 , H_1 , H_2 , H_3 ; каждая из них состоит из поворотов на углы 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ вокруг некоторой граневой медианы. *Все эти группы также образуют один класс сопряженных подгрупп.*

Итак, все 10 подгрупп группы поворотов правильного тетраэдра следующим образом распадаются на классы сопряженных подгрупп:

три класса, состоящие каждый из одного элемента: классы, содержащие лишь по одной несобственной подгруппе, и

класс, состоящий из одной подгруппы H четвертого порядка;

класс, состоящий из трех подгрупп второго порядка;

класс, состоящий из четырех подгрупп третьего порядка.

§ 2. ИНВАРИАНТНЫЕ ПОДГРУППЫ (НОРМАЛЬНЫЕ ДЕЛИТЕЛИ)

1. Определение. Если подгруппа H данной группы G не имеет никакой отличной от себя сопряженной подгруппы (т. е. если класс всех подгрупп, сопряженных в группе G подгруппе H , состоит лишь из одной группы H), то подгруппа H называется *инвариантной*¹⁾ *подгруппой* (или *нормальным делителем*) группы G .

Очевидно, определение инвариантной подгруппы можно сформулировать и так:

подгруппа H группы G называется инвариантной, если трансформация любого элемента группы H при помощи любого элемента группы G есть элемент группы H .

Понятие инвариантной подгруппы — одно из важнейших понятий всей алгебры: если и невозможно в этом кратком изложении довести читателя до полного понимания всей важности этого понятия, раскрывающегося в алгебре, особенно в так называемой теории Галуа, то можно все же надеяться, что из рассуждений этой и следующей глав читатель поймет, насколько велико значение инвариантных подгрупп в логическом построении самой теории групп.

2. Примеры. Тривиальными примерами инвариантных подгрупп являются обе несобственные подгруппы любой группы. Кроме того, любая подгруппа коммутативной группы является, очевидно, инвариантной.

Укажем некоторые менее тривиальные примеры.

1. Группа скольжений прямой самой по себе есть инвариантная подгруппа группы всех самосовмещений прямой (гл. V, § 2).

2. Циклическая группа A порядка n , состоящая из всех самосовмещений первого рода n -угольного

¹⁾ Инвариантная — в переводе с латинского «неизменяемая» (по отношению к операции трансформирования подгруппы).

В настоящее время в математической литературе вместо термина инвариантная все большее распространение получает термин нормальная подгруппа. По нашему мнению, этот термин совершенно не отражает основного свойства рассматриваемых подгрупп: инвариантности по отношению к операции трансформирования подгрупп.

диэдра, есть инвариантная подгруппа группы всех поворотов n -угольного диэдра¹⁾.

3. Знакопеременная группа A_n подстановок из n элементов есть инвариантная подгруппа группы S_n всех подстановок из n элементов. В самом деле, если b есть произвольная четная подстановка, а a есть любой элемент группы S_n (т. е. любая подстановка — четная или нечетная), то подстановка $a^{-1}ba$ имеет в качестве знака произведение трех чисел, равных $+1$ или -1 :

$$(\text{зн } a^{-1}) \cdot (\text{зн } b) \cdot (\text{зн } a).$$

Так как $(\text{зн } a^{-1}) = \text{зн } a$, то $(\text{зн } a^{-1}) \cdot (\text{зн } a)$ в каждом случае (т. е. для любого a) равняется $+1$; следовательно,

$$(\text{зн } a^{-1}ba) = (\text{зн } a^{-1}) \cdot (\text{зн } b) \cdot (\text{зн } a) = (\text{зн } b) = +1,$$

а это значит, что $a^{-1}ba$ есть четная подстановка, т. е. элемент группы A_n .

Итак, трансформация любого элемента b группы A_n есть элемент группы A_n (вообще говоря, отличный от a), т. е. A_n есть инвариантная подгруппа группы S_n .

Возвращаемся к примерам инвариантных и неинвариантных подгрупп.

Мы уже видели, что в группе всех поворотов тетраэдра имеется одна собственная инвариантная подгруппа четвертого порядка. Так как группа всех поворотов тетраэдра изоморфна знакопеременной группе A_4 подстановок из четырех элементов (т. е. группе всех четных подстановок из четырех элементов), то полученный результат можно сформулировать и так:

знакопеременная группа подстановок из четырех элементов имеет инвариантную подгруппу четвертого порядка.

Это обстоятельство заслуживает внимания: оказывается, при $n > 4$ знакопеременная группа A_n подстановок из n элементов не содержит никакой инвари-

¹⁾ Так как, если a есть самосовмещение первого, а b — самосовмещение второго рода, то имеем (как было указано в гл. V, § 3)

$$ab = ba^{-1},$$

откуда

$$b^{-1}ab = a^{-1};$$

так как это справедливо для любого элемента подгруппы A , то

$$b^{-1}Ab = A.$$

антной подгруппы (кроме двух несобственных подгрупп). Этот факт, доказательство которого читатель может найти, например, в книге «Теория групп» А. Г. Куроша, имеет большое значение в алгебре: он тесно связан с тем, что общее уравнение степени $n > 4$ неразрешимо в радикалах.

Группа поворотов куба, как мы знаем, изоморфна группе S_4 . Значит, в ней заведомо имеется инвариантная подгруппа, изоморфная группе A_4 ; эта группа нам уже знакома из гл. V, § 5: она состоит из поворотов, переводящих в себя каждый из двух тетраэдров, вписанных в куб.

Мы уже упоминали также о трех подгруппах восьмого порядка, содержащихся в группе самосовмещений куба. Эти три группы образуют класс сопряженных между собой групп; следовательно, ни одна из них не инвариантна. Зато инвариантной подгруппой является пересечение этих трех групп, которое, как мы знаем, представляет собой группу, состоящую из нейтрального элемента и из трех поворотов куба на 180° вокруг каждой из трех прямых, соединяющих центры двух противоположных его граней¹⁾.

Никаких инвариантных собственных подгрупп, кроме указанных групп двенадцатого и четвертого порядка, в группе самосовмещений куба не имеется.

Упомянем еще следующие классы сопряженных групп:

1. Класс, состоящий из трех циклических групп порядка 4 (каждая из этих групп состоит из поворотов вокруг одной из осей, соединяющих центры двух противоположных граней куба).

2. Класс, состоящий из четырех циклических групп порядка 3 (каждая из этих групп состоит из поворотов вокруг одной из диагоналей).

3. Класс, состоящий из шести циклических групп порядка 2 (каждая из этих групп состоит из поворотов вокруг одной из осей, соединяющих середины двух противоположных ребер).

¹⁾ Читателю рекомендуется доказать следующую общую теорему: пересечение всех групп, входящих в некоторый класс сопряженных между собой подгрупп, есть инвариантная подгруппа.

ГОМОМОРФНЫЕ ОТОБРАЖЕНИЯ

§ 1. ОПРЕДЕЛЕНИЕ ГОМОМОРФНОГО ОТОБРАЖЕНИЯ И ЕГО ЯДРА

Пусть каждому элементу a группы A поставлен в соответствие элемент

$$b = f(a)$$

группы B . Совокупность всех полученных таким образом элементов $b = f(a)$ группы B обозначим через $f(A)$. Мы говорим, что имеем отображение f группы A в группу B , а именно: на множество $f(A) \subset B$.

Введем теперь следующее фундаментальное определение.

Отображение f группы A в группу B называется *гомоморфным*, если для любых двух элементов a_1 и a_2 группы A выполнено условие

$$f(a_1 \cdot a_2) = f(a_1) \cdot f(a_2), \quad (1)$$

причем знак \cdot в левой части равенства (1) надо, естественно, понимать как *знак умножения в группе A* , а в правой части равенства (1) как *знак умножения в группе B* .

Теорема. *Если f есть гомоморфное отображение группы A в группу B , то множество $f(A) \subset B$ есть подгруппа группы B .*

Доказательство. Достаточно показать, что:

1) если b_1 и b_2 суть элементы множества $f(A)$, то $b_1 \cdot b_2$ есть также элемент множества $f(A)$;

2) нейтральный элемент группы B есть элемент множества $f(A)$;

3) если b есть элемент множества $f(A)$, то b^{-1} есть также элемент множества $f(A)$.

Докажем последовательно утверждения 1), 2), 3).

1) Пусть b_1 и b_2 суть два элемента множества $f(A)$. Это значит, что существуют такие элементы a_1 и a_2 группы A , что

$$f(a_1) = b_1, \quad f(a_2) = b_2.$$

Но в силу гомоморфности отображения f имеем:

$$f(a_1 \cdot a_2) = b_1 \cdot b_2.$$

Следовательно, $b_1 \cdot b_2$ как образ при отображении f элемента $a_1 \cdot a_2$ группы A есть элемент множества $f(A)$. Первый пункт, таким образом, доказан.

2) Пусть 1 — нейтральный, а a — какой-нибудь элемент группы A . Имеем (в группе A)

$$a \cdot 1 = a,$$

откуда (в группе B) получаем

$$f(a \cdot 1) = f(a),$$

и в силу гомоморфности отображения f левую часть последнего равенства можно переписать в виде

$$f(a) \cdot f(1) = f(a);$$

отсюда видно, что $f(1)$ есть нейтральный элемент группы B . Этим доказан второй пункт.

3) Пусть b — произвольный элемент множества $f(A) \subset B$. Существует такой элемент a группы A , что

$$f(a) = b.$$

Обозначим через b' элемент $f(a^{-1})$ множества $f(A)$.

Докажем, что

$$b' = b^{-1}.$$

В самом деле,

$$a \cdot a^{-1} = 1.$$

Следовательно,

$$f(a) \cdot f(a^{-1}) = 1$$

(1 справа означает нейтральный элемент группы B), т. е.

$$b \cdot b' = 1,$$

и следовательно,

$$b' = b^{-1},$$

что и требовалось доказать.

Итак, всякое гомоморфное отображение группы A в группу B есть гомоморфное отображение группы A на некоторую подгруппу группы B .

Замечание 1. В только что проделанных рассуждениях содержится доказательство следующих важных утверждений, справедливых для всякого гомоморфного отображения группы A в группу B :

$$f(1) = 1 \quad (2)$$

(где слева 1 есть нейтральный элемент группы A , а справа — нейтральный элемент группы B),

$$f(a^{-1}) = f(a)^{-1}. \quad (3)$$

Замечание 2. На основании примечания в гл. III § 1 мы можем сказать:

Взаимно однозначное гомоморфное отображение группы A на группу B есть изоморфное отображение.

Определение. Пусть f есть гомоморфное отображение группы A в группу B . Множество всех элементов x группы A , отображающихся в силу f на нейтральный элемент группы B , называется **ядром** гомоморфного отображения f и обозначается через $f^{-1}(1)$.

Теорема. Ядро гомоморфного отображения f группы A в группу B есть инвариантная подгруппа группы A .

Доказательство. Из определения гомоморфного отображения непосредственно следует, что, если

$$f(a_1) = 1, \quad f(a_2) = 1, \quad \text{то} \quad f(a_1 \cdot a_2) = 1,$$

т. е. если a_1 и a_2 суть элементы $f^{-1}(1)$, то и $a_1 \cdot a_2$ есть элемент $f^{-1}(1)$.

Далее, мы видели при доказательстве предыдущей теоремы, что $f(1)$ есть нейтральный элемент группы B , т. е. 1 есть элемент $f^{-1}(1)$.

Наконец, если $f(a) = 1$, то $f(a^{-1}) = f(a)^{-1} = 1$, т. е. если a есть элемент $f^{-1}(1)$, то a^{-1} есть также элемент $f^{-1}(1)$. Отсюда уже следует, что $f^{-1}(1)$ есть подгруппа группы A .

Чтобы доказать, что $f^{-1}(1)$ есть инвариантная подгруппа группы A , надо убедиться в том, что трансформация $a^{-1}xa$ произвольного элемента x группы $f^{-1}(1)$ при помощи любого элемента a группы A есть элемент группы $f^{-1}(1)$. Другими словами, надо убедиться в том, что

$$f(a^{-1}xa) = 1,$$

если только $f(x) = 1$. Но это почти очевидно, так как при $f(x) = 1$ имеем

$$f(a^{-1}xa) = f(a)^{-1} \cdot f(x) \cdot f(a) = f(a)^{-1} \cdot 1 \cdot f(a) = \\ = f(a)^{-1} \cdot f(a) = 1.$$

Итак, наша теорема полностью доказана.

В дальнейшем мы увидим, что и обратно, всякая инвариантная подгруппа группы A есть ядро некоторого гомоморфного отображения группы A .

§ 2. ПРИМЕРЫ ГОМОМОРФНЫХ ОТОБРАЖЕНИЙ

1. Рассмотрим группу G всех целых чисел $\dots, -n, -(n-1), \dots, -2, -1, 0, 1, 2, \dots$
 $\dots, (n-1), n, \dots$

и группу второго порядка G_2 . Эта группа является абелевой. Пусть ее элементы будут b_0, b_1 , а таблица сложения такая:

$$b_0 + b_0 = b_0, \quad b_0 + b_1 = b_1 + b_0 = b_1, \quad b_1 + b_1 = b_0.$$

Очевидно, что b_0 есть нейтральный элемент группы G_2 .

Установим следующее отображение f группы G на группу G_2 . Каждому четному числу ставим в соответствие элемент b_0 группы G_2 , каждому нечетному числу ставим в соответствие элемент b_1 группы G_2 .

Это отображение *гомоморфно*. В самом деле, пусть a и a' — два целых числа. Если a и a' оба четные числа, то $a + a'$ тоже четное, и мы имеем

$$f(a + a') = f(a) = f(a') = b_0 = f(a) + f(a').$$

Если одно из двух чисел a и a' (пусть a) четное; а другое нечетное, то $a + a'$ нечетное, так что

$$f(a) = b_0, \quad f(a') = b_1, \\ f(a + a') = b_1 = b_0 + b_1 = f(a) + f(a').$$

Если, наконец, и a и a' нечетные числа, то $a + a'$ четное, и мы имеем:

$$f(a) = f(a') = b_1, \\ f(a + a') = b_0 = b_1 + b_1 = f(a) + f(a').$$

Ядром нашего гомоморфизма, очевидно, является группа всех четных чисел.

Обобщим этот пример. Пусть дано произвольное натуральное число $m \geq 2$. Рассмотрим циклическую группу G_m порядка m с элементами $b_0, b_1, b_2, \dots, b_{m-1}$ и таблицей сложения:

	b_0	b_1	b_2	...	b_{m-2}	b_{m-1}
b_0	b_0	b_1	b_2	...	b_{m-2}	b_{m-1}
b_1	b_1	b_2	b_3	...	b_{m-1}	b_0
b_2	b_2	b_3	b_4	...	b_0	b_1
\vdots	\vdots	\vdots	\vdots	\vdots	\vdots	\vdots
b_{m-2}	b_{m-2}	b_{m-1}	b_0	...	b_{m-4}	b_{m-3}
b_{m-1}	b_{m-1}	b_0	b_1	...	b_{m-3}	b_{m-2}

(нейтральный элемент обозначен через b_0).

Установим гомоморфное отображение f группы G всех целых чисел на группу G_m .

Для этого напомним прежде всего следующую арифметическую теорему:

Каждое целое число a при делении на натуральное число m дает в качестве остатка одно из чисел $0, 1, \dots, m-1$. При этом остаток числа a определяется как единственное неотрицательное целое число r , удовлетворяющее соотношениям

$$a = mq + r, \quad 0 \leq r \leq m-1, \quad (4)$$

при целом q (называемом неполным частным при делении a на m).

Теорема эта всем, конечно, известна для случая положительного a . Для $a=0$ имеем, очевидно,

$$0 = m \cdot 0 + 0,$$

т. е. при делении нуля на любое натуральное число и в частном и в остатке получается нуль.

Случай отрицательного a требует, может быть, некоторых разъяснений. Если a отрицательно, то $-a$ положительно. Разделим натуральное число $-a$ на натуральное число m , обозначим частное через q' и остаток через r' . Можем предположить, что $r' > 0$ (так как если

бы $r' = 0$, то $-a$, а следовательно, и a делилось бы на m без остатка). Итак,

$$-a = mq' + r', \quad 0 < r' \leq m - 1$$

или

$$\begin{aligned} a &= -mq' - r' = \\ &= -m - mq' + m - r' = m(-1 - q') + (m - r'). \end{aligned}$$

Из $0 < r' \leq m - 1$ следует, очевидно,

$$0 \leq m - r' \leq m - 1.$$

Поэтому, полагая $q = -1 - q'$, $r = m - r'$, имеем для целых чисел a , q соотношения

$$a = mq + r, \quad 0 \leq r \leq m - 1. \quad (5)$$

Легко убедиться в том, что представление целых чисел a в виде уравнений (5) при данном целом m и целых q и r , $0 \leq r \leq m - 1$ единственно, т. е. что целые числа q и r условиями (5) вполне определены.

В самом деле, пусть

$$a = mq_1 + r_1, \quad 0 \leq r_1 \leq m - 1. \quad (5')$$

Тогда вычтем почленно равенство (5') из равенства (5). Получим

$$0 = m(q - q_1) + (r - r_1)$$

или

$$r - r_1 = m(q_1 - q).$$

Отсюда следует, что целое число $r - r_1$ делится без остатка на m . Но $r - r_1$ есть разность двух неотрицательных чисел, не превосходящих $m - 1$; следовательно, абсолютная величина этой разности также не превосходит $m - 1$; в этих условиях число $r - r_1$ может делиться без остатка на m только в том случае, если оно есть нуль.

Итак,

$$r - r_1 = 0, \quad \text{т. е.} \quad r = r_1$$

и, заменяя r_1 на r в формуле (5'), получаем

$$a = mq_1 + r. \quad (6)$$

Из равенств (6) и (5) получаем

$$q_1 = \frac{a - r}{m}, \quad q = \frac{a - r}{m},$$

т. е. $q_1 = q$, что и требовалось доказать.

Целому числу r в силу неравенства

$$0 \leq r \leq m-1$$

соответствует элемент b_r группы G_m . Итак, при зафиксированном натуральном числе $m \geq 2$ каждому целому числу a соответствует вполне определенный элемент циклической группы G_m порядка m , а именно: элемент b_r , где r есть остаток при делении a на m . Этот элемент b_r называется **вычетом числа a по модулю m** .

Только что указанным соответствием и устанавливается отображение f группы G на группу G_m . Докажем, что отображение f гомоморфно.

Пусть a и a' два целых числа и пусть

$$\left. \begin{aligned} a &= mq + r, & 0 \leq r \leq m-1, \\ a' &= mq' + r', & 0 \leq r' \leq m-1. \end{aligned} \right\} \quad (7)$$

Тогда

$$a + a' = m(q + q') + r + r'.$$

Однако $r + r'$, удовлетворяя, конечно, неравенству $0 \leq r + r'$, может не удовлетворять неравенству $r + r' \leq m-1$.

Но во всяком случае

$$r + r' = mq'' + \rho,$$

где q'' есть частное от деления $r + r'$ на m (оно, как нетрудно видеть, равно 0 или 1) и ρ есть остаток при этом делении, так что

$$a + a' = m(q + q' + q'') + \rho, \quad 0 \leq \rho < m-1.$$

Итак, элементу $a + a'$ при нашем отображении f соответствует элемент b_ρ группы G_m .

Рассматривая таблицу сложений в циклической группе порядка m , видим, что

$$b_r + b_{r'} = b_\rho$$

(где ρ по-прежнему есть остаток при делении $r + r'$ на m). Итак,

$$f(a + a') = b_\rho = b_r + b_{r'} = f(a) + f(a'),$$

чем и доказано, что отображение f гомоморфно.

Только что построенное гомоморфное отображение f группы всех целых чисел в циклическую группу по-

рядка m является основным фактом элементарной теории чисел; мы это гомоморфное отображение будем обозначать через f_m .

Ядром гомоморфизма f_m является группа всех целых чисел, делящихся без остатка на m .

2. В главе V, § 2, второй пример, было указано, что каждому действительному числу соответствует некоторый элемент группы $SO(2)$. Этим соответствием устанавливается гомоморфное отображение группы всех действительных чисел на группу $SO(2)$, причем ядром этого отображения является бесконечная циклическая группа, состоящая из всех действительных чисел, являющихся целочисленными кратными 2π .

РАЗБИЕНИЕ ГРУППЫ НА КЛАССЫ ПО ДАННОЙ ПОДГРУППЕ. ФАКТОРГРУППА

§ 1. ЛЕВОСТОРОННИЕ И ПРАВОСТОРОННИЕ КЛАССЫ

1. Левосторонние классы. Пусть даны группа G и ее подгруппа U . Наша задача заключается сейчас в том, чтобы показать следующее: задание подгруппы U определяет (и притом, вообще говоря, двумя различными способами) разбиение группы G на некоторую систему попарно непересекающихся подмножеств, одно из которых есть сама подгруппа U , а остальные некоторым весьма простым законом могут быть взаимно однозначно отображены на U .

Для получения этого разбиения будем поступать так.

Назовем два элемента a и b группы G **эквивалентными**, если элемент $a^{-1}b$ есть элемент подгруппы U .

Эта эквивалентность (называемая *левой эквивалентностью*) обладает свойством *симметрии*, так как, если

$$a^{-1}b = u,$$

где u есть элемент подгруппы U , то

$$b^{-1}a = (a^{-1}b)^{-1} = u^{-1}$$

также есть элемент подгруппы U .

Наша эквивалентность обладает, далее, свойством транзитивности, так как, если

$$a^{-1}b = u_1,$$

$$b^{-1}c = u_2,$$

где u_1 и u_2 — суть элементы подгруппы U , то

$$a^{-1}c = a^{-1}b \cdot b^{-1}c = u_1 u_2$$

также есть элемент подгруппы U .

Наша эквивалентность обладает, наконец, свойством рефлексивности, так как

$$a^{-1}a = 1$$

есть элемент подгруппы U .

Итак, группа G на основании теоремы 3 гл. I распадается на классы элементов, эквивалентных между собой относительно подгруппы U . Эти классы называются *левосторонними классами* группы G по подгруппе U . Заметим, что левосторонний класс $'K_a$ элемента a группы G состоит из всех таких элементов x , что $a^{-1}x = u$ есть элемент группы U , т. е. другими словами, из всех элементов вида $x = au$, где u есть элемент подгруппы U .

Заметим еще, что если a есть элемент U (в частности, если $a = 1$), то $'K_a = U$, так как в этом случае au при любом u , принадлежащем к U , есть элемент группы U , и всякий элемент u группы U может быть представлен в виде au_1 , где $u_1 = a^{-1}u$ есть элемент группы U . Так как всякий элемент множества $'K_a$ может быть представлен в виде au , и при различных элементах u_1 и u_2 группы U элементы au_1 и au_2 множества $'K_a$ различны, то мы получим взаимно однозначное соответствие между U и любым $'K_a$, если каждому элементу u группы U поставим в соответствие элемент au класса $'K_a$.

Заметим, наконец, что среди всех классов $'K_a$ имеется лишь один класс, являющийся подгруппой группы G , а именно U .

В самом деле, если $'K_a$ есть подгруппа, то нейтральный элемент группы G должен входить в $'K_a$; он, следовательно, является общим элементом класса $'K_a$ и класса U , а поэтому $'K_a$ совпадает с U .

2. Случай конечной группы G . В силу взаимно однозначного соответствия, существующего между каждым из $'K_a$ и подгруппой U , все $'K_a$ — в случае конечности группы G — состоят из одного и того же числа элементов t , где t есть порядок группы U . Если число всех различных классов равно j , а n есть порядок группы G , то имеем, очевидно, $n = tj$.

Отсюда, в частности, следует ранее упомянутый нами факт (гл. II, § 2), а именно:

Теорема Лагранжа. Порядок всякой подгруппы конечной группы G есть делитель порядка группы G .

Число j , т. е. число левосторонних классов¹⁾ группы G по подгруппе U , называется *индексом подгруппы U в группе G* .

3. Правосторонние классы. Назовем два элемента a и b *эквивалентными* (*правая эквивалентность*) относительно подгруппы U , если ba^{-1} есть элемент подгруппы U . Легко убеждаемся, что свойства симметрии, транзитивности и рефлексивности при этом выполнены.

В самом деле, из

$$ba^{-1} = u,$$

где u — элемент группы U , следует

$$ab^{-1} = (ba^{-1})^{-1} = u^{-1},$$

а из

$$ba^{-1} = u_1, \quad cb^{-1} = u_2$$

при u_1 и u_2 , принадлежащих к U , следует:

$$ca^{-1} = cb^{-1} \cdot ba^{-1} = u_2 \cdot u_1.$$

Наконец,

$$aa^{-1} = 1$$

принадлежит к U .

Правая эквивалентность определяет разбиение группы G на *правосторонние* классы, причем *правосторонний класс K'_a данного элемента a* состоит из всех таких элементов x , для которых $xa^{-1} = u$ есть элемент группы U , т. е. из всех элементов вида

$$x = ua,$$

где u принадлежит U .

Для a , принадлежащего U , класс K'_a совпадает с U .

Ставя в соответствие элементу u подгруппы U элемент ua класса K'_a , получим взаимно однозначное соответствие между U и любым классом K'_a . В случае, если подгруппа U конечна, все классы K'_a по этой подгруппе конечны и состоят из того же числа элементов, что и U . Если группа G конечна и имеет порядок n , а подгруппа U имеет порядок m , то имеем, как прежде,

$$n = mj,$$

¹⁾ Это число может быть конечным и в случае бесконечной группы G , например, если G есть группа всех целых чисел, а U — подгруппа G , состоящая из всех чисел, делящихся без остатка на целое число $m \geq 2$.

где j — число всех различных правосторонних классов по подгруппе U , равное, таким образом, числу всех различных левосторонних классов.

Итак, индекс подгруппы U относительно конечной группы G может быть определен и как число левосторонних, и как число правосторонних классов группы G по подгруппе U : он равен частному от деления порядка группы G на порядок группы U .

4. Совпадение правосторонних классов с левосторонними в случае инвариантных подгрупп. Зададим себе вопрос: в каком случае для всякого элемента a группы G выполняется равенство

$${}'K_a = K'_a?$$

Для этого, очевидно, необходимо и достаточно, чтобы всякий элемент вида ai равнялся некоторому $u'a$ и, наоборот, всякий элемент ia равнялся некоторому элементу ai' (при этом всегда u , u' и так далее обозначают элементы подгруппы U). Оба условия при этом эквивалентны. В самом деле, первое условие означает: к каждому a из G и u из U можно подобрать такое u' из U , чтобы

$$ai = u'a,$$

т. е. чтобы

$$aia^{-1} = u',$$

или

$$(a^{-1})^{-1} U a^{-1} = U.$$

Так как любой элемент группы G может быть при надлежащем выборе элемента a представлен в виде a^{-1} , то первое условие означает просто: трансформация подгруппы U при помощи любого элемента группы G совпадает с U , или U есть инвариантная подгруппа группы G .

Второе условие гласит: к каждому a из G и u из U можно подобрать u' из U так, чтобы

$$ia = ai',$$

т. е.

$$a^{-1}ia = u',$$

т. е.

$$a^{-1}Ua = U.$$

Таким образом, второе условие также выражает требование, чтобы U было инвариантной подгруппой группы G .

Итак, мы видим, что верна следующая

Теорема. Пусть U — подгруппа группы G . Для того чтобы для каждого элемента a группы G левосторонний класс этого элемента относительно подгруппы U совпадал с правосторонним классом того же элемента, необходимо и достаточно, чтобы U было инвариантной подгруппой группы G .

Так как в случае инвариантной подгруппы U для любого элемента a группы G выполняется равенство

$${}'K_a = K'_a,$$

то можно вместо ${}'K_a$ и K'_a писать $K_a = {}'K_a = K'_a$, и это множество называть просто классом элемента a относительно инвариантной подгруппы U .

В частности, совпадение правосторонних классов с левосторонними имеет место, если U есть подгруппа коммутативной группы G , так как все подгруппы коммутативных групп инвариантны (гл. VI, § 2, п. 2).

5. Примеры. I. Пусть G — группа всех целых чисел, а $U \subset G$ — группа всех чисел, делящихся без остатка на m .

Если a — произвольное целое число, то K_a состоит из всех чисел вида $a + mq$ при целом q : это будут все те числа, которые при делении на m дают тот же остаток, что и число a . Таким образом, различных классов будет столько же, сколько имеется различных остатков при делении на m ; а этих последних имеется m , так как в качестве остатков при делении на m появляются числа $0, 1, 2, \dots, m-1$, и только они. Итак, мы имеем следующие классы:

0) Класс всех чисел, дающих при делении на m остаток 0. Этот класс совпадает с группой U и состоит из чисел

$$\dots, -qm, -(q-1)m, \dots, -3m, -2m, -m, \\ 0, m, 2m, 3m, \dots, qm, \dots$$

1) Класс всех чисел, дающих при делении на m остаток 1. Это будут:

$$\dots, -qm+1, -(q-1)m+1, \dots, -3m+1, \\ -2m+1, -m+1, 1, m+1, 2m+1, 3m+1, \dots$$

2) Класс всех чисел, дающих при делении на m остаток 2. Это будут:

$$-qm+2, -(q-1)m+2, \dots, -3m+2, \\ -2m+2, -m+2, 2, m+2, \dots, qm+2, \dots$$

$m-1$) Класс всех чисел, дающих при делении на m остаток $(m-1)$. Этот класс состоит из чисел:

$$\dots, -qm+(m-1), -(q-1)m+(m-1), \dots, \\ -3m+(m-1), -2m+(m-1), -m+ \\ +(m-1), (m-1), m+(m-1), 2m+(m-1), \dots,$$

или, что то же самое,

$$\dots, -2m-1, -m-1, -1, m-1, 2m-1, 3m-1, \dots$$

II. Пусть G есть группа S_3 всех подстановок из трех элементов, а U — подгруппа порядка 2 (следовательно, индекса 3), состоящая из подстановок

$$P_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \text{и} \quad P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Распадение группы G на лево- и правосторонние классы видно из следующей таблицы:

Левосторонние классы	Правосторонние классы
$U = \{P_0, P_2\}$	$U = \{P_0, P_2\}$
$\{P_1, P_3\}$	$\{P_1, P_4\}$
$\{P_4, P_5\}$	$\{P_3, P_5\}$

III. Знакопеременная группа A_n подстановок из n элементов представляет собой инвариантную подгруппу индекса 2 симметрической группы S_n . Два класса, определяемые этой подгруппой, суть: сама группа A_n и класс всех нечетных подстановок.

IV. В группе поворотов n -угольного диэдра самовмещения первого рода образуют инвариантную подгруппу индекса 2. Один из двух классов по этой под-

группе есть она сама, другой класс состоит из всех самосовмещений второго рода.

V. Группа U всех скольжений прямой по самой себе есть инвариантная подгруппа индекса 2 в группе G всех самосовмещений прямой. Два класса, определяемые этой подгруппой, суть: сама группа U и класс всех самосовмещений второго рода.

VI. Пусть G есть группа всех комплексных чисел (с операцией обычного сложения как групповой операцией). Пусть U — подгруппа всех действительных чисел. Классы, на которые распадается коммутативная группа G относительно своей подгруппы U , суть множества K_β , каждое из которых состоит из всех комплексных чисел вида

$$x + i\beta,$$

где x и β — действительные числа, β дано, а x пробегает все действительные значения. Если, как это обычно делается, изображать комплексные числа в виде точек плоскости¹⁾, то каждый класс изобразится в виде прямой, параллельной действительной оси (т. е. оси абсцисс).

§ 2. ФАКТОРГРУППА ПО ДАННОЙ ИНВАРИАНТНОЙ ПОДГРУППЕ

1. **Определение.** Пусть U есть инвариантная подгруппа некоторой данной группы G . Рассмотрим множество всех классов, на которые распадается группа G относительно U . Это множество обозначим через V и докажем, что в нем можно определить операцию умножения таким образом, что V станет группой, на которую группу G можно будет гомоморфно отобразить.

Пусть v_1 и v_2 — два произвольных элемента из V ; таким образом, v_1 и v_2 суть два класса группы G по инвариантной подгруппе U . Выберем в каждом из этих классов по одному элементу, а именно: выберем элемент x_1 из класса v_1 и элемент x_2 из класса v_2 . Обозначим через v_3 класс, к которому принадлежит элемент $x_1 x_2$ группы G .

¹⁾ Считая за изображение комплексного числа $x + iy$ точку плоскости с координатами (x, y) .

Докажем, что класс v_3 не зависит от того, какие именно элементы x_1 и x_2 мы выбрали из классов v_1 и v_2 . Другими словами, докажем: если x'_1 есть какой-нибудь элемент класса v_1 , вообще говоря, отличный от x_1 , а x'_2 какой-нибудь элемент класса v_2 , вообще говоря, отличный от x_2 , то элемент $x'_1 x'_2$ принадлежит к тому же классу v_3 , к которому принадлежит $x_1 x_2$.

В самом деле, два элемента a и b принадлежат тогда и только тогда к одному и тому же классу относительно инвариантной подгруппы U , если элемент ab^{-1} принадлежит к U .

Рассмотрим элемент

$$x_1 x_2 (x'_1 x'_2)^{-1} = x_1 x_2 (x'_2)^{-1} (x'_1)^{-1} = x_1 \cdot (x_2 (x'_2)^{-1}) (x'_1)^{-1}.$$

Так как x_2 и x'_2 принадлежат одному и тому же классу v_2 , то

$$x_2 (x'_2)^{-1} = u_2,$$

где u_2 есть некоторый элемент U , и мы имеем

$$x_1 x_2 (x'_1 x'_2)^{-1} = x_1 u_2 (x'_1)^{-1}. \quad (1)$$

Но U есть инвариантная подгруппа, поэтому $x_1 u_2 = u' x_1$, где u' есть некоторый элемент группы U .

Подставляя это в формулу (1), получаем

$$x_1 x_2 (x'_1 x'_2)^{-1} = u' x_1 (x'_1)^{-1}.$$

Но x_1 и x'_1 принадлежат к одному и тому же классу v_1 , поэтому $x_1 (x'_1)^{-1} = u_1$, где u_1 — некоторый элемент группы U . Следовательно,

$$x_1 x_2 (x'_1 x'_2)^{-1} = u' u_1,$$

т. е. $x_1 x_2 (x'_1 x'_2)^{-1}$ есть некоторый элемент $u = u' u_1$ группы U , что и требовалось доказать.

Так как класс v_3 , таким образом, определен, коль скоро определены классы v_1 и v_2 , то полагаем:

$$v_1 \cdot v_2 = v_3. \quad (2)$$

Это есть *определение* произведения $v_1 \cdot v_2$ двух классов v_1 и v_2 . Итак:

произведением двух классов v_1 и v_2 называется класс v_3 построенный по следующему правилу: в каждом из классов v_1 и v_2 выбираем по произвольному элементу,

перемножаем эти два элемента и берем класс, к которому принадлежит их произведение; этот класс и есть класс v_3 .

Из этого определения и из того, что произведение элементов в группе G удовлетворяет условию ассоциативности, непосредственно следует, что и умножение классов удовлетворяет условию ассоциативности.

Докажем, что класс U по отношению к только что определенному умножению играет роль нейтрального элемента, т. е. что для всякого класса v справедливо равенство

$$v \cdot U = U \cdot v = v. \quad (3)$$

Для этого выберем произвольный элемент x класса v , а в качестве элемента класса U выберем нейтральный элемент 1 . Тогда, по определению умножения, класс $v \cdot U$ есть класс, содержащий элемент $x \cdot 1 = x$, т. е. тот же класс v . Точно так же класс $U \cdot v$ есть класс, содержащий элемент $1 \cdot x = x$, т. е. тот же класс v . Этим формула (3) доказана.

Докажем наконец, что к каждому классу K имеется некоторый обратный класс, который обозначим через K^{-1} и который удовлетворяет условию

$$K \cdot K^{-1} = K^{-1} \cdot K = U.$$

Для этого возьмем в классе K какой-нибудь элемент a и определим класс K^{-1} как класс, содержащий элемент a^{-1} . По определению произведений классов, каждое из двух произведений $K \cdot K^{-1}$ и $K^{-1} \cdot K$ представляет собой класс, содержащий элемент $a \cdot a^{-1} = a^{-1} \cdot a = 1$, а это и есть класс U .

Итак, определенное нами умножение удовлетворяет всем аксиомам понятия групп. Следовательно, *при нашем определении произведения множество классов группы G по ее инвариантной подгруппе U есть некоторая группа V . Класс U при этом есть нейтральный элемент группы V .*

Группа V называется **факторгруппой** группы G по ее инвариантной подгруппе U .

2. Теорема о гомоморфных отображениях. Пусть по-прежнему даны группа G и ее инвариантная подгруппа U . Каждому элементу x группы G поставим в соответствие определенный элемент факторгруппы V , а именно: тот класс, который содержит в себе элемент x .

Этим устанавливается отображение φ группы G на группу V и из определения умножения в группе V непосредственно следует, что это отображение гомоморфно.

Какие элементы группы G отображаются на нейтральный элемент группы V ? Так как этим нейтральным элементом является U , то очевидным ответом на наш вопрос является:

Все элементы инвариантной подгруппы U и только они при отображении φ отображаются на нейтральный элемент группы V .

Из рассуждений этого и предыдущего пунктов следует: всякая инвариантная подгруппа U группы G является ядром некоторого гомоморфного отображения группы G , а именно, гомоморфного отображения группы G на ее факторгруппу по отношению к U .

Пусть теперь дано произвольное гомоморфное отображение f какой-нибудь группы A на какую-нибудь группу B . Пусть U есть ядро этого гомоморфного отображения. Мы знаем, что U — инвариантная подгруппа группы A . Обозначим через V факторгруппу группы A по отношению к U .

Пусть b есть какой-нибудь элемент группы B . Существует по крайней мере один элемент a группы A , отображающийся отображением f на элемент b :

$$b = f(a).$$

Определим полный прообраз элемента b при отображении f , т. е. множество элементов x группы A , отображающихся отображением f на b . Этот полный прообраз обозначим, как обычно, через $f^{-1}(b)$.

Итак, $f^{-1}(b)$, по определению, есть множество всех тех элементов x группы A , для которых справедливо равенство

$$f(x) = b.$$

Пусть, как уже было сказано, a — какой-нибудь элемент, отображающийся на b ; если x есть другой элемент множества $f^{-1}(b)$, то $f(a) = b$, $f(x) = b$,

$$\begin{aligned} f(a^{-1}) &= b^{-1}, \\ f(xa^{-1}) &= b \cdot b^{-1} = 1 \end{aligned}$$

(единица справа есть нейтральный элемент группы B); это значит, что xa^{-1} есть некоторый элемент u группы U ,

т. е. $x = au$ есть элемент того класса по инвариантной подгруппе U , к которому принадлежит a . Обратно, если a и x принадлежат к одному классу, то

$$x = a \cdot u, \\ f(x) = f(a) \cdot f(u) = f(a) \cdot 1 = f(a),$$

т. е. a и x отображаются в один и тот же элемент b группы B , или, другими словами, содержатся в том же полном прообразе $f^{-1}(b)$.

Итак, полные прообразы $f^{-1}(b)$ элементов группы B суть классы группы A по инвариантной подгруппе U .

Этим обстоятельством устанавливается взаимно однозначное соответствие ψ между группой B и группой V .

Каждому элементу группы V , который есть некоторый класс группы A по инвариантной подгруппе U , т. е. полный прообраз некоторого элемента b группы B , соответствует именно этот элемент b группы B ; при этом каждый элемент b группы B оказывается поставленным в соответствие одному-единственному классу, т. е. одному-единственному элементу группы V , именно тому классу, который является полным прообразом элемента b . Отображение ψ гомоморфно: пусть v_1 и v_2 — два элемента группы V и

$$v_1 \cdot v_2 = v_3. \quad (4)$$

Пусть a_1 есть какой-нибудь элемент класса v_1 , a_2 — какой-нибудь элемент класса v_2 , $a_3 = a_1 \cdot a_2$. Мы знаем, что тогда a_3 принадлежит v_3 . Положим

$$f(a_1) = b_1, \quad f(a_2) = b_2, \quad f(a_3) = b_3.$$

Так как f гомоморфно, то

$$b_1 \cdot b_2 = b_3. \quad (5)$$

Но так как v_1, v_2, v_3 суть соответственно полные прообразы элементов b_1, b_2, b_3 , то

$$\psi(v_1) = b_1, \quad \psi(v_2) = b_2, \quad \psi(v_3) = b_3,$$

так что равенство (5) может быть переписано в виде

$$\psi(v_1) \cdot \psi(v_2) = \psi(v_3),$$

чем и доказан гомоморфный характер отображения ψ . Как взаимно однозначное гомоморфное отображение группы V на группу B , отображение ψ есть изоморф-

ное отображение V на B . Итогом всего предыдущего является следующее предложение.

Теорема Э. Нетер о гомоморфных отображениях.

Всякое гомоморфное отображение одной группы A на другую группу B имеет своим ядром некоторую инвариантную подгруппу группы A . Обратно, всякая инвариантная подгруппа U группы A есть ядро некоторого гомоморфного отображения φ группы A на факторгруппу V группы A по подгруппе U . Отображение φ получается, если каждому элементу группы A поставить в соответствие его класс относительно инвариантной подгруппы U . Если f есть произвольное гомоморфное отображение группы A на группу B , то полные прообразы элементов группы B при этом отображении суть классы группы A по ядру U отображения f и группа B изоморфна факторгруппе группы A по подгруппе U .

Итак, инвариантные подгруппы данной группы A совпадают с ядрами всевозможных гомоморфных отображений этой группы, а все группы, являющиеся гомоморфными образами группы A , совпадают с группами, изоморфными факторгруппам группы A по всевозможным ее инвариантным подгруппам¹⁾.

Следствие. *Для того чтобы гомоморфное отображение группы A на группу B было изоморфным, необходимо и достаточно, чтобы ядро этого отображения состояло из одного нейтрального элемента группы A .*

¹⁾ Читателю рекомендуется еще раз продумать с точки зрения только что изложенной теоремы о гомоморфных отображениях ранее приведенные примеры инвариантных подгрупп и гомоморфных отображений и определить относящиеся к ним факторгруппы.

ГРУППЫ ПЕРЕМЕЩЕНИЙ ПЛОСКОСТИ И ПРОСТРАНСТВА И ИХ ПОДГРУППЫ

Ю. П. Соловьев

Это добавление является введением в интересный раздел элементарной геометрии, а именно, в теорию геометрических преобразований плоскости и пространства. Уместность такого добавления в данной книге определяется тем, что геометрия и, в особенности, названный раздел ее, доставляют многочисленные примеры и иллюстрации к основным понятиям теории групп, причем примеры простые, интересные, а главное очень наглядные. На этих примерах читатель не только еще раз проверит, насколько он усвоил эти понятия, но сможет, так сказать, увидеть их в конкретном геометрическом воплощении.

1. Группа перемещений плоскости. Напомним, что перемещением плоскости называется такое преобразование, которое сохраняет расстояния. Другими словами, преобразование F называется перемещением, если для любых двух различных точек A и B плоскости справедливо соотношение $|AB| = |A'B'|$, где $A' = F(A)$ и $B' = F(B)$. Примеры перемещений хорошо известны читателю из школьного курса геометрии. Это *параллельный перенос* T_a , *поворот* R_O^α вокруг точки O на угол α , *симметрия* S_l относительно оси l , а также *скользящая симметрия* S_l^a ($a \parallel b$), которая по определению есть композиция $S_l^a = T_a \circ S_l = S_l \circ T_a$. Оказывается, что других перемещений плоскости нет.

Теорема 1.1 (Шаль). *Любое перемещение плоскости есть либо параллельный перенос, либо поворот, либо скользящая симметрия (в частности, симметрия, если $a = 0$).*

Доказательство. Доказательство этого утверждения основано на так называемой «аксиоме подвижности плоскости» (см. Геометрия 8, стр. 92), согласно

которой существует ровно два перемещения, переводящих пару (различных) точек A, B плоскости в любую другую пару точек A_1, B_1 , для которых $|A_1B_1| = |AB|$. Пусть теперь F — некоторое перемещение, A_0 — некоторая точка на плоскости, $A_1 = F(A_0)$, $A_2 = F(A_1)$. Рассмотрим три случая:

- 1) $A_2 = A_0$;
- 2) $A_2 \neq A_0$, но точка A_2 лежит на прямой (A_0A_1) ;
- 3) точка A_2 не лежит на прямой (A_0A_1) .

Если в каждом из этих трех случаев мы найдем по два различных перемещения из тех, которые были указаны в формулировке теоремы, то в силу упомянутой выше аксиомы это и является доказательством теоремы.

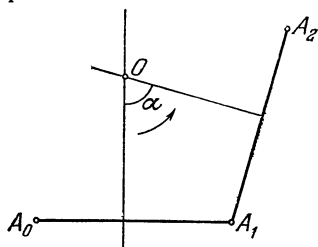


Рис. 15.

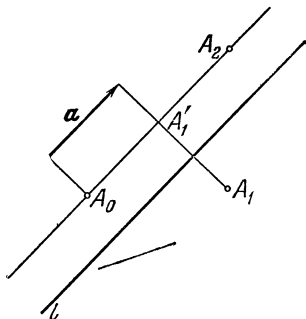


Рис. 16.

В случае 1) эти перемещения суть поворот вокруг середины отрезка $[A_0A_1]$ на угол π и симметрия относительно прямой, перпендикулярной к $[A_0A_1]$ и проходящей через ее середину.

В случае 2) требуемыми перемещениями являются параллельный перенос на вектор $\mathbf{a} = \overrightarrow{A_0A'_1}$ и симметрия относительно прямой, перпендикулярной к (A_0A_2) и проходящей через точку A_1 .

В случае же 3) это поворот вокруг точки O — точки пересечения перпендикуляров, восстановленных из середины отрезков $[A_0A_1]$ и $[A_1A_2]$ (рис. 15) и скользящая симметрия, ось которой параллельна оси (A_0A_2) и проходит через середину $[A_1A'_1]$, где A'_1 — прямоугольная проекция точки A_1 на (A_0A_2) , а вектор $\mathbf{a} = \overrightarrow{A_0A'_1}$ (рис. 16). Теорема доказана.

Параллельный перенос и поворот называются перемещениями *первого рода*, а симметрия и скользящая симметрия — *перемещениями второго рода*.

Имеет место следующее утверждение: *композиция двух перемещений первого рода есть перемещение первого рода, композиция перемещений первого и второго рода есть перемещение второго рода, а композиция перемещений второго рода есть перемещение первого рода.*

Приведем краткое доказательство этого утверждения, оставляя детали читателю.

Доказательство основывается на следующем простом факте: композиция двух симметрий $S_{l_2} \cdot S_{l_1}$ есть параллельный перенос T_a в случае, когда $l_1 \parallel l_2$ и поворот R_O^α , когда эти прямые пересекаются в точке O . Кроме того, вектор a в перемещении T_a перпендикулярен к l_1 и l_2 , направлен от l_1 к l_2 и по величине равен удвоенному расстоянию между этими прямыми. Угол α в повороте R_O^α есть удвоенный угол между прямыми l_1 и l_2 .

Из этого факта вытекает, что любой параллельный перенос и любой поворот можно представить в виде композиции двух симметрий. Например, чтобы получить такое представление для данного параллельного переноса T_a , выбираем произвольную прямую l_1 , перпендикулярную к a и параллельно переносим ее с помощью $T_{a/2}$; тогда $T_a = S_{l_2} \cdot S_{l_1}$, где $l_2 = T_{a/2}(l_1)$. Аналогично и для поворота. Значит, любое перемещение плоскости есть композиция некоторого числа симметрий: поворот и параллельный перенос — композиция двух симметрий, сама симметрия — композиция одной симметрии, скользящая симметрия — композиция трех симметрий. Заметим, что перемещения первого рода суть *композиции четного числа симметрий*, а перемещения второго рода — *композиции нечетного числа симметрий*. Верно и обратное: если перемещение первого (второго) рода каким бы то ни было способом представлено в виде композиции некоторого числа симметрий, то это число симметрий четное (нечетное). Доказательство этого утверждения предоставляем читателю. (У к а з а н и е. Оно эквивалентно следующему утверждению: *не существует представления тождественного преобразования в виде нечетного числа симметрий.*)

В силу сказанного выше перемещения первого и второго рода можно определить как такие перемещения, которые разлагаются в композиции соответственно четного и нечетного числа симметрий. Следовательно, композиция двух перемещений первого рода есть пере-

мещение первого рода, композиция перемещений первого и второго рода — перемещение второго рода, а композиция двух перемещений второго рода — перемещение первого рода, что и требовалось.

В этом приложении мы не можем останавливаться на подробном рассмотрении композиций перемещений на плоскости. Читателям же, которых заинтересовал данный вопрос, советуем обратиться к превосходной книге Коксетера «Введение в геометрию».

Все перемещения плоскости образуют группу, *операцией* в которой является *композиция перемещений*. Действительно, если два преобразования сохраняют расстояние между точками, то сохраняет его и композиция этих преобразований, т. е. композиция перемещений есть перемещение. Аксиома ассоциативности выполнена, поскольку она выполнена для всех вообще преобразований плоскости¹⁾. Далее, тождественное преобразование есть перемещение. И наконец, преобразование, обратное к перемещению, также сохраняет расстояние, т. е. является перемещением.

Группа всех перемещений плоскости обозначается $E(2)$. Она содержит бесконечное число подгрупп. Прежде всего, в силу сказанного выше подгруппу образуют все перемещения первого рода. Мы будем обозначать эту подгруппу через $E_0(2)$. Если F — перемещение первого рода, а G — произвольное перемещение, то $G \cdot F \cdot G^{-1}$ есть непременно перемещение первого рода, поэтому подгруппа перемещений первого рода $E_0(2)$ инвариантна в группе всех перемещений $E(2)$. Легко видеть, что существуют ровно два класса по этой подгруппе: она сама и класс перемещений второго рода. Следовательно, подгруппа $E_0(2)$ имеет индекс 2 в группе всех перемещений $E(2)$ и факторгруппа $E(2)$ по $E_0(2)$ является циклической группой из двух элементов.

Займемся теперь группой $E_0(2)$. Среди подгрупп этой группы отметим прежде всего бесконечное число *групп поворотов*: совокупность всех поворотов плоскости вокруг какой-нибудь определенной ее точки образует группу, и каждая из этих групп, как нетрудно видеть, изоморфна группе $SO(2)$ (см. гл. V, § 2); следовательно, *все эти группы коммутативны*.

¹⁾ Как легко видеть, ассоциативностью обладает вообще композиция отображений, Докажите!

Совокупность всех поворотов подгруппы не образует. Чтобы убедиться в этом, достаточно рассмотреть два поворота вокруг двух различных точек на углы, в сумме составляющие 2π — их композицией будет *параллельный перенос* (докажите!).

Наряду с группами поворотов, в группе $E_0(2)$ имеются *подгруппы параллельных переносов вдоль различных прямых*.

Если задана прямая l , то *параллельные переносы вдоль l* — это такие переносы, векторы которых параллельны l . Очевидно, что такие параллельные переносы образуют подгруппу в $E_0(2)$. Так как любой такой параллельный перенос однозначно характеризуется длиной и направлением вектора переноса, то группа всех параллельных переносов вдоль данной прямой l *изоморфна группе всех действительных чисел* (с обыкновенным сложением в качестве групповой операции).

Рассмотрим два параллельных переноса T_a и T_b , векторы которых не параллельны. Композиция этих параллельных переносов в любом порядке есть параллельный перенос T_{a+b} . Поэтому множество всех параллельных переносов плоскости образует коммутативную подгруппу в группе $E_0(2)$. Эта подгруппа обозначается $T(2)$.

Пусть даны два перемещения F и G из группы $E_0(2)$. Выясним, что происходит при трансформации перемещения F с помощью перемещения G . По определению, это будет перемещение

$$H(P) = G \cdot F \cdot G^{-1}(P). \quad (1)$$

Так как G — взаимно однозначное отображение плоскости, то перемещение H будет вполне описано, если будет указано, куда в результате этого перемещения перейдет точка $G(P)$ при любой P . Другими словами, отображение H будет определено для любой точки P , если мы будем знать, куда оно переводит точку $G(P)$.

Поэтому, заменяя в формуле (1) точку P точкой $G(P)$, и учитывая, что $G^{-1} \cdot G(P) = P$, мы получим

$$H \cdot G(P) = G \cdot F(P). \quad (2)$$

Эта формула определяет перемещение $H(P)$. Обозначим $F(P) = Q$; тогда

$$H \cdot G(P) = G(Q),$$

т. е. перемещение H переводит точку $G(P)$ в точку $G(Q)$.

Предложение 1.2. Если F — поворот вокруг точки O на угол α , то H — поворот вокруг точки $G(O)$ также на угол α .

Доказательство. Так как F — поворот вокруг точки O , то $F(O) = O$, откуда по формуле (2)

$$H \cdot G(O) = G(O),$$

т. е. H есть поворот вокруг точки $G(O)$.

Поскольку перемещение переводит угол в конгруэнтный ему угол, то угол поворота H , по-прежнему, равен α , что и требовалось доказать.

Следствие. Трансформация группы поворотов плоскости вокруг точки P при помощи произвольного перемещения F есть группа поворотов плоскости вокруг точки $F(P)$. В частности, никакая группа поворотов не является инвариантной подгруппой в $E_0(2)$.

Рассмотрим теперь группу параллельных переносов. Для нее справедливо следующее утверждение.

Предложение 1.3. Группа $T(2)$ всех параллельных переносов плоскости является инвариантной подгруппой в группе $E_0(2)$.

Доказательство. Пусть F — некоторый параллельный перенос, а G — произвольное перемещение плоскости. Пусть l — некоторая прямая, параллельная вектору переноса F . Тогда имеет место равенство

$$F(l) = l,$$

означающее, что при перемещении F прямая l переходит в себя. Перемещение G переводит прямую l в прямую $G(l)$. Из формулы (2), примененной к любой точке P прямой l , следует

$$H \cdot G(l) = G(l);$$

т. е. перемещение H переводит прямую $G(l)$ в себя и, следовательно, является параллельным переносом вдоль этой прямой. Поскольку G — перемещение, то расстояние между точками P и $Q = F(P)$ равно расстоянию между точками $G(P)$ и $G \cdot F(P)$, т. е. между $G(P)$ и $H \cdot G(P)$. Следовательно, вектор параллельного переноса H совпадает с вектором параллельного переноса F . Предложение доказано.

Выделив в группе $E_0(2)$ подгруппу $T(2)$ параллельных переносов и подгруппы поворотов вокруг раз-

личных точек, естественно задать такой вопрос: можно ли представить любое перемещение из $E_0(2)$ как композицию переноса из $T(2)$ и поворота вокруг некоторой фиксированной точки.

Ответ на этот вопрос является утвердительным, что вытекает из следующего предложения.

Предложение 1.4. Любое перемещение первого рода можно однозначно представить в виде композиции $R_0^\alpha \cdot T_a$ параллельного переноса и поворота вокруг фиксированной точки O плоскости.

Доказательство. Пусть F — некоторое перемещение первого рода, O' — прообраз точки O при перемещении F , т. е. $O' = F^{-1}(O)$. Рассмотрим композицию $T_{\overrightarrow{O'O}} \cdot F^{-1}$. Это перемещение, очевидно, оставляет точку O на месте и является перемещением первого рода. Поэтому $T_{\overrightarrow{O'O}} \cdot F^{-1}$ поворот. Так как перемещение, обратное повороту, есть поворот, мы получаем требуемую композицию. Единственность этой композиции непосредственно следует из единственности параллельного переноса $T_{\overrightarrow{O'O}}$. Предложение доказано.

Замечание. Верно, кроме того, и следующее утверждение: *любое перемещение первого рода однозначно разлагается в композицию $T_b \cdot R_0^\beta$ поворота вокруг фиксированной точки плоскости и параллельного переноса.* Для доказательства рассмотрим некоторое перемещение первого рода G . Пусть $G(O) = O'$. Тогда композиция $T_{\overrightarrow{O'O}} \cdot G$ переводит точку O в себя и, значит, есть поворот вокруг этой точки:

$$T_{\overrightarrow{O'O}} \cdot G = R_0^\beta.$$

Рассмотрим композицию поворота R_0^β и параллельного переноса $T_{\overrightarrow{O'O}}$. Имеем

$$T_{\overrightarrow{O'O}} \cdot R_0^\beta = T_{\overrightarrow{O'O}} \cdot T_{\overrightarrow{O'O}} \cdot G = G,$$

что и требовалось.

Пусть G_1 и G_2 — два перемещения из группы $E_0(2)$. В силу только что доказанного предложения $G_1 = R_0^\alpha \cdot T_a$ и $G_2 = R_0^\beta \cdot T_b$. Композиция $G_2 \cdot G_1$ этих перемещений, с одной стороны, есть перемещение $R_0^\beta \cdot T_b \cdot R_0^\alpha \cdot T_a$, а с другой стороны, согласно предложению $G_2 \cdot G_1 = R_0^\gamma \cdot T_c$ для некоторого угла γ и век-

тора c . Угол γ и вектор c нетрудно вычислить, зная углы α , β и векторы a , b . Мы оставляем читателю эти вычисления и укажем здесь лишь окончательный ответ:

$$\gamma = \alpha + \beta, \quad c = a + R_0^{-\alpha}(b).$$

Полученный результат можно сформулировать следующим образом. Каждый элемент группы $E_0(2)$ однозначно представляется в виде упорядоченной пары (R_0^α, T_a) , где $R_0^\alpha \in SO(2)$, $T_a \in T(2)$. Умножение упорядоченных пар (R_0^α, T_a) и (R_0^β, T_b) в группе $E_0(2)$ производится по формуле

$$(R_0^\beta, T_b) \cdot (R_0^\alpha, T_a) = (R_0^{\alpha+\beta}, T_{a+R_0^{-\alpha}(b)}).$$

2. Группа перемещений пространства. Аналогично перемещениям плоскости перемещения пространства определяются как преобразования пространства, сохраняющие расстояния между точками. К ним прежде всего относится *параллельный перенос* T_a на вектор a , определение которого дословно повторяет соответствующее определение для плоскости. Другими примерами перемещений пространства являются *поворот* R_l^α *вокруг оси* l *на угол* α , *винтовое перемещение* $S_{l,\alpha}^a$, *симметрия* S_π *относительно плоскости* π , *скользящая симметрия*, *поворотная симметрия*. Эти перемещения определяются следующим образом:

а) Поворот R_l^α вокруг оси l на угол α — это перемещение, состоящее в повороте каждой точки пространства в плоскости, проходящей через эту точку и перпендикулярной к данной прямой l (оси поворота), на данный угол α (угол поворота) вокруг точки пересечения этой плоскости с осью.

Ось и угол поворота задают поворот неоднозначно. Действительно, один и тот же результат можно получить, совершая поворот вокруг данной оси на угол α в одном направлении и на угол $2\pi - \alpha$ в другом направлении.

Впрочем, такая же неоднозначность существует и для поворотов на плоскости. Чтобы избежать этой неоднозначности, на плоскости вводят понятие положительного направления поворота — это поворот против часовой стрелки. В случае поворотов в пространстве поступают так: выбирают на оси поворота определенное направление и считают, что поворот является

положительным относительно данного направления на оси, если любая точка поворачивается в своей плоскости против часовой стрелки для зрителя, стоящего вдоль оси так, что направление от его ног к его голове и есть направление, которое было выбрано на оси.

В случае, когда угол поворота равен π , поворот называют *опрокидыванием* относительно данной оси¹⁾. В этом случае нет надобности указывать направление поворота. Опрокидывание R_l^π обладает следующим свойством: $R_l^\pi \cdot R_l^\pi = E$, где E — тождественное перемещение.

б) *Винтовым перемещением* $S_{l,a}^\alpha$ называется композиция поворота R_l^α вокруг оси l и параллельного переноса T_a , при условии, что вектор a параллелен оси поворота.

Порядок, в котором выполняются указанные перемещения, безразличен (что не имело бы места, если бы вектор a не был параллелен оси l).

Частными случаями винтового перемещения являются поворот и параллельный перенос.

Если задано некоторое винтовое перемещение, то тем самым задано и направление на оси поворота — это направление вектора a . В соответствии с этим винтовое перемещение называется *положительным* (правым) или *отрицательным* (левым), в зависимости от того, имеет ли данный поворот положительное или отрицательное направление оси по отношению к направлению a .

с) *Симметрия* S_π относительно плоскости π — это перемещение, которое оставляет все точки данной плоскости π на месте, а любую другую точку A пространства переводит в точку A' такую, что прямая (AA') перпендикулярна к плоскости π и $|AO| = |OA'|$, где O — точка пересечения прямой (AA') и плоскости π .

д) *Скольльзящая симметрия* — это композиция $T_a \cdot S_\pi = S_\pi \cdot T_a$, где вектор a параллелен плоскости π (благодаря чему порядок операций в композиции безразличен).

е) *Поворотная симметрия* — это композиция $R_l^{180^\circ} \cdot S_\pi = S_\pi \cdot R_l^{180^\circ}$, где ось l перпендикулярна к плоскости π (что снова делает безразличным порядок операций в композиции).

¹⁾ Другое название перемещения R_l^π — осевая симметрия.

Оказывается, что этими примерами исчерпываются все перемещения пространства; точнее, справедлива следующая теорема (которую мы приведем без доказательства).

Теорема 2.1. Любое перемещение пространства есть либо параллельный перенос, либо поворот вокруг оси, либо винтовое перемещение, либо симметрия относительно плоскости, либо скользящая симметрия, либо поворотная симметрия.

Чтобы идти дальше, нам понадобятся некоторые сведения о композициях пространственных перемещений.

Теорема 2.2. Композиция двух опрокидываний относительно различных осей представляет собой:

а) если оси параллельны — параллельный перенос, перпендикулярный к обеим осям, равный удвоенному переносу, переводящему первую ось во вторую;

б) если оси пересекаются — поворот вокруг общего перпендикуляра к обеим осям, проходящего через точку пересечения, на угол, равный удвоенному углу поворота, переводящего первую ось во вторую;

с) если оси не лежат в одной плоскости — винтовое перемещение, имеющее своей осью общий перпендикуляр к обеим осям и равное удвоенному винтовому перемещению¹⁾, переводящему первую ось во вторую²⁾.

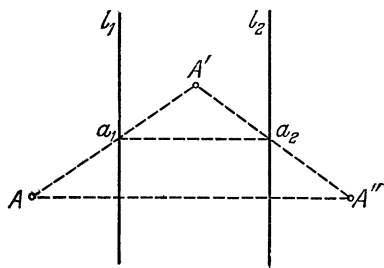


Рис. 17.

Доказательство. а) Пусть l_1 и l_2 — оси данных опрокидываний, A — некоторая точка пространства, a_1 — ее прямоугольная проекция на ось l_1 , A' — образ точки A при опрокидывании относительно оси l_1 , a_2 — прямоугольная проекция точки A' на ось l_2 и A'' — образ точки A' при опрокидывании относительно оси l_2 (рис. 17). Плоскость, перпендикулярная осям

¹⁾ Термин удвоенное винтовое перемещение означает следующее. Если $S_{l, \alpha}^a$ — некоторое винтовое перемещение, то удвоенное по отношению к $S_{l, \alpha}^a$ винтовое перемещение — это $S_{l, 2\alpha}^{2a}$.

²⁾ Существование такого перемещения будет следовать из доказательства теоремы.

l_1 и l_2 и проходящая через точку A , проходит через прямую (AA') перпендикулярную к l_1 , и через прямую (AA'') , перпендикулярную к l_2 . Поэтому прямая (a_1a_2) является общим перпендикуляром к прямым l_1 и l_2 , а точка A'' получается из точки A параллельным переносом, равным удвоенному переносу, переводящему прямую l_1 в прямую l_2 .

б) Пусть O — точка пересечения осей l_1 и l_2 , π — содержащая их плоскость, (OC) — перпендикуляр к этой плоскости, проходящей через точку O (рис. 18). Пусть, далее A — произвольная точка пространства, A' — ее образ при опрокидывании относительно оси l_1 (причем прямая (AA') пересекает ось l_1 в точке a_1) и A'' — образ точки A' при опрокидывании относительно оси l_2 (причем прямая $(A'A'')$ пересекает ось l_2 в точке a_2).

Опрокидывания относительно осей l_1 и l_2 переводят плоскость π в себя. Поэтому если мы спроектируем

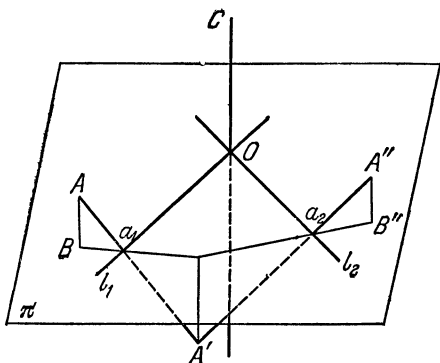


Рис. 18.

точки A , A' , A'' на эту плоскость в точки B , B' и B'' , то точки B и B'' будут получаться из B' с помощью опрокидываний относительно осей l_1 и l_2 соответственно. Значит, точка A'' получается из точки A поворотом вокруг оси (OC) на угол, равный удвоенному углу между l_1 и l_2 . Так как отрезки $[BA]$ и $[B''A'']$ конгруэнтны, параллельны (OC) и направлены в одну и ту же сторону, то этот же поворот вокруг оси (OC) совместит точку A с точкой A'' .

с) Пусть теперь оси l_1 и l_2 не лежат в одной плоскости. Обозначим через (O_1O_2) общий перпендикуляр

к l_1 и l_2 , причем точка O_1 лежит на оси l_1 , а точка O_2 лежит на оси l_2 (рис. 19). Проведем через точку O_2 прямую l'_1 , параллельную l_1 . Рассмотрим композицию следующих четырех опрокидываний: $R_{l_2}^\pi \cdot R_{l'_1}^\pi \cdot R_{l'_1}^\pi \cdot R_{l_1}^\pi$.

Так как $R_{l'_1}^\pi \cdot R_{l'_1}^\pi$ — тождественное преобразование, то эта композиция совпадает с искомой композицией $R_{l_2}^\pi \cdot R_{l_1}^\pi$. С другой стороны, $R_{l'_1}^\pi \cdot R_{l_1}^\pi$ есть параллельный перенос, равный удвоенному переносу, переводящему ось l_1 в ось l'_1 ; композиция же $R_{l_2}^\pi \cdot R_{l'_1}^\pi$ есть поворот вокруг прямой (O_1O_2) на угол, равный удвоенному углу между осями l'_1 и l_2 . Следовательно, исходная композиция $R_{l_2}^\pi \cdot R_{l_1}^\pi$ представляет собой винтовое перемещение, равное удвоенному винтовому перемещению, переводящему l_1 в l_2 . Теорема доказана.

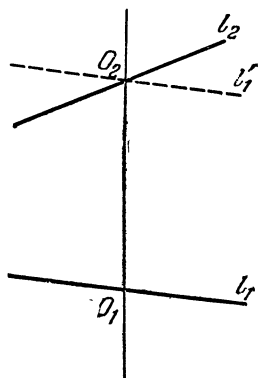


Рис. 19.

Последняя теорема позволяет разложить любое винтовое перемещение в композицию двух опрокидываний. Именно, имеет место следующее утверждение.

Теорема 2.3. Любое винтовое перемещение можно представить в виде композиции двух опрокидываний относительно двух различных прямых.

Эти прямые удовлетворяют следующим условиям:

а) если винтовое перемещение есть параллельный перенос, то они перпендикулярны к направлению перемещения;

б) если винтовое перемещение есть поворот или винтовое перемещение в собственном смысле слова, то они пересекают ось под прямым углом.

Одну из этих прямых можно выбрать в остальном произвольно; другая прямая при этом определяется однозначно.

С помощью теоремы 2.3 можно установить следующий важный результат.

Теорема 2.4. Композиция двух винтовых перемещений есть винтовое перемещение.

Если эти винтовые перемещения суть повороты вокруг осей, проходящих через одну точку, то их композиция есть также поворот вокруг оси, проходящей через ту же точку.

Если эти винтовые перемещения суть параллельные переносы, то их композиция также будет параллельным переносом.

Доказательство. Рассмотрим два винтовых перемещения, имеющих своими осями прямые l_1 и l_2 (рис. 20). Первое из них есть композиция двух опрокидываний относительно осей m_1 и m'_1 , причем m'_1 можно взять произвольно среди прямых, пересекающих l_1 под прямым углом. Аналогично, второе винтовое перемещение есть композиция опрокидываний относительно осей m_2 и m'_2 , причем m'_2 можно взять произвольно среди прямых, пересекающих l_2 под прямым углом.

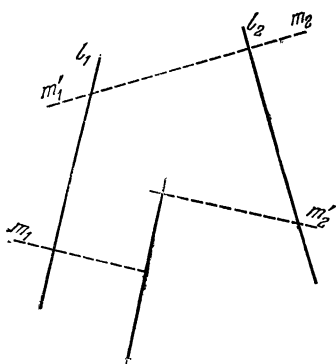


Рис. 20.

Совместим теперь прямые m'_1 и m_2 с общим

перпендикуляром к осям l_1 и l_2 . Тогда эти прямые совпадут и опрокидывания относительно них взаимно уничтожатся. В результате останутся лишь опрокидывания относительно прямых m_1 и m'_2 , композиция которых в силу теоремы 2.2 будет винтовым перемещением.

Если данные винтовые перемещения являются поворотами вокруг осей l_1 и l_2 , проходящих через точку O , то через эту же точку пройдут прямые m'_1 , m_1 и m'_2 . Поэтому композицией этих перемещений будет поворот вокруг оси, проходящей через точку O .

Если же данные перемещения суть параллельные переносы, то прямые m_1 , m'_1 и m'_2 параллельны между собой. Следовательно, результирующее перемещение также будет параллельным переносом, что и требовалось.

Рассмотрим теперь композицию двух симметрий S_{π_1} и S_{π_2} .

Теорема 2.5. Композиция $S_{\pi_2} \cdot S_{\pi_1}$ представляет собой:

а) если плоскости π_1 и π_2 параллельны — параллельный перенос, перпендикулярный к обоим плоскостям и равный удвоенному переносу, переводящему плоскость π_1 в плоскость π_2 ;

б) если плоскости π_1 и π_2 пересекаются по прямой l — поворот вокруг l на угол, равный удвоенному углу между плоскостями π_1 и π_2 .

Доказательство. Пусть A — некоторая точка пространства. Так как симметрии S_{π_1} и S_{π_2} переводят в себя плоскость, проходящую через A и перпендикулярную к плоскостям π_1 и π_2 , то теорема сводится к изучению композиции двух осевых симметрий на плоскости. Эта композиция есть либо параллельный перенос, перпендикулярный к осям, равный удвоенному переносу, переводящему первую ось во вторую, либо же поворот вокруг точки пересечения осей на удвоенный угол между ними. Отсюда следует утверждение теоремы.

Теорема 2.5 позволяет представить параллельный перенос и поворот в виде композиции двух симметрий. В частности, опрокидывание есть композиция двух симметрий относительно перпендикулярных плоскостей. Так как винтовое перемещение представляет собой композицию двух опрокидываний, то его можно разложить в композицию четырех симметрий.

Назовем параллельный перенос, поворот и винтовое перемещение — *перемещениями первого рода*, а симметрию относительно плоскости, скользящую симметрию и поворотную симметрию — *перемещениями второго рода*.

Так же как и для перемещений плоскости, имеет место следующее утверждение:

композиция двух перемещений первого рода есть перемещение первого рода, композиция перемещений первого рода и второго рода есть перемещение второго рода и композиция двух перемещений второго рода есть перемещение первого рода.

Доказательство этого утверждения аналогично доказательству соответствующего утверждения для плоскости. Прежде всего, в силу теоремы 2.5 любое перемещение пространства можно представить в виде композиции некоторого числа симметрий относительно различных плоскостей. Именно, параллельный перенос и поворот есть композиция двух таких симметрий,

винтовое перемещение — композиция четырех симметрий, сама симметрия — композиция одной симметрии, скользящая симметрия и поворотная симметрия — композиция трех симметрий. Следовательно, любое перемещение первого рода есть композиция четного числа симметрий, любое перемещение второго рода — композиция нечетного числа симметрий.

Обратное тоже верно: если перемещение есть композиция четного числа симметрий, то это перемещение первого рода; если же перемещение есть композиция нечетного числа симметрий, то это перемещение второго рода.

Для доказательства предположим, что некоторое перемещение разлагается в композицию симметрий двумя способами:

$$F = S_{2k} \cdot S_{2k-1} \cdot \dots \cdot S_2 \cdot S_1$$

и

$$F = S'_{2l+1} \cdot S'_{2l} \cdot \dots \cdot S'_2 \cdot S'_1,$$

причем в одном случае число этих симметрий четное, а в другом — нечетное. Тогда имеем тождество

$$S'_{2k} \cdot S_{2k-1} \cdot \dots \cdot S_2 \cdot S_1 = S'_{2l+1} \cdot S'_{2l} \cdot \dots \cdot S'_2 \cdot S'_1.$$

Рассмотрим композицию левой и правой части этого тождества с S'_{2l+1} . Учитывая, что $S'_{2l+1} \cdot S'_{2l+1} = E$ — тождественное перемещение, получим

$$S'_{2l+1} \cdot S_{2k} \cdot S_{2k-1} \cdot \dots \cdot S_2 \cdot S_1 = S'_{2l} \cdot \dots \cdot S'_2 \cdot S'_1,$$

т. е. мы «перенесли симметрию S'_{2l+1} в левую часть». Продолжая эту процедуру, в конце концов мы придем к тождеству

$$S'_1 \cdot S'_2 \cdot \dots \cdot S'_{2l} \cdot S'_{2l+1} \cdot S_{2k} \cdot S_{2k-1} \cdot \dots \cdot S_2 \cdot S_1 = E, \quad (3)$$

где в левой части стоит нечетное число симметрий. Доказав, что такое невозможно, мы получим, что для любого перемещения четность или нечетность числа симметрий, входящих в произвольное разложение этого перемещения в виде композиции симметрий, не зависит от конкретного разложения. Это и будет означать, что четность или нечетность числа симметрий полностью определяет род перемещения. Доказательство того, что тождество (3) не выполняется ни при каком выборе нечетного числа симметрий, мы оставляем читателю.

Из всего сказанного следует, что перемещение первого (второго) рода можно определить как перемеще-

ния, разлагающиеся в композиции четного (нечетного) числа симметрий, откуда немедленно вытекает требуемое утверждение.

Замечание 1. Тот факт, что композиция перемещений первого рода есть перемещение первого рода, непосредственно следует из теоремы 2.4, что является еще одним его доказательством.

Замечание 2. Мы не имеем возможности осветить в этом коротком добавлении все аспекты теории пространственных перемещений. Подробно эта теория изложена в уже упомянутой книге Коксетера «Введение в геометрию».

Так же как в случае плоскости, множество всех перемещений пространства образует группу, операций в которой является композиция перемещений. Эта группа обозначается $E(3)$.

Согласно сказанному выше множество всех перемещений первого рода образует подгруппу $E_0(3)$ в группе $E(3)$. Поскольку трансформация $G^{-1} \cdot F \cdot G$ произвольного перемещения первого рода есть снова перемещение первого рода, то эта подгруппа инвариантна в группе $E(3)$. Аналогично случаю плоскости существует ровно два класса по этой подгруппе: она сама и класс перемещений второго рода. Поэтому $E_0(3)$ имеет индекс 2 в группе $E(3)$ и факторгруппа $E(3)$ по $E_0(3)$ есть циклическая группа из двух элементов.

Рассмотрим теперь подгруппы группы $E_0(3)$. В качестве своей подгруппы эта группа содержит группу $T(3)$ всех параллельных переносов пространства. Этот факт непосредственно следует из теоремы 2.4, согласно которой композиция двух параллельных переносов есть снова параллельный перенос. Группа $T(3)$ коммутативна. Проще всего это установить, если заметить, что композиция двух параллельных переносов изображается диагональю параллелограмма, сторонами которых служат эти параллельные переносы.

Дословным повторением доказательства предложения 1.3 получается

Предложение 2.6. Группа $T(3)$ является инвариантной подгруппой в группе перемещений первого рода $E_0(3)$.

Бесконечную серию подгрупп группы $E_0(3)$ образуют подгруппы поворотов вокруг фиксированных осей. Действительно, если l — некоторая ось, R_l^α , R_l^β — два

поворота вокруг нее, то композиция $R_l^\alpha \cdot R_l^\beta$ есть поворот вокруг этой же оси на угол $\alpha + \beta$. Тожественное перемещение можно рассматривать как поворот вокруг оси l на нулевой угол. И, наконец, обратным к повороту R_l^α является поворот вокруг оси l на угол $-\alpha$. Поскольку $R_l^\alpha \cdot R_l^\beta = R_l^{\alpha+\beta} = R_l^{\beta+\alpha} = R_l^\beta \cdot R_l^\alpha$, то группа поворотов вокруг фиксированной оси коммутативна.

В качестве полезного упражнения предлагаем читателю доказать, что множество всех поворотов в пространстве подгруппы не образует. (Указание: проверить, что композиция двух поворотов вокруг осей, не лежащих в одной плоскости, представляет собой винтовое перемещение в собственном смысле слова; другими словами, в такую композицию входит нетождественный параллельный перенос.)

Более интересную серию подгрупп в $E_0(3)$ образуют перемещения первого рода, имеющие данную неподвижную точку. Пусть A — некоторая точка пространства. Рассмотрим все такие перемещения из $E_0(3)$, для которых точка A является неподвижной, т. е. такие перемещения F , что $F(A) = A$. Если F_1 и F_2 — два таких перемещения, то для $F_2 \cdot F_1$ имеем $F_2 \cdot F_1(A) = F_2(A) = A$. Значит, для $F_2 \cdot F_1$ точка A также является неподвижной. Ясно, что тождественное перемещение оставляет точку A на месте. Кроме того, если $F(A) = A$, то $F^{-1}(A) = A$. Это доказывается так:

Поскольку $F^{-1} \cdot F = E$ — тождественное перемещение, то

$$A = F^{-1} \cdot F(A) = F^{-1}(A).$$

Таким образом, перемещение, обратное к перемещению с неподвижной точкой A , само есть перемещение с неподвижной точкой A .

Итак, перемещения, имеющие данную неподвижную точку, образуют группу. Понятно, что эта группа является подгруппой в $E_0(3)$. Кроме того, любые такие подгруппы, одна из которых оставляет неподвижной какую-нибудь точку A , а другая — точку A' , — изоморфны между собой. Эти изоморфные группы принято обозначать $SO(3)$ или $SO(3)_A$, если мы хотим указать конкретную неподвижную точку A .

Группа $SO(3)_A$ содержит в качестве подгрупп все группы поворотов вокруг осей, проходящих через

точку A . Более подробная информация о группе $SO(3)_A$ получается из следующего предложения.

Предложение 2.7. Любое перемещение F из $SO(3)_A$ имеет вид

$$F = R_{l_2}^\beta \circ R_{l_1}^\alpha,$$

где l_1 и l_2 — некоторые прямые, проходящие через точку A .

Доказательство. Пусть B — некоторая точка пространства, отличная от A и $B' = F(B)$. Имеем $|AB| = |AB'|$; следовательно, точку B' можно совместить с точкой B посредством поворота $R_{l_2}^\gamma$ вокруг оси l_2 , перпендикулярной к плоскости BAB' (и проходящей через точку A) на угол γ , равный углу $\widehat{B'AB}$. Таким образом, композиция $R_{l_2}^\gamma \circ F$ оставляет на месте точки A и B , а значит, и любую точку прямой $l_1 = (AB)$. Следовательно, перемещение $R_{l_2}^\gamma \circ F$ есть поворот вокруг оси l_1 на некоторый угол α :

$$R_{l_2}^\gamma \circ F = R_{l_1}^\alpha.$$

Возьмем композицию этого поворота $R_{l_1}^\alpha$ и поворота $R_{l_2}^\beta = R_{l_2}^{-\gamma}$:

$$R_{l_2}^\beta \circ R_{l_1}^\alpha = R_{l_2}^{-\gamma} \circ R_{l_1}^\alpha = R_{l_2}^{-\gamma} \circ R_{l_2}^\gamma \circ F = R_{l_2}^{-\gamma + \gamma} \circ F = F,$$

что и требовалось доказать.

Выясним теперь, что происходит при трансформации группы $SO(3)_A$ некоторым элементом $G \in E_0(3)$. Прежде всего заметим, что для перемещений пространства дословно остаются в силе рассуждения, предшествующие предложению 1.2 предыдущего пункта. Именно, если F и G два перемещения из $E_0(3)$ и $H = G \circ F \circ G^{-1}$, то перемещение H полностью определяется формулой

$$H \circ G(P) = G \circ F(P),$$

совпадающей с формулой (2) предыдущего пункта. Поэтому имеет место следующее утверждение.

Предложение 2.8. Если F — перемещение из $SO(3)_A$, то $H = G \circ F \circ G^{-1}$ есть перемещение из группы $SO(3)_{G(A)}$.

Доказательство. Так как $F(A) = A$, то указанная выше формула принимает вид

$$H \cdot G(A) = G \cdot F(A) = G(A),$$

т. е. перемещение H оставляет неподвижной точку $G(A)$. Следовательно, $H \in \mathbf{SO}(3)_{G(A)}$.

Из этого предложения вытекает, в частности, что никакая из групп $\mathbf{SO}(3)_A$ не является инвариантной подгруппой в $E_0(3)$.

Замечание. Предложение 2.8 можно усилить. Именно, можно показать, что если перемещение $F \in \mathbf{SO}(3)_A$ разложено в композицию $F = R_{l_2}^\beta \cdot R_{l_1}^\alpha$, то $H \in \mathbf{SO}(3)_{G(A)}$ представляется в виде композиции $H = R_{m_2}^\beta \cdot R_{m_1}^\alpha$, где прямые m_1 и m_2 проходят через точку $G(A)$, причем угол между этими прямыми равен углу между прямыми l_1 и l_2 . Доказательство этого утверждения мы оставляем читателю.

И, наконец, имеет место предложение, аналогичное предложению 1.4.

Предложение 2.9. (1) Любое перемещение из $E_0(3)$ однозначным образом представляется в виде композиции

$$F \cdot T_a,$$

где $F \in \mathbf{SO}(3)_A$ — перемещение, имеющее данную неподвижную точку A , а T_a — параллельный перенос.

(2) Любое перемещение из $E_0(3)$ однозначным образом представляется в виде композиции

$$T_b \cdot G,$$

где $G \in \mathbf{SO}(3)_A$ — перемещение, имеющее данную неподвижную точку A , а T_b — параллельный перенос.

Доказательство этого предложения почти дословно совпадает с доказательством предложения 1.4 и поэтому мы его опускаем.

3. Конечные подгруппы группы перемещений пространства. В главе V были рассмотрены группы самосовмещений правильных пирамид, группы диэдров (двойных пирамид) и группы самосовмещений правильных многогранников. Все эти группы имели конечный порядок. Решим теперь обратную задачу: найти все группы, состоящие из конечного числа перемещений пространства. Оказывается, что это именно только что пере-

численные группы и никакие другие. Тем самым мы получаем полный список конечных подгрупп группы перемещений пространства.

Пусть G — такая конечная группа. Установим прежде всего следующий результат.

Предложение 3.1. Группа G состоит только из поворотов пространства.

Доказательство. Пусть X — некоторое перемещение, содержащееся в группе G ; тогда G будет содержать также и все последовательные степени X^2, X^3, \dots перемещения X . Поэтому прежде всего необходимо, чтобы среди этих степеней было конечное число различных элементов. Следовательно, перемещение X не может быть параллельным переносом.

Действительно, предполагая противное, обозначим через a длину вектора параллельного переноса X . Степени X также будут параллельными переносами, длины векторов которых равны $2a, 3a$ и т. д. Все эти параллельные переносы различны между собой и их имеется бесконечное число.

Далее, перемещение X не может быть винтовым перемещением. В самом деле, если обозначить через a длину вектора параллельного переноса, входящего в винтовое перемещение X , то перемещения X^2, X^3 и т. д. будут содержать параллельные переносы, длины векторов которых равны $2a, 3a, \dots$. Следовательно, все такие винтовые перемещения будут различны. Остаются только повороты. Предложение доказано.

Предложение 3.2. Все повороты группы G , имеющие общую ось, являются степенями одного из них, именно того, которому соответствует наименьший угол поворота.

Доказательство. Пусть $A \subset G$ — подмножество поворотов из группы G , имеющих общую ось, $R \in A$ — поворот, имеющий наименьший угол α . Покажем, что $\alpha = \frac{2\pi}{n}$, где n — положительное целое число. Действительно, в противном случае мы имели бы $k\alpha < 2\pi < (k+1)\alpha$ (k — целое число). Поэтому углы $\alpha_1 = 2\pi - k\alpha$ и $\alpha_2 = (k+1)\alpha - 2\pi$ были бы отличны от нуля и не превышали угла α . Кроме того, углы α_1 и α_2 были бы углами поворотов около той же оси, что противоречит предположению,

Итак, мы показали, что поворот R , имеющий наименьший угол среди всех поворотов с общей осью, удовлетворяет условию $R^n = E$.

Докажем теперь, что всякий поворот из множества A является степенью R . Действительно, если это не так, то аналогично только что доказанному соответствующий повороту угол β будет удовлетворять неравенствам $m\alpha < \beta < (m+1)\alpha$. Значит, поворот, которому соответствует угол $\beta - m\alpha$, и который, очевидно, принадлежит множеству A , будет иметь угол, строго меньший α . Предложение доказано.

Число n , фигурирующее в этом предложении (т. е. такое наименьшее положительное число, что $R^n = E$), называется **порядком поворота**.

Предложение 3.3. *Оси всех поворотов, принадлежащих группе Γ , проходят через одну точку.*

Доказательство. Пусть R_1 и R_2 — два поворота из группы Γ . Покажем прежде всего, что их оси лежат в одной плоскости. Предположим противное, т. е., что оси l_1 и l_2 поворотов R_1 и R_2 являются скрещивающимися прямыми. Согласно теореме 2.3 поворот R_1 есть композиция двух опрокидываний относительно пересекающихся осей m_1 и m'_1 , пересекающих l_1 под прямыми углами, причем m'_1 можно взять произвольно. Точно так же поворот R_2 есть композиция двух опрокидываний относительно пересекающихся осей m_2 и m'_2 , пересекающих l_2 под прямыми углами, причем m'_2 можно выбрать произвольно. Совместим прямые m'_1 и m'_2 с общим перпендикуляром к осям l_1 и l_2 . Опрокидывания относительно них взаимно уничтожаются, так что композиция $R_2 \circ R_1$ представляет собой композицию опрокидываний относительно прямых m_1 и m_2 . Прямые m_1 и m_2 не могут пересекаться. В противном случае определяемая ими плоскость содержала бы общий перпендикуляр к l_1 и l_2 . Поэтому прямые l_1 и l_2 оказались бы перпендикулярными к этой плоскости (как прямые, перпендикулярные каждой к двум прямым, лежащим в плоскости) и, значит, параллельными в противоречие с предположением. Следовательно, прямые m_1 и m_2 не имеют общих точек, т. е. $R_2 \circ R_1$ не является поворотом.

Итак, мы доказали, что оси любых двух поворотов из группы Γ лежат в одной плоскости.

Далее, эти оси не могут быть параллельными. Действительно, если бы повороты R_1 и R_2 вокруг

параллельных осей имели равные, но имеющие противоположные направления углы поворота, то $R_2 \circ R_1$ было бы нетождественным параллельным переносом. Если же повороты R_1 и R_2 вокруг параллельных осей имели бы неравные углы или же равные и одинаково направленные углы, то композиции $R_1 \circ R_2$ и $R_2 \circ R_1$ были бы поворотами на один и тот же угол вокруг различных осей, так что композиция $R_1 \circ R_2 \circ (R_2 \circ R_1)^{-1} = R_1 \circ R_2 \circ R_1^{-1} \circ R_2^{-1}$ (очевидно, принадлежащая группе Γ) была бы нетождественным параллельным переносом.

Итак, *оси двух поворотов обязательно пересекаются в некоторой точке O .*

Покажем теперь, что в группе Γ содержится поворот R , ось которого проходит через точку O и не лежит в плоскости, проходящей через оси поворотов R_1 и R_2 .

В самом деле, если R_1 и R_2 — опрокидывания, то таким поворотом будет композиция $R_2 \circ R_1$. В противном случае, если один из поворотов, скажем, R_1 , не является опрокидыванием, то таким поворотом будет $R_1 \circ R_2 \circ R_1^{-1}$. Следовательно, ось любого поворота из группы Γ должна проходить через точку O , так как она должна пересекать оси поворотов R_1 , R_2 и R . Предложение 3.3 доказано.

Пусть O — точка пересечения всех осей поворотов, принадлежащих группе Γ . Примем эту точку за центр сферы S единичного радиуса. Для того чтобы изучить повороты, принадлежащие Γ , достаточно изучить их действие на сфере S .

Любая ось поворота пересекает сферу S в двух точках. Очевидно, что эти точки будут единственными неподвижными относительно данного поворота точками на сфере. Назовем их *полюсами данного поворота*. Полус поворота может принадлежать сразу нескольким поворотам группы Γ . Пусть, например, некоторому полюсу соответствуют повороты R_1, \dots, R_k с углами $\alpha_1, \dots, \alpha_k$, причем угол α_1 наименьший из них. Тогда α_1 необходимо имеет вид $\alpha_1 = \frac{2\pi}{n}$ (n — целое положительное число). Действительно, если бы было не так, т. е. $\alpha_1 = \frac{m}{n} 2\pi$, где m и n — взаимно простые¹⁾, то в

¹⁾ То есть наибольший общий делитель m и n равен единице.

группе Γ содержался бы поворот на угол, строго меньший α_1 .

Для того чтобы доказать это, будем считать, что $m < n$ (случай $m > n$ рассматривается аналогично). Представим число n в виде

$$n = lm + r,$$

где $0 < r < m$, и рассмотрим поворот R_1^{-l} , очевидно принадлежащий группе Γ . Наименьший положительный угол этого поворота равен

$$2\pi - \frac{lm}{n} 2\pi = 2\pi \frac{n-lm}{n} = \frac{r}{n} \cdot 2\pi < \alpha_1,$$

что и требовалось доказать.

Все остальные повороты R_2, \dots, R_k будут степенями поворота R_1 . Действительно, если бы угол β , соответствующий одному из этих поворотов, удовлетворял неравенствам

$$\frac{m}{n} \cdot 2\pi < \beta < \frac{m+1}{n} 2\pi,$$

то, взяв композицию этого поворота и поворота R_1^{-m} , мы получили бы поворот той же оси на угол, строго меньший $\frac{2\pi}{n} = \alpha_1$, что противоречит сделанному предположению.

Назовем число n **порядком** данного полюса поворота. Легко видеть, что полюс n -го порядка принадлежит $n-1$ поворотам, не считая тождественного.

Нашей ближайшей целью является получение формулы, связывающей порядок N группы Γ и порядки n_1, \dots, n_k различных полюсов поворота. Для этого введем следующее определение. Точки P_1 и P_2 на сфере S называются *эквивалентными* относительно группы Γ , если существует такой поворот $R \in \Gamma$, что $R(P_1) = P_2$. Таким образом, любая точка P на сфере S имеет N эквивалентных ей точек, которые получатся, если применять к P все повороты из группы Γ . Если точка P не является полюсом, то все эквивалентные ей точки различны между собой. В самом деле, если несколько эквивалентных точек совпадают с точкой P' , то эта точка будет полюсом некоторого поворота R' , но тогда точка P будет полюсом поворота R .

Если же точка P есть полюс n -го порядка для поворота R , то она совпадает с $n-1$ эквивалентными

ей точками. Пусть теперь P' — некоторая точка, эквивалентная точке P и получающаяся из нее поворотом R' : $P' = R'(P)$. Тогда n из точек, эквивалентных точке P , а именно точки $R'(P)$, $RR'(P)$, $R^2R'(P)$, ..., $R^{n-1}R'(P)$, будут совпадать с точкой P' .

Других точек, эквивалентных точке P и совпадающих с P' , не существует. Действительно, если бы такие точки существовали, то P' была бы полюсом поворота порядка m , причем $m > n$. Но тогда и точка P , которая получается из P' поворотом $(R')^{-1}$, была бы полюсом поворота порядка m . Следовательно, все N точек, эквивалентных полюсу n -го порядка P , по n совпадают между собой. Таким образом, в этом случае точка P имеет всего лишь $\frac{N}{n}$ различных эквивалентных ей точек, учитывая и самую точку P .

Пусть теперь P_1, \dots, P_k — неэквивалентные полюсы поворотов, входящих в группу Γ , n_1, \dots, n_k — порядки этих полюсов и N — порядок группы Γ .

Предложение 3.4. Числа N, n_1, \dots, n_k связаны между собою следующим соотношением:

$$\left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right) + \dots + \left(1 - \frac{1}{n_k}\right) = 2 - \frac{2}{N}. \quad (4)$$

Доказательство. Подсчитаем число поворотов, которым принадлежат данные неэквивалентные полюсы P_1, \dots, P_k . Полюс P_1 имеет порядок n_1 ; только что мы установили, что эта точка имеет $\frac{N}{n_1}$ различных эквивалентных ей точек. В то же время P_1 есть полюс $n_1 - 1$ поворотов, не считая тождественного. Каждая из точек, эквивалентных точке P_1 , также будет полюсом $n_1 - 1$ поворотов. Поэтому всего мы имеем $\frac{N}{n_1}(n_1 - 1) = N\left(1 - \frac{1}{n_1}\right)$ поворотов. Аналогичные вычисления можно проделать и для всех остальных полюсов, в результате чего мы получим полное число поворотов

$$N \left[\left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right) + \dots + \left(1 - \frac{1}{n_k}\right) \right].$$

В это число не вошел тождественный поворот, зато каждый из $N - 1$ оставшихся поворотов вошел ровно

два раза (ведь все полюсы разбиваются на пары диаметрально противоположных). Следовательно,

$$N \left[\left(1 - \frac{1}{n_1} \right) + \left(1 - \frac{1}{n_2} \right) + \dots + \left(1 - \frac{1}{n_k} \right) \right] = 2(N-1),$$

откуда

$$\left(1 - \frac{1}{n_1} \right) + \left(1 - \frac{1}{n_2} \right) + \dots + \left(1 - \frac{1}{n_k} \right) = 2 - \frac{2}{N},$$

что и требовалось доказать.

Соотношение (4) позволяет описать все конечные подгруппы группы перемещений пространства.

Теорема 3.5. *Конечные циклические группы (группы правильных пирамид), группы диэдров и группы правильных многогранников являются единственными конечными подгруппами группы перемещений пространства.*

Доказательство. Так как числа n_1, \dots, n_k в соотношении (4) больше или равны 2, то $1 - \frac{1}{n_j} > \frac{1}{2}$ для всех $j = 1, \dots, k$. Поэтому число k не может превосходить трех, поскольку правая часть $2 - \frac{2}{N}$ соотношения (4) строго меньше 2. В то же время $2 - \frac{2}{N} \geq 1$, а каждая из скобок в левой части (4) меньше 1. Следовательно, число k не может быть равным 1. Итак, для числа k имеются две возможности: $k = 2$ и $k = 3$.

I. $k = 2$. В этом случае соотношение (4) превращается в

$$\left(1 - \frac{1}{n_1} \right) + \left(1 - \frac{1}{n_2} \right) = 2 - \frac{2}{N}$$

или в

$$\frac{1}{n_1} + \frac{1}{n_2} = \frac{2}{N}. \quad (5)$$

Уравнение (5) имеет единственное решение $n_1 = n_2 = N$. Действительно, в противном случае одно из чисел n_1 или n_2 превосходило бы N , что невозможно, поскольку N должно быть кратным чисел n_1 и n_2 .

Так как $\frac{N}{n_1} = \frac{N}{n_2} = 1$, то имеется всего лишь два различных полюса поворота и, значит, единственная ось поворота.

Все повороты вокруг этой оси представляют собой степени данного из них, т. е. мы имеем циклическую группу конечного порядка. Такую группу образуют самосовмещения правильного многогранного угла или, что то же самое, самосовмещения правильной пирамиды (см. § 3, гл. V).

II. $k=3$. В этом случае по крайней мере одно из чисел n_1 , n_2 или n_3 равно 2, так как если бы одновременно $n_1 \geq 3$, $n_2 \geq 3$ и $n_3 \geq 3$, то $1 - \frac{1}{n_1} \geq \frac{2}{3}$, $1 - \frac{1}{n_2} \geq \frac{2}{3}$, $1 - \frac{1}{n_3} \geq \frac{2}{3}$, откуда

$$\left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right) + \left(1 - \frac{1}{n_3}\right) \geq 2,$$

что невозможно. Положим $n_3 = 2$. Тогда соотношение (4) примет вид

$$\left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right) + \left(1 - \frac{1}{2}\right) = 2 - \frac{2}{N}$$

или

$$\frac{1}{n_1} + \frac{1}{n_2} = \frac{1}{2} + \frac{2}{N}. \quad (6)$$

Решим уравнение (6) в целых положительных числах. Прежде всего заметим, что если одно из искоемых чисел, например, n_1 , равно 2, то другое число n_2 находится из формулы

$$n_2 = \frac{N}{2}.$$

В этом случае имеются два полюса и, следовательно, единственная ось n_2 -го порядка. Все остальные повороты, оси которых отличны от этой оси, будут опрокидываниями. Очевидно, что оси этих опрокидываний будут перпендикулярны к оси n_2 -го порядка и составляют между собой равные углы.

Такую группу образуют самосовмещения правильного многоугольника в трехмерном пространстве или двойной пирамиды (диздра), см. § 3, гл. V.

Итак, мы рассмотрели случай, когда одно из чисел n_1 или n_2 равно 2. Исключая его, мы имеем одновременно $n_1 \geq 3$ и $n_2 \geq 3$. Однако оба эти числа не могут быть больше 3, так как для $n_1 \geq 4$ и $n_2 \geq 4$ мы имеем $\frac{1}{n_1} + \frac{1}{n_2} \leq \frac{1}{2} < \frac{1}{2} + \frac{2}{N}$. Следовательно, по крайней

мере одно из чисел n_1 и n_2 равно 3. Будем считать, что это число n_1 (в противном случае можно поменять местами в уравнении (6) числа n_1 и n_2); тогда

$$\frac{1}{3} + \frac{1}{n_2} = \frac{1}{2} + \frac{2}{N} > \frac{1}{2},$$

откуда $n_2 < 6$. Итак, n_2 может принимать только три значения, 3, 4, 5. Поэтому (с учетом симметрии уравнения (6) относительно переменных n_1 и n_2) мы получаем следующие пять решений:

- 1) $n_1 = n_2 = 3, N = 12$;
- 2) $n_1 = 3, n_2 = 4, N = 24$;
- 3) $n_1 = 4, n_2 = 3, N = 24$;
- 4) $n_1 = 3, n_2 = 5, N = 60$;
- 5) $n_1 = 5, n_2 = 3, N = 60$.

Для того чтобы завершить доказательство теоремы нужно показать еще, что каждому полученному таким образом решению соответствует некоторый правильный многогранник, и, следовательно, группа всех его самосмещений. Эту часть доказательства мы опускаем — она требует средств, несколько выходящих за рамки настоящей книги. Полное доказательство читатель найдет во втором томе «Элементарной геометрии» Ж. Адамара.

В заключение отметим, что перечисленными подгруппами отнюдь не исчерпывается множество всех подгрупп, лежащих в группах $E(2)$ и $E(3)$. Среди всех подгрупп $E(2)$ и $E(3)$ особое значение для различных областей естествознания имеют так называемые кристаллографические группы. Они определяются следующим образом.

Назовем *пространственной решеткой Бравэ* (или *пространственным кристаллом*) множество L , образованное всеми точками пространства с радиусами-векторами R вида

$$R = n_1 e_1 + n_2 e_2 + n_3 e_3,$$

где e_1, e_2 и e_3 — три некопланарных вектора, а n_1, n_2 и n_3 — всевозможные целые числа. Аналогично определяется *плоская решетка Бравэ* (*плоский кристалл*).

Множество перемещений пространства (соответственно плоскости), переводящих решетку L в себя, называется *пространственной кристаллографической группой* (соответственно *плоской кристаллографической группой*) и

обозначается через $G_3(L)$ (соответственно $G_2(L)$). Ясно, что множество $G_3(L)$ (соответственно $G_2(L)$) является подгруппой группы $E(3)$ (соответственно группы $E(2)$).

Аналогично тому, как мы описали конечные группы перемещений, можно получить полную классификацию всех кристаллографических групп (правда, затратив на это значительно больше времени и усилий). Оказывается, что существуют ровно 17 неизоморфных друг другу плоских кристаллографических групп и 230 неизоморфных пространственных кристаллографических групп. Каждой из этих групп отвечает соответствующая плоская или пространственная решетка. Интересно отметить, что эти плоские решетки были обнаружены еще в древности египетскими архитекторами и художниками, в то время как классификация трехмерных решеток была получена лишь в конце прошлого столетия.

Павел Сергеевич Александров
ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП

М., 1980 г., 144 стр. с илл.

(Серия: Библиотечка «Квант»)

Редактор *В. Ф. Пахомов*

Техн. редактор *Е. В. Морозова*

Корректор *Т. С. Вайсберг*

ИБ № 11625

Сдано в набор 29.04.80. Подписано к печати 28.07.80. Т-14613. Бумага $84 \times 108 \frac{1}{32}$, тип. № 1. Литературная гарнитура. Высокая печать. Услови. печ. л. 7,56. Уч.-изд. л. 7,46. Тираж 100 000 экз. Заказ № 1312. Цена 25 коп.

Издательство «Наука»

Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

Ордена Октябрьской Революции, ордена Трудового Красного Знамени Ленинградское производственно-техническое объединение «Печатный Двор» имени А. М. Горького «Союзполиграфпрома» при Государственном комитете СССР по делам издательств, полиграфии и книжной торговли. 197136, Ленинград, П-136, Чкаловский пр., 15.

25 коп.

БИБЛИОТЕЧКА «КВАНТ»

ВЫШЛИ ИЗ ПЕЧАТИ

Вып. 1. М. П. Бронштейн. Атомы и электроны.

Вып. 2. М. Фарадей. История свечи.

Вып. 3. О. Оре. Приглашение в теорию чисел.

Вып. 4. Опыты в домашней лаборатории.

**Вып. 5. Л. Г. Асламазов, И. Ш. Слободецкий.
Задачи по физике.**

Вып. 6. Л. П. Мочалов. Головоломки.

Вып. 7. П. С. Александров. Введение в теорию групп.

ГОТОВЯТСЯ К ПЕЧАТИ В 1980 г.

Вып. 8. Г. Штейнгауз. Математический калейдоскоп.

Вып. 9. Замечательные ученые.

**Вып. 10. В. М. Глушков, В. Я. Валах. Что такое
ОГАС!**