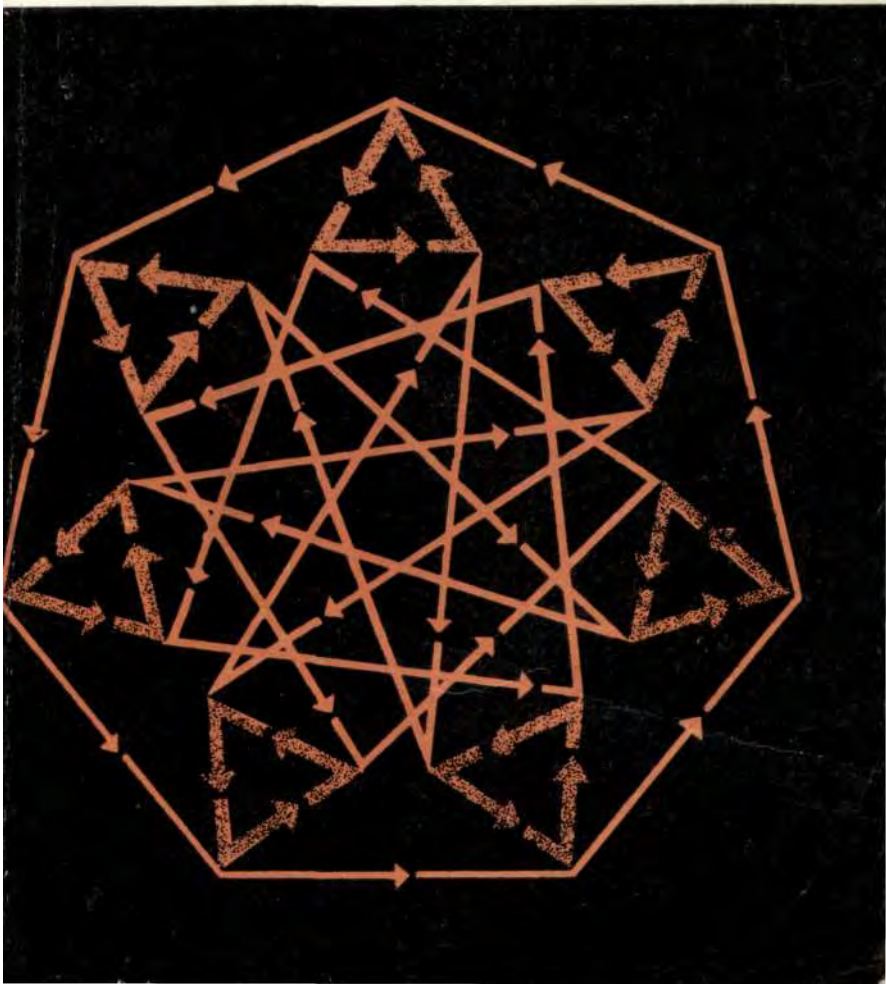
И. ГРОССМАН
В. МАГНУС

СОВРЕМЕННАЯ МАТЕМАТИКА
ПОПУЛЯРНАЯ СЕРИЯ

# ГРУППЫ И ИХ ГРАФЫ



# GROUPS

and

# THEIR GRAPHS

by

**I. GROSSMAN**

*Albert Leonard Junior High School*

and

**W. MAGNUS**

*New York University*

RANDOM HOUSE

The L. W. Singer Company

1964

«СОВРЕМЕННАЯ МАТЕМАТИКА»

*Популярная серия*

И. ГРОССМАН, В. МАГНУС

# Группы и их графы

*Перевод с английского*
*Г. М. Цукерман*

*Под редакцией*
*В. Е. Тараканова*

ИЗДАТЕЛЬСТВО «МИР»
*Москва 1971*

брасывая лишь сжатый его план или даже ограничиваясь примерами. Более прочному закреплению основных понятий способствуют упражнения, немногочисленные, но тщательно подобранные; решение их принесет читателю большую пользу.

Книга не требует от читателей никаких специальных знаний, выходящих за пределы программы старших классов средней школы. Она может быть с интересом прочитана студентами младших курсов университетов, педагогических и технических вузов, а также использована в работе школьных математических кружков. Для тех, кто заинтересуется теорией групп и пожелает подробнее познакомиться с этой прекрасной областью математики, в конце книги приведен список литературы.

*В. Тараканов*

# ПРЕДИСЛОВИЕ

У школьников обычно складывается впечатление, что математика занимается исключительно числами и измерениями. Однако на самом деле математика — это нечто гораздо большее, чем просто наука для счетоводов и кассиров; скорее, она имеет дело с логикой и качественными связями между понятиями.

Теория групп — один из важных разделов «неколичественной» (если можно так сказать) математики. Хотя понятие группы появилось в математике сравнительно недавно, оно оказалось на редкость плодотворным. Например, теория групп дала мощные средства для исследования алгебраических уравнений, геометрических преобразований, а также для решения ряда задач топологии и теории чисел.

Две особенности теории групп привели к тому, что создалась традиция откладывать ее изучение на более поздние этапы. Первая из них — это высокая степень абстракции, свойственная теоретико-групповым понятиям, а умение обращаться с абстрактными понятиями приходит с математической зрелостью. Вторая особенность состоит в том, что теория групп имеет глубокие связи с другими областями науки, проследить которые можно лишь тогда, когда учащийся уже знаком с основами этих наук.

В этой книге мы старались изложить теорию групп в форме, доступной для начинающих читателей. Чтобы обойти трудности, связанные с абстрактным характером понятий, мы прибегли к наглядным образам — графам групп. При этом абстрактная группа обрела конкретное представление, отражающее ее групповую структуру. Конечно, не приходится рассчитывать, что это обращение к наглядности позволит избежать серьезного изучения теории, без которого нельзя овладеть основными понятиями в любой области математики. Мы лишь попытались ма-

ксимально использовать наглядность, чтобы лучше разъяснить смысл некоторых теорем и понятий.

Мы сознаем, что нам далеко не всегда удалось показать, как понятия теории групп связаны с практикой. В конечном счете нам пришлось положиться на внутреннюю привлекательность самой теории. И, разумеется, самое главное — это заинтересованность, которую должен проявить сам читатель.

ГЛАВА 1

# ВВЕДЕНИЕ

Теория групп начала оформляться в качестве самостоятельного раздела математики в конце восемнадцатого века. В течение первых десятилетий девятнадцатого века она развивалась медленно и практически не привлекала к себе внимания. Но затем, около 1830 года, благодаря работам Галуа и Абеля о разрешимости алгебраических уравнений всего за несколько лет она совершила гигантский скачок, который оказал глубокое влияние на развитие всей математики.

С тех пор основные понятия теории групп стали детально исследоваться. Постепенно они проникли во многие разделы математики и нашли применение в таких различных областях знания, как, например, квантовая механика, кристаллография и теория узлов.

Эта книга посвящена группам и их графическому представлению. Наша первая задача — выяснить, что же такое «группа».

Основная идея дальнейших рассмотрений, проникающая в самую сущность понятия группы, связана с концепцией структуры. Перед читателем развернется ряд примеров и пояснений, определений и теорем, варьирующих одну основную тему — как группы и их графы представляют и иллюстрируют одну из разновидностей математической структуры.

До сих пор мы употребляли слово «группа», не давая читателю ни малейшего намека на то, что́ же оно может означать. Если дать сразу полное формальное определение, то читатель, вероятно, останется в таком же недоумении, как и прежде. Поэтому мы

будем развивать понятие группы постепенно и начнем с двух примеров. (Читателю следует помнить о них во время дальнейшего первоначального обсуждения структурных признаков группы.)

**Группа *A*:** *Множество* всех целых чисел, рассматриваемых как числа, которые можно *складывать* одно с другим. Другими словами, элементами группы $A$ являются целые числа $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, и единственная *операция*, которую мы сейчас рассматриваем, — это сложение *любых двух элементов указанного множества*; например, $2 + 5 = 7$.

**Группа *B*:** *Множество* всех положительных рациональных чисел, рассматриваемых как числа, которые можно *умножать* одно на другое. В этом случае элементами множества являются все числа, которые можно представить в виде $a/b$, где $a$ и $b$ — положительные целые числа, и единственная *операция*, которую мы здесь рассматриваем, — это умножение *любых двух элементов данного множества*; например, $\frac{2}{3} \cdot \frac{5}{8} = \frac{5}{12}$.

Теперь читатель познакомился с примерами групп, но, вероятно, все еще не слишком приблизился к пониманию того, что же такое группа, поскольку, быть может, не смог сразу выделить в этих примерах то существенное, что определяет группу. В приведенном описании групп $A$ и $B$ некоторые слова были выделены курсивом, чтобы подчеркнуть основные структурные признаки, присущие всем группам, а именно: 1) наличие множества элементов и 2) наличие бинарной операции:

*Множество* элементов:
- группа $A$ — все целые числа,
- группа $B$ — все положительные рациональные числа;

*Бинарная операция* на множестве:
- группа $A$ — сложение любых двух целых чисел,
- группа $B$ — умножение любых двух положительных рациональных чисел.

Мы назвали операции в группах $A$ и $B$ *бинарными*, поскольку в каждой из них участвуют одновременно *два* элемента.

*Бинарная операция на множестве* — это *соответствие*, при котором каждой упорядоченной *паре* элементов данного множества отвечает однозначно определенный элемент этого же множества. Так, в группе $A$ сложение есть бинарная операция *на множестве целых* чисел; в самом деле, если $r$ и $s$ — любые два элемента этого множества, то $r + s$ *также является элементом этого множества.* Обозначив элемент $r + s$ символом $t$, можно перефразировать это следующим образом: если $r$ и $s$ — два произвольных элемента множества, то существует один и только один элемент $t$ того же множества, такой, что $r + s = t$. Например, если выбрать в нашем множестве два элемента, 2 и 5, то в нем найдется *единственный* элемент 7, такой, что $2 + 5 = 7$.

Умножение есть бинарная операция в группе $B$. Действительно, если $r$ и $s$ — любые два элемента данного множества (положительных рациональных чисел), то существует один и только один элемент $t$ этого множества, такой, что $r \cdot s = t$. (Единственность элемента $t$ следует из того факта, что эквивалентные рациональные числа, такие, как $\frac{4}{8}$ и $\frac{1}{2}$, представляют собой одно и то же число.) Если в нашем множестве выбрать два элемента, например $\frac{2}{3}$ и $\frac{5}{8}$, то в нем найдется единственный элемент $\frac{5}{12}$, такой, что $\frac{2}{3} \cdot \frac{5}{8} = \frac{5}{12}$.

Заметим, что понятие бинарной операции неразрывно связано с множеством, на котором она определена. Вот почему мы говорим: «бинарная операция на множестве». Два элемента и третий элемент, который сопоставляется им посредством бинарной операции, должны быть элементами одного и того же множества. Итак, мы видим, что два основных признака, характеризующих группу, — это наличие (1) множества элементов, (2) бинарной операции на этом мно-

жестве. И хотя они тесно переплетены и неразделимы, иногда оказывается удобным переносить центр внимания с одного признака на другой.

Рассмотренные нами примеры групповых операций — это обычное сложение целых чисел, обозначаемое символом $+$, и умножение положительных рациональных чисел, обозначаемое символом $\cdot$. В дальнейшем мы увидим, что существует много различных бинарных операций, связанных с разными группами, но иногда будет удобно пользоваться каким-то одним символом для произвольной бинарной операции. Для этой цели мы будем использовать символ $\otimes$.

Это обозначение позволяет нам следующим образом описать выявленные у групп $A$ и $B$ структурные признаки (1) и (2): задано множество $S$ и бинарная операция $\otimes$ на $S$. Если $r$ и $s$ — два произвольных элемента множества $S$, то в $S$ существует единственный элемент $t$, такой, что

$$r \otimes s = t.$$

Для группы $A$ символ $\otimes$ обозначает операцию «сложение целых чисел», для группы $B$ — «умножение положительных рациональных чисел».

Чтобы подчеркнуть ту мысль, что бинарная операция есть *соответствие*, можно описать рассмотренные выше группы еще одним способом. В случае группы $A$ мы можем сказать, что любой паре $r$ и $s$ целых чисел соответствует однозначно определенное целое число $t$, и записать это так:

$$(r, s) \to t,$$

где стрелка означает «соответствует». В случае группы $B$ мы можем сказать, что любой паре $r$ и $s$ положительных рациональных чисел соответствует однозначно определенное положительное рациональное число $t$.

Чтобы расширить наше представление о бинарных операциях на множестве, рассмотрим следующий вопрос: может ли бинарная операция на множестве быть бинарной операцией и на *подмножестве*? (Назо-

вем множество $U$ *подмножеством* множества $S$, если любой элемент множества $U$ является элементом множества $S$.) Например, пусть $S$ — множество всех положительных рациональных чисел, а $U$ — его подмножество, состоящее из положительных целых чисел. Выясним сначала, будет ли деление бинарной операцией на множестве $S$. Читатель может без труда убедиться, что деление *является* бинарной операцией на множестве $S$ положительных рациональных чисел: для любых двух положительных рациональных чисел $r$ и $s$ существует единственное положительное рациональное число $t$, такое, что

$$r : s = t.$$

Теперь посмотрим, будет ли деление — бинарная операция на множестве $S$ — бинарной операцией и на подмножестве $U$ положительных целых чисел. Очевидно, что если взять два таких элемента множества $U$, как, например, 2 и 3, то для них *не существует* положительного целого числа $t$, для которого

$$2 : 3 = t.$$

Следовательно, деление *не является* бинарной операцией на подмножестве $U$ положительных целых чисел, так как существуют пары положительных целых чисел, которым *не* соответствует никакое третье положительное целое число.

В противоположность только что описанной ситуации рассмотрим множество $S$ всех целых чисел и подмножество $U$ всех четных чисел. Мы уже видели, что сложение есть бинарная операция на множестве $S$ всех целых чисел. Что же будет происходить, если применять операцию сложения к элементам множества четных чисел? Если сложить два четных числа, то в результате снова получится четное число. Иными словами, сложение *является* бинарной операцией на подмножестве $U$ четных чисел. Если сложить два элемента из подмножества $U$, то их сумма тоже будет принадлежать этому подмножеству. Это свойство можно выразить иначе: подмножество $U$ четных чисел *замкнуто* относительно бинарной операции сло-

жения. Читатель может проверить, что подмножество $T$ нечетных чисел *не замкнуто* относительно этой операции.

Опишем свойство *замкнутости* подмножества относительно бинарной операции следующим, более общим образом: если $\otimes$ — бинарная операция на множестве $S$ и $U$ — подмножество множества $S$, обладающее тем свойством, что для любых элементов $u$ и $v$ подмножества $U$ элемент $u \otimes v$ также принадлежит $U$, то подмножество $U$ называется *замкнутым* относительно бинарной операции $\otimes$. Термин «замкнутый» отражает то обстоятельство, что операция $\otimes$, рассматриваемая лишь на парах элементов из $U$, не выводит нас за пределы подмножества $U$, т. е. $\otimes$ можно рассматривать как бинарную операцию на множестве $U$.

В гл. 8 мы увидим, что свойство замкнутости подмножества относительно бинарной операции играет главную роль при изучении подгрупп.

Упражнение 1. (a) Является ли сложение бинарной операцией на множестве нечетных положительных чисел? (b) Будет ли умножение бинарной операцией на указанном в п. (a) множестве? (c) Пусть рассматриваемое множество состоит из следующих элементов: $1, i, -1, -i$, где $i = \sqrt{-1}$. Будет ли сложение бинарной операцией на этом множестве? (d) Будет ли умножение бинарной операцией на множестве, указанном в п. (c)?

До сих пор мы видели, что группа — это *множество с заданной на нем бинарной операцией.* Если $r$ и $s$ — два произвольных элемента данного множества, то существует однозначно определенный элемент $t$ того же множества, такой, что

$$r \otimes s = t \quad \text{или} \quad (r, s) \to t.$$

Выражение «$r$ и $s$ — два произвольных элемента данного множества» не исключает из рассмотрения случая, когда $r$ и $s$ совпадают (т. е. представляют собой один и тот же элемент). Не предполагается также, что элементы $r$ и $s$ берутся в каком-то определенном

*порядке*. Таким образом, если $r$ и $s$ — два произвольных элемента данного множества, то

$$r \otimes s, \quad r \otimes r, \quad s \otimes s, \quad s \otimes r$$

также являются элементами этого множества (не обязательно, чтобы все они были различными).

Возникает вопрос: могут ли в некоторой группе $r \otimes s$ и $s \otimes r$ быть *различными* элементами исходного множества? В группах $A$ и $B$, очевидно, всегда справедливо равенство $r \otimes s = s \otimes r$. Например, в группе $A$ имеем $3 + 5 = 5 + 3$, а в группе $B$ имеем $\frac{2}{3} \cdot \frac{7}{2} = \frac{7}{2} \cdot \frac{2}{3}$. Но в множестве положительных рациональных чисел, где в качестве бинарной операции рассматривается деление, имеем, например, $\frac{2}{3} : \frac{7}{2} \neq \frac{7}{2} : \frac{2}{3}$. Вообще в этом множестве $r : s \neq s : r$ при $r = s$. Значит *порядок*, в котором берутся элементы, существен; в некоторых множествах перестановка элементов приводит к изменению результата, т. е. возможен случай, когда

$$(a, b) \to c \quad \text{и} \quad (b, a) \to d,$$

где $a$, $b$, $c$, $d$ — элементы данной группы и $c \neq d$.

В случае, когда $r \otimes s = s \otimes r$, мы говорим, что элементы $r$ и $s$ *перестановочны*, или *коммутируют* между собой (относительно данной операции $\otimes$); если $r \otimes s \neq s \otimes r$, то мы говорим, что элементы $r$ и $s$ *неперестановочны*, или *не коммутируют* между собой (относительно данной операции). Впредь мы не должны заранее считать само собой разумеющимся, что при данной операции $\otimes$ упорядоченной[1]) паре $(r, s)$ соответствует тот же элемент, что и упорядоченной паре $(s, r)$. В каждом случае нужно отдельно разбирать, будут ли элементы перестановочными.

В связи с тем что в общем случае необходимо различать элементы $r \otimes s$ и $s \otimes r$, мы следующим образом уточним характеризацию множества с заданной на нем бинарной операцией: для любой *упорядоченной* пары элементов $r$ и $s$ данного множества

[1]) То есть паре, в которой один из элементов считается первым, а другой — вторым. — *Прим. перев.*

существует единственный элемент $t$ того же множества, такой, что

$$r \otimes s = t \quad \text{или} \quad (r, s) \to t.$$

До сих пор рассматривались примеры лишь таких множеств с заданной на них бинарной операцией, элементами которых служат числа, а бинарными операциями — обычные арифметические действия. Но в дальнейшем мы увидим, что элементами группы могут быть и нечисловые объекты, такие, как движения, перестановки, функции, геометрические преобразования или вообще множества каких-либо символов. В этих случаях бинарная операция может оказаться и не связанной с действиями над числами.

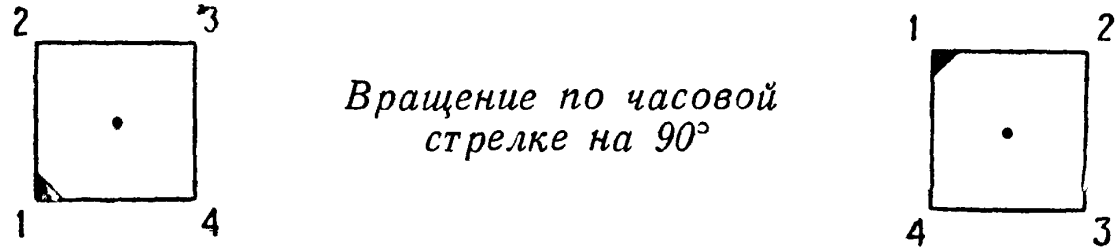



Рис. 1.1.

Например, рассмотрим квадрат, который может свободно вращаться в своей плоскости вокруг оси, проходящей через его центр. Будем считать допустимыми лишь те вращения, в результате которых повернутый квадрат совмещается с исходным. Одно из допустимых вращений — это поворот на 90° по часовой стрелке (рис. 1.1). Обозначим это вращение через $a$. Вот некоторые другие допустимые вращения: (1) вращение на 180° по часовой стрелке, которое мы обозначим через $b$, и (2) вращение на 270° по часовой стрелке, которое мы обозначим через $c$.

Будем рассматривать эти вращения $a$, $b$ и $c$ как возможные элементы некоторой группы. Удастся ли нам так определить бинарную операцию, чтобы имело смысл равенство $a \otimes b = c$? Вот один из способов рассуждения:

Последовательное выполнение вращения на 90° по часовой стрелке и вращения на 180° по часовой стрелке
эквивалентно
вращению на 270° по часовой стрелке,

или

Последовательное выполнение вращений $a$ и $b$
дает
вращение $c$,

или

$$a \otimes b = c.$$

Эту операцию, которая сопоставляет двум элементам $a$ и $b$ элемент $c$, мы будем называть *суперпозицией* или операцией *последовательного выполнения*. Такая операция имеет смысл для вращений. Мы увидим в дальнейшем, что она может иметь смысл и для объектов другого рода.

Упражнение 2. Какое вращение из множества вращений квадрата представляет собой элемент $b \otimes c$ при только что определенной операции последовательного выполнения? Какое вращение представляет собой элемент $a \otimes c$?

ГЛАВА 2

# АКСИОМЫ ГРУППЫ

В предыдущей главе мы сосредоточили наше внимание на понятии бинарной операции. Однако читатель не должен думать, что наличие бинарной операции является единственным определяющим признаком группы. Бинарная операция на множестве элементов должна, кроме того, обладать некоторыми свойствами, чтобы это множество вместе с данной бинарной операцией представляло собой группу. Эти основные свойства описываются аксиомами. Мы потребуем выполнения трех следующих аксиом: (1) ассоциативность, (2) о единичном элементе, (3) об обратных элементах.

*Ассоциативность.* Свойство ассоциативности состоит в том, что для любых трех элементов $r$, $s$, $t$ исходного множества выполняется равенство

$$r \otimes (s \otimes t) = (r \otimes s) \otimes t;$$

т. е. если $s \otimes t$ является элементом $x$ исходного множества, а $r \otimes s$ — элемент $y$ этого множества, то $r \otimes x = y \otimes t$.

Рассмотрим группы $A$ и $B$ (см. стр. 10). В группе $A$ ассоциативность означает, что

$$r + (s + t) = (r + s) + t$$

для любых целых чисел $r$, $s$, $t$. Например,

$$5 + (3 + 8) = 5 + 11 = 16$$

и

$$(5 + 3) + 8 = 8 + 8 = 16.$$

В группе $B$ имеет место равенство

$$r \cdot (s \cdot t) = (r \cdot s) \cdot t.$$

Например,

$$\frac{3}{8}\cdot\left(4\cdot\frac{2}{3}\right)=\frac{3}{8}\cdot\frac{8}{3}=1$$

и

$$\left(\frac{3}{8}\cdot 4\right)\cdot\frac{2}{3}=\frac{3}{2}\cdot\frac{2}{3}=1.$$

Из элементарной алгебры мы знаем, что бинарные операции в группах $A$ и $B$ ассоциативны.

Рассмотрим теперь деление как бинарную операцию на множестве положительных рациональных чисел и проверим, выполняется ли для него свойство ассоциативности.

Имеем

$$\frac{3}{2}:\left(3:\frac{3}{4}\right)=\frac{3}{2}:4=\frac{3}{8},$$

в то время как

$$\left(\frac{3}{2}:3\right):\frac{3}{4}=\frac{1}{2}:\frac{3}{4}=\frac{2}{3};$$

следовательно,

$$r:(s:t)\neq(r:s):t.$$

Таким образом, деление *не является* ассоциативной бинарной операцией на множестве положительных рациональных чисел.

Какой смысл следует придавать выражению $r\otimes s\otimes t$? Как применить *бинарную* операцию $\otimes$ сразу к *трем* элементам данного множества? Можно придать определенное значение выражению $r\otimes s\otimes t$, заключив в скобки либо два первых, либо два последних символа. В первом случае выражение примет вид $(r\otimes s)\otimes t$, а во втором — $r\otimes(s\otimes t)$. Так как $\otimes$ есть бинарная операция на нашем множестве, то $y=r\otimes s$ и $x=s\otimes t$ являются элементами этого множества. Значит, и $(r\otimes s)\otimes t$ и $r\otimes(s\otimes t)$ можно рассматривать как выражения, в которых участвуют лишь два элемента рассматриваемого множества, а именно $y$ и $t$ в первом случае и $r$ и $x$ во втором.

Если бинарная операция $\otimes$ *не ассоциативна*, то элементы $r\otimes x$ и $y\otimes t$, вообще говоря, различны, и

Элемент $a^{-1}$ называется *обратным* к элементу $a$. Ясно, что обратным к элементу $a^{-1}$ будет $(a^{-1})^{-1} = a$. В обозначении для обратного элемента используется отрицательный показатель степени, как и в элементарной алгебре, где обратный к любому $u \neq 0$ обозначается через $u^{-1}$.

Подытожим теперь все сказанное о группе. *Группой* называется множество $G$ с бинарной операцией $\otimes$ на нем, такое, что выполняются следующие аксиомы:

**Аксиома 1** *(ассоциативность)*. Для произвольных элементов $r$, $s$, $t$ из $G$

$$r \otimes (s \otimes t) = (r \otimes s) \otimes t.$$

**Аксиома 2** *(о единичном элементе)*. В группе $G$ существует единственный элемент $I$, такой, что

$$r \otimes I = I \otimes r = r.$$

**Аксиома 3** *(об обратных элементах)*. Для любого элемента $r$ из $G$ существует единственный элемент $r^{-1}$ из $G$, такой, что

$$r \otimes r^{-1} = r^{-1} \otimes r = I.$$

Читатель не должен думать, что это аксиоматическое определение группы целиком и полностью сложилось в уме какого-то одного математика. Часто математические понятия являются результатом деятельности многих математиков; процесс их развития протекает неравномерно, скачками, порой он заводит в тупик, а порой приводит к неожиданным открытиям. Формальные аксиомы, которые легли в основу определения группы, были сформулированы в явном виде лишь спустя почти 100 лет после начала работы в области теории групп. Первая важная теорема была сформулирована и доказана в 1771 г. Лагранжем. (Мы рассмотрим ее в одной из последующих глав.)

Коши[1]), чья деятельность в области теории групп началась в 1815 г., рассматривал только группы, элементы которых представлены в виде подстановок. Слово «группа» было введено в 1832 г. Галуа, впервые показавшим, что группу можно определить и не используя в качестве элементов подстановки. И лишь к 1854 г. процесс выявления структуры группы достиг той стадии, на которой Кэли[2]) сумел показать, что группу можно определить, не упоминая о конкретной природе ее элементов. Структура группы зависит, как показал Кэли, лишь от того, как задана операция на парах элементов.

Прежде чем перейти к дальнейшим примерам групп, упростим и обобщим обозначения, используемые для бинарной групповой операции. Опыт элементарной алгебры подсказывает, что удобно писать $ab = c$ вместо $a \otimes b = c$ и читать это так: элементу $a$, *умноженному* на элемент $b$, сопоставляется элемент $ab$, называемый произведением $a$ и $b$ (и обозначаемый через $c$). В дальнейшем мы не обязательно будем использовать символ $\otimes$ для обозначения бинарной операции; часто мы будем употреблять обозначение $ab$ для группового произведения элементов $a$ и $b$; иногда произведение $ab$ в группе мы будем записывать так: $a \cdot b$.

«Умножение» как общий термин для групповой операции не следует путать с умножением в обычной арифметике. Может случиться, что элементами группы

---

[1]) Огюстен-Луи Коши (1789—1857) внес крупный вклад в развитие математики, выдвинув требование строгой обоснованности рассуждений в математическом анализе. Введенные им понятия предела, непрерывности и сходимости принадлежат к основным понятиям современного анализа. Коши был одним из первых, кто занимался систематическим развитием теории групп, в особенности групп подстановок. Он известен также как автор важнейших теорем в теории функций комплексного переменного.

[2]) Артур Кэли (1821—1895) получил много важных результатов в самых различных областях математики — от геометрии и алгебры до теоретической механики и астрономии. При этом он находил время для занятий (в течение 14 лет) адвокатской практикой. Наиболее известными в наше время являются работы Кэли по теории матриц и теории групп.

являются числа, а групповой операцией — обычное умножение. Но это частный случай. В общем же случае групповое умножение следует рассматривать как абстрактное обобщение умножения чисел.

Предостережение. Хотя на элементах данного множества можно определить много операций, в каждой конкретной группе определена *единственная* операция, которая является групповой операцией именно *этой* группы.

ГЛАВА 3

# ПРИМЕРЫ ГРУПП

Если мы хотим выяснить, является ли данное множество с определенной на нем бинарной операцией группой, нам следует проверить, выполняются ли сформулированные в предыдущей главе аксиомы. Давайте выясним, какие из рассмотренных далее множеств можно считать группами. Начнем с группы $A$ (см. стр. 10).

**Пример 1.** *Множество элементов:* все целые числа (положительные, отрицательные и нуль).

*Бинарная операция:* сложение.

*Ассоциативность:* сложение чисел ассоциативно.

*Единичный элемент:* нуль является элементом рассматриваемого множества и для любого целого числа $u$ выполняются равенства $u + 0 = 0 + u = u$. Нуль является единицей группы.

*Обратные элементы:* если $u$ — целое число, то $-u$, противоположное число, также является целым и $u + (-u) = (-u) + u = 0$; таким образом, $-u$ является обратным к $u$ элементом, или, в групповых обозначениях, $u^{-1} = -u$.

Итак, проверка показывает, что $A$ есть группа. Так как она содержит бесконечно много элементов, то мы будем говорить, что эта группа *бесконечна*, и называть ее *бесконечной аддитивной группой*, или *аддитивной группой целых чисел*.

**Пример 2.** Рассмотрим то же множество, что и в примере 1, но теперь с операцией умножения. Читатель может убедиться, что умножение является бинарной операцией на множестве целых чисел и что для этой операции справедливы аксиома ассоциатив-

ности и аксиома о единичном элементе. Чтобы выяснить, выполняется ли аксиома 3, попытаемся найти элемент, обратный к элементу 2. Нам нужно найти целое число $u$, такое, что $2 \otimes u = I$, или $2u = 1$. Такого целого числа не существует. Следовательно, это *не* группа.

**Пример 3.** Множество состоит из двух чисел 1 и $-1$, а в качестве бинарной операции возьмем умножение:

$$1 \cdot 1 = 1; \quad (-1) \cdot (-1) = 1; \quad 1 \cdot (-1) = (-1) \cdot 1 = -1.$$

*Ассоциативность:* очевидно.

*Единичный элемент*: единицей является 1.

*Обратные элементы:* имеем $1 \cdot 1 = 1$ и $(-1)(-1) = 1$, т. е. $(1)^{-1} = 1$ и $(-1)^{-1} = -1$. Таким образом, обратным к любому элементу является он сам.

Итак, это группа. Число элементов в ней конечно, и поэтому мы будем говорить, что эта группа *конечна*. *Порядок* конечной группы равен числу ее элементов. Рассматриваемая группа есть группа порядка 2.

**Пример 4.** Существует ли группа порядка 1? Будет ли группой множество, состоящее из одного числа 1 с умножением в качестве бинарной операции? Проверка трех аксиом показывает, что это действительно группа порядка 1.

**Пример 5.** Теперь рассмотрим группу, элементами которой являются движения геометрической фигуры. При изучении этой группы мы столкнемся со многими существенными особенностями таких движений. Возникающие при этом понятия будут часто встречаться в дальнейшем, и потому мы займемся этим вопросом довольно подробно. К тому же это поможет читателю заложить прочную основу для дальнейшего.

Рассмотрим движение равностороннего треугольника, который может вращаться в своей плоскости вокруг оси, проходящей через его центр. За элементы предполагаемой группы примем некоторые вращения этого треугольника, а в качестве бинарной опера-

ции — их суперпозицию, или «последовательное выполнение» (см. стр. 17). Нас будут интересовать только те движения, в результате которых *повернутый треугольник совмещается с исходным.* Такие движения назовем *самосовмещениями.*

Чтобы дать конкретное описание самосовмещений, выберем некоторое произвольное положение нашего равностороннего треугольника на плоскости в

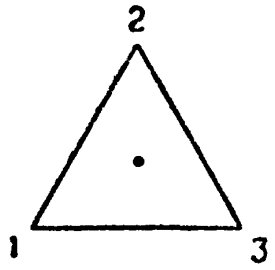



Рис. 3.1.

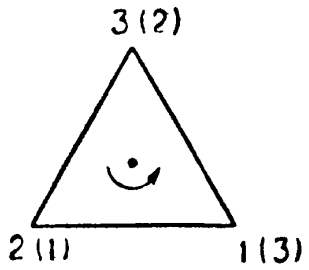



Рис. 3.2.

качестве его начального положения. Затем мы сопоставим каждой вершине некоторое число как ее опознавательную метку. Тогда наш равносторонний треугольник будет выглядеть, как это показано на рис. 3.1. Точка в центре — это точка пересечения оси вращения с плоскостью треугольника. Метки при вершинах помогут нам их узнать, когда вершины будут смещены некоторым движением из нашего множества. Нужно помнить, что для совмещения треугольника с самим собой не обязательно, чтобы каждая (помеченная) вершина совпала с собой, нужно только, чтобы множество точек, составляющих стороны треугольника после поворота, совпало с множеством точек, составляющим его стороны в начальном положении. Например, если треугольник, изображенный на рис. 3.1, будет повернут вокруг оси на 120° против часовой стрелки, то мы сможем рассматривать повернутый треугольник как второй треугольник, наложенный на треугольник, находящийся в начальном положении. Эта ситуация изображена на рис. 3.2. Цифры в скобках соответствуют расположению вершин треугольника, когда он находился в начальном положении. Мы видим, что такое вращение связано с пе-

рестановкой вершин, а именно вершина 1 замещается вершиной 2, вершина 2 — вершиной 3, вершина 3 — вершиной 1.

Совмещение с собой в результате вращения удобно представлять себе с помощью «разделения» двух положений треугольника (см. рис. 3.3). Заметим, что угол при вершине 1 зачернен, для того чтобы легче было следить за движениями треугольника. Хотя два


Рис. 3.3.
Слева треугольник изображен в начальном положении, а справа — после вращения на 120° против часовой стрелки.

положения треугольника изображены рядом, не следует забывать, что этот рисунок — лишь удобное представление такого вращения треугольника, после которого он совмещается с собой.

Существуют ли другие вращения, которые переводят треугольник из исходного положения во второе положение, изображенное выше? Конечно, таким будет вращение на 240° по часовой стрелке, равно как и вращение против часовой стрелки на 480 или 840°. Читатель может сам убедиться, что любое вращение из бесконечного множества

$$A = \{\text{вращение против часовой стрелки на } 120° \pm (360k)°, \quad k = 0,\ 1,\ 2,\ \ldots\}$$

обладает этим свойством (вращения против часовой стрелки на отрицательный угол интерпретируются как вращения по часовой стрелке).

Все движения из множества $A$ обладают общим свойством, а именно все они одинаковым образом объединяют в пары вершины нашего треугольника

в начальном положении с вершинами того же треугольника после поворота:

| Начальное положение | | Положение после поворота |
|---|---|---|
| 1 | → | 2 |
| 2 | → | 3 |
| 3 | → | 1 |

Читателю следует обратить внимание на то, что *вращения из множества A обладают этим свойством вне зависимости от того, какое положение треугольника мы выбрали в качестве начального.*

Пусть теперь $a$ — произвольный элемент множества $A$. Движение $a$ можно рассматривать как *представитель* множества $A$ в том смысле, что вращение $a$

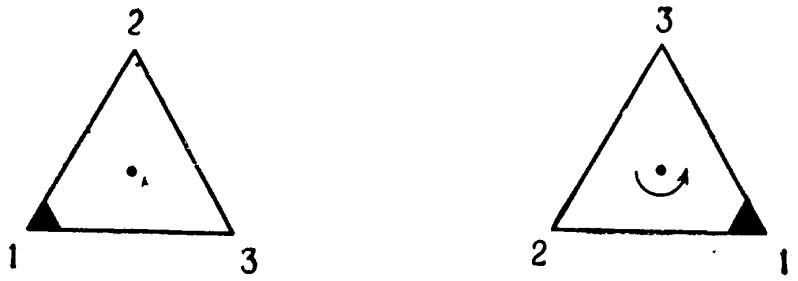



Рис. 3.4.

Слева изображено начальное положение треугольника; справа — положение, которое принял треугольник в результате движения $a$.

переводит треугольник из (произвольно) выбранного начального положения в такое положение, когда он совмещается с исходным, а вершины объединяются в пары следующим образом (рис. 3.4):

$$a\colon\quad 1 \to 2,\quad 2 \to 3,\quad 3 \to 1.$$

(Помните, что *все* движения из множества $A$ обладают этим свойством.)

В этой ситуации нам кажется удобным обозначить через $a$ некоторое движение из множества $A$. Например, можно взять в качестве $a$ поворот на 120° против часовой стрелки. Такой выбор соответствует $k = 0$ в выражении $120 \pm (360\,k)°$. Если читатель предпочтет какое-либо другое $a$, он может выбрать, скажем, $k = 13$ и запомнить, что вращение на 4800° против часовой стрелки является «его собственным» представителем множества $A$. Тот или иной выбор — это лишь вопрос

удобства. Существенно здесь лишь то, что все движения, входящие в множество $A$, объединяют вершины нашего треугольника в пары одинаковым образом, не

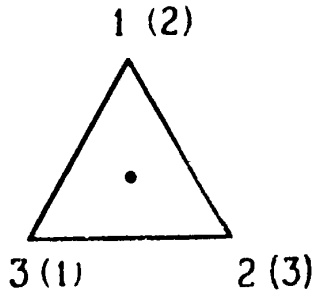



Рис. 3.5.

зависящим от выбора начального положения треугольника. Используя наши опознавательные метки обозначим это объединение в пары так:

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

Существуют ли другие, не входящие в множество $A$ вращения, которые являются самосовмещениями этого треугольника? Рассмотрим множество вращений

$$B = \{\text{вращения против часовой стрелки на } 240° \pm (360k)°, \quad k = 0, 1, 2, \ldots\}.$$

В результате каждого из этих движений происходит наложение, изображенное на рис. 3.5. Рис. 3.6 изо-

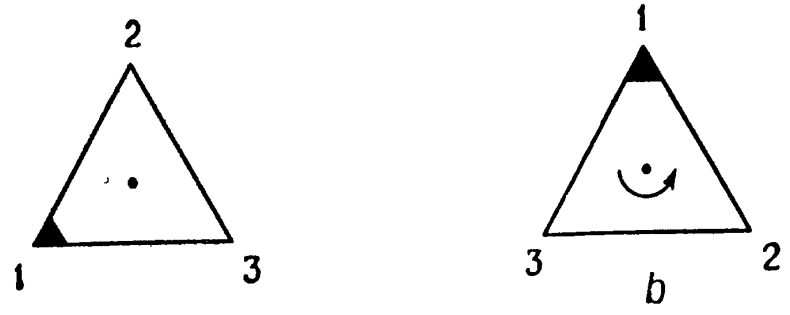



Рис. 3.6.
Слева изображен треугольник в начальном положении.

бражает то же самое, но в «разделенной» форме. Как и выше, пусть $b$ обозначает произвольный элемент множества $B$, который и будет его «представителем». Для удобства мы пометили на рисунке символом $\cdot$ *положение*, которое принял треугольник в результате движения $b$. Вне зависимости от того, какое вращение

мы выбрали в множестве $B$, мы получаем следующую группировку в пары вершин нашего треугольника:

$$b\colon\quad 1\to 3,\quad 3\to 2,\quad 2\to 1.$$

(т. е. вершина 1 замещается вершиной 3, вершина 3 — вершиной 2 и вершина 2 — вершиной 1).

Есть еще одно множество движений, которые переводят треугольник в себя, — это множество

$$C=\{\text{вращения против часовой стрелки на } 0^\circ\pm(360k)^\circ,\quad k=0,\ 1,\ 2,\ \ldots\}.$$

На рис. 3.7 символом $c$ обозначен произвольный элемент множества $C$. Отметим, что результат движения $c$ состоит в следующем: треугольник совмещается со

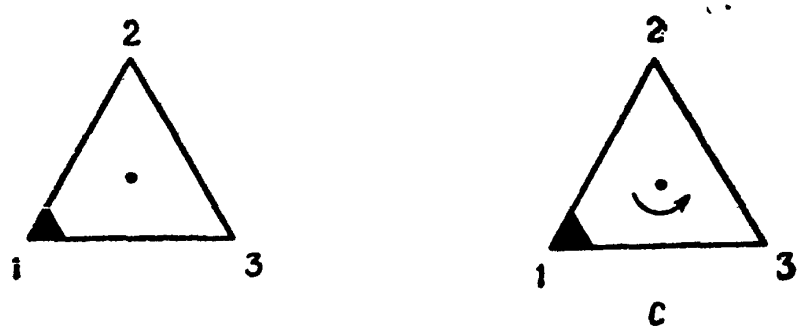



Рис. 3.7.

Слева изображен треугольник в начальном положении.

своим исходным положением; при этом вершины группируются следующим образом:

$$c\colon\quad 1\to 1,\quad 2\to 2,\quad 3\to 3.$$

Наша цель — получить группу движений, и, так как группа должна иметь единицу (аксиома о единичном элементе), нам следует убедиться, что любое движение $c$ из множества $C$ удовлетворяет требованиям, предъявляемым к единичному элементу. Действительно, если $x$ — произвольный элемент множества $A$, $B$ или $C$, то как суперпозиция движений $c$ и $x$, так и суперпозиция $x$ и $c$ суть вращения *из того же множества, что и* $x$. Чтобы проверить это, вспомним, что вращения, например, из множества $A$ — это вращения на $120^\circ\pm(360k)^\circ$, $k=0,\ 1,\ 2,\ \ldots$, а вращения из множества $C$ — это вращения на $0^\circ\pm(360m)^\circ$, $m=0,\ 1,$

2, ... . Если два вращения выполняются последовательно, то угол, на который окажется повернутым в результате обоих вращений треугольник, есть сумма углов, на которые поворачивается треугольник при каждом из них. Таким образом, суперпозиция вращений $a$ и $c$ есть поворот на угол

$$120° \pm (360k)° + 0° \pm (360m)°,$$

или

$$120° \pm (360(k+m))°.$$

Так как $k$ и $m$ — целые числа, то $k+m$ — также целое число и, следовательно, суперпозиция $a$ и $c$ есть вращение из множества $A$. Аналогично, суперпозиция $c$ и $a$ есть вращение на $120° \pm (360(m+k))°$ из множества $A$.

В обозначениях группового умножения (стр. 23) это запишется так:

$$ac = ca = a, \quad bc = cb = b, \quad cc = c,$$

и результат не зависит от того, какие элементы $a$, $b$ и $c$ выбраны в качестве представителей множеств $A$, $B$ и $C$ соответственно. Эти соотношения объясняют, почему мы будем использовать символ $I$ (обозначающий единичный элемент) для произвольного элемента из множества $C$.

Мы перебрали все возможные вращения вокруг выбранной нами оси, являющиеся самосовмещениями данного треугольника. Каждое такое вращение содержится в одном из трех множеств $A$, $B$, $C$ с представителями $a$, $b$, $I$, соответствующими положениям треугольника, изображенным (в «разделенном» виде) на рис. 3.8. Отметим, что каждое из трех положений треугольника помечено символом, обозначающим то *движение* треугольника, которое переводит его из заданного начального положения в изображенное на рисунке.

Мы утверждаем, что *множество, состоящее из трех классов самосовмещений с представителями $I$, $a$, $b$, образует группу с операцией «последовательного выполнения» в качестве бинарной операции.* Чтобы про-

верить, что операция «последовательного выполнения» является на этом множестве бинарной операцией, и убедиться в том, что аксиомы группы выполнены, найдем произведение любых двух элементов.

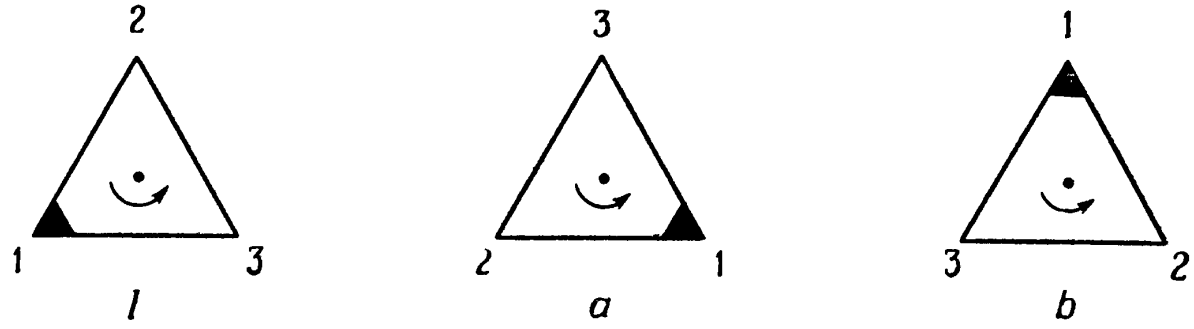



Рис. 3.8.

Найдем, например, $ab$, определяя, какая группировка вершин в пары соответствует суперпозиции вращений $a$ и $b$:

$$\begin{array}{lll} a: & 1 \to 2 & b: \quad 1 \to 3 \\ & 2 \to 3 & \quad\;\; 3 \to 2 \\ & 3 \to 1 & \quad\;\; 2 \to 1 \end{array}$$

Движение $a$ связывает вершину 1 с вершиной 2 (так, как это было описано на стр. 29), а движение $b$ — вершину 2 с вершиной 1; таким образом, в результате суперпозиции движений $a$ и $b$ вершина 1 объединяется в пару сама с собой. То же самое происходит и с другими вершинами. Итак,

$$\begin{array}{lllll} ab: & 1 \to 2 \to 1 & \text{или} & 1 \to 1 \\ & 2 \to 3 \to 2 & \text{или} & 2 \to 2 \\ & 3 \to 1 \to 3 & \text{или} & 3 \to 3 \end{array}$$

Ясно, что

$$ab = I.$$

Читатель может легко убедиться в том, что $aa = b$, $bb = a$ и $ba = I$ (и тогда будут рассмотрены уже все произведения).

Мы установили таким образом, что суперпозиция — бинарная операция на нашем множестве. Осталось проверить лишь выполнение групповых аксиом.

*Ассоциативность.* Мы уже проверили (стр. 20), что операция «последовательного выполнения» ассоциативна, когда элементами множества являются движения.

*Единичный элемент.* Предыдущие рассуждения показывают, что множество $C$ с представителем $I$ есть единица.

*Обратные элементы.* Так как $ab = I$ и $ba = I$ (и, разумеется, $II = I$), то каждый элемент в нашем множестве обладает обратным.

**Пример 6.** Предположим, что нас интересуют не сами целые числа, а лишь их остатки от деления на 2; будем считать два числа *эквивалентными*, если они дают при делении на 2 один и тот же остаток. Два целых числа эквивалентны, если оба они четные или оба нечетные.

Тот факт, что числа 6 и 8 имеют один и тот же остаток при делении на 2, мы будем выражать записью

$$8 \equiv 6 \pmod 2,$$

где $\equiv$ означает «эквивалентно», а mod — «по модулю»[1]). Аналогично можно написать

$$7 \equiv 3 \pmod 2,$$

так как 7 и 3 дают одинаковые остатки при делении на 2. Таким образом, если через $x$ обозначить произвольное четное число, а через $y$ — нечетное, то

$$x \equiv 0 \pmod 2 \quad \text{и} \quad y \equiv 1 \pmod 2.$$

Действительно, понятие «эквивалентность по модулю 2» дает нам возможность взять 0 и 1 в качестве «представителей» четных и нечетных чисел соответственно.

Мы теперь можем исследовать группу с элементами 0 и 1 и бинарной операцией «сложение по модулю 2». Определим *сложение по модулю* 2 (обозна-

---

[1]) Часто в этой ситуации говорят, что числа *сравнимы* по данному модулю. — *Прим. перев.*

чаемое через $\oplus$) двух целых чисел $a$ и $b$ следующим образом:

$$a \oplus b = 0, \quad \text{если} \quad a + b \equiv 0 \pmod 2,$$

т. е. если обычная сумма — четное число, и

$$a \oplus b = 1, \quad \text{если} \quad a + b \equiv 1 \pmod 2.$$

Сложение по модулю 2 является бинарной операцией на множестве $\{0, 1\}$, так как

$$0 + 0 \equiv 0 \pmod 2, \quad 0 + 1 \equiv 1 \pmod 2,$$
$$1 + 0 \equiv 1 \pmod 2, \quad 1 + 1 \equiv 0 \pmod 2,$$

или

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1, \quad 1 \oplus 0 = 1, \quad 1 \oplus 1 = 0.$$

*Ассоциативность.* Легко проверить, что сложение по модулю 2 ассоциативно; например,

$$1 + (1 + 1) \equiv (1 + 0) \equiv 1 \pmod 2,$$
$$(1 + 1) + 1 \equiv (0 + 1) \equiv 1 \pmod 2.$$

*Единичный элемент.* Здесь 0 является единицей.

*Обратные элементы.* Каждый элемент является обратным к самому себе, так как $0 + 0 \equiv 0 \pmod 2$ и $1 + 1 \equiv 0 \pmod 2$.

Мы, таким образом, разбили множество целых чисел на два класса — класс четных чисел с представителем 0 и класс нечетных с представителем 1. Можно также разбить это множество на три класса, рассматривая остатки от деления на 3. Все целые числа, которые дают остаток 0 при делении на 3, составляют один класс, все те, которые дают остаток 1, — второй класс, и все те, которые дают остаток 2, — третий. Мы пишем, например,

$$12 \equiv 15 \pmod 3, \quad 7 \equiv 1 \pmod 3, \quad 5 \equiv 8 \pmod 3,$$

т. е. целые числа, которые дают один и тот же остаток при делении на 3, эквивалентны по модулю 3.

Аналогично можно рассматривать классы чисел, эквивалентных по модулю 4, исследуя остатки от деления на 4, и вообще классы целых чисел, эквива-

лентных по модулю произвольного целого $n$. Так как при делении на $n$ возможны остатки $0, 1, \ldots, n-1$, мы получаем $n$ классов с представителями $0, 1, \ldots, \ldots, n-1$.

Читателю следует попытаться самостоятельно проверить, что множество

$$\{0, 1, 2, \ldots, n-1\}$$

с бинарной операцией «сложение по модулю $n$» составляет группу. [Если $x$ — произвольный элемент нашего множества, то каков его обратный? Ищем элемент $y$, такой, что $x + y \equiv 0 \pmod{n}$, замечая, что $n \equiv 0 \pmod{n}$.]

**Пример 7.** Рассмотрим теперь множество целых чисел $\{1, 2, 3, 4\}$ с бинарной операцией «умножение по модулю 5». Таким образом, для любых целых чисел $r$ и $s$ из нашего множества

$$r \otimes s = t \quad \text{или} \quad (r, s) \to t, \quad \text{если} \quad r \cdot s \equiv t \pmod{5},$$

т. е. если целые числа $r \cdot s$ и $t$ дают один и тот же остаток при делении на 5. Например,

$$3 \otimes 4 = 2 \text{ или } (3, 4) \to 2, \text{ так как } 3 \cdot 4 = 12 \equiv 2 \pmod{5}.$$

Читателю следует проверить, что умножение по модулю 5 есть бинарная операция на указанном выше множестве, убедившись, что произведение любых двух элементов нашего множества эквивалентно целому числу из того же множества.

*Ассоциативность* следует из ассоциативности обычного умножения целых чисел. (Проверьте это.)

*Единичный элемент.* Единицей является элемент 1.

*Обратные элементы.* Элемент 1 совпадает со своим обратным. Элементы 2, 3 и 4 удовлетворяют следующим соотношениям, которые определяют их обратные:

$2 \cdot 3 \equiv 1 \pmod{5}$, обратным к 2 является 3,

$3 \cdot 2 \equiv 1 \pmod{5}$, обратным к 3 является 2,

$4 \cdot 4 \equiv 1 \pmod{5}$, обратным к 4 является 4.

Читателю следует попытаться установить, было ли необходимым отсутствие в нашем множестве элемента 0, т. е. будет ли множество $\{0, 1, 2, 3, 4\}$ группой относительно операции умножения по модулю 5.

Другой вопрос к читателю: составляет ли группу множество $\{1, 2, 3\}$ с бинарной операцией умножения по модулю 4? Попытайтесь сначала найти обратный к 2, т. е. такой элемент $x$ из нашего множества, что $2x \equiv 1 \pmod 4$.

**Пример 8.** Пусть $p > 1$ — *простое число*, т. е. число, у которого всего два целых положительных делителя: 1 и $p$. Рассмотрим множество

$$\{1, 2, 3, \ldots, p-1\}.$$

Мы утверждаем, что «умножение по модулю $p$» есть бинарная операция на этом множестве и что групповые аксиомы здесь выполняются. Предоставляем читателю показать, что выполнены аксиома ассоциативности и аксиома о единичном элементе. Доказательство того, что справедлива аксиома об обратных элементах, мы также предоставляем читателю в качестве упражнения.

Упражнение 4. Рассмотрите множество $\{1, 2, 3, \ldots, p-1\}$, где $p$ — простое число, с бинарной операцией «умножение по модулю $p$». Покажите, что для любого элемента $x$ из этого множества существует элемент $y$ того же множества, такой, что $xy \equiv 1 \pmod p$.

ГЛАВА 4

# ТАБЛИЦА УМНОЖЕНИЯ ГРУППЫ

Нам нужно теперь рассмотреть следующую проблему: каким образом можно *задать* конкретную группу? Иными словами, какое количество информации необходимо для того, чтобы можно было задать группу как единый математический объект? И как выявить те данные, которые позволяют определить ту или иную конкретную группу?

Ответ на эти вопросы был дан Кэли в 1854 г., когда он ввел *таблицу умножения группы*. Она похожа на привычную арифметическую таблицу умножения. Элементы группы располагаются в верхней строке и в том же порядке в левом столбце таблицы, а внутри нее размещаются произведения элементов.

Рассмотрим сначала группу порядка 2, состоящую из двух элементов, 1 и —1, с обычным умножением в качестве бинарной операции. В табл. 4.1 содержатся все возможные произведения двух элементов нашей группы. Так как обычное умножение коммутативно, любые два элемента этой группы перестановочны между собой.

*Таблица 4.1*

| | 1 | −1 |
|---|---|---|
| 1 | 1 | −1 |
| −1 | −1 | 1 |

Далее, построим таблицу умножения для группы самосовмещений равностороннего треугольника на плоскости (см. пример 5, стр. 26). Используя сим-

волы $I$, $a$, $b$ для обозначения трех элементов этой группы, мы запишем сами элементы и их произведения в виде табл. 4.2. Тут следует сделать ряд пояснений и упрощений. Мы не можем считать заранее заданным, что любые два элемента нашей группы коммутируют между собой. Поэтому сомножители в каждом произведении мы пишем в том порядке, в котором выполняется умножение: *первым* ставится сомножитель из левого столбца, а *вторым* — из верхней строки.

*Таблица 4.2*

| | II сомножитель | | |
|---|---|---|---|
| I сомножитель | $I$ | $a$ | $b$ |
| $I$ | $II$ | $Ia$ | $Ib$ |
| $a$ | $aI$ | $aa$ | $ab$ |
| $b$ | $bI$ | $ba$ | $bb$ |

Напомним, что, подробно изучив эту группу, мы вывели такие соотношения:

$$aa = b, \quad ab = ba = I, \quad bb = a$$

(см. стр. 33).

Используя эти результаты и свойства единицы $I$, мы можем записать таблицу умножения в следующем виде:

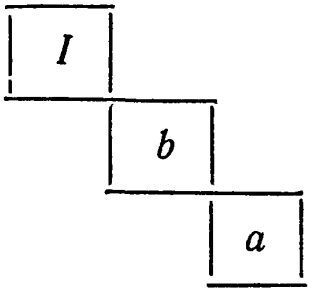
*Таблица 4.3*

| | II сомножитель | | |
|---|---|---|---|
| I сомножитель | $I$ | $a$ | $b$ |
| $I$ | $I$ | $a$ | $b$ |
| $a$ | $a$ | $b$ | $I$ |
| $b$ | $b$ | $I$ | $a$ |

Многие свойства рассматриваемой группы вращений можно извлечь прямо из этой таблицы умноже-

ния. Обратные элементы можно найти, проследив, на пересечении каких строк и столбцов встречается в таблице элемент *I*. Отметим интересное «совпадение»: строки таблицы являются перестановками верхней строки, а столбцы — перестановками левого столбца.

Таблица показывает также, что все элементы группы попарно перестановочны, так как все произведения, расположенные *симметрично* относительно главной диагонали, совпадают. *Главная диагональ* проходит из левого верхнего угла в правый нижний и в нашем случае выглядит так:




В любой таблице умножения симметрично по отношению к произведению *rs* располагается произведение *sr*. Мы называем группу *коммутативной*, если *любые* два ее элемента перестановочны. Таким образом, мы можем сказать, что

> *конечная группа коммутативна тогда и только тогда, когда ее таблица умножения обладает тем свойством, что произведения, расположенные симметрично относительно главной диагонали, представляют собой один и тот же элемент группы.*

Существует важное свойство группы самосовмещений равностороннего треугольника, которое нельзя извлечь из таблицы умножения в ее теперешнем виде. Однако оно станет очевидным, если мы введем новые обозначения и используем их для того, чтобы придать таблице иную форму.

В соответствии с представлением, что групповое умножение является обобщением обычного умножения, мы будем обозначать элемент *aa* группы через $a^2$, *aaa* — через $a^3$, в общем случае произведение $k$ экземпляров элемента $a$ — через $a^k$. Аналогично мы

будем писать $a^{-2}$ вместо $(a^{-1})(a^{-1})$ и произведение $k$ экземпляров элемента $a^{-1}$ будем обозначать через $a^{-k}$. Так как $a^k \cdot a^{-k} = I$, естественно *определить* $a^0 = I$. Элемент $a^n$ группы, где $n$ — произвольное целое число, мы будем называть *степенью элемента a*. Читатель может проверить для себя, что обычные правила умножения степеней сохраняются и для группового умножения степеней элемента группы.

Используя полученные раньше результаты, убеждаемся, что

$$b = aa = a^2,$$
$$ab = aaa = a^3 = I,$$

так что таблица умножения данной группы может быть представлена в виде табл. 4.4. В этой последней форме таблица показывает, что *любой элемент этой группы есть степень одного элемента a*. Группа с таким свойством называется *порожденной* элементом $a$, а сам этот элемент называют *образующей* группы.

*Таблица 4.4*

| | $I$ | $a$ | $a^2$ |
|---|---|---|---|
| $I$ | $I$ | $a$ | $a^2$ |
| $a$ | $a$ | $a^2$ | $I$ |
| $a^2$ | $a^2$ | $I$ | $a$ |

Подробнее это понятие мы рассмотрим позже, в главе об образующих группы.

**Некоммутативная группа.** Хотя мы уже приводили примеры не коммутирующих между собой пар элементов, некоммутативной группы мы еще не видели. Напомним, что коммутативной группой называется группа, любые два элемента которой коммутируют между собой. Такую группу называют также *абелевой*

в честь Н. Х. Абеля [1]), впервые применившего такие группы к теории уравнений.

Если в группе существует два не коммутирующих между собой элемента, то группа называется *некоммутативной* независимо от того, сколько найдется в ней пар коммутирующих между собой элементов. Может ли существовать группа, в которой никакие два элемента не перестановочны? Ясно, что нет, так как любая группа содержит единичный элемент, который коммутирует с каждым ее элементом.

Построим теперь некоммутативную группу порядка 6. В дальнейшем станет ясно, что это наименьший из всех возможных порядков некоммутативных групп. Для построения группы рассмотрим движения равностороннего треугольника, в результате которых он совмещается с самим собой. Мы уже рассматривали одно множество таких движений, но тогда налагалось ограничение, что треугольник должен вращаться в своей плоскости. Эти вращения, как мы убедились, образуют группу третьего порядка. Если отбросить указанное ограничение, то станут возможными новые движения, поскольку треугольник теперь можно опрокидывать. Например, опрокидывая треугольник относительно какой-либо его высоты, мы совмещаем его с самим собой, но это движение не совпадает ни с одним из рассмотренных в примере 5 (стр. 26) вращений. Мы увидим, что теперь существует уже шесть положений, в которых треугольник совпадает с самим собой. Мы обозначим их через $I$, $r$, $r^2$, $f$, $fr$, $fr^2$ (по причинам, которые станут ясны читателю позже). Эти положения изображены на рис. 4.1. (Время от времени мы будем давать геометрическую интерпретацию групповых свойств, взывая к интуитивному

---

[1]) Норвежский математик Нильс Хенрик Абель (1802—1829) доказал неразрешимость в радикалах общего алгебраического уравнения пятой степени. При изучении алгебраических уравнений он широко использовал понятие коммутативной группы, и потому теперь такие группы называются «абелевыми». Он также создал новые области анализа, в частности теорию эллиптических функций. Абель умер от туберкулеза в возрасте двадцати шести лет.

пространственному представлению читателя. Рекомендуем воспользоваться какой-либо моделью, например вырезать из бумаги равносторонний треугольник, и воспроизводить те движения, которые мы здесь описываем.)

При построении нашей группы мы применим способ, аналогичный использованному в примере 5

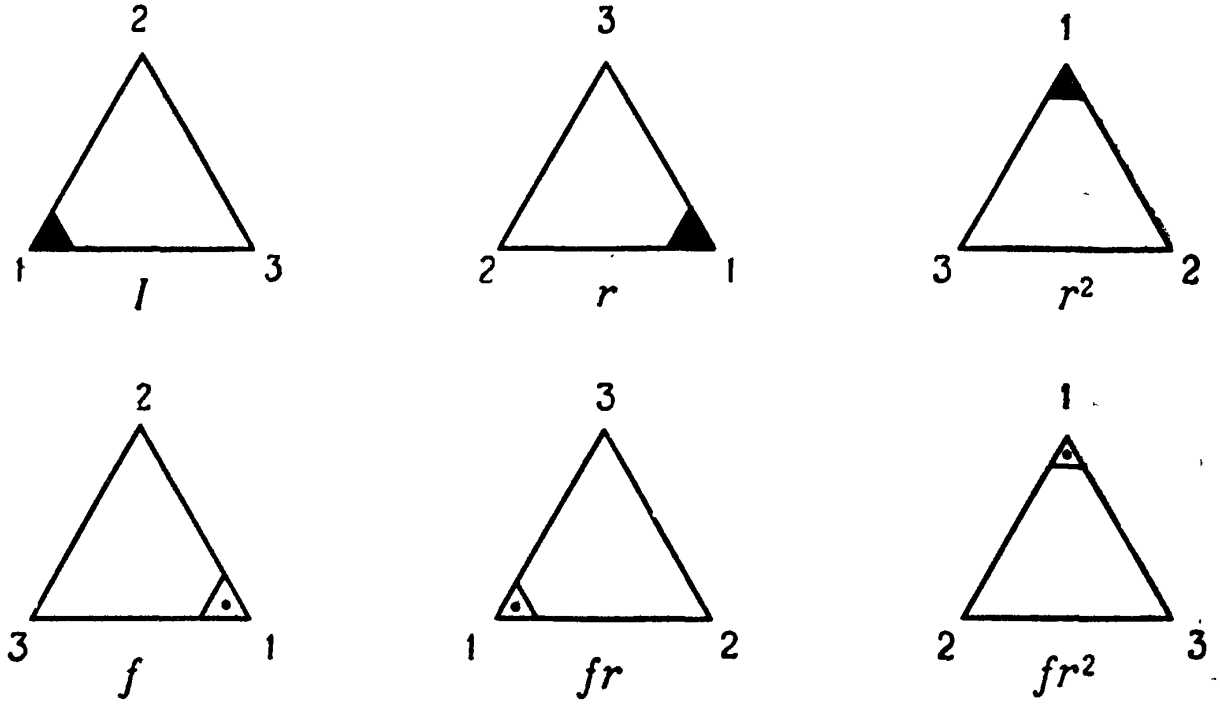



Рис. 4.1.

(стр. 26). Такие способы оказываются удобными в тех случаях, когда мы имеем дело с группой движений.

Символу, которым обозначается движение, часто придается некоторое конкретное значение. В этом разделе символ $r$ означает поворот на 120° против часовой стрелки вокруг оси, проходящей через центр равностороннего треугольника, хотя этот же символ может обозначать любой другой элемент множества $A$ вращений против часовой стрелки на углы $120° \pm \pm (360k)°$, $k = 0, 1, 2, \ldots$. Аналогичным образом позже мы введем движение $f$, которому придадим для наглядности конкретное значение, хотя тот же символ будет представлять любой элемент из некоторого множества движений. Существенно здесь то, что *мы будем рассматривать как «одно и то же» движение все*

*те движения, которые одинаковым образом объединяют в пары вершины треугольника.*

Нам хотелось бы иметь наглядное изображение движений нашей группы, однако мы не можем сделать этого с помощью тех неподвижных диаграмм, которые используются в этой книге. И потому мы предлагаем читателю интерпретировать эти диаграммы так, как это объяснялось на стр. 32, а именно если символ $x$, обозначающий движение, приписан диаграмме, изображающей положение фигуры, то *мы*

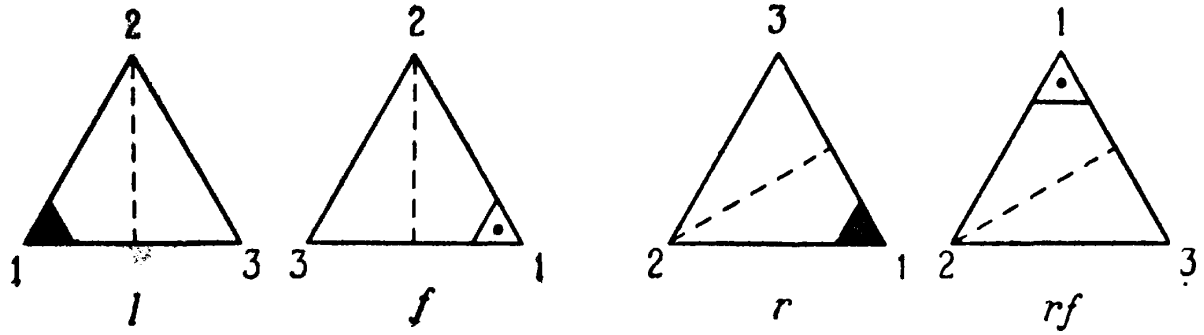



Рис. 4.2.

*будем считать, что диаграмма изображает движение x, которое переводит фигуру из заданного исходного положения в положение, отмеченное символом x.*

В дальнейшем мы убедимся, что удобно через $r$ обозначать вращение на 120° против часовой стрелки вокруг оси, проходящей через центр треугольника перпендикулярно его плоскости. Тогда первые три положения, как мы уже видели, передают движения $I$, $r$, $r^2$. (Напомним, что $I$ есть вращение на угол $0° \pm (360k)°$.)

Чтобы получить одно из новых положений, необходимо опрокинуть треугольник. Мы достигнем этого, повернув треугольник на 180° вокруг высоты, проходящей через одну из вершин. Выберем в качестве оси вращения высоту, проходящую через вершину 2. Вращение на 180° вокруг этой высоты (как оси вращения) мы обозначим через $f$. Конечно, $f$ может быть и любым вращением на угол $180° \pm (360k)°$ вокруг этой оси. Оно изображено на рис. 4.2.

Попытаемся уяснить себе, что следует понимать под символом $fr$. Положения, помеченные на рис. 4.1 символами $f$ и $fr$, показаны отдельно на рис. 4.3. Когда мы смотрим на этот рисунок, то создается впечатление, что $r$ обозначает вращение на 120° *по* часовой стрелке, а не *против*, как мы условились прежде. Это

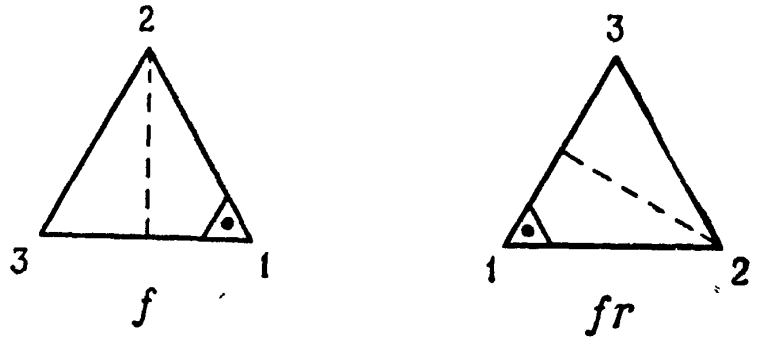



Рис. 4.3.

кажущееся противоречие исчезнет, если мы заметим, что *опрокидывание треугольника приводит к изменению направления оси вращения r на противоположное*. Прежде всего нам надо подробнее описать вращение $r$. За ось вращения мы взяли прямую, проходящую через центр равностороннего треугольника

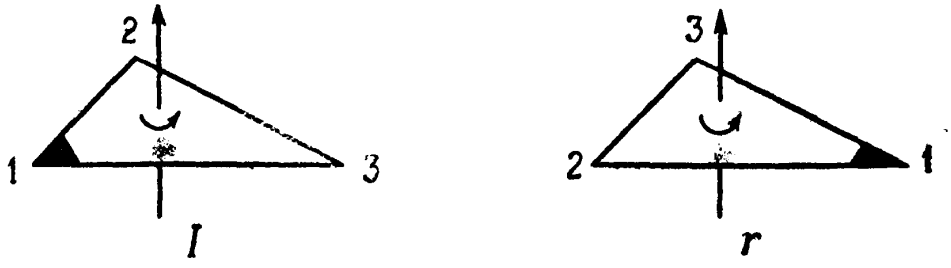



Рис. 4.4.

перпендикулярно его плоскости. На этой оси задано направление, как показывает стрелка на рис. 4.4, и наше вращение $r$ связано со следующим объединением вершин в пары: $1 \to 2$, $2 \to 3$, $3 \to 1$ (т. е. вершина 1 замещается вершиной 2, вершина 2 — вершиной 3 и вершина 3 — вершиной 1).

Представим себе теперь, что направляющая стрелка оси — это нарезанный конец правостороннего винта. Чтобы выполнить вращение $r$, повернем треугольник на 120° в направлении, в котором мы стали бы ввинчивать правосторонний винт. Если первый

треугольник подвергнуть движению $f$, то он займет положение, которое помечено буквой $f$ на рис. 4.5. Заметим, что направление оси изменилось при этом на противоположное. Если после этого треугольник подвергнуть вращению $r$, которое можно интерпретировать как ввинчивание правостороннего винта, то он займет положение, помеченное на рис. 4.5 символом $fr$. Таким образом, применяется ли вращение $r$

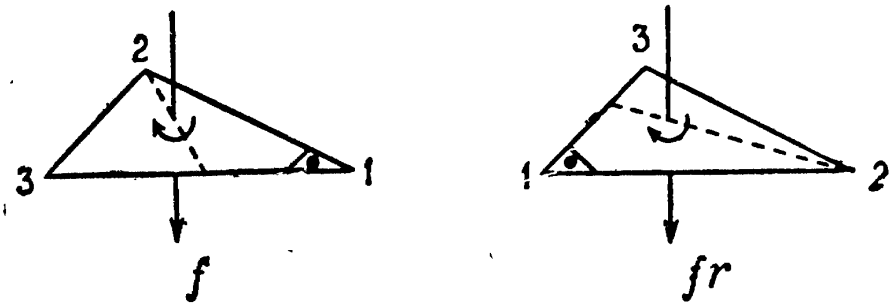



Рис. 4.5.

к треугольнику, находящемуся в положении, помеченном символом $I$, или к треугольнику, находящемуся в положении, помеченном буквой $f$, оно одинаковым образом разбивает на пары вершины треугольника: $1 \to 2$, $2 \to 3$, $3 \to 1$.

Множество, состоящее из шести классов движений, изображенных с помощью шести положений треугольника, с бинарной операцией суперпозиции, или «последовательного выполнения», образует группу. Мы знаем, что эта операция ассоциативна и что единичный элемент $I$ является элементом рассматриваемого множества. Справедливость аксиомы об обратном элементе очевидна в силу следующих интуитивных соображений: если данное движение преобразует одно положение в другое, то существует преобразование, возвращающее фигуру в исходное положение (обратное преобразование).

Поучительно продемонстрировать некоторые групповые свойства с помощью таблицы умножения. Отметим, что $r^3 = I$ и $f^2 = I$ (это следует из самого характера рассматриваемых движений). Используя эти свойства, составим табл. 4.5. Чтобы завершить построение таблицы умножения нашей группы, надо представить каждое из стоящих в ячейках табл. 4.5 выражений как один из элементов $I$, $r$, $r^2$, $f$, $fr$, $fr^2$.

*Таблица 4.5*

| I сомножитель \ II сомножитель | $I$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
|---|---|---|---|---|---|---|
| $I$ | $I$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
| $r$ | $r$ | $r^2$ | $I$ | $rf$ | $rfr$ | $rfr^2$ |
| $r^2$ | $r^2$ | $I$ | $r$ | $r^2f$ | $r^2fr$ | $r^2fr^2$ |
| $f$ | $f$ | $fr$ | $fr^2$ | $I$ | $r$ | $r^2$ |
| $fr$ | $fr$ | $fr^2$ | $f$ | $frf$ | $frfr$ | $frfr^2$ |
| $fr^2$ | $fr^2$ | $f$ | $fr$ | $fr^2f$ | $fr^2fr$ | $fr^2fr^2$ |

Мы проведем подробно упрощение двух из этих выражений, а остальное предоставим сделать читателю. Прежде всего покажем, что $frfr = I$. Рассмотрим последовательность диаграмм на рис. 4.6. Первая из

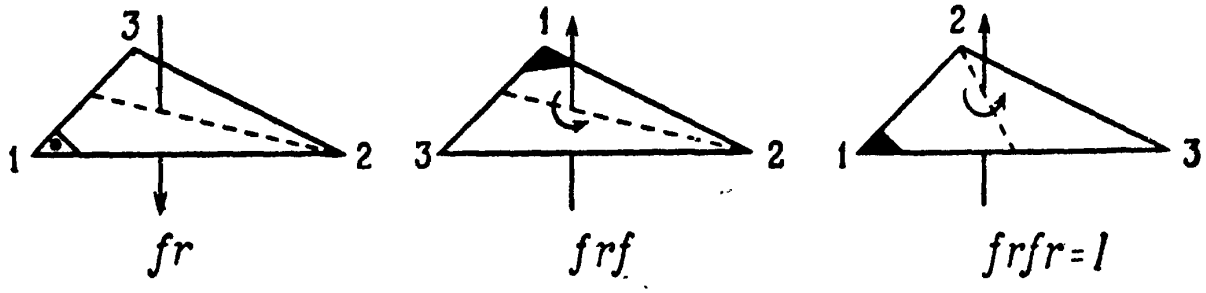



Рис. 4.6.

них изображает движение $fr$. Исходя из этого положения треугольника, произведем его поворот на 180° вокруг высоты, проходящей через вершину 2. В результате получается движение $frf$ (последовательно выполняются движения $fr$ и $f$), изображенное на второй диаграмме. Затем мы повернем треугольник на 120° в направлении, как если бы мы *ввинчивали* правосторонний винт, вокруг оси, проходящей через центр; окончательный результат $frfr$ изображен на последней диаграмме и выглядит как начальное

положение, обозначенное через $I$. Таким образом, $frfr = I$.

Теперь покажем, что $rfr^2 = I$ при помощи диаграмм на рис. 4.7.

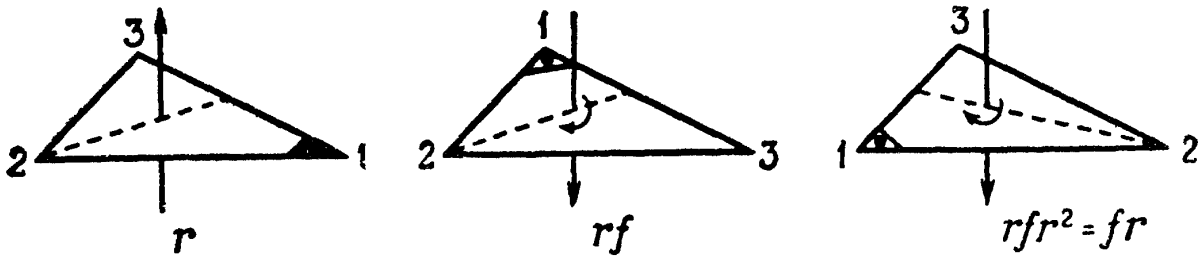



Рис. 4.7.

Используя все такие упрощенные произведения, мы составим табл. 4.6. Таблица показывает, что

*Таблица 4.6*

| I сомножитель \ II сомножитель | $I$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
|---|---|---|---|---|---|---|
| $I$ | $I$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
| $r$ | $r$ | $r^2$ | $I$ | $fr^2$ | $f$ | $fr$ |
| $r^2$ | $r^2$ | $I$ | $r$ | $fr$ | $fr^2$ | $f$ |
| $f$ | $f$ | $fr$ | $fr^2$ | $I$ | $r$ | $r^2$ |
| $fr$ | $fr$ | $fr^2$ | $f$ | $r^2$ | $I$ | $r$ |
| $fr^2$ | $fr^2$ | $f$ | $fr$ | $r$ | $r^2$ | $I$ |

(1) Операция «последовательного выполнения» является бинарной операцией на нашем множестве элементов.

(2) Аксиома об обратных элементах выполнена, так как $I$ встречается точно один раз в каждой строке и столбце[1]). Мы можем сразу определить обрат-

[1]) Из этого свойства таблицы ясно, что для каждого элемента существует левый обратный и правый обратный. Их совпадение легко проверить, используя ассоциативность операции, но можно усмотреть и из таблицы, заметив, что элементы $I$ расположены симметрично относительно главной диагонали. — *Прим. перев.*

ный для любого элемента группы. Например, схема

$$\begin{array}{c} fr \\ \vdots \\ fr \ \ldots \ I \end{array}$$

показывает, что $(fr)^{-1} = fr$.

(3) Группа некоммутативна. Достаточно беглого взгляда на элементы таблицы, расположенные симметрично относительно главной диагонали, чтобы убедиться, например, в том, что $(fr)f = r^2 \neq r = f(fr)$.

(4) Строки и столбцы являются перестановками элементов верхней строки или левого столбца соответственно — «совпадение», уже отмечавшееся прежде.

(5) $(3 \times 3)$-квадрат в левом верхнем углу — это в точности таблица умножения группы порядка 3 вращений равностороннего треугольника в его плоскости. На другом конце главной диагонали, в правом нижнем углу расположен $(3 \times 3)$-квадрат, который получается перестановкой элементов левого верхнего квадрата. В левом нижнем и правом верхнем углах находятся $(3 \times 3)$-квадраты, которые воспроизводят два «главных» (расположенных на главной диагонали) квадрата с той лишь разницей, что перед каждым элементом стоит символ $f$. Если $M$ означает *множество* элементов в левом верхнем квадрате, то табл. 4.7 в схематической форме отражает только что описанные особенности внутреннего строения таблицы умножения:

*Таблица 4.7*

| | |
|---|---|
| $M$ | $fM$ |
| $fM$ | $M$ |

Эта схема наводит нас на размышления о возможностях дальнейшего уточнения методов анализа структуры группы. Мы исследуем эти возможности в главе, посвященной нормальным подгруппам и факторгруппам.

**Строение таблицы умножения группы.** Теперь мы ближе познакомимся с внутренним строением таблицы умножения группы. Прежде всего мы исследуем «совпадение», отмеченное выше в п. (4), а именно тот факт, что строки и столбцы таблицы умножения группы являются перестановками верхней строки и левого столбца соответственно. Мы покажем, что это совсем не случайное совпадение, а скорее характеристическое свойство таблицы умножения произвольной группы. После того как это будет сделано, мы станем рассматривать таблицу умножения группы как квадратную таблицу, которая образована расположенными в определенном порядке символами[1]). В этой таблице мы будем выявлять взаимное расположение (конфигурации) символов и показывать, как оно отражает групповые связи. Таким путем структура группы будет выражена через «геометрические» свойства ее таблицы умножения. Можно показать, что и, обратно, квадратная таблица с такими «геометрическими» свойствами является таблицей умножения некоторой группы.

*«Разрешимость» групповых «уравнений».* Когда мы имеем дело с элементами группы и соотношениями между ними, то часто бывает необходимо уметь отвечать на следующий вопрос: существует ли для заданных элементов $a$ и $b$ в некоторой группе элемент $x$ этой группы, такой, что $ax = b$? Мы утверждаем, что $x = a^{-1}b$ и есть искомый элемент группы, так как

$$a(a^{-1}b) = (aa^{-1})\,b = Ib = b,$$

т. е. $x = a^{-1}b$ удовлетворяет групповому «уравнению» $ax = b$.

Возможны ли другие решения этого уравнения? Мы ответим на этот вопрос, показав, что *если $y$ есть*

---

[1]) То есть в дальнейшем мы под таблицей умножения будем понимать не всю построенную выше таблицу, а только ее внутренний квадрат, в котором стоят произведения. О верхней строке и левом столбце мы будем говорить как о строке, стоящей над таблицей, и столбце, стоящем слева от таблицы. — *Прим. перев.*

*решение уравнения* $ax = b$, *то* $y = a^{-1}b$; другими словами, элемент $a^{-1}b$ является *единственным* решением. Сначала предположим, что существует элемент $y$ нашей группы, для которого $ay = b$. Мы знаем, что

$a^{-1}$ существует (аксиома об обратных элементах).

Можно умножить каждую часть уравнения $ay = b$ слева на $a^{-1}$ и убедиться, что $a^{-1}(ay)$ и $a^{-1}(b)$ представляют собой один и тот же элемент группы, т. е.

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

Следовательно,

$$(a^{-1}a)\,y = a^{-1}b \qquad \text{(ассоциативность)},$$

$$Iy = a^{-1}b,$$

или

$$y = a^{-1}b \qquad \text{(аксиома о единице)}.$$

Так как мы уже проверили подстановкой, что элемент $a^{-1}b$ удовлетворяет уравнению $ax = b$, наше утверждение, что элемент $a^{-1}b$ является единственным решением, доказано. Отметим, что *для доказательства были необходимы все групповые аксиомы.*

Решение уравнения вида

$$xa = b,$$

где $a$ и $b$ — элементы группы, может быть получено аналогично. Умножая справа на $a^{-1}$, получаем решение

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

Сформулируем наш способ решения как «правило»: чтобы «решить» уравнение $ax = b$, умножаем его *слева* на $a^{-1}$ и получаем $x = a^{-1}b$; чтобы «решить» уравнение $xa = b$, умножаем его *справа* на $a^{-1}$ и получаем $x = ba^{-1}$.

Упражнение 5. Найти $x$ в каждом из следующих уравнений:

(a) $abx = c$;
(b) $axb = c$;
(c) $xab = c$;
(d) $a = bx^2$ и $x^3 = I$;
(e) $x^3 = a$ и $x^4 = I$;
(f) $x^{-1} = abc$.

В качестве первого приложения предыдущих результатов докажем одно соотношение между элементами группы и их обратными, которое будет полезно в дальнейшем. Предположим, что мы рассматриваем элемент группы, который представлен как произведение других элементов группы. Пусть, например,

$$d = ab.$$

Вопрос таков: как можно представить элемент $d^{-1}$, обратный к элементу $d$? Эквивалентный вопрос: как найти элемент группы $x$, такой, что $dx = I$ или $abx = I$? Из предыдущих рассуждений мы знаем, что это уравнение имеет единственное решение. Чтобы найти его, умножим сначала уравнение слева на $a^{-1}$; мы получим

$$a^{-1}abx = a^{-1}I, \quad \text{или} \quad bx = a^{-1}.$$

Затем умножим его слева на $b^{-1}$ и получим

$$b^{-1}bx = b^{-1}a^{-1}, \quad \text{или} \quad x = b^{-1}a^{-1}.$$

Чтобы убедиться в справедливости равенства $d^{-1} = b^{-1}a^{-1}$, мы покажем, что $d(b^{-1}a^{-1}) = I$. Действительно,

$$\begin{aligned} d(b^{-1}a^{-1}) &= ab(b^{-1}a^{-1}) = \\ &= a(bb^{-1}a^{-1}) = a[(bb^{-1})a^{-1}] = \\ &= aa^{-1} = \\ &= I. \end{aligned}$$

Аналогично, если $d = abc$, то $d^{-1} = c^{-1}b^{-1}a^{-1}$. Схема ясна, и мы можем высказать общее утверждение: если $d = a_1a_2 \ldots a_n$, то $d^{-1} = a_n^{-1}a_{n-1}^{-1} \ldots a_2^{-1}a_1^{-1}$, или, иначе, *обратный к произведению есть произведение обратных к сомножителям, взятых в противоположном порядке.*

В качестве еще одного приложения процедуры решения групповых уравнений докажем теорему, которая объясняет, почему любая строка (столбец) таблицы умножения группы является перестановкой элементов любой другой строки (столбца).

Предположим, что мы рассматриваем группу порядка $n$, состоящую из элементов $a_1, a_2, \ldots, a_n$ (конечно, среди них есть единичный элемент $I$, но он не обозначен этим символом). Выберем среди них произвольный элемент $a_j$ и обозначим его через $b$. Образуем множество из $n$ произведений

$$ba_1, \ ba_2, \ \ldots, \ ba_n,$$

умножая элементы слева на $b$. Мы утверждаем, что эти произведения дают $n$ исходных элементов группы, быть может, в другом порядке. Чтобы доказать это, мы покажем сейчас, что никакие два элемента в множестве таких произведений не могут представлять собой один и тот же элемент группы. Предположим, например, что $ba_i = ba_j$, где $i \neq j$. Тогда, умножая слева на $b^{-1}$, получаем

$$b^{-1}ba_i = b^{-1}ba_j, \quad \text{или} \quad a_i = a_j \quad (i \neq j).$$

Но $a_i$ и $a_j$ — различные элементы группы, если $i \neq j$; следовательно, предположение, что $ba_i = ba_j$, приводит к противоречию, и, значит, $ba_i \neq ba_j$ при $i \neq j$. Таким образом, все $n$ произведений различны. Так как каждый из *различных* элементов $ba_1, ba_2, \ldots, ba_n$ является элементом исходной группы, то все вместе они должны давать все $n$ ее элементов. Это завершает доказательство.

Мы доказали наше утверждение для умножения слева. Аналогичные соображения можно применить к множеству произведений, получающихся умножением элементов группы на фиксированный элемент справа, и это завершит доказательство следующей теоремы о конечных группах:

Теорема 1. *Если* $a_1, a_2, \ldots, a_n$ *— различные элементы группы порядка* $n$ *и если* $b$ *— фиксированный элемент этой группы (он должен, конечно, совпадать с одним из элементов* $a_1, \ldots, a_n$*), то каждое из множеств произведений*

$$ba_1, \ ba_2, \ \ldots, \ ba_n \quad \text{и} \quad a_1b, \ a_2b, \ \ldots, \ a_nb$$

*содержит все элементы группы, возможно, в другом порядке (а именно всякий раз, когда $b \neq I$).*

Эта теорема окончательно убеждает нас в том, что любая групповая таблица умножения состоит из строк и столбцов, которые являются перестановками строки, стоящей над таблицей, и столбца, стоящего слева от таблицы, соответственно.

Соображения, которые мы сейчас изложим, преследуют цель показать, с одной стороны, что групповые аксиомы и их следствия налагают определенные требования на взаимное расположение элементов в таблице умножения и, с другой стороны, что квадратная таблица «такого образца» является таблицей умножения некоторой группы. Эти частные рассуждения стоят несколько в стороне от основной линии изложения, так что не беда, если это короткое отступление и не будет полностью усвоено при первом чтении.

Предположим, что задано множество символов, образующих квадратную таблицу, которая является таблицей умножения некоторой группы. Тогда таблица обладает следующими пятью свойствами. (Читатель может обратиться к таблице умножения группы порядка 6 на стр. 48, чтобы проследить эти свойства на конкретном примере.)

(1) Таблица содержит в точности столько различных символов, сколько у нее строк (столбцов); таким образом, *если квадратная таблица имеет $n$ строк и $n$ столбцов, то среди $n^2$ символов, составляющих таблицу, находится в точности $n$ различных.* Это свойство таблицы отражает тот факт, что группа есть множество из $n$ элементов с бинарной операцией.

(2) *Каждая строка и каждый столбец содержат каждый символ в точности один раз.* Это в сущности утверждение теоремы 1.

(3) Предположим, что символы, представляющие все различные элементы некоторой группы, расположены в произвольном, но фиксированном порядке и что строки и столбцы групповой таблицы умножения

помечены согласно этому упорядочению. Например, пусть мы имеем упорядоченные символы $a$, $b$, $I$, $c$, ..., ..., $k$. Мы знаем, что символ $I$ для единичного элемента должен встретиться при любом упорядочении символов. (В нашем примере мы поставили его на третье место.) В соответствии с групповой аксиомой о *единичном элементе* квадратная таблица должна обладать таким свойством: *одна из строк нашей таблицы, а именно строка, помеченная символом I, тождественна строке символов, расположенной над таблицей, и один из столбцов, а именно столбец, помеченный символом I, тождествен столбцу символов, расположенному слева от таблицы.* Это свойство иллюстрируется таблицей 4.8.

*Таблица 4.8*

| | $a$ | $b$ | $I$ | $c$ | ... | $k$ |
|---|---|---|---|---|---|---|
| $a$ | | | $a$ | | | |
| $b$ | | | $b$ | | | |
| $I$ | $a$ | $b$ | $I$ | $c$ | ... | $k$ |
| $c$ | | | $c$ | | | |
| . | | | . | | | |
| . | | | . | | | |
| . | | | . | | | |
| $k$ | | | $k$ | | | |

(4) Групповая аксиома об *обратных элементах* определяет такое свойство квадратной таблицы: *каждый символ таблицы можно связать с другим символом так, что на пересечении строки, помеченной первым из этих символов, скажем r, и столбца, над которым стоит второй символ (обозначим его s), стоит символ I; на пересечении строки, помеченной символом s, и столбца, над которым стоит символ r, также стоит символ I, и эти два символа I расположены симметрично относительно главной диагонали.* Это расположение элементов (табл. 4.9) отражает тот факт, что $rs = sr = I$ или что $s$ есть обратный к $r$ элемент.

(5) Закон ассоциативности соответствует следующему свойству квадратной таблицы, являющейся таблицей умножения некоторой группы. Предположим, что мы так выбрали *внутри* таблицы два произвольных символа $r$ и $s$, что на пересечении столбца, содержащего $r$, и строки, содержащей $s$, стоит символ $I$.

*Таблица 4.9*

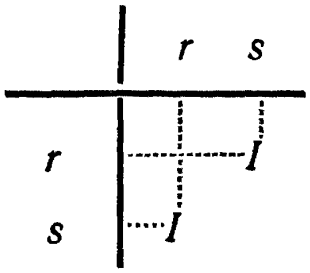
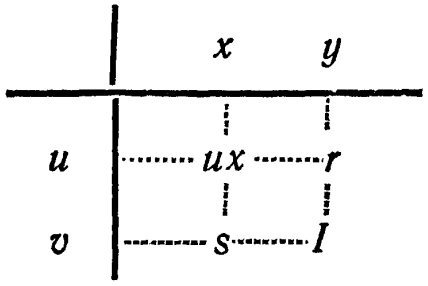



*Таблица 4.10*



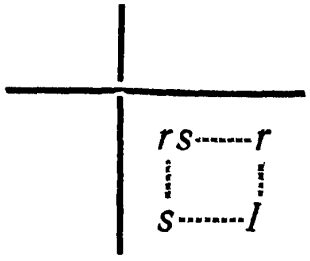

Над столбцом, содержащим символ $r$, стоит некоторый элемент группы, скажем $y$. Строка, содержащая символ $r$, помечена слева с помощью некоторого элемента группы, который мы обозначим через $u$. Аналогично, над столбцом, содержащим $s$, стоит элемент $x$, а строка, содержащая $s$, помечена элементом $v$ (табл. 4.10). Закон ассоциативности проявляется в том, что *на пересечении строки, содержащей r, и столбца, содержащего s, т. е. в клетке для их произведения, должен находиться элемент rs.* Чтобы убедиться в этом, заметим, что

$$vy = yv = I, \quad uy = r, \quad vx = s,$$

т. е.

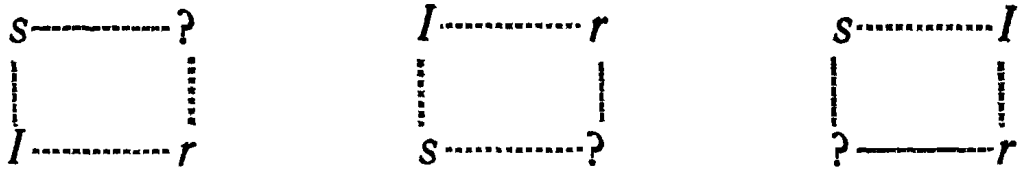
$$ux = u(yv)x = (uy)(vx) = rs.$$

Таким образом, таблица умножения должна включать такую конфигурацию:




Упражнение 6. Пусть задана квадратная таблица, которая является таблицей умножения некоторой группы. Какой элемент должен стоять в четвер-

той (с вопросительным знаком) вершине каждого из следующих «прямоугольников» *внутри* таблицы:




Чтобы завершить обсуждение свойств таблицы умножения группы, мы вернемся к вопросам, поднятым в начале этой главы. Сколько информационных символов требуется, чтобы задать группу как единый математический объект? И как можно записать эту информацию? Вот ответы на эти вопросы: для конечной группы порядка $n$ нам нужно $n^2$ информационных символов, а именно все возможные попарные произведения элементов группы. Эти $n^2$ произведений расположены в квадратной таблице умножения. Квадратная таблица будет таблицей умножения группы тогда и только тогда, когда она обладает указанными выше пятью «геометрическими» свойствами.

Упражнение 7. Построить таблицу умножения группы с элементами 1, 2, 3, 4 и бинарной операцией «умножение по модулю 5» (см. стр. 36, где разбиралась эта группа остатков).

ГЛАВА 5

# ОБРАЗУЮЩИЕ ЭЛЕМЕНТЫ ГРУППЫ

Хотя из таблицы умножения группы можно извлечь все то, что мы хотим знать о группе, поскольку в ней указаны все попарные произведения элементов группы, можно предвидеть ряд трудностей, которые возникнут при любой попытке неограниченно расширить область ее применения. Представьте себе, например, что вам нужно проанализировать группу порядка 60 с помощью ее таблицы умножения.

Возвратимся к понятию образующей. Оно позволяет описывать группу способом, не зависящим от ее порядка. Кроме того, понятие образующей группы будет играть основную роль при переходе к осуществлению одной из основных наших целей — графическому представлению групп.

Пусть $a$ и $b$ — элементы некоторой группы. Тогда, согласно аксиоме об обратных элементах, $a^{-1}$ и $b^{-1}$ также являются элементами данной группы наряду с $ab^{-1}a$, $aba^{-1}b$ и т. д. Любое произведение, которое можно записать, используя в качестве сомножителей элементы $a$, $b$, $a^{-1}$, $b^{-1}$ в любом порядке и в любом конечном числе, является элементом этой группы, согласно определению бинарной операции. Если *все* элементы группы можно записать в виде произведений, включающих лишь $a$ и $b$ (и их обратные), то мы назовем $a$ и $b$ *образующими* (или образующими элементами) группы. Мы можем распространить это понятие образующих на множество из более чем двух элементов. Если $S$ — множество элементов группы $G$,

$$S = \{a, b, c, \ldots\},$$

и если *все* элементы группы $G$ могут быть выражены в виде произведений элементов из $S$ (и их обратных),

то мы назовем элементы множества $S$ *образующими* группы $G$ [1]).

Простейший случай — это группа с одной образующей, скажем $a$; все ее элементы могут быть представлены как произведения, содержащие в качестве сомножителей $a$ и $a^{-1}$. Мы уже сталкивались с группой, порожденной одним элементом: группа вращений треугольника в его плоскости имеет таблицу умножения 5.1 (см. стр. 38—39), и так как $I = aa^{-1}$, то ясно, что каждый из трех элементов группы $I$, $a$, $a^2$ является произведением, содержащим в качестве сомножителей лишь $a$ и $a^{-1}$.

*Таблица 5.1*

| | $I$ | $a$ | $a^2$ |
|---|---|---|---|
| $I$ | $I$ | $a$ | $a^2$ |
| $a$ | $a$ | $a^2$ | $I$ |
| $a^2$ | $a^2$ | $I$ | $a$ |

**Циклические группы.** Мы получим одно из существенных свойств группы вращений треугольника, если выпишем степени образующей $a$:

$$a, a^2, a^3, a^4, a^5, a^6, a^7, \ldots .$$

Так как $a^3 = I$, то эту последовательность можно переписать так:

$$a, a^2, I, a, a^2, I, a, \ldots .$$

Она представляет собой *циклическое* повторение основной серии $a$, $a^2$, $I$. Именно по этой причине данная группа называется *циклической группой порядка* 3.

Можно определить циклическую группу любого порядка: если любой элемент группы выражается

[1]) И будем говорить, что они *порождают* группу $G$. — *Прим. перев.*

в виде степени единственной образующей, то группа называется *циклической*. Обычно мы будем использовать для обозначения циклической группы букву $C$, а ее порядок обозначать числом в нижнем индексе. Таким образом, $C_3$ обозначает циклическую группу порядка 3, а $C_n$ — циклическую группу порядка $n$.

Если $n$ — наименьшее целое положительное число, для которого $a^n = I$, то группа, порожденная элементом $a$, будет иметь *порядок* $n$. Наименьшая положительная степень $n$, такая, что $a^n = I$, называется *порядком* или *периодом* элемента $a$. Например, в описанной выше циклической группе $C_3$ выполняются

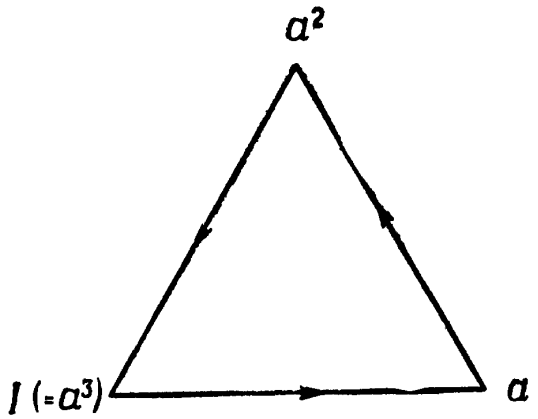



Рис. 5.1.

соотношения $a^6 = I$, $a^9 = I$, $a^{-3} = I$ и т. д. Так как $a^3 = I$ и 3 — наименьшая положительная степень, для которой $a^n = I$, то мы говорим, что $a$ есть элемент *порядка* (*периода*) 3.

Если $a$ порождает циклическую группу $C_n$, то последовательность степеней элемента $a$ представляет собой циклическое повторение основной серии $a, a^2, \ldots, a^n = I$. Это свойство допускает геометрическую интерпретацию, которая в свою очередь приводит к осуществлению нашей цели — построению графического представления группы. Например, циклическая группа порядка 3 наводит на мысль о *треугольнике, каждая вершина которого соответствует элементу группы* (рис. 5.1). Каждой стороне треугольника приписано направление, которое указано стрелкой. *Движение в направлении, указанном стрелкой, соответствует умножению справа на образующий элемент $a$ группы.* Таким образом, отправляясь из

вершины, помеченной символом $a^2$, передвинуться в направлении, указанном стрелкой, к вершине $I$ — это все равно, что образовать произведение $a^2a = a^3 = I$. *Движение в направлении, противоположном указанному стрелкой, соответствует умножению справа на элемент* $a^{-1}$, *обратный к образующей* $a$. Например, отправляясь из вершины, помеченной символом $a^2$, передвинуться в направлении, противоположном указанному стрелкой, направленной к этой вершине, — это все равно, что образовать произведение $a^2a^{-1} = aaa^{-1} = a$.

ГЛАВА 6

# ГРАФ ГРУППЫ

Возникает предположение, что многоугольник, сторонам которого приписано направление, можно рассматривать как геометрический эквивалент циклической группы, или *граф* циклической группы. Давайте посмотрим, что мы знаем об основных свойствах группы и как они отражаются в только что предложенной геометрической интерпретации.

Если $a$ — образующая циклической группы, то по определению каждый элемент может быть представлен как произведение сомножителей $a$ и $a^{-1}$. Обратно, любое произведение сомножителей $a$ и $a^{-1}$ есть элемент группы. Рассмотрим, например, произведения

$$a, \quad aaa^{-1}, \quad a^{-1}aaa^{-1}a;$$

ясно, что все три произведения представляют собой один и тот же элемент группы.

По очевидной аналогии мы назовем конечную последовательность образующих и их обратных *словом*. Тогда каждому слову, составленному из символов $a$ и $a^{-1}$ (как мы будем говорить, «слову от символов $a$ и $a^{-1}$»), соответствует элемент циклической группы, порожденной $a$. Так как любой наперед заданный элемент может быть представлен в виде слова бесконечно многими способами, то представление элемента группы в виде слова неоднозначно.

Если $x$ — некоторый элемент циклической группы порядка 3, то любое слово, представляющее элемент $x$, можно понимать как движение по графу, рассмотренному в конце предыдущей главы. Пусть слово $aaa^{-1}$ представляет элемент $x$. Будем интерпретиро-

вать его как такое движение по графу, изображенному на рис. 6.1:

1. *Возьмем за исходную точку вершину, помеченную символом I.* Так как первым сомножителем в слове, представляющем элемент $x$, является $a$, мы движемся из *I в направлении, указанном стрелкой,* к другому концу отрезка, который изображен на рис. 6.2. Этот конец является вершиной, помеченной символом $a$, и будет служить исходной точкой для дальнейшего движения.

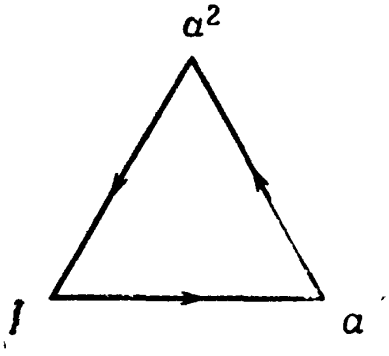



Рис. 6.1.

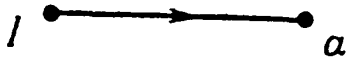



Рис. 6.2.

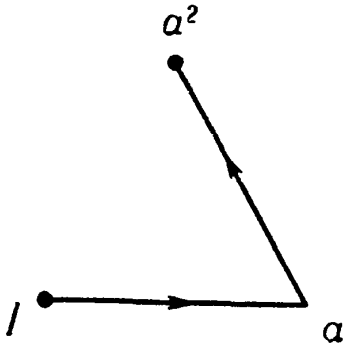



Рис. 6.3.

2. Так как второй сомножитель равен $a$, мы выходим из достигнутой на первом шаге вершины и движемся *в направлении, указанном стрелкой,* к другому концу отрезка (рис. 6.3). Этот конец есть вершина, помеченная символом $a^2$; он и будет служить исходной точкой для дальнейшего движения.

3. Так как третий сомножитель есть $a^{-1}$, *обратный* к $a$, мы отправляемся из вершины, в которую пришли на втором шаге, и движемся в направлении, *противоположном* указанному стрелкой, к другому концу отрезка. Этот конец — вершина, помеченная символом $a$, — мог бы служить исходной точкой для дальнейшего движения. Однако в данном слове третий сомножитель последний, и потому дальнейших движений не происходит, т. е. путь, соответствующий слову $aaa^{-1}$, заканчивается в вершине, помеченной символом $a$.

Слово, соответствующее элементу $x$, интерпретируется, таким образом, как *множество направлений при движении вдоль некоторого пути* в графической

сети. Каждому слову соответствует определенная последовательность движений вдоль направленных отрезков, и, обратно, любой путь вдоль направленных отрезков графа группы, начинающийся из вершины $I$, соответствует конкретному слову.

Представление группы как сети, состоящей из направленных отрезков (или ребер), где вершины соответствуют элементам, а отрезки — умножению на образующие группы и их обратные, было введено Кэли еще в XIX веке. Такая сеть, или граф, часто называется *диаграммой Кэли.*

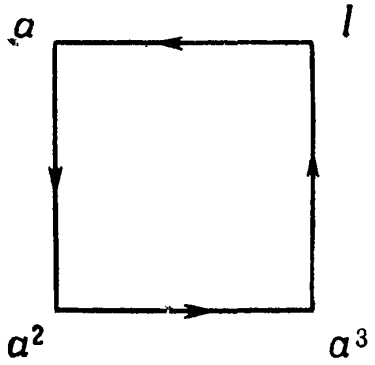



Рис. 6.4.

Вращения квадрата в его плоскости (стр. 16) составляют циклическую группу порядка 4, $C_4$. Граф этой группы представлен на рис. 6.4.

Замечания. 1) Вершин у графа столько же, сколько элементов в группе.

2) Вершина $I$ выбирается произвольно.

3) В каждой вершине сходятся два отрезка, один соответствует умножению справа на образующую $a$ и направлен *от* вершины, а другой соответствует умножению справа на элемент $a^{-1}$, обратный к образующей, и направлен *к* вершине.

4) Конкретная форма графической сети не имеет значения. Важна лишь конфигурация связей между вершинами. Направленные отрезки, связывающие вершины, не обязаны быть прямолинейными, а граф не обязан иметь форму правильного многоугольника. Вы можете проявить свой вкус, выбирая ту форму, которая вам нравится, если только при этом не искажается математический смысл.

Графом циклической группы $C_n$ порядка $n$, связанной с вращениями правильного $n$-угольника в его плоскости, является $n$-угольник с направленными отрезками в качестве сторон. Например, циклическая группа порядка 6, $C_6$, соответствующая самосовмещениям правильного шестиугольника, вращающегося в своей плоскости, состоит из элементов $a$, $a^2$, $a^3$, $a^4$,

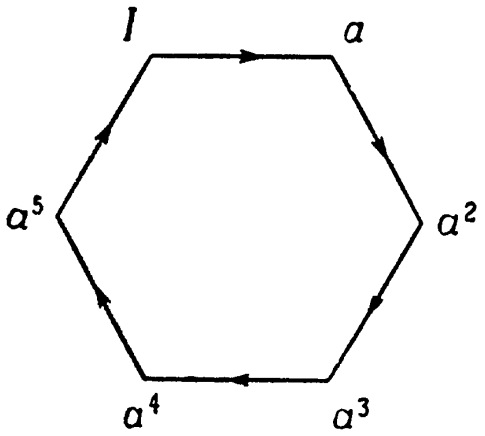



Рис. 6.5.

$a^5$ и $a^6 = I$. Шестиугольник, ребрами которого являются отрезки, направленные как на рис. 6.5, будет графом этой группы.

**Бесконечная циклическая группа.** Теперь мы построим граф *бесконечной* циклической группы. Циклическая группа определялась тем свойством, что все ее элементы можно выразить как степени одного образующего элемента $a$. Группа, порожденная элементом $a$, конечна, если существует положительное целое число $n$, такое, что $a^n = I$. Если такого положительного целого числа не существует, то каждая следующая степень элемента $a$ представляет собой новый элемент группы, и в таком случае циклическая группа будет *бесконечной*. Бесконечная аддитивная группа (стр. 25) представляет собой пример такой группы.

Конечную циклическую группу можно связать с самосовмещениями правильного $n$-угольника на плоскости и прийти к соответствующей диаграмме Кэли. Чтобы построить граф бесконечной циклической группы, нам также будет удобно опираться на некоторое геометрическое представление. Рассмотрим прямую

линию, разделенную на равные интервалы, скажем, длины 1, и ее самосовмещения, которые сдвигают эту линию вдоль самой себя на одну или несколько единиц вправо или влево. Множество всех таких самосовмещений есть бесконечная циклическая группа, порожденная сдвигом на единицу вправо. Диаграмма Кэли этой группы представлена на рис. 6.6.

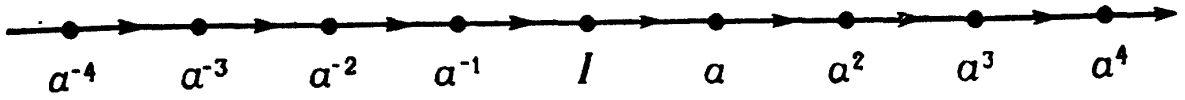



Рис. 6.6.

Примечания. 1) Естественным образом обобщив наши предыдущие обозначения, мы обозначим бесконечную циклическую группу через $C_\infty$.

2) Ясно, что за $I$ можно взять любую вершину.

3) Снова мы видим, что в каждой вершине сходятся два направленных отрезка. Движение от вершины вдоль отрезка в направлении, указанном стрелкой, соответствует умножению справа на образующую $a$; движение в направлении, противоположном указанному стрелкой, соответствует умножению справа на $a^{-1}$.

Упражнение 8. Выяснить, является ли сложение бинарной операцией на каждом из следующих множеств и, если да, то будет ли это множество бесконечной циклической группой с бинарной операцией сложения.

(a) Множество всех целых чисел, кратных 4, т. е. множество $\{\ldots, -8, -4, 0, 4, 8, \ldots\}$.

(b) Множество всех целых чисел, кратных целому числу $k$.

(c) Множество $\{\ldots, a-3, a-2, a-1, a, a+1, a+2, a+3, \ldots\}$, где $a$ — *нецелое* число.

(d) Множество $\{\ldots, -3a, -2a, -a, 0, a, 2a, 3a, \ldots\}$, где $a$ — *нецелое* число.

**Группа с двумя образующими.** Таблица умножения группы самосовмещений равностороннего тре-

угольника является примером группы с двумя образующими: вращением $r$ и опрокидыванием $f$. Элементами этой группы (стр. 47) являются

$$I, r, r^2,$$
$$f, fr, fr^2,$$

где каждый элемент первой строки получается из соседнего слева (справа) умножением справа на $r$ (или $r^{-1}$), а элементы второй строки получаются из элементов первой умножением слева на $f$. Это наводит на мысль, что для графа этой группы надо использовать *два треугольника*, соединенные отрезками, соответствующими образующей $f$ (рис. 6.7).

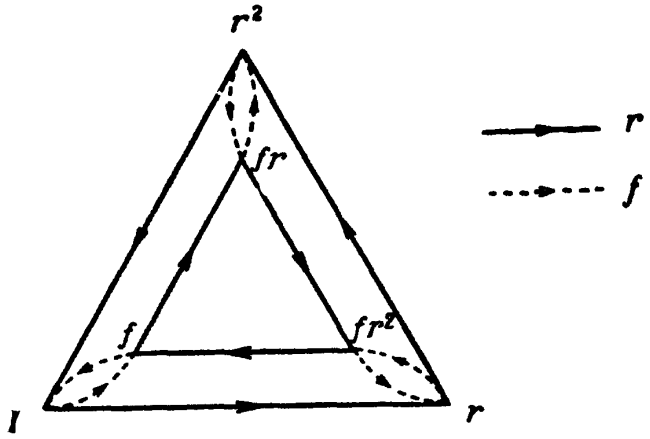



Рис. 6.7.

Мы отличаем на графе образующую $r$ от образующей $f$, используя непрерывную линию для умножения на $r$ и пунктирную для умножения на $f$. Сам Кэли предлагал различные образующие выделять различными цветами и называл этот процесс графического представления методом *цветных групп*.

В качестве следствия того факта, что рассматриваемая группа имеет *две* образующие, мы получаем, что любой путь нашего графа может быть описан последовательностью, содержащей лишь символы из множества

$$r, f, r^{-1}, f^{-1}.$$

Примерами таких последовательностей являются

$$rfr^{-1}f^{-1} \text{ и } rf^{-1}rf^{-1}r,$$

которые мы, как и раньше, будем называть *словами*. Конечно, каждое слово от образующих и их обратных является элементом группы или, говоря точнее, представляет элемент группы.

Читателю следует проверить, что произведение любых двух элементов, определенное с помощью таблицы умножения этой группы (стр. 48), совпадает с произведением, полученным с помощью графа, изображенного на рис. 6.7. Чтобы, например, проверить

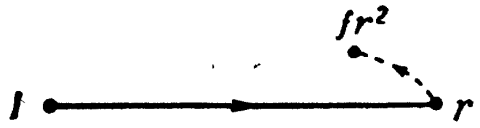



Рис. 6.8.

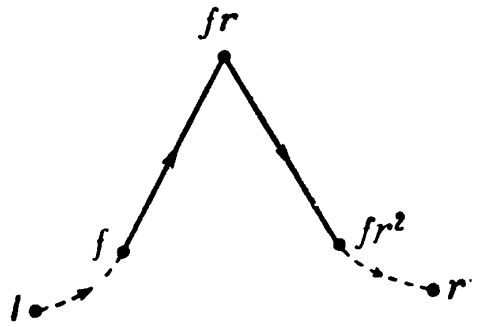



Рис. 6.9.

равенство $rf = fr^2$, пройдем сначала $r$-отрезок, выходящий из $I$, а затем $f$-отрезок, входящий в вершину, помеченную символом $fr^2$ (рис. 6.8). Путь на рис. 6.9 показывает, что $frrf = r$.

**Основные свойства графа группы.** Наши примеры графов различных групп имеют некоторые общие существенные свойства.

(1) Элемент группы ⟷ Вершина графа.

*Элементы группы находятся во взаимно однозначном соответствии с вершинами графа.* Каждая вершина графа соответствует в точности одному элементу группы, и наоборот.

(2) Образующая ⟷ Ребра одного «цвета».

*Каждое ребро графической сети есть направленный отрезок, и отрезки одного «цвета» связаны с одной и той же образующей группы.* Движение, начинающееся в некоторой вершине, вдоль отрезка в направлении, указанном стрелкой, соответствует умножению справа на связанный с этим отрезком образующий элемент (назовем его $a$), в то время как движение вдоль отрезка в направлении, противоположном

указанному стрелкой, соответствует умножению справа на $a^{-1}$ — элемент, обратный к образующей. Например, если $A$, $B$ и $C$ на рис. 6.10 суть вершины графа, соответствующие элементам $x, y$ и $z$ некоторой группы соответственно, то движение от $B$ к $C$ отвечает

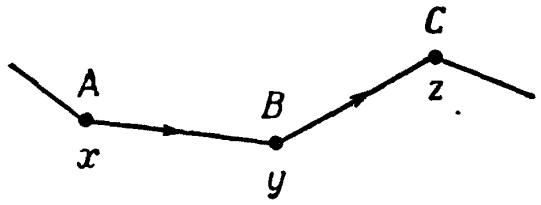



Рис. 6.10.

умножению элемента $y$ на $a$, так что $ya = z$, а движение от $B$ к $A$ отвечает умножению элемента $y$ на $a^{-1}$, т. е. $ya^{-1} = x$.

(3) Слово ⟷ Путь.

*Каждое слово, представляющее элемент группы, можно интерпретировать как путь, или некоторую последовательность направленных отрезков графа, и наоборот.* В каждой вершине пути, соответствующего некоторому слову, очередное движение определяется следующим сомножителем в слове. Так как любой сомножитель — это или одна из образующих, или элемент, обратный к образующей, то каждая вершина является концевой точкой *двух* направленных отрезков одинакового «цвета» — одного, направленного к вершине, и другого, направленного от нее. Если группа имеет две образующие, $a$ и $b$, то в каждой вершине сходятся *четыре* ребра, так как четыре элемента $a$, $a^{-1}$, $b$, $b^{-1}$ соответствуют четырем возможным движениям, начинающимся в этой вершине. Вообще в каждой вершине есть одно «входящее» и одно «исходящее» ребро для каждой образующей.

(4) Умножение элементов ⟷ Последовательное прохождение путей.

*Умножение двух элементов группы соответствует прохождению на графе пути, составленного из двух последовательных путей.* Произведение $rs = t$ элементов $r$ и $s$ группы можно интерпретировать как путь

в графе, который строится следующим образом. Запишем $r$ и $s$ как слова от образующих и их обратных. *Выходя из вершины, соответствующей элементу* $I$, пройдем путь, описанный словом, определенным элементом $r$. Конечная точка этого пути соответствует элементу $r$. Теперь, принимая за начальную точку $r$-вершину[1]), пройдем путь, описанный словом, соответствующим элементу $s$. Этот путь закончится в вершине, соответствующей элементу $t = rs$, *вне зависимости от того, какие слова используются для представления элементов* $r$ *и* $s$.

(5) Слово, представляющее $I$ ⟷ Замкнутый путь.

*Любое слово, представляющее элемент* $I$, *соответствует замкнутому пути на графе.* Предположим, что $W$ — слово, представляющее элемент $I$. Например, в группе самосовмещений равностороннего треугольника за $W$ можно взять $frfr$. Если принять вершину, соответствующую элементу $I$, за начальную точку, то путь, определяемый словом $W$, окончится в $I$-вершине. Мы называем путь *замкнутым*, если его начальная и конечная точки совпадают. Если за начальную точку взята вершина, соответствующая элементу $t$, отличному от $I$, то путь, заданный словом $W$, окончится в $t$-вершине, так как $tW = t$. Таким образом, *если* $W$ *— слово, представляющее элемент* $I$, *то путь, определяемый этим словом, будет замкнутым вне зависимости от того, какая точка принята за начальную.*

Таким образом, граф группы обладает некоторым свойством однородности[2]). Из этого свойства графа группы следует, что его вершины можно пометить так, чтобы *любая наперед заданная вершина соответствовала элементу* $I$; см. упр. 9 на стр. 74. (См. упр. 11. на стр. 74, чтобы получить пример графа

---

[1]) То есть вершину, соответствующую элементу $r$. — *Прим. перев.*

[2]) Произвольный граф называется *однородным* степени $n$, если в каждую его вершину входит и из каждой его вершины выходит одинаковое число направленных отрезков, равное $n$. Граф группы будет однородным графом в этом смысле. — *Прим. ред.*

с направленными ребрами, который *не* однороден, т. е. *не* является графом группы. Граф из упр. 11 «дефектен», потому что содержит направленное ребро с совпадающими концевыми точками.)

(6) Разрешимость уравнения $rx = s$ ⟷ Сеть связна.

*Граф группы является связной сетью, т. е. существует путь из любой вершины в любую другую вершину.* Если $r$ и $s$ — два произвольных элемента группы, то существует элемент $x = r^{-1}s$, такой, что $rx = s$ (стр. 50). Ясно, что если $W$ — произвольное слово, представляющее элемент $x = r^{-1}s$, то $rW = s$; таким образом, если вершина, соответствующая элементу $r$, взята за начальную точку, то путь, описанный словом $W$, ведет от $r$-вершины к $s$-вершине.

Выпишем вместе все соответствия, установленные в ходе предыдущих рассуждений:

| *Группа* | *Граф* |
|---|---|
| Элемент | Вершина |
| Образующая | Направленные ребра одного «цвета» |
| Слово | Путь |
| Умножение элементов | Последовательное прохождение путей |
| Слово, представляющее элемент $I$ | Замкнутый путь |
| Разрешимость уравнения $rx = s$ | Сеть связна |

Так как мы можем произвольно выбирать вершину диаграммы Кэли, которая будет соответствовать элементу $I$, то граф является представлением одной и той же группы вне зависимости от того, помечены ли его вершины. Например, любая из неразмеченных диаграмм на рис. 6.11 полностью описывает циклическую группу порядка 4. Однако от стрелок, указывающих направление на ребрах, нам не следует пытаться избавиться. Рассмотрим два графа на рис. 6.12. Они отличаются только направлениями, которые предписаны ребрам внутреннего треугольника, но группы, которые они представляют, совершенно различны, так как только одна из них коммутативна (см. упр. 10

на стр. 74). Здесь и далее мы будем помечать вершины графов групп постольку, поскольку это необходимо для большей ясности изложения.

*Замечание о словах, представляющих элемент I.* Слово представляет элемент $I$ тогда и только тогда,

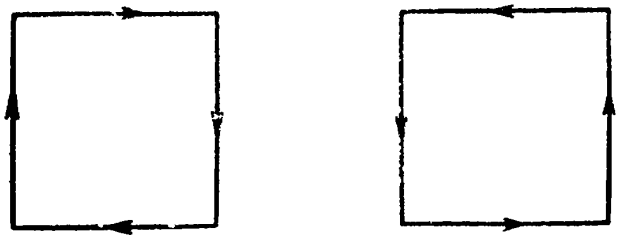


Рис. 6.11.

когда соответствующий этому слову путь в графической схеме группы замкнут. (Напомним, что путь замкнут, если совпадают его начальная и конечная точки.) Мы можем выделить два совершенно различных вида замкнутых путей. Они показаны на рис. 6.13

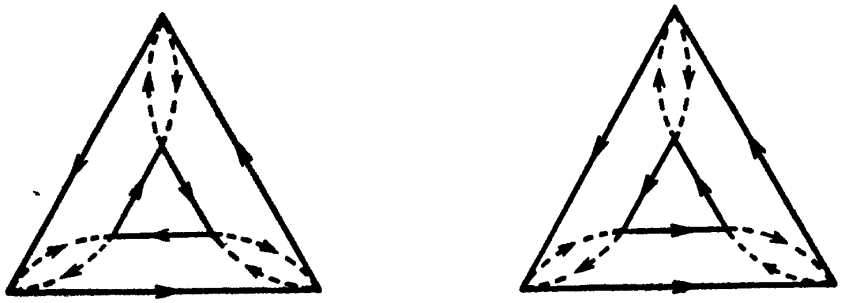


Рис. 6.12.

как пути в графе группы движений равностороннего треугольника (см. стр. 67). Оба пути замкнуты, но они существенно отличаются друг от друга как с *топологической* точки зрения, так и с точки зрения теории групп. *Топология* — это ветвь геометрии, которая изучает взаимное расположение геометрических объектов и совсем не интересуется такими их свойствами, как длина. Топология рассматривает лишь те свойства геометрической конфигурации, которые сохраняются при деформациях, не разрывающих линий и связей. С топологической точки зрения пути, соответствующие словам $W_1 = r^3$ и $W_2 = fr^{-1}r^{-1}rrf^{-1}$, существенно различаются между собой: замкнутый путь,

соответствующий слову $W_1$, не проходит второй раз ни по одному из отрезков, в то время как замкнутый путь, соответствующий слову $W_2$, возвращается по себе назад, проходя каждый отрезок второй раз, в обратном порядке и направлении. (Читателю следует сравнить эту особенность пути $W_2$ со свойством элемента, обратного к произведению элементов в группе, которое рассматривалось на стр. 52.)

Основное различие между путями $W_1$ и $W_2$ можно увидеть и исходя из аксиом, которые лежат в основе

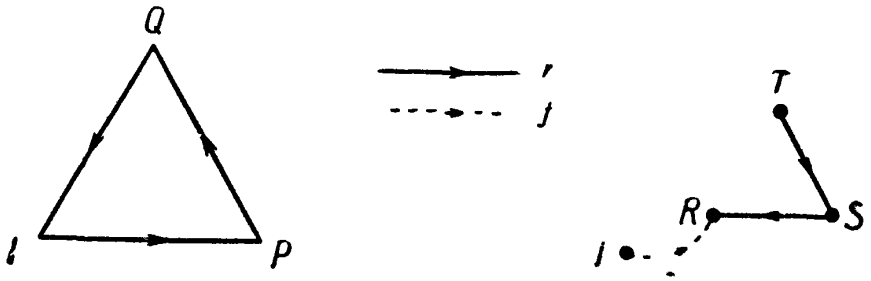



Рис. 6.13.
Слева изображен путь, ведущий из $I$ в $P$, $Q$ и $I$; соответствующее слово $W_1 = rrr = r^3 = I$.
Справа изображен путь, ведущий из $I$ в $R$, $S$, $T$, $S$, $R$ и $I$; соответствующее слово $W_2 = fr^{-1}r^{-1}rrf^{-1}$.

всех свойств группы. Путь $W_2 = fr^{-1}r^{-1}rrf^{-1}$ определяет элемент $I$ в любой группе, содержащей два элемента (которые мы обозначаем через $r$ и $f$), а путь $W_1 = r^3$ определяет элемент $I$ *только в тех специальных группах, в которых* $r^3 = I$.

Чтобы убедиться в том, что $W_2 = I$ в *любой* группе, выпишем следующие соотношения:

$$W_2 = fr^{-1}r^{-1}rrf^{-1} = fr^{-1}(r^{-1}r)rf^{-1} = fr^{-1}(I)rf^{-1} =$$
$$= fr^{-1}rf^{-1} = f(r^{-1}r)f^{-1} = f(I)f^{-1} = ff^{-1} = I.$$

Путем применения аксиом группы мы последовательно исключаем *все* символы, обозначающие образующие и обратные к ним, и сводим слово $W_2$ к $I$. Мы называем $W_2$ *пустым* словом, так как, применяя аксиомы группы, можно убедиться, что оно отлично от любого элемента группы, кроме $I$. Итак,

(1) Замкнутый путь в графической сети, которым можно возвратиться назад, проходя по каждому отрезку второй раз (изменив на обратные и порядок

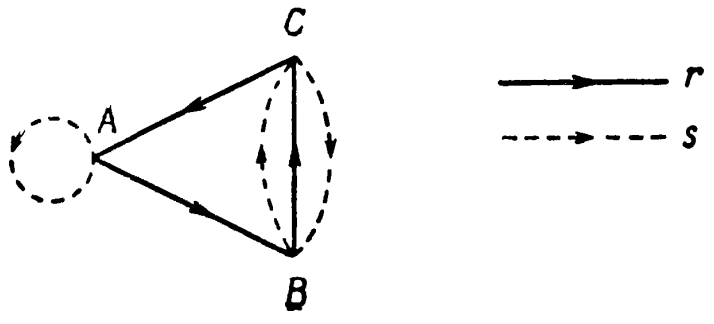
прохождения отрезков и направление движения по ним), соответствует пустому слову.

(2) Все другие замкнутые пути соответствуют специальным *соотношениям* между образующими группы, которые не обязаны выполняться в произвольной группе.

Упражнение 9. Пусть на графе группы самосовмещений равностороннего треугольника (рис. 6.7) в качестве $I$ выбрана вершина внутреннего треугольника, первоначально обозначенная через $fr$. Нарисуйте диаграмму Кэли этой группы, соответствующим образом обозначив все вершины.

Упражнение 10. Возьмите диаграмму Кэли группы самосовмещений равностороннего треугольника и видоизмените ее, направив стрелки на внутреннем треугольнике в противоположную сторону, а все остальное оставив без изменения. Затем обозначьте вершины внутреннего треугольника в соответствии с таким изменением направления на отрезках и составьте таблицу умножения этих шести элементов, используя для определения новых произведений видоизмененный граф. Будет ли это множество группой?

Упражнение 11. Ниже изображен граф, состоящий из направленных ребер двух типов, или «цветов», обозначенных через $r$ и $s$. Граф связен, и в каждой из трех его вершин $A$, $B$, $C$ можно начать четыре движения, соответствующие четырем возможным сомножителям в слове: $r$, $r^{-1}$, $s$, $s^{-1}$. Докажите, что тем не менее этот граф не может быть графом группы: составьте слово от $r$ и $s$ или их обратных, которое в одной из вершин соответствовало бы замкнутому пути, а в другой — нет. (Попробуйте, например, слова $sr^3s$ и $rsr$.)



*Распознавание графов групп.* Уже отмечалось, что диаграмму Кэли группы можно деформировать любым способом, но только так, чтобы не разорвалась ни одна связь между вершинами. Например, на рис. 6.14 изображена деформация диаграммы Кэли группы самосовмещений равностороннего треугольника. (См. рис. 6.7 на стр. 67.) Диаграмму Кэли этой группы можно деформировать в трехмерную сеть (рис. 6.15).

Трехмерный граф точно передает действительные физические движения, составляющие эту группу.

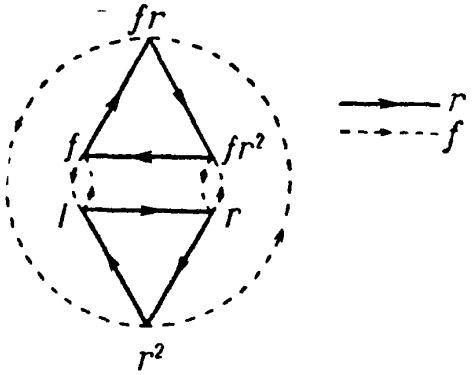



Рис. 6.14.

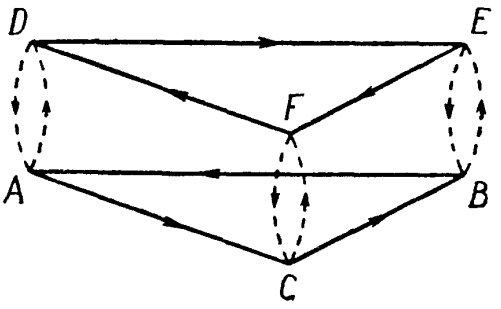



Рис. 6,15.

Нижний треугольник $ABC$ можно принять за изображение неопрокинутого треугольника со стрелками, соответствующими вращениям в плоскости треугольника. Верхний треугольник $DEF$ изображает треугольник после того, как его опрокинули, и дает положения, которые принимает вращающийся после опрокидывания треугольник. Пары образующих петлю дуг в каждой из вершин отражают обратимый характер опрокидывания.

Эта связь между диаграммой Кэли и графическим представлением совокупности движений является счастливой случайностью. Мы иногда будем действовать в обратном порядке: начинать с изображения множества движений, составляющих группу, а затем путем абстрагирования получать из него диаграмму Кэли этой группы.

**Группа диэдра.** Рассмотрим множество таких движений квадрата, в результате которых он совмещается с самим собой — множество самосовмещений

квадрата. Как подсказывает нам случай равностороннего треугольника, образующими движениями будут: $r$ — вращение на 90° в плоскости квадрата и $f$ — опрокидывание относительно диагонали квадрата (на 180°). Эти движения наводят на мысль о трехмерном представлении, изображенном на рис. 6.16. Этот граф *является* диаграммой Кэли группы порядка 8 с образующими $r$ и $f$, такими, что $r^4 = I$ и $f^2 = I$. Он обладает всеми свойствами, которыми должна обладать

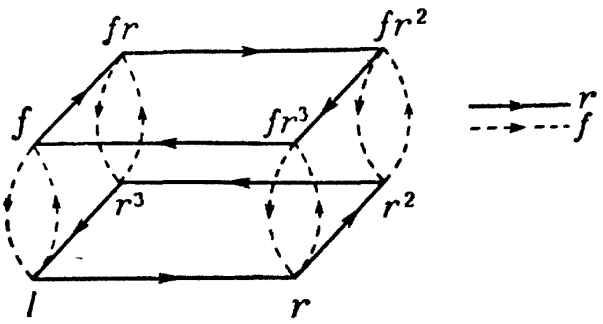



Рис. 6.16.

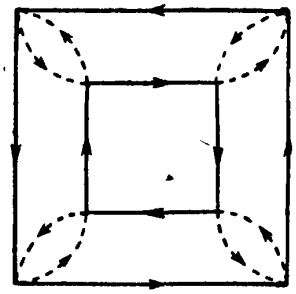


Рис. 6.17.

сеть, чтобы она была графом группы. Если мы продеформируем ее в двухмерную сеть, то получим рис. 6.17.

Аналогия со случаем равностороннего треугольника совершенно ясна, и эти рассуждения очевидным образом распространяются на случай группы самосовмещений любого правильного многоугольника.

Группа самосовмещений правильного многоугольника называется *группой диэдра*. Слово «диэдр» — «двугранник» — наводит на мысль о двух плоскостях, и, действительно, трехмерный вариант диаграммы Кэли группы диэдра представляет собой два плоских многоугольника, у которых соответствующие вершины связаны отрезками, обозначающими «опрокидывание». Здесь и в дальнейшем мы будем использовать для обозначения групп диэдра символ $D$ с нижним индексом, чтобы обозначить число вершин в многоугольнике, ассоциированном с данной группой. Таким образом, группа диэдра порядка 6 равностороннего треугольника будет обозначаться через $D_3$, а группа диэдра порядка 8 квадрата — через $D_4$. Для общего случая группы диэдра, ассоциированной с правильным $n$-угольником, мы будем употреблять

обозначение $D_n$. Ясно, что $D_n$ есть группа порядка $2n$.

Граф группы с образующей порядка 2 можно несколько упростить. Так как «опрокидывающий» элемент группы диэдра имеет порядок 2, то можно проиллюстрировать это упрощение на ее графе; однако можно было бы это сделать и для графа любой другой группы с образующей порядка 2.

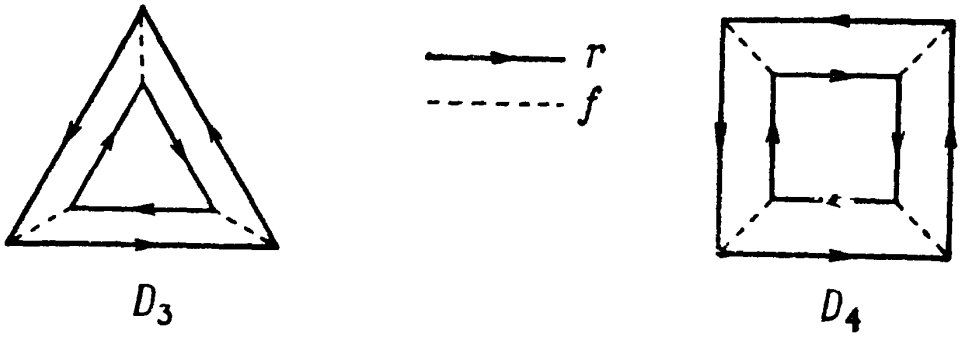



Рис. 6.18.

Все графы, в которые входит образующая порядка 2, скажем $f$, в каждой вершине содержат «петлю», составленную из $f$-дуг. Условимся заменить каждую такую петлю одним отрезком, который будет обозначать одновременно и образующую $f$ и обратный к ней элемент $f^{-1}$. Мы откажемся тогда от обычной стрелки на этом отрезке, и *с этого момента отрезок без стрелки будет соответствовать образующей порядка* 2. Так как для элемента порядка 2 $f = f^{-1}$, то прохождение этого отрезка в каком-либо направлении означает умножение справа на $f$ или $f^{-1}$. Графы групп диэдра $D_3$ и $D_4$, упрощенные согласно изложенному выше принципу, изображены на рис. 6.18. Отметим еще раз, что образующая $r$, порядок которой больше 2, представляется отрезками со стрелкой, в то время как отрезки, соответствующие образующей $f$ порядка 2, стрелки не имеют.

ГЛАВА 7

# ЗАДАНИЕ ГРУППЫ ОБРАЗУЮЩИМИ И ОПРЕДЕЛЯЮЩИМИ СООТНОШЕНИЯМИ

Мы видели, что конкретная группа может быть определена следующими способами:

(i) Как множество элементов с бинарной операцией, удовлетворяющей трем групповым аксиомам. Это основное определение, из которого можно получить все другие.

(ii) При помощи квадратной таблицы символов, которую мы назвали таблицей умножения группы и свойства которой были разобраны в гл. 4. Такая таблица задает группу, поскольку в ней указаны все произведения элементов группы.

(iii) При помощи графической схемы (сети), составленной из направленных отрезков и обладающей основными свойствами, которыми (как мы установили) должен обладать граф группы. Внутренней структурой такой сети группа вполне определяется, так как нам известно, каким образом последовательному прохождению путей должно соответствовать умножение элементов группы.

Цель этой главы — показать, что есть еще один способ задания группы — с помощью образующих и определяющих соотношений. С образующими мы уже сталкивались в одной из предыдущих глав.

**Циклическая группа $C_3$.** Мы начнем с изучения простой ситуации, возникающей в группе $C_3$, циклической группе порядка 3. Это группа вращений равностороннего треугольника в плоскости (стр. 26). Группа $C_3$ как циклическая группа может быть порождена одним из своих элементов, например $r$, и три ее элемента можно представить как $r$, $r^2$, $r^3 = I$.

Рассмотрим теперь обратную ситуацию:
(1) $G$ — группа, порожденная элементом $r$;
(2) $r^3 = I$.

Будут ли эти условия *полностью* определять структуру группы $G$? В частности, *обязательно* ли группа $G$ будет циклической группой порядка 3? Ответ на эти вопросы отрицательный. Достаточно обратить внимание на то, что соотношение $r^3 = I$ выполняется для $r = I$ — значит, группа $G$ может состоять из одного элемента, т. е. быть группой порядка 1. Поэтому, чтобы *полностью* определить группу $G$, мы должны видоизменить наше описание. Мы утверждаем, что если условие (2) заменить условием

(2′) единственное соотношение $r^3 = I$ образует множество определяющих соотношений группы $G$,

то условия (1) и (2′) вполне определяют $G$ как циклическую группу порядка 3. Чтобы пояснить это утверждение, надо указать точный смысл слова «соотношение» и затем перейти к понятию «определяющие соотношения» группы. Только тогда мы сможем решить вопрос, является ли «соотношение» $r^3 = I$ в группе $C_3$ *определяющим* соотношением этой группы.

Соотношение — это равенство вида

$$W = I,$$

где $W$ — слово в группе (стр. 62). Есть два существенно различных типа слов $W$, для которых может выполняться равенство $W = I$. Первый тип — это слова, для которых утверждение

$$W = I$$

означает, что слово представляет собой тот же элемент группы, что и $I$ (такие, как $rrr$, или $r^3$, в группе $C_3$). Это равенство *не* является следствием групповых аксиом и в произвольной группе может не выполняться. Например, в группе $C_2$, порожденной элементом $r$, *не* справедливо равенство $r^3 = I$. Напротив, равенство

$$rr^{-1} = I$$

является прямым следствием аксиомы группы (об обратных элементах) и выполняется для любого

элемента $r$ любой группы. Заметим, что $rr^{-1}$ — пустое слово, т. е. такое, что все образующие группы исчезают, когда мы применяем к нему групповые аксиомы и заменяем пары стоящих рядом взаимно обратных элементов элементом $I$ (стр. 73). Но слово $r^3$ — *не* пустое слово, и только в некоторых специальных группах справедливо соотношение $r^3 = I$. Примем такое соглашение: в определении соотношения $W = I$ *из рассмотрения исключается случай, когда* $W$ — *пустое слово*. Читатель должен помнить, что оба равенства $r^3 = I$ и $rr^{-1} = I$ соответствуют в графе группы $C_3$ замкнутым путям, причем второе — тривиальному пути (ведущему «обратно» по тем же отрезкам, что и «туда»), а первое — нетривиальному замкнутому пути (см. стр. 72—73).

Мы будем пользоваться таким определением соотношения в группе: если $W$ — непустое слово в группе $G$ и

$$W = I,$$

то это равенство называется *соотношением* группы $G$. Так как слово $W$ является произведением образующих группы $G$, то мы также будем говорить, что $W = I$ — *соотношение между образующими группы* $G$ [1]).

Чтобы ввести понятие *определяющих соотношений* группы $G$, рассмотрим множество, состоящее из всех нетривиальных соотношений группы $G$, т. е. множество $\{R_k = I\}$, $k = 1, 2, \ldots$, где $R_k$ — непустое слово. Обозначим это множество через $A$.

Остановимся предварительно на таком вопросе: может ли множество соотношений $A$ быть пустым (не содержать ни одного элемента)? Существует ли группа, в которой *нет* соотношений между образующими? Тривиальную группу, состоящую из един-

---

[1]) Казалось бы, следовало рассмотреть в группе $G$ соотношения более общего вида $W_1 = W_2$, но так как равенство $W_1 = W_2$ можно с помощью групповых аксимом преобразовать к виду $W = W_1 W_2^{-1} = I$, то достаточно рассматривать только соотношения вида $W = I$.

ственного элемента $I$, можно было бы рассматривать как группу без соотношений между образующими. Но мы определим ту же группу, если скажем, например, что она имеет образующие $a$ и $b$, удовлетворяющие соотношениям $a = I$, $b = I$. В этом случае любое слово равно $I$. Чтобы исключить из рассмотрения эту ситуацию, ограничимся группами, в которых существует по крайней мере одно слово, не равное $I$. Примером группы без соотношений является бесконечная циклическая группа $C_\infty$, порожденная элементом $a$. Мы видели (стр. 65), что если слово этой группы непусто, то оно не может равняться $I$, так как $a^n \neq I$ при $n \neq 0$; таким образом, группа $G$ не имеет соотношений, в которые входила бы ее единственная образующая $a$. Бесконечная циклическая группа $C_\infty$, порожденная одним элементом, принадлежит классу групп, не имеющих соотношений. Такие группы называются *свободными*.

Предположим, что множество $A$ содержит хотя бы одно соотношение $R = I$. Мы покажем, что тогда $A$ содержит бесконечно много соотношений. Для этого достаточно применить к соотношению $R = I$ групповые аксиомы. В частности, тогда

$$R^{-1} = I \text{ (так как } RR^{-1} = I\text{)}, \quad R^2 = R \cdot I = I$$

и аналогично $R^{-2} = I$. Последовательным умножением на слово, равное $I$, получаем

$$R^n = I \quad \text{и} \quad R^{-n} = I, \quad n = 1, 2, \ldots .$$

Это показывает, что из одного соотношения $R = I$ можно в качестве следствий получить бесконечно много соотношений, и $A$ должно содержать бесконечно много соотношений $R_k = I$, где $R_k$ — непустые слова. Из соотношения $R = I$ и групповых аксиом вытекают не только соотношения вида $R^n = I$ и $R^{-n} = I$, $n = 1, 2, \ldots$. Ясно, что если $W$ — *произвольное* слово от образующих группы $G$, то $W^{-1}RW = W^{-1}IW = I$ и $W^{-1}R^{-1}W = W^{-1}IW = I$.

Более того, можно показать, что множество всех соотношений, которые можно вывести из соотношения $R = I$, получается приравниванием к $I$ всевозможных

произведений с сомножителями вида $W^{-1}RW$ и $W^{-1}R^{-1}W$.

Вернемся к множеству $A$ всех нетривиальных соотношений группы $G$ (не забывая о только что сделанных выводах) и выберем в нем, если это возможно, подмножество $B$, такое, что *соотношения из $B$ влекут за собой все соотношения из множества $A$*. Это множество $B$ соотношений называется множеством *определяющих соотношений* группы $G$. Хотя бы одно множество $B$ определяющих соотношений существует (если $A$ непусто), так как в качестве $B$ можно взять все множество $A$. Однако более интересной и плодотворной оказывается ситуация, когда $B$ является собственным подмножеством множества $A$ (т. е. когда оно не совпадает с $A$).

Прежде чем перейти к деталям, связанным с рассмотрением конкретных групп, мы разъясним, что подразумевается под выражением: «соотношения из множества $B$ влекут за собой все соотношения из множества $A$». Оно означает, что, применяя групповые аксиомы, можно все соотношения из множества $A$ получить из соотношений, входящих в множество $B$; мы уже видели, например, как можно из единственного соотношения $R = I$ вывести бесконечно много соотношений $R^n = I$, $R^{-n} = I$, $W^{-1}RW = I$ и $W^{-1}R^{-1}W = I$.

Вернемся теперь к вопросу о том, будет ли соотношение $r^3 = I$ *определяющим* соотношением группы $C_3$ — циклической группы порядка 3 с образующей $r$. Образуем прежде всего множество $A$ всех соотношений в $C_3$ (напомним, что любое слово от $r$, $r^{-1}$ может быть записано как степень элемента $r$). Имеем

$$A = \{r^{3k} = I\}, \qquad k = \pm 1, \pm 2, \ldots .$$

Отметим, что множество $A$ можно также описать следующим образом (стр. 34):

$$A = \{r^n = I\}, \quad n \equiv 0 \pmod 3, \quad n \neq 0.$$

Любое нетривиальное соотношение группы $C_3$ лежит в множестве $A$, так как если бы $r^{3k+1} = I$ было соот-

ношением группы $C_3$, то как следствие мы получили бы, что $r = I$. Но в группе $C_3$ $r \neq I$, следовательно, и $r^{3k+1} \neq I$. Аналогично, равенство $r^{3k+2} = I$ влечет за собой соотношение $r^2 = I$, которое не выполняется в группе $C_3$.

Мы утверждаем, что в качестве множества $B$ определяющих соотношений группы $C_3$ можно взять одно соотношение

$$r^3 = I.$$

Любое соотношение из множества $A$ является следствием этого соотношения и аксиом группы. Действительно,

$$r^3 = I \text{ влечет за собой } r^{-3} = I,$$

и потому

$$(r^3)^k = I, \quad (r^{-3})^k = I, \quad k = 1, 2, \ldots .$$

Таким образом, соотношение $r^3 = I$ влечет за собой соотношения $r^n = I$, $n \equiv 0 \pmod 3$, $n \neq 0$, а это в точности все соотношения из множества $A$. (Мы исключаем из рассмотрения случай $n = 0$, так как $r^0$ — пустое слово.)

Можно указать другие множества определяющих соотношений группы $C_3$: например, *одно* соотношение $r^{-3} = I$ или *два* соотношения $r^6 = I$, $r^{-9} = I$.

Потенциальные возможности понятия определяющих соотношений полностью раскрываются в следующей общей теореме, которая утверждает, что любое множество соотношений между образующими на произвольном множестве образующих полностью задает некоторую группу:

Теорема 2. *Если задано множество $B$ соотношений $R_k = I$, где каждое $R_k$ есть непустое слово от заданного множества символов, то существует группа $G$, для которой $B$ является множеством определяющих соотношений.*

Доказательство этой теоремы выходит за рамки содержания данной книги. Тем не менее мы

проиллюстрируем ее на примере двух множеств определяющих соотношений.

Нам необходимо понятие *эквивалентных слов*. Рассмотрим два слова:

$$W_1 = rr^{-1}r \quad \text{и} \quad W_2 = r^{-1}rr.$$

Если рассматривать эти слова как последовательности символов, обозначающих образующие и обратные к ним элементы, то они различны, поскольку отличаются первыми (и вторыми) символами. Но если рассматривать их как форму записи элементов группы, то они определяют один и тот же элемент, поскольку

$$W_1 = rr^{-1}r = (rr^{-1})\,r = Ir = r$$

и

$$W_2 = r^{-1}rr = (r^{-1}r)\,r = Ir = r.$$

Слова $W_1$ и $W_2$ мы будем называть *эквивалентными*, если они определяют один и тот же элемент группы.

Отметим, что мы «преобразовали» $W_1$ и $W_2$ в $r$, вычеркивая сочетания $rr^{-1} = I$ и $r^{-1}r = I$, как только они появлялись. Рассмотрим теперь слова

$$W_3 = r^{-1}r^{-1} \quad \text{и} \quad W_4 = rrr$$

*в циклической группе* $C_3$. Мы уже видели, что эта группа определяется соотношением $r^3 = I$ (которое влечет за собой соотношение $r^{-3} = I$). «Преобразуем» слова $W_3$ и $W_4$, вставляя или вычеркивая слова, равные $I$:

$$W_3 = r^{-1}r^{-1} = (rr^{-1})\,r^{-1}r^{-1} \quad \text{(вставка)} =$$
$$= r\,(r^{-1}r^{-1}r^{-1}) = rr^{-3} = rI = r \quad \text{(вычеркивание)}$$

и

$$W_4 = rrrr = r\,(rrr) = r\,(r^3) = rI = r \quad \text{(вычеркивание)}.$$

Мы будем говорить, что $W_3$ и $W_4$ — *эквивалентные слова в группе* $C_3$; будучи различными, они представляют один и тот же элемент циклической группы $C_3$.

Это понятие эквивалентности можно обобщить с тем, чтобы оно было применимо к любым двум словам $W_1$ и $W_2$ от произвольного множества символов:

*слово $W_1$ эквивалентно слову $W_2$, если $W_1$ можно преобразовать в слово $W_2$, вставляя или вычеркивая слова, равные $I$.* Так как операции вставки и вычеркивания обратимы, то процесс преобразования слова $W_1$ в слово $W_2$ можно «обратить» и преобразовать слово $W_2$ в $W_1$. Это замечание служит обоснованием следующего утверждения: если $W_1$ эквивалентно $W_2$, то $W_2$ эквивалентно $W_1$. Мы предоставляем читателю показать, что если $W_1$, $W_2$ и $W_3$ — такие слова, что $W_1$ эквивалентно $W_2$, а $W_2$ эквивалентно $W_3$, то $W_1$ эквивалентно $W_3$. Этими свойствами должно обладать отношение, которое называется *отношением эквивалентности*[1]).

Используя понятие эквивалентности, разобьем множество слов на классы эквивалентных слов. Пусть $F$ — множество всех слов от заданного множества символов, т. е. $F$ — множество всех конечных последовательностей символов, которые являются образующими или их обратными. *Все слова из $F$ делятся на классы следующим образом:* если $W_1$ и $W_2$ — эквивалентные слова из $F$, то $W_1$ и $W_2$ принадлежат одному классу; если $W_1$ и $W_2$ — *не* эквивалентные слова из $F$, то $W_1$ и $W_2$ *не* лежат в одном классе. Иначе говоря, *слова $W_1$ и $W_2$ лежат в одном классе тогда и только тогда, когда они эквивалентны.* (Общая проблема, состоящая в том, чтобы решить в случае произвольной группы, будут ли два слова эквивалентны, крайне трудна. Эта проблема, известная как проблема тождества слов[2]), решена для сравнительно немногих групп). Пример того, как можно разбить $F$ на классы эквивалентных слов, будет дан ниже, когда мы вернемся к группе, определяемой соотношением $r^3 = I$. Когда множество $F$ разбито на классы эквивалентных слов, задающих один и тот же элемент

---

[1]) Точное определение отношения эквивалентности можно найти, например, в книге Л. А. Скорнякова «Элементы теории структур», «Наука», М., 1970, стр. 5. — *Прим. перев.*

[2]) П. С. Новиковым в 1957 г. было показано, что в общем виде эта проблема неразрешима, т. е. невозможно построить алгоритм, который в произвольной группе решал бы вопрос об эквивалентности слов. — *Прим. ред.*

группы, мы можем в качестве *представителя* класса выбрать любое его слово [1]).

Вернемся к теореме 2 (стр. 83) и дадим набросок основной процедуры построения группы при помощи образующих и соотношений. Мы сделаем это в абстрактных и общих терминах, которым придадим в дальнейшем конкретный смысл, когда будем разбирать некоторые примеры.

(1) Зададим множество порождающих символов и множество $B$ соотношений $R_k = I$, где каждое $R_k$ есть непустое слово от заданных символов.

(2) Рассмотрим множество $F$ всех слов от заданных порождающих символов.

(3) Образуем подмножество $K$, состоящее из всех слов $W$ из $F$, таких, что равенство $W = I$ есть *следствие* заданного множества соотношений $R_k = I$. Один из способов «построения» $K$ указан в приведенном ниже замечании.

(4) Разобьем $F$ на классы эквивалентных слов, т. е. таких слов, которые могут быть преобразованы одно в другое с помощью вставки и вычеркивания слов, равных $I$.

(5) Выберем множество $G$ представляющих слов по одному из каждого класса эквивалентности. Любое такое множество $G$ есть группа [2]), для которой заданные соотношения $R_k = I$ являются определяющими.

*Замечание о построении множества $K$.* Мы утверждаем, что $K$ есть множество всех произведений (т. е. конечных последовательностей) слов вида $T^{-1}RT$ или $T^{-1}R^{-1}T$, где $R = I$ — соотношение из заданного множества $B$, а $T$ — произвольное слово из $F$. Если $R = I$, то ясно, что любое слово описанного вида равно $I$, так как $T^{-1}IT = I$. Обратно, можно показать, что

---

[1]) Мы уже использовали понятие представителя класса, когда говорили о группе вращений (стр. 29) и об «эквивалентности по модулю 2» (стр. 34).

[2]) С такой операцией: произведение двух представителей — это представитель класса, которому принадлежит формальное произведение. — *Прим. перев.*

если $V$ — слово из $F$ и если равенство $V = I$ есть следствие наших соотношений, то $V$ есть произведение сомножителей вида $T^{-1}RT$.

**Задание группы $C_3$ определяющими соотношениями.** (1) Применим описанную выше процедуру для «отыскания» группы $G$, задаваемой определяющим соотношением $r^3 = I$ от одной образующей $r$. (Мы, конечно, ожидаем, что группа $G$ окажется циклической группой порядка 3.)

(2) В нашем случае множество $F$ всех слов от $r$ состоит из всех конечных произведений символов $r$ и $r^{-1}$. Ясно, что любое слово $T$ из $F$ можно преобразовать к виду $r^n$, $n = 0, \pm 1, \pm 2, \ldots$ .

(3) Чтобы образовать множество $K$, найдем все слова, «порожденные» словами вида $T^{-1}RT$ или $T^{-1}R^{-1}T$, т. е. слова вида

$$(r^n)^{-1}(r^3)(r^n) \quad \text{или} \quad (r^n)^{-1}(r^{-3})(r^n).$$

Но если удалить из этих слов все стоящие рядом пары взаимно обратных элементов, то мы получим

$$r^3 \quad \text{и} \quad r^{-3}.$$

Таким образом, множество $K$ включает в себя все произведения степеней элементов $r^3$ и $r^{-3}$:

$$K = \{r^n\}, \quad \text{где } n \text{ кратно } 3,$$

или

$$K = \{r^n\}, \qquad n \equiv 0 \pmod 3.$$

Этими словами из $K$ исчерпываются *все* слова $W$, для которых равенство $W = I$ есть следствие из $r^3 = I$.

(4) Преобразуя слова $r^n$ из $F$ путем вставки или вычеркивания слов, для которых $n \equiv 0 \pmod 3$, мы замечаем теперь, что множество $F$ делится на три класса:

$A$: слова $r^n$, для которых $n \equiv 0 \pmod 3$, например $n = 6$;

$B$: слова $r^n$, для которых $n \equiv 1 \pmod 3$, например $n = 4$;

$C$: слова $r^n$, для которых $n \equiv 2 \pmod 3$, например $n = -1$,

(5) В качестве представителей этих классов выберем

$$I \text{ из } A \ (n=0),\ r \text{ из } B,\ r^2 \text{ из } C.$$

(Это удобно, но, вообще говоря, вместо них мы могли бы выбрать, например, таких представителей: $r^3$ из $A$, $r^{-2}$ из $B$, $r^5$ из $C$.) Три представляющих слова $I$, $r$, $r^2$ образуют группу, а именно циклическую группу порядка 3 с элементом $r$ в качестве образующей. (Мы должны помнить, что элементу группы соответствует целый класс эквивалентных слов. Например, слово $(r^2)(r^2) = r^4$ лежит в том же классе, что и слово $r$, и,

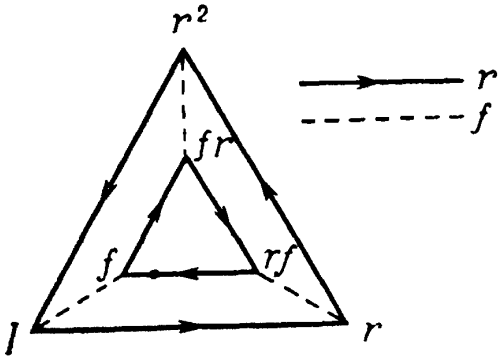



Рис. 7.1.

следовательно, мы можем сказать, что элемент $(r^2)^2$ есть не что иное, как элемент $r$.)

Мы видим, что группа $G$ с определяющим соотношением $r^3 = I$, как мы и ожидали, оказалась циклической группой порядка 3.

**Предполагаемое множество определяющих соотношений группы $D_3$.** Ту же основную процедуру нахождения определяющих соотношений мы применим теперь в случае группы $D_3$. Прежде всего надо найти множество таких соотношений, которые (как мы будем надеяться) могут оказаться ее определяющими соотношениями. Ключ к решению этой задачи должен дать нам граф группы, и поэтому мы вновь обратимся к нему (рис. 7.1).

Мы ищем такое множество соотношений от $r$ и $f$, из которого можно вывести все соотношения вида $W = I$, где $W$ — слово от $r$ и $f$. Напомним, что любому соотношению в группе можно сопоставить (нетривиальный) замкнутый путь в ее графе. На рис. 7.2

показаны некоторые нетривиальные замкнутые пути графа группы $D_3$. Путь *а*) соответствует соотношению $r^3 = I$, путь *б*) — соотношению $f^2 = I$ и путь *в*) — соотношению $rfrf = I$. Отметим, что такие замкнутые пути в силу однородности графа группы (см. стр. 70) берут начало в каждой из вершин графа.

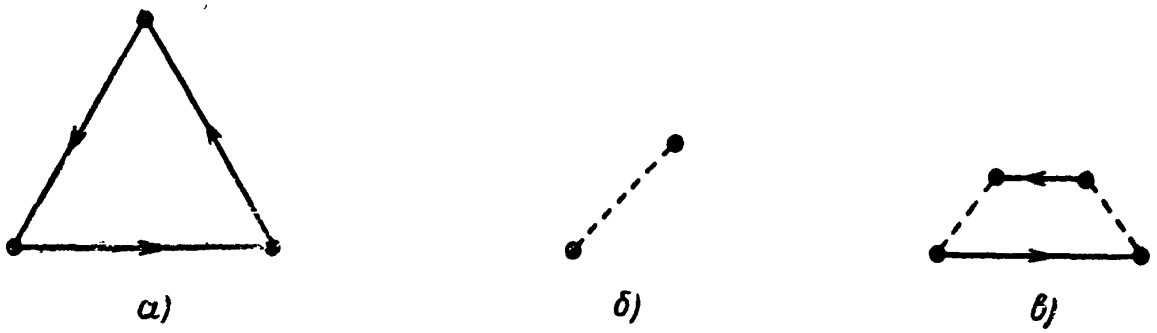



Рис. 7.2.

Мы утверждаем, что соотношения

$$r^3 = I, \qquad f^2 = I, \qquad rfrf = I$$

составляют множество определяющих соотношений группы $D_3$.

**Задание группы $D_3$ множеством соотношений.** (1) Множество порождающих символов — это $\{r, f\}$, а множество соотношений между ними — это

$$r^3 = I, \quad f^2 = I, \quad rfrf = I.$$

(2) $F$ — множество всех слов от $r$, $f$, $r^{-1}$, $f^{-1}$. В противоположность предыдущему примеру у нас нет простого способа описать все эти слова.

(3) Подмножество $K$ содержит все слова $W$, для которых соотношение $W = I$ является следствием заданных соотношений. Обратим внимание на одно специальное слово из $K$, которое нам понадобится в дальнейшем. Рассмотрим это слово $V$, составленное из сомножителей вида $T^{-1}RT$ или $T^{-1}R^{-1}T$:

$$V = f^{-2}(f^2)f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3}(r^{-3})r^3 =$$
$$= f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3} = f(rfr)(f^2)r^{-3} = frfr^{-2}.$$

Так как $V$ — слово из множества $K$, то

$$V = frfr^{-2} = I \quad \text{или} \quad fr = r^2f.$$

(4), (5) Преобразуем теперь слова из множества $F$, вставляя или вычеркивая слова, равные $I$, и разобьем $F$ на классы эквивалентных слов. Мы утверждаем, что *существует шесть классов эквивалентных слов с таким множеством представителей*:

$$I,\ r,\ f,\ r^2,\ rf,\ fr.$$

Чтобы доказать это утверждение, покажем сначала, что не может быть более шести классов эквивалентных слов, т. е. что любое слово из множества $F$ можно преобразовать в одно из указанных шести слов, а затем — что никакие два из них не эквивалентны. Будем основываться на том, что любое слово из $K$ равно $I$, и использовать специальное слово $V$ из $K$.

Из того, что

$$V = f^2 \cdot f^{-1}(rfrf)f \cdot r^{-3}$$

принадлежит множеству $K$, как мы видели, следует[1]) равенство

$$fr = r^2f.$$

Используем это для доказательства такого факта: *каждое слово из множества $F$ эквивалентно некоторому слову вида $r^af^b$, где $a$ и $b$ — неотрицательные целые числа.* Действительно, если задано произвольное слово из множества $F$, то можно применить равенство $fr = r^2f$ для того, чтобы «переставлять» $f$ и $r$, заменяя одновременно $r$ на $r^2$; таким путем мы можем «сдвинуть» все символы $f$ вправо, а все символы $r$ влево. В конечном счете мы придем к эквивалентному слову, в котором все символы $r$ стоят впереди всех символов $f$. Кроме того, все степени элементов $r$ и $f$ в преобразованном слове можно считать неотрицательными, поскольку соотношения $r^3 = I$, $f^2 = I$ влекут за собой соотношения $r^{-1} = r^2$, $f^{-1} = f$. Таким

---

[1]) Соотношение $fr = r^2f = r^{-1}f$ есть частный случай более общего результата: соотношения $f^2 = I$ и $rfrf = I$ *вместе* влекут за собой равенство $fr^n = r^{-n}f$ для всех целых $n$. Кроме того, *единственное* соотношение $rfrf = I$ влечет за собой равенство $f^ar^b = r^xf^y$, где $x = (-1)^ab$ и $y = (-1)^ba$.

образом, каждое слово из множества $F$, как и утверждалось, эквивалентно слову вида $r^a f^b$. Например, $r^2fr^2fr$ оказывается эквивалентным слову $r$:

$$\begin{aligned} r^2fr^2fr &= r^2(fr)rfr = r^2(r^2f)rfr = \\ &= r^4frfr = r(fr)fr = \\ &= r(r^2f)fr = r^3f^2r = \\ &= r. \end{aligned}$$

Далее, из соотношений $r^3 = I$ и $f^2 = I$ следует, что каждое из слов $r^a f^b$ эквивалентно слову вида $r^{a'} f^{b'}$, где $a'$ равно 0, 1 или 2, а $b'$ равно 0 или 1, т. е. произвольное слово из множества $F$ эквивалентно одному из слов

$$I,\ r,\ f,\ r^2,\ rf,\ r^2f = fr.$$

Пока мы доказали, что существует *не более* шести классов эквивалентных слов из множества $F$. Но некоторые из этих шести классов с представителями $I$, $r$, $f$, $r^2$, $rf$ и $fr$, быть может, совпадают, т. е. некоторые из предполагаемых представителей могут быть преобразованы один в другой. Остается доказать, что такого быть не может — никакие два из указанных шести слов не эквивалентны. Существенная часть доказательства состоит в том, чтобы показать, что $r \neq I$ и $f \neq I$. Хотя соотношения $r = I$ и $f = I$ не входят в наше множество определяющих соотношений, мы не можем заранее предполагать, что эти равенства не являются следствиями наших исходных соотношений [1]).

Покажем сначала, что $f \neq I$. Если соотношение $f = I$ является следствием заданных соотношений, то $f$ — слово из множества $K$. Следовательно, в $K$ есть слово, представимое в виде произведения сомножителей $T^{-1}RT$ или $T^{-1}R^{-1}T$, которое можно преобразовать в слово $f$. Нам надо показать, что, как бы мы ни применяли групповые аксиомы и заданные соотношения, представить $f$ в виде произведения таких

---

[1]) Например, два соотношения $xyx^2 = I$ и $x^3 = I$ влекут за собой равенство $y = I$.

сомножителей невозможно. Сущность нашего метода состоит в рассмотрении суммы показателей степени элемента $f$ в произвольном слове из множества $K$. Мы подсчитаем, сколько вносится в эту сумму каждым из возможных сомножителей вида $T^{-1}RT$. Слово $R$ — это одно из слов $r^3$, $f^2$, $rfrf$ (или их обратных), а сумма показателей степени элемента $f$ в этих словах равна 0, 2, 2 (или 0, —2, —2 для обратных) соответственно. Так как $T$ — произвольное слово из множества $F$, то сумма показателей степени элемента $f$ в слове $T$ может быть любым числом. Пусть она равна $t$. Тогда соответствующая сумма для слова $T^{-1}$ равна $-t$. (Вспомним, что если, например, $T = r^2fr^{-3}f^3$, то $T^{-1} = f^{-3}r^3f^{-1}r^{-2}$; см. рассуждение об элементе, обратном к произведению, на стр. 52.) Совместный вклад от $T^{-1}$ и $T$ в эту сумму для любого сомножителя равен нулю. Следовательно, *сумма показателей степени элемента $f$ в любом сомножителе вида $T^{-1}RT$ равна* 0, 2 *или* —2. Таким образом, сумма показателей степени элемента $f$ в любом слове из множества $K$ есть четное число. Поскольку соответствующая сумма для $f$ равна 1, слово $f$ не может принадлежать множеству $K$.

Попытаемся теперь применить наш метод «сумм показателей» к доказательству того, что $r \neq I$. Мы сразу же убедимся, что здесь он ничего не дает. Действительно, сумма показателей степени элемента $r$ в слове вида $T^{-1}RT$ может быть равна 0, 2 или 3, т. е. суммы показателей для слов из множества $K$ могут быть как четными, так и нечетными. Наше доказательство того, что $r \neq I$, будет основано на известных нам фактах о строении группы $D_3$, группы самосовмещений равностороннего треугольника. Предположим, что соотношение $r = I$ является следствием соотношений

$$r^3 = I,\ f^2 = I,\ rfrf = I.$$

Тогда $r = I$ будет следствием указанных соотношений в любой группе, в которой они имеют место. Мы знаем, что эти соотношения справедливы в группе $D_3$, но в группе $D_3$ не имеет места соотношение $r = I$,

Значит, оно *не* является следствием указанных выше соотношений.

Может ли соотношение $r = f$ быть следствием заданных соотношений? Если $r = f$, то $r^2 = fr = r^2 f$, откуда $f = I$, но $f \neq I$, следовательно, $r \neq f$.

Мы доказали, что никакие два из слов $I$, $r$, $f$ не эквивалентны. Предоставляем читателю в качестве упражнения доказать, что остальные три из наших шести слов-представителей попарно различны между собой (как элементы группы) и не эквивалентны ни одному из слов $I$, $r$, $f$. Например, может ли быть $r = r^2$? Ясно, что тогда было бы $r = I$, и т. д.

Упражнение 12. Множество

$$A = \{r^3 = I,\ f^2 = I,\ rfrf = I\}$$

является множеством определяющих соотношений группы $D_3$. Докажите, что множество

$$B = \{f^2 = I,\ frfr^{-2} = I\}$$

также является множеством определяющих соотношений этой группы.

[*Указание.* Мы знаем, что соотношения из множества $B$ являются следствиями соотношений из множества $A$ (стр. 89). Следовательно, показав, что соотношения из $A$ являются следствиями соотношений из $B$, мы докажем, что эти множества соотношений эквивалентны, т. е. оба они определяют одну и ту же группу.]

Теперь мы предлагаем читателю приступить к упражнениям 13—17; для их решения требуется несколько больше, чем простое применение основной процедуры. Если читателю эти упражнения покажутся трудными, то можно отложить их, пока не будут изучены следующие главы книги.

Упражнение 13. (а) Предположим, что группа $G$ порождается двумя элементами $x$ и $y$, удовлетворяющими соотношениям

$$x^2 = I,\ xyx^{-1} = y^3.$$

Покажите, что $y$ является элементом конечного порядка, установив, что $y^8 = I$.

(b) Предположим, что группа $G$ порождается элементами $x$ и $y$, такими, что

$$x^2 = I, \quad xyx^{-1} = y^n, \quad \text{где } n > 1.$$

Покажите, что

$$y^{n^2-1} = I.$$

Упражнение 14. (a) Пусть $u$ и $v$ — элементы группы $H$; предположим, что

$$u^3 = I, \quad uvu^{-1} = v^4.$$

Докажите, что $v$ есть элемент конечного порядка.

(b) Пусть в группе $H$ есть элементы $u$ и $v$, для которых справедливы равенства

$$u^m = I, \quad uvu^{-1} = v^k,$$

где $m$ и $k$ — такие целые числа, что $k > 1$ и $m \neq 0$. Докажите, что $v$ — элемент конечного порядка.

Упражнение 15. Покажите, что существует группа порядка 16, образующими которой являются два элемента $x$ и $y$, удовлетворяющие соотношениям

$$x^2 = I, \quad xyx^{-1} = y^3.$$

(Предполагается, что доказательство будет заключаться в построении графа группы.)

Упражнение 16. Покажите, что любая группа $G$ с двумя образующими $s$ и $t$, удовлетворяющими соотношениям

$$s^n = I, \quad sts^{-1} = t^k,$$

где $n$ и $k$ — целые числа, $n \neq 0$, $k > 1$, будет группой конечного порядка. Покажите также, что $G$ не может содержать более чем $(k^n - 1)n$ различных элементов. [*Указание*: используйте метод, примененный на стр. 90 для доказательства того, что все слова группы $D_3$ можно преобразовать к виду $r^a f^b$, поскольку в ней имеет место соотношение $fr = r^2 f$.]

Упражнение 17. Пусть в предыдущем упражнении $n = 3$, $k = 2$. Покажите, что действительно существует группа порядка 21, обладающая двумя образующими $s$ и $t$, для которых

$$s^3 = I, \quad sts^{-1} = t^2.$$

Выполните это упражнение, построив граф такой группы.

**Образующие и соотношения группы диэдра $D_n$.** Мы подробно исследовали определяющие соотношения одной из групп диэдра, а именно группы $D_3$. Те же самые методы можно использовать для доказательства того, что *общая группа диэдра $D_n$ полностью определяется следующими требованиями*:

(1) *$D_n$ порождается двумя своими элементами, обозначаемыми через $r$ и $f$;*

(2) *эти образующие удовлетворяют трем определяющим соотношениям*

$$r^n = I, \quad f^2 = I, \quad (rf)^2 = I.$$

(На стр. 82 объяснялось, какое множество соотношений мы называем множеством определяющих соотношений.) Особый интерес представляют частные случаи групп диэдра $D_n$ для малых $n$. При $n = 1$ определяющие соотношения группы диэдра принимают следующий вид:

$$r = I, \quad f^2 = I, \quad (rf)^2 = I.$$

Поскольку если $r = I$, то $(rf)^2 = f^2 = I$, у нас остается два определяющих соотношения: $f^2 = I$, $r = I$. Но они определяют циклическую группу $C_2$ порядка 2. Таким образом, $D_1 = C_2$. Есть другой способ убедиться в этом. Достаточно представить группу $D_1$ как группу самосовмещений «многоугольника» с одной стороной, или отрезка. Два положения отрезка, в которых он совмещается сам с собой, таковы:

$$1 \text{——} 2 \quad \text{и} \quad 2 \text{——} 1,$$

и граф группы $D_1$ в компактной форме (стр. 77) имеет вид

$$I \text{— — — — —} f.$$

Если $n = 2$, то определяющие соотношения (2) группы $D_2$ имеют вид

$$r^2 = I, \quad f^2 = I, \quad (rf)^2 = I,$$

или

$$r^2 = f^2 = (rf)^2 = I.$$

Мы построим граф группы $D_2$, изображая «2-угольник» как плоскую фигуру с двумя сторонами-дугами. Рис. 7.3 изображает самосовмещения 2-угольника.

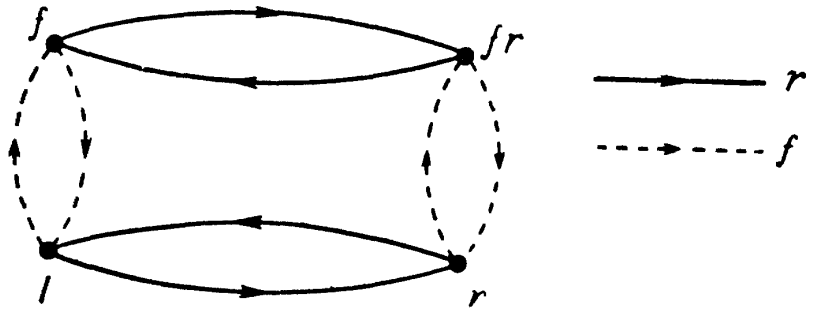



Рис. 7.3.

Здесь $r$ — вращение, а $f$ — опрокидывание. Если мы примем во внимание установленные ранее (стр. 68) свойства графа группы, то убедимся, что изображение самосовмещений 2-угольника на рис. 7.3 есть на самом деле диаграмма Кэли группы $D_2$.

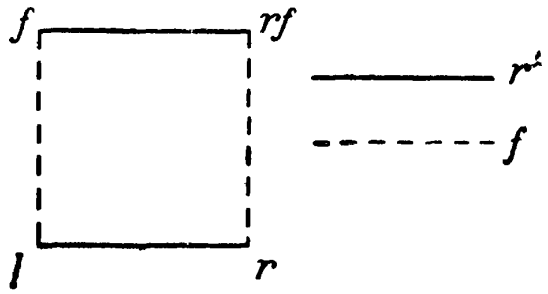



Рис. 7.4.

Используя компактное представление для образующих порядка 2 и учитывая, что и $r$ и $f$ имеют порядок 2, мы можем упростить граф группы $D_2$ (рис. 7.4). Отметим, что вершина, расположенная на одной диагонали с вершиной $I$, помечена символом $rf$, но граф ясно показывает, что путь, соответствующий слову $fr$, приводит в ту же вершину, что и путь,

соответствующий слову $rf$. Таким образом, $rf = fr$, и $D_2$ — *коммутативная группа.*

Поскольку группа $D_2$ порядка 4 встречается довольно часто, она получила специальное название *четверной группы.* Ее также называют квадратичной группой из-за показателя 2 в ее соотношениях. Мы снова встретимся с ней при изучении группы самосовмещений тетраэдра.

*Коммутативные группы диэдра.* Группы $D_1$ и $D_2$ коммутативны, но достаточно взглянуть на графы групп $D_3$ и $D_4$ (стр. 77), чтобы убедиться в том, что они не коммутативны. Можем ли мы сформулировать общее утверждение о коммутативности группы диэдра $D_n$? Да, мы покажем, что единственными коммутативными группами диэдра являются группы $D_1$ и $D_2$.

Теорема 3. *Соотношение*

$$fr = rf$$

*будет следствием определяющих соотношений*

$$r^n = I, \quad f^2 = I, \quad (rf)^2 = I$$

*группы диэдра $D_n$ с образующими $r$ и $f$ только в том случае, когда $n = 1$ или $n = 2$; или, в иной формулировке: если $n > 2$, то группа диэдра $D_n$ не коммутативна.*

Для доказательства этой теоремы заметим прежде всего, что в любой коммутативной группе диэдра

$$I = (rf)^2 = (rf)(rf) = (rf)(fr) = rf^2r = r^2.$$

Если $n$ *четно*, то соотношение $r^2 = I$ влечет за собой соотношение $r^n = I$, так что наши исходные определяющие соотношения эквивалентны таким соотношениям:

$$r^2 = I, \quad f^2 = I, \quad (rf)^2 = I,$$

т. е. определяющим соотношениям группы $D_2$. Если $n$ *нечетно*, скажем $n = 2k + 1$, то

$$r^2 = I = r^n = r^{2k+1} = r^{2k}r = Ir = r.$$

Следовательно, $r = I$ и исходные определяющие соотношения эквивалентны соотношениям

$$r = I, \quad f^2 = I,$$

определяющим соотношениям группы $D_1$. Доказательство завершено.

*Группа диэдра* $D_\infty$. Существует ли группа диэдра $D_\infty$ бесконечного порядка? Построив ее граф, мы докажем, что она действительно существует. Граф группы $D_n$ состоит из двух $n$-угольников, составленных из $r$-отрезков, и связывающих их $f$-отрезков. Если

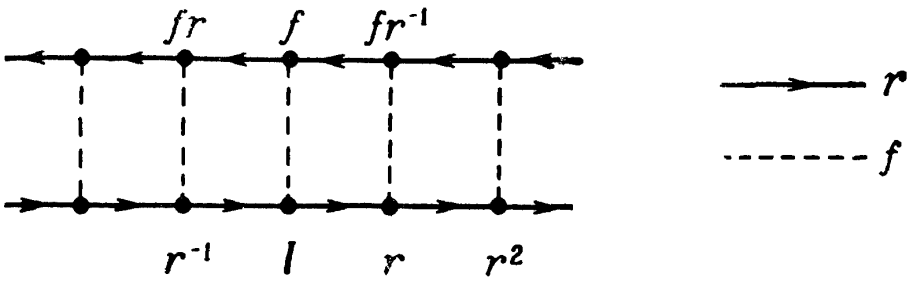



Рис. 7.5.

вспомнить сейчас, как граф группы $C_\infty$ связан с графом группы $C_n$ ($n$-угольник заменяется прямой, разбитой на бесконечное множество отрезков), то возникает мысль построить граф группы $D_\infty$ из графа группы $D_n$, заменив два $n$-угольника двумя связанными между собой параллельными прямыми (рис. 7.5). Эта схема, состоящая из направленных отрезков, обладает всеми свойствами графа группы, и мы обозначим соответствующую группу через $D_\infty$.

Исследуем теперь группу $D_\infty$ с точки зрения образующих и определяющих соотношений. Заметим, что первое из определяющих соотношений

$$r^n = I, \quad f^2 = I, \quad (rf)^2 = I$$

группы $D_n$ в графе группы $D_\infty$ не выполняется. (Аналогично в случае группы $C_\infty$ соотношение $a^n = I$ не выполняется, и мы его отбросили.) Отбросим соотношение $r^n = I$ и сохраним в качестве предполагаемых определяющих соотношений группы $D_\infty$ лишь

$$f^2 = I \quad \text{и} \quad (rf)^2 = I.$$

Чтобы выполнялось $f^2 = I$, в каждой вершине графа группы $D_\infty$ должна быть петля или, в компактной форме, $f$-отрезок. Соотношение $(rf)^2 = I$ соответствует четырехугольнику в каждой вершине, причем сторонами четырехугольника должны быть чередующиеся $r$-отрезки и $f$-отрезки. Граф на рис. 7.5 обладает именно этими свойствами [1]).

*Прямое произведение.* При взгляде на диаграммы Кэли всех групп диэдра возникает ощущение, что это «продублированные» диаграммы Кэли циклических групп. Группа $D_n$ представляется с помощью двух $n$-угольников, составленных из $r$-отрезков и связанных один с другим посредством $f$-отрезков. Группа $D_\infty$ представляется двумя параллельными прямыми, составленными из $r$-отрезков, связанных $f$-отрезками. Это наводит на мысль о том, что новые, «бóльшие» группы можно иногда образовывать, комбинируя «меньшие» группы.

Рассмотрим граф группы диэдра, в котором мы изменили на противоположное направление отрезков одного из многоугольников и соответствующим образом переобозначили вершины. На рис. 7.6 изображена диаграмма Кэли группы $D_3$ после этой модификации. В группе, соответствующей этому новому графу, соотношения $r^3 = f^2 = I$ по-прежнему выполняются, а соотношение $(rf)^2 = I$ — нет. Вместо него выполняется, как видно на графе, соотношение $fr = rf$, или $frf^{-1}r^{-1} = I$ (соответствующее замкнутому пути от $I$ к вершине $f$, затем к вершине $fr$, к вершине $r$, а потом

---

[1]) Каждое другое соотношение следует из этих двух. Действительно, любое соотношение соответствует замкнутому пути на графе, а всякий замкнутый путь, как легко видеть, — это последовательное прохождение $r$- и $f$-отрезков, которое можно записать в виде $r^{i_1}fr^{i_2}f \ldots r^{i_k}f$ или в виде $fr^{i_1}fr^{i_2} \ldots fr^{i_k}$, где $k$ четно, а $i_1 + i_3 + \ldots + i_{k-1} = i_2 + i_4 + \ldots + i_k$ (прохождение отрезков по «верхней» и «нижней» прямой). Но каждое $W = I$, где $W$ — слово указанного вида, является следствием наших двух соотношений, так как, например, $r^{i_1}f \ldots r^{i_k}f$ эквивалентно слову $r^{i_1 - i_2 + \ldots + i_{k-1} - i_k}f^k = I$. — *Прим. ред.*

обратно к $I$). Новая группа является абелевой, или коммутативной, группой с соотношениями

$$r^3 = f^2 = frf^{-1}r^{-1} = I.$$

Она обозначается через $C_2 \times C_3$, так как является «комбинацией» циклической группы $C_2$ ($f^2 = I$) и циклической группы $C_3$ ($r^3 = I$).

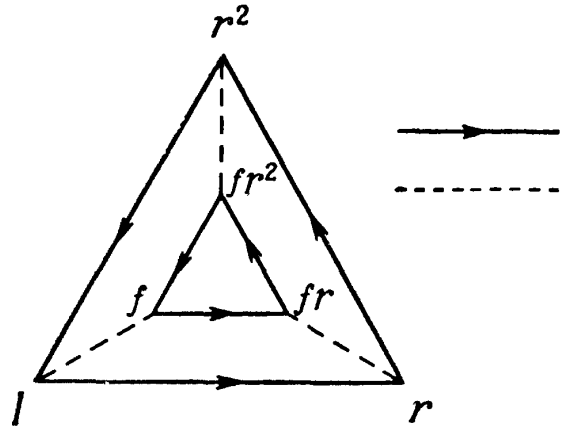



Рис. 7.6.

Упражнение 18. Используйте диаграмму Кэли группы $C_2 \times C_3$ для вычисления последовательных степеней элемента $fr$. Какой элемент группы соответствует степени $(fr)^6$? Докажите, что $C_2 \times C_3 = C_6$.

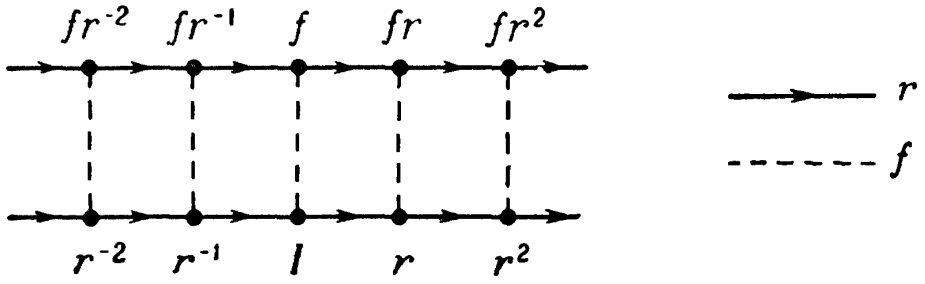



Рис. 7.7.

[*Указание*: положите $g = fr$ и докажите, что любой элемент группы можно представить как степень элемента $g$.]

Если мы модифицируем граф группы диэдра $D_n$, изменив на противоположное направление отрезков одного из $n$-угольников, то получим граф «дважды циклической» группы $C_2 \times C_n$ с соотношениями

$$r^n = f^2 = frf^{-1}r^{-1} = I.$$

Из графа группы $D_\infty$ мы получим граф бесконечной «дважды циклической» группы $C_2 \times C_\infty$ (рис. 7.7).

Эта диаграмма Кэли напоминает две параллельные улицы с односторонним движением, связанные улицами с двусторонним движением.

Рассмотрим диаграмму на рис. 7.8. Она выглядит как схема улиц с односторонним движением, возможно, как план городского квартала. В группе, соответ-

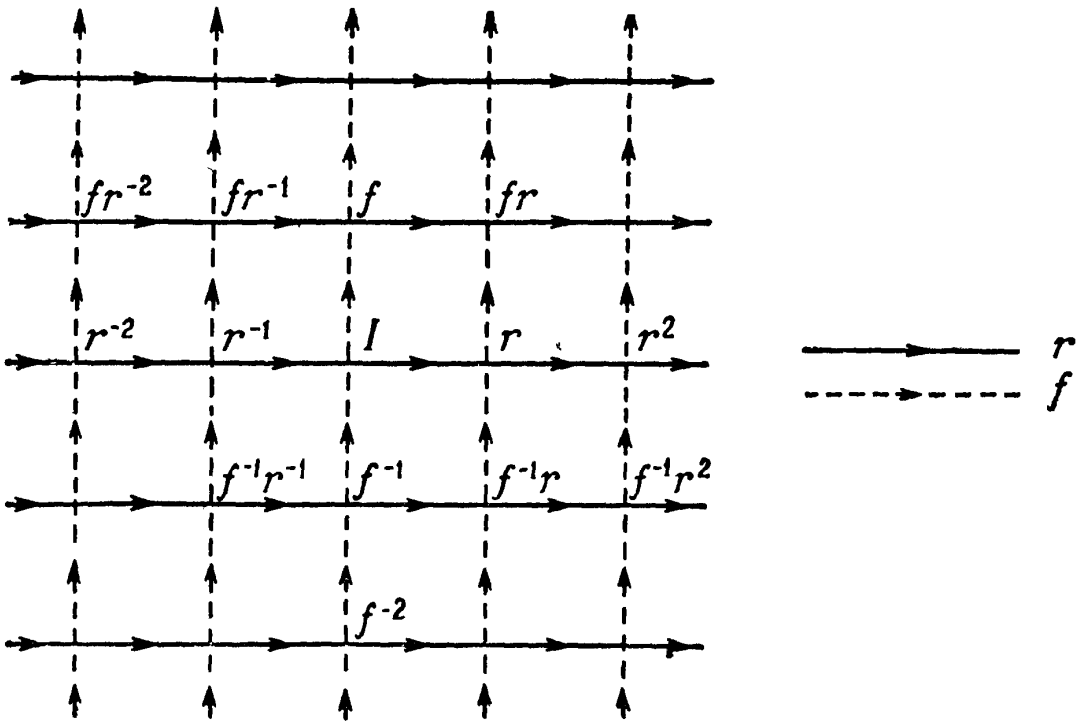



Рис. 7.8.

ствующей этому графу, соотношение $f^2 = I$ не выполняется, т. е. порядок элемента $f$ не равен 2. Поэтому мы $f$-отрезки изображаем со стрелками. Определяет эту группу единственное соотношение

$$frf^{-1}r^{-1} = I \quad (\text{или } fr = rf),$$

означающее коммутативность. В строении ее графа оно проявляется в том, что каждая его вершина служит началом *замкнутого* четырехугольного пути, соответствующего слову $frf^{-1}r^{-1}$. Эта группа «городских улиц» является наиболее общей абелевой группой с двумя образующими. (Естественно считать группу тем более общей, чем меньше существует условий, которым должны удовлетворять ее элементы, а в данном случае единственным условием является $rf = fr$.) Группа «городских улиц» обозначается через $C_\infty \times C_\infty$ или $C_\infty^2$.

Группа $C_2 \times C_3$ называется *прямым произведением* циклических групп $C_2$ и $C_3$; аналогично, группа $C_\infty \times C_\infty$ является прямым произведением группы $C_\infty$ и группы $C_\infty$. Понятие «прямого произведения» в его наиболее общей и абстрактной форме чрезвычайно полезно; например, можно показать, что *любая конечная абелева группа является прямым произведением*[1]) *циклических групп.* Мы лишь очень бегло коснемся свойств прямого произведения, рассчитывая на то, что основные понятия будут усвоены из примеров.

Пусть $S$ — множество с бинарной операцией $\otimes$, а $G$ и $H$ — его подмножества, являющиеся группами относительно операции $\otimes$. Пусть группа $G$ имеет образующие $g_1, g_2, \ldots$, а группа $H$ — образующие $h_1, h_2, \ldots$. Мы будем также считать, что у групп $G$ и $H$ есть *только один общий элемент — единица* и что *любой элемент из G перестановочен с любым элементом из H.* При этих условиях можно построить *прямое произведение* $G \times H$, образовав множество всех произведений элементов из $G$ и $H$. Можно показать, что множество $G \times H$ есть группа с образующими $g_1, g_2, \ldots, h_1, h_2, \ldots$[2]).

В качестве примера прямого произведения рассмотрим группу «городских улиц» с образующими $r$ и $f$ (рис. 7.8). Каждая из образующих $r$ и $f$ в отдельности порождает некоторую бесконечную циклическую группу. (Напомним, что ни в одной из этих двух циклических групп на образующую не налагается никаких соотношений.) Эти две бесконечные циклические группы не имеют общих элементов, кроме $I$. Поскольку мы условились, что $rf = fr$, или $rfr^{-1}f^{-1} = I$, то любой элемент первой группы будет перестановочен с любым элементом второй группы и множество обра-

---

[1]) Для абелевых групп часто употребляется термин «прямая сумма», поскольку операция в них обычно обозначается символом $+$. — *Прим. перев.*

[2]) В примерах прямого произведения множество $S$ будет группой. Группы $G$ и $H$ тогда оказываются «группами внутри группы». Глава 8 посвящена систематическому изучению таких «подгрупп».

зующих $r$, $f$ порождает прямое произведение $C_\infty \times \times C_\infty = C_\infty^2$.

*Прямое произведение и определяющие соотношения.* В общем случае определяющие соотношения прямого произведения $G \times H$ можно получить из определяющих соотношений групп-сомножителей $G$ и $H$ *присоединением к ним соотношений, выражающих перестановочность любой образующей группы $G$ с любой образующей группы $H$.* Присоединенные соотношения гарантируют нам, что любой элемент группы $G$ коммутирует с любым элементом группы $H$, — такое требование входит в определение прямого произведения. Рассмотрим теперь несколько групп, являющихся прямыми произведениями, и исследуем их определяющие соотношения.

Чтобы построить группу $G = C_2 \times C_2$, зададим циклическую группу порядка 2, порожденную элементом $x$ с соотношением $x^2 = I$, и другую циклическую группу порядка 2, порожденную элементом $y$ с соотношением $y^2 = I$. Группа $G = C_2 \times C_2$ имеет образующие $x$ и $y$, удовлетворяющие соотношениям $x^2 = y^2 = I$. Требование, чтобы $x$ и $y$ коммутировали между собой, можно записать формулой $xyx^{-1}y^{-1} = I$, что, конечно, эквивалентно соотношению $xy = yx$. Таким образом, группа $G = C_2 \times C_2$ задается определяющими соотношениями групп-сомножителей

$$x^2 = I, \quad y^2 = I$$

и дополнительно соотношением

$$xyx^{-1}y^{-1} = I.$$

Так как $x^{-1} = x$ и $y^{-1} = y$, то определяющие соотношения группы $C_2 \times C_2$ можно переписать в виде

$$x^2 = I, \quad y^2 = I, \quad xyxy = I,$$

или

$$x^2 = y^2 = (xy)^2 = I.$$

Но это определяющие соотношения группы $D_2$ (четверной группы; см. стр. 97). Таким образом, $C_2 \times \times C_2 = D_2$.

Рассмотрим теперь прямое произведение $C_2 \times D_2$. Пусть группа $C_2$ порождается элементом $x$, удовлетворяющим соотношению $x^2 = I$, а $D_2$ — элементами

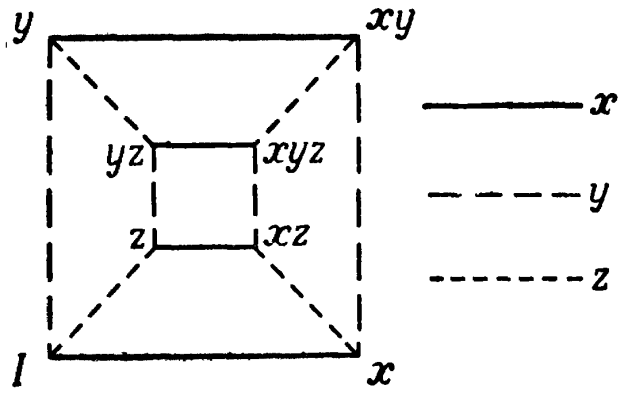



Рис. 7.9.

$y$ и $z$, удовлетворяющими соотношениям $y^2 = z^2 = (yz)^2 = I$. Чтобы получить определяющие соотношения группы $C_2 \times D_2$, мы присоединим к определяющим соотношениям групп $C_2$ и $D_2$ два соотношения

$$xyx^{-1}y^{-1} = I, \quad xzx^{-1}z^{-1} = I;$$

первое из них означает, что элемент $x$ перестановочен с элементом $y$, а второе — что $x$ перестановочен с эле-

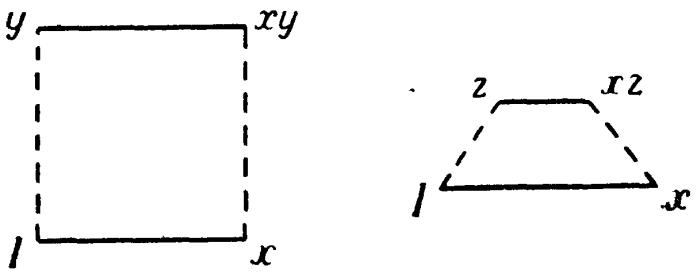



Рис. 7.10.

ментом $z$. Так как все образующие имеют порядок 2, то мы можем переписать эти присоединенные соотношения в таком виде:

$$(xy)^2 = I, \quad (xz)^2 = I,$$

и полная система определяющих соотношений группы $C_2 \times D_2$ выглядит так:

$$x^2 = y^2 = z^2 = (yz)^2 = (xy)^2 = (xz)^2 = I.$$

Рассмотрим графическое представление группы $C_2 \times D_2$ на рис. 7.9. Заметим, что некоторые части этого графа, взятые независимо от других его частей, можно рассматривать как графы групп. Например, ка-

ждая из конфигураций, изображенных на рис. 7.10, является графом четверной группы. В следующей главе, посвященной *подгруппам*, мы выясним значение такого «графа внутри графа».

Упражнение 19. Найдите множества определяющих соотношений и графы прямых произведений

(a) $G = C_2 \times C_4$ и (b) $H = C_3 \times C_3$.

Упражнение 20. Покажите, что $D_6 = C_2 \times D_3$, используя диаграммы Кэли, таблицы умножения или соотношения между образующими. (Вообще $D_{2k} = C_2 \times D_k$, где $k$ — четное число.)

Упражнение 21. Нарисуйте граф группы, определяемой соотношениями $a^2 = b^2 = (ab)^2$. [*Указание*: сначала покажите или, если нужно, *предположите*, что $a^4 = b^4 = I$.]

Упражнение 22. (a) Пусть $H$ — группа с образующими $f$ и $g$ и определяющими соотношениями $f^2 = g^2 = I$. Нарисуйте граф этой группы.

(b) Напомним, что определяющими соотношениями группы $D_\infty$ с образующими $r$ и $f$ будут равенства $f^2 = (rf)^2 = I$ (стр. 98). Покажите, что соотношения $f^2 = g^2 = I$, где $g = rf$, также будут определяющими для группы $D_\infty$.

ГЛАВА 8

# ПОДГРУППЫ

Изучение внутренней структуры конкретной группы позволяет установить многие ее свойства. Внутреннюю структуру некоторых групп можно описать с помощью их подгрупп. Слово «подгруппа» означает «группа внутри группы»; точнее, множество $H$ называется подгруппой группы $G$, если

(A) Каждый элемент множества $H$ является элементом группы $G$;

(B) $H$ есть группа (относительно бинарной операции, определенной в группе $G$).

Значение этих условий будет раскрыто в дальнейшем. Мы начнем с отыскания и исследования некоторых подгрупп в данной группе.

Рассмотрим циклическую группу порядка 4

$$C_4: \quad I,\ a,\ a^2,\ a^3$$

и найдем ее подгруппы порядка 2. Так как подгруппа является *группой* и, следовательно, должна содержать элемент $I$, то все подгруппы порядка 2 группы $C_4$ должны находиться среди множеств

$$R = \{I, a\}, \quad S = \{I, a^2\}, \quad T = \{I, a^3\}.$$

Прежде всего мы видим, что все эти множества удовлетворяют условию (A), так как их элементы принадлежат группе $C_4$. Что же касается условия (B), то множество $R$ из двух элементов было бы, очевидно, циклической группой порядка 2, если бы выполнялось соотношение $a^2 = I$. Но при определенной в группе $C_4$ бинарной операции $a^2 \neq I$. Таким образом, $R$ не является подгруппой группы $C_4$. Пользуясь этим

методом «проб и ошибок», убеждаемся, что единственной подгруппой порядка 2 группы $C_4$ является множество $S$. В дальнейшем для выявления подгрупп будет применяться более простой и систематический метод.

Для доказательства того, что множество образует группу относительно некоторой операции, например $\otimes$, надо убедиться в выполнении всех групповых аксиом. Если мы знаем заранее, что рассматриваемое множество является подмножеством группы, то проверка выполнения аксиом упрощается. Чтобы убедиться в этом, рассмотрим условие (B) из определения подгруппы. Сначала мы должны показать, что

(i) операция $\otimes$ группы $G$, рассматриваемая лишь на элементах множества $H$, является бинарной операцией на множестве $H$.

Это сводится к проверке того, что если $h_1$, $h_2$ — два элемента множества $H$, то и $h_1 \otimes h_2$ принадлежит $H$. Если подмножество $H$ группы $G$ обладает этим свойством, то мы говорим, что оно *замкнуто относительно операции* $\otimes$. (См. рассуждение о замкнутости на стр. 13.) Чтобы доказать, что $H$ — группа, нужно также проверить выполнение следующих условий:

(ii) операция $\otimes$ ассоциативна;

(iii) обратный к любому элементу из множества $H$ принадлежит $H$;

(iv) единица группы $G$ принадлежит множеству $H$.

Условие (ii) выполняется автоматически, так как $\otimes$ — групповая операция группы $G$ и, следовательно, она ассоциативна. Кроме того, условие (iv) следует из условий (i) и (iii), так как если $h$ — элемент множества $H$, то, согласно условию (iii), элемент $h^{-1}$ принадлежит $H$, а по условию (i) $h \otimes h^{-1} = I$ также принадлежит $H$. Таким образом, *подмножество $H$ группы $G$ является подгруппой группы $G$, если выполнены два условия*:

(1) *элемент $h_1 \otimes h_2$ принадлежит множеству $H$, если $h_1$ и $h_2$ — элементы множества $H$ (замкнутость)*;

(2) *элемент $h^{-1}$ принадлежит множеству $H$, если $h$ принадлежит $H$ (обратимость)*.

Упражнение 23. Покажите, что предыдущее утверждение эквивалентно следующему: *подмножество $H$ группы $G$ является подгруппой группы $G$, если элемент $ab^{-1}$ принадлежит $H$, как только $a$ и $b$ принадлежат $H$.* (Это утверждение содержит лишь одно условие.)

Теперь мы используем условия (1) и (2), чтобы относительно каждого из подмножеств $R$, $S$, $T$ группы $C_4$ выяснить, является ли оно подгруппой. Если множество не удовлетворяет хотя бы одному из этих условий, то оно не может быть подгруппой. Для решения вопроса о замкнутости множества можно воспользоваться таблицей умножения элементов этих множеств (следует помнить, что $a^4 = I$, $a^2 \neq I$, $a^3 \neq I$):

*Таблица 8.1*

Множество $R$

| | $I$ | $a$ |
|---|---|---|
| $I$ | $I$ | $a$ |
| $a$ | $a$ | $a^2$ |

Множество $S$

| | $I$ | $a^2$ |
|---|---|---|
| $I$ | $I$ | $a^2$ |
| $a^2$ | $a^2$ | $I$ |

Множество $T$

| | $I$ | $a^3$ |
|---|---|---|
| $I$ | $I$ | $a^3$ |
| $a^3$ | $a^3$ | $a^6 = a^2$ |

Множество $S$ является единственным среди рассматриваемых множеств, таблица умножения которого *замкнута* относительно групповой бинарной операции, т. е. *содержит только элементы этого множества*. Следовательно, множество $S$ является подгруппой, если только оно удовлетворяет условию обратимости (2). Из таблицы умножения видно, что обратными для элементов $I$ и $a^2$ являются элементы $I$ и $a^2$ соответственно. Таким образом, обратный к любому из элементов множества $S$ принадлежит $S$, поэтому $S$ — подгруппа группы $C_4$.

Есть ли в группе $C_4$ подгруппы порядка 3? Рассмотрим некоторое множество элементов группы $C_4$, состоящее из $I$ и двух других элементов, например множество

$$D = \{I, a, a^3\}.$$

Так как $aa = a^2$ входит в таблицу умножения множества $D$, но *не* является элементом множества $D$, то рассматриваемое множество не будет замкнутым относительно бинарной операции группы $C_4$. Поэтому оно не является подгруппой. Читатель может легко убедиться, что и никакое другое подмножество из *трех* элементов группы $C_4$ не удовлетворяет условию (1). Таким образом, $C_4$ не содержит подгрупп порядка 3.

Каждая группа имеет две особые подгруппы. Множество, состоящее из всех элементов группы $G$, является подмножеством группы $G$ и группой относительно определенной в ней бинарной операции. Поэтому группа будет *подгруппой самой себя*. Подмножество $H$, состоящее из единственного элемента $I$, удовлетворяет условиям (1) и (2), так как $I \cdot I = I$. Следовательно, *каждая группа содержит подгруппу, состоящую из единственного элемента I*.

Обычно нас будут интересовать подгруппы, отличные от этих особых подгрупп. Мы будем называть их *собственными*, а эти две особые подгруппы — *несобственными*.

Упражнение 24. Пусть $D_3$ — группа диэдра порядка 6 с элементами

$$I, \quad a, \quad a^2, \quad b, \quad ba, \quad ba^2$$

и соотношениями

$$a^3 = b^2 = (ba)^2 = I.$$

(a) Покажите, что $\{I, ba\}$ — подгруппа группы $D_3$.
(b) Найдите в $D_3$ подгруппу порядка 3.
(c) Есть ли в группе $D_3$ подгруппы порядка 4?

Упражнение 25. Пусть $C_5$ — циклическая группа порядка 5. Найдите все ее собственные подгруппы.

**Бесконечные подгруппы.** Рассмотрим бесконечную циклическую группу $C_\infty$ с образующей $a$ и элементами

$$\ldots, a^{-2}, a^{-1}, I, a, a^2, \ldots .$$

Любая подгруппа группы $C_\infty$ является циклической [1]). Посмотрим, имеются ли в группе $C_\infty$ *конечные* собственные подгруппы. Рассмотрим подмножество

$$S_4 = \{I, a, a^2, a^3\}.$$

На первый взгляд может показаться, что $S_4$ — это циклическая группа $C_4$, которую мы рассматривали на стр. 64. Однако $a^4 \neq I$ *при операции, определенной в группе* $C_\infty$, и, следовательно, $S_4$ *не* совпадает с группой $C_4$. Множество $S_4$ *не замкнуто* относительно операции, определенной в группе $C_\infty$, так как все степени элемента $a$ в группе $C_\infty$ различны; например, элемент $a^2a^3 = a^5$ не принадлежит множеству $S_4$. Следовательно, $S_4$ не является подгрупой группы $C_\infty$.

Те же самые соображения показывают, что *бесконечная циклическая группа* $C_\infty$ *вообще не имеет собственных конечных подгрупп.*

Существуют ли бесконечные подгруппы группы $C_\infty$? Подмножество

$$D = \{\ldots, a^{-4}, a^{-2}, I, a^2, a^4, \ldots\}$$

состоит из четных степеней образующей $a$ группы $C_\infty$. Условие замкнутости (1) выполняется, так как произведение двух четных степеней элемента $a$ является его четной степенью. Чтобы убедиться в выполнении условия (2), отметим, что обратным к элементу $a^{2k}$ служит элемент $a^{-2k}$, также принадлежащий множеству $D$. Таким образом, $D$ — подгруппа группы $C_\infty$.

---

[1]) Действительно, ясно, что сама группа $C_\infty$ и группа $\{I\}$ — циклические группы. Пусть $T$ — некоторая собственная подгруппа группы $C_\infty$. Тогда все ее элементы являются степенями элемента $a$, причем если $a^k$ принадлежит подгруппе $T$, то $a^{-k}$ также принадлежит ей, поскольку этот элемент является обратным к элементу $a^k$. Благодаря этому свойству и условию $T \neq \{I\}$ среди элементов подгруппы $T$ можно выбрать элемент с наименьшим положительным показателем степени, скажем $a^m$. Тогда любой другой элемент $a^n$ $(n > 0)$ из $T$ можно представить в виде $a^n = a^{km+q} = a^{km}a^q$, где $q$ — остаток от деления $n$ на $m$ и $0 \leqslant q < m$. Элемент $a^{km}$ есть степень элемента $a^m$ и принадлежит подгруппе $T$ вместе со своим обратным $a^{-km}$. Тогда $a^{-km}a^n = a^{-km}a^{km}a^q = a^q$ является элементом из $T$, но $q < m$, значит, $q = 0$, $a^n = (a^m)^k$ и $a^m$ является образующей группы $T$. — *Прим. перев.*

Группа $D$ также является бесконечной циклической группой с образующей $a^2$. Существуют также подгруппа, порожденная элементом $a^3$, подгруппа, порожденная элементом $a^4$, и т. д.

Таким образом, *группа $C_\infty$ имеет бесконечно много собственных подгрупп, каждая из которых является бесконечной циклической группой.*

Мы уже достаточно хорошо знаем бесконечную циклическую группу $N$ всех целых чисел с бинарной операцией сложения.

*Элементы группы* — все целые числа (положительные, отрицательные и нуль).

*Групповая операция* — сложение.

*Единичный элемент* — нуль.

*Обратный к данному элементу* — противоположное ему число.

*Образующая* — число 1 (или его обратный — 1).

Мы назовем эту группу *аддитивной* циклической группой.

Является ли множество $E$ *четных* чисел подгруппой группы $N$? Проверим выполнение двух условий:

(1) *Замкнутость*: сумма любых двух четных чисел есть четное число.

(2) *Обратимость*: обратным для четного числа $k$ является число $-k$, которое также четно.

Эти условия выполнены. Таким образом, четные числа образуют подгруппу аддитивной циклической группы целых чисел.

Будет ли подгруппой группы $N$ множество $O$ всех *нечетных* чисел? Так как сумма двух нечетных чисел является четным числом, то это множество *не* замкнуто относительно сложения. Потому оно не составляет подгруппу.

Упражнение 26. Покажите, что

(a) множество всех чисел, кратных 3, образует подгруппу аддитивной циклической группы целых чисел;

(b) множество всех чисел, кратных $n$ (где $n$ — любое целое число), образует подгруппу аддитивной циклической группы.

Упражнение 27. Покажите, что если $R$ и $S$ — две подгруппы группы $G$, то множество элементов, принадлежащих одновременно подгруппам $R$ и $S$, является группой (и, следовательно, подгруппой группы $G$).

Упражнение 28. Докажите, что

(a) все комплексные числа $a + ib$, где $a$ и $b$ — целые числа, образуют группу относительно операции сложения;

(b) множество чисел $r + is$, где $r$ и $s$ — *четные* целые числа, образует подгруппу группы из п. (a).

**Порядки подгрупп.** Как известно, *простым числом* называется целое число, большее единицы, которое не имеет положительных делителей, кроме самого себя и единицы. Интересно, что существуют группы с аналогичными свойствами, т. е. группы, не содержащие других подгрупп, кроме самой себя и подгруппы, состоящей из одного единичного элемента $I$. В самом деле, конечная группа не имеет *собственных* подгрупп тогда и только тогда, когда ее порядок — простое число. Часть «тогда» этого утверждения является следствием более общей теоремы, устанавливающей числовое соотношение между порядком конечной группы и порядком любой из ее подгрупп. Эта теорема, доказанная Лагранжем[1]), была сформулирована в 1771 г. В дальнейшем мы к ней вернемся.

Лагранж одним из первых применил строгие математические методы к задачам аналитической механики. До сих пор в знак уважения к его заслугам одну из основных функций в динамике обозначают буквой $L$ — первой буквой его фамилии. Он внес также вклад в развитие теории групп и ее приложений

---

[1]) Жозеф-Луи Лагранж (1736—1831) создал мощные аналитические методы для решения проблем механики. Он гордился отсутствием в его трактате «Аналитическая механика» каких-либо чертежей. Его методы были использованы в небесной механике для решения проблемы трех тел в применении к движению Луны. Проявляя интерес к созданию общих методов решения алгебраических уравнений, Лагранж одним из первых уловил связь между понятием группы и решением уравнений.

к решению алгебраических уравнений. «Резольвента Лагранжа» была позднее использована Галуа в работах по исследованию разрешимости алгебраических уравнений с помощью теории групп, которые произвели подлинный переворот в науке. Вернемся теперь к теореме Лагранжа о порядках подгрупп конечной группы.

Теорема Лагранжа. *Порядок конечной группы кратен порядку любой из ее подгрупп.*

Эта теорема утверждает, что если $g$ — порядок группы $G$ и $h$ — порядок ее подгруппы $H$, то $g = nh$, где $n$ — одно из целых чисел 1, 2, 3, ..., $g$. Для несобственных подгрупп $G$ и $I$ $n$ равно 1 и $g$ соответственно. Если $H$ — *собственная* подгруппа, то $n$ — одно из целых чисел 2, 3, ..., $g - 1$.

В доказательстве этой теоремы мы используем некоторые множества элементов группы, называемые *смежными классами*. Понятие смежного класса играет важную роль в теории групп. После того как мы вкратце ознакомимся со смежными классами и их свойствами, доказательство теоремы не составит труда.

*Смежные классы группы.* Пусть $H$ — подгруппа группы $G$. Предположим для простоты, что $H$ содержит, например, четыре (различных) элемента, так что

$$H = \{I, h_1, h_2, h_3\}.$$

Пусть $b$ — элемент группы $G$, *не* принадлежащий подгруппе $H$. Рассмотрим множество

$$H_b = \{b, bh_1, bh_2, bh_3\},$$

полученное умножением элементов множества $H$ *слева* на элемент $b$. (Для определенности мы выбираем здесь умножение слева.) Мы утверждаем, что

(i) все элементы множества $H_b$ различны;

(ii) $H$ и $H_b$ не имеют общих элементов.

Чтобы доказать (i), предположим, например, что $bh_1 = bh_3$. Умножив обе части этого равенства слева

на $b^{-1}$, получим равенство

$$b^{-1}bh_1 = b^{-1}bh_3, \quad \text{или} \quad h_1 = h_3,$$

в противоречие с предположением о том, что группа $H$ содержит четыре *различных* элемента.

Чтобы доказать утверждение (ii), допустим сначала, что некоторый элемент подгруппы $H$ равен некоторому элементу множества $H_b$, например пусть $h_2 = bh_1$. Тогда, умножая это равенство справа на $h_1^{-1}$, мы придем к соотношению

$$h_2h_1^{-1} = bh_1h_1^{-1} = b.$$

Элемент $h_2h_1^{-1}$ принадлежит подгруппе $H$, так как $H$ — группа, в то время как по предположению элемент $b$ не принадлежал $H$. Таким образом, допущение, что $H$ и $H_b$ имеют общий элемент, приводит к противоречию.

Мы получили, таким образом, восемь элементов группы $G$: четыре в *подгруппе* группы $G$

$$H = \{I, h_1, h_2, h_3\}$$

и остальные четыре в *множестве* элементов из группы $G$

$$H_b = \{b, bh_1, bh_2, bh_3\}.$$

Множество $H_b$ называется *левым смежным классом группы $G$ по подгруппе $H$* и обозначается через

$$bH = \{b, bh_1, bh_2, bh_3\}.$$

Сама подгруппа $H$ является смежным классом группы $G$ по $H$, так как

$$H = IH = \{I, Ih_1, Ih_2, Ih_3\} = \{I, h_1, h_2, h_3\}.$$

Если $c$ — элемент группы $G$, не принадлежащий ни смежному классу $H$, ни смежному классу $bH$, то его можно использовать для образования нового смежного класса по подгруппе $H$:

$$cH = \{c, ch_1, ch_2, ch_3\}.$$

Мы уже знаем, что все элементы смежного класса $cH$ различны и что множества $H$ и $cH$ не имеют общих элементов. Элементы смежного класса $cH$ отличны также и от элементов класса $bH$. Доказательство этого утверждения составляет часть решения упражнения 29 (см. ниже). Теперь у нас есть двенадцать элементов группы $G$, содержащихся в трех левых смежных классах

$$H = \{I, h_1, h_2, h_3\},$$
$$bH = \{b, bh_1, bh_2, bh_3\}, \quad cH = \{c, ch_1, ch_2, ch_3\}.$$

Если в группе $G$ всего двенадцать элементов, то мы их все уже выписали и получили, таким образом, разбиение группы $G$ на непересекающиеся[1]) *множества*. Тот факт, что группа $G$ является объединением[2]) этих подмножеств, мы будем выражать записью

$$G = H \cup bH \cup cH.$$

Если в группе $G$ больше двенадцати элементов, то в ней существует элемент $d$, не принадлежащий множеству $H \cup bH \cup cH$. Образуем тогда новый левый смежный класс

$$dH = \{d, dh_1, dh_2, dh_3\}.$$

Все элементы класса $dH$ различны, и, как следует из результата упражнения 29, ни один из этих элементов не содержится ни в каком из рассмотренных выше смежных классов. Таким образом, мы получили шестнадцать различных элементов группы $G$, содержащихся в четырех левых смежных классах, по четыре элемента в каждом. Если группа $G$ состоит из шестнадцати различных элементов, то мы можем записать

$$G = H \cup bH \cup cH \cup dH.$$

План доказательства теперь ясен. Выбрав в группе $G$ некоторую подгруппу $H$ порядка $h$ и элемент $b$,

---

[1]) То есть не содержащие общих элементов. — *Прим. перев.*

[2]) *Объединением* двух или нескольких множеств называется множество, состоящее из всех элементов, принадлежащих хотя бы одному из данных множеств.

не принадлежащий этой подгруппе, образуем смежный класс $bH$. Этот смежный класс содержит $h$ элементов, а множества $H$ и $bH$ вместе содержат $2h$ различных элементов группы. Если есть элемент $c$, не вошедший в эти $2h$ элементов, то мы образуем новый смежный класс $cH$ и получим всего $3h$ различных элементов группы $G$. И всякий раз, когда найдется хотя бы один элемент группы $G$, не вошедший в объединение ранее образованных смежных классов, мы можем образовать новый смежный класс (содержащий $h$ различных элементов). Так как порядок группы $G$ конечен, то, добавляя на каждом шаге $h$ различных элементов, через конечное число шагов мы должны исчерпать все элементы группы $G$. Если после образования $n$ левых смежных классов по подгруппе $H$ все элементы группы $G$ окажутся использованными, то мы получаем разбиение группы $G$ на $n$ левых смежных классов по $h$ элементов в каждом:

$$G = \underbrace{H \cup bH \cup cH \cup \ldots \cup kH}_{n \text{ классов по } h \text{ элементов в каждом}}.$$

Таким образом, *порядок группы $G$ есть число, кратное порядку любой ее подгруппы $H$.*

Итак, рассмотрев понятие смежных классов группы по ее подгруппе, мы попутно доказали теорему Лагранжа.

Упражнение 29. Пусть $rH$ и $sH$ — два левых смежных класса группы $G$ по подгруппе $H$. Покажите, что классы $rH$ и $sH$ либо не имеют общих элементов, либо совпадают.

*Несовпадение левых и правых смежных классов.* В приведенном доказательстве теоремы Лагранжа были использованы левые смежные классы. Если использовать правые смежные классы, то доказательство по существу не изменится. Поставим такой вопрос: совпадают ли соответствующие левые и правые смежные классы по одной и той же подгруппе? Если это не так, то можно ли, по крайней мере, надеяться, что любой левый смежный класс $bH$ содержит в точ-

ности те же элементы, что и некоторый правый смежный класс $Hc$?

Рассмотрим группу диэдра $D_3$ шестого порядка (рис. 8.1). Она содержит циклическую подгруппу второго порядка

$$H = \{1, b\}.$$

Образуем левые и правые смежные классы группы $D_3$ по подгруппе $H$. (На графе видно, что $a^2b = ba$ и $ba^2 = ab$.)

| Левые смежные классы | Правые смежные классы |
|---|---|
| $H = \{1, b\}$, | $H = \{1, b\}$, |
| $aH = \{a, ab\}$, | $Ha = \{a, ba\}$, |
| $a^2H = \{a^2, a^2b\} = \{a^2, ba\}$, | $Ha^2 = \{a^2, ba^2\} = \{a^2, ab\}$. |

Заметим, что в этих разбиениях никакие два смежных класса, за исключением самой подгруппы

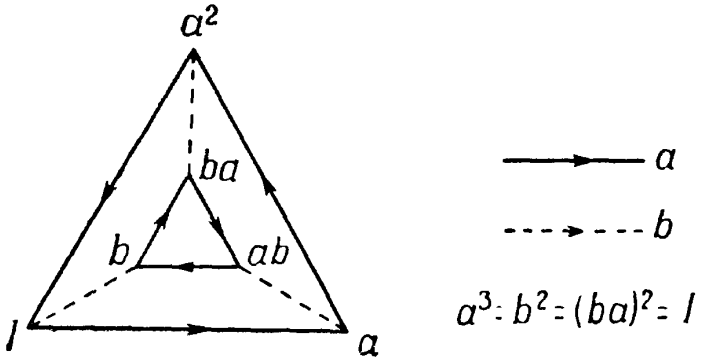



Рис. 8.1.

$H$, не совпадают. Как смежный класс $aH$, так и смежный класс $a^2H$ отличаются от обоих правых смежных классов $Ha$ и $Ha^2$. Мы получили два различных разбиения группы $D_3$ на левые и правые классы соответственно:

$$D_3 = H \cup aH \cup a^2H$$

и

$$D_3 = H \cup Ha \cup Ha^2.$$

Этот пример показывает, что *левые и правые смежные классы группы $G$ по подгруппе $H$ могут давать различные разбиения группы $G$.*

*Бесконечные смежные классы.* Мы уже знаем, что множество $N$ всех целых чисел является группой с бинарной операцией сложения (аддитивной циклической группой) и что множество $E$ всех четных чисел является подгруппой этой группы (стр. 111). Попытаемся представить группу $N$ как объединение смежных классов по подгруппе $E$. Пусть $a$ — элемент группы $G$, не принадлежащий $E$, т. е. $a$ — некоторое нечетное число; рассмотрим множество $aE$, полученное применением групповой операции (сложения) к элементу $a$ и всем элементам множества $E$. Если обозначить элементы множества $E$ через $e_1$, $e_2$, $e_3$, ..., то множество $aE$ будет состоять из элементов

$$a+e_1, \quad a+e_2, \quad a+e_3, \ldots .$$

Так как сумма четного и нечетного чисел есть число нечетное и каждое нечетное число может быть записано в виде суммы нечетного числа $a$ и некоторого четного числа, то смежный класс $aE$ совпадает с множеством $O$ всех нечетных чисел, какое бы нечетное число мы ни взяли в качестве $a$. Ясно, что объединение смежных классов $E$ и $O$ совпадает со всем множеством целых чисел $N$. Таким образом,

$$N = E \cup aE,$$

или

$$N = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \cup \{\ldots, -3, -1, 1, 3, \ldots\}.$$

(Отметим, что ввиду коммутативности группы $N$ левые и правые смежные классы совпадают, так что смежный класс $Ea$ — это также множество $O$.)

Подгруппа $E$ — это множество чисел, кратных числу 2, а смежный класс $aE$ — это множество всех целых чисел, дающих остаток 1 при делении на 2. Аналогичным способом можно найти смежные классы множества $N$ по подгруппе $T$ всех чисел, кратных 3. Выпишем их:

$$T = \{\ldots, -6, -3, 0, 3, 6, \ldots\} =$$

$$= \{\text{все целые числа, дающие при делении на 3 остаток 0}\},$$

$aT = \{\ldots, -5, -2, 1, 4, 7, \ldots\} =$

$=$ {все целые числа, дающие при делении на 3 остаток 1},

$bT = \{\ldots, -4, -1, 2, 5, 8, \ldots\} =$

$=$ {все целые числа, дающие при делении на 3 остаток 2}.

(Здесь число $a$ может быть представлено в виде $3n + 1$, а число $b$ — в виде $3n + 2$.) Тогда

$$N = T \cup aT \cup bT$$

— представление множества $N$ с помощью смежных классов по подгруппе $T$.

Упражнение 30. Пусть $rJ$ и $cJ$ — смежные классы группы $L$ по подгруппе $J$. Покажите, что

(a) если $c$ — элемент смежного класса $rJ$, то смежные классы $cJ$ и $rJ$ совпадают;

(b) смежные классы $cJ$ и $rJ$ совпадают в том и только том случае, когда элемент $r^{-1}c$ принадлежит подгруппе $J$.

Упражнение 31. Докажите, что если

$$L = J \cup rJ \cup sJ \cup \ldots \cup vJ$$

— представление группы $L$ в виде объединения *левых* смежных классов по подгруппе $J$, то

$$L = J \cup Jr^{-1} \cup Js^{-1} \cup \ldots \cup Jv^{-1}$$

является ее представлением с помощью правых смежных классов.

Упражнение 32. Найдите правые и левые смежные классы группы диэдра $D_3$ шестого порядка по ее подгруппе $K = \{I, a, a^2\}$.

*Некоторые следствия из теоремы Лагранжа.* Укажем теперь некоторые непосредственные следствия из теоремы Лагранжа о порядках подгрупп.

Теорема 4. *Если порядок группы $G$ есть простое число, то*

(1) *группа $G$ не имеет собственных подгрупп;*

(2) *группа $G$ является циклической.*

Утверждение (1) следует непосредственно из теоремы Лагранжа и определения простого числа. Для доказательства утверждения (2) обозначим через $r$ любой отличный от $I$ элемент группы $G$ простого порядка. Если порядок $r$ равен $n$, то $r^n = I$ и $n > 1$. Множество

$$H = \{I, r, r^2, \ldots, r^{n-1}\}, \qquad n - 1 > 0,$$

составляет циклическую группу $n$-го порядка в группе $G$ (см. упр. 33), так что $H$ — подгруппа данной группы $G$ простого порядка. По теореме Лагранжа порядок $n$ этой подгруппы является делителем числа $p$. Так как $n \neq 1$, то $n = p$. Но $H$ — подгруппа группы $G$; следовательно, $H$ *совпадает* с группой $G$. Это доказывает утверждение (2).

Из теоремы Лагранжа следует только, что если в группе $G$ *есть* подгруппа $H$, то порядок группы $G$ кратен порядку группы $H$. Пока для нас остается открытым вопрос, верно ли обратное утверждение: обязательно ли в группе $G$, порядок которой кратен некоторому числу $k$, содержится подгруппа порядка $k$? Мы ответим на этот вопрос позднее, когда перейдем к изучению группы тетраэдра двенадцатого порядка.

Решив некоторые из следующих ниже упражнений, можно вывести одно интересное следствие теоремы Лагранжа. Читатель, который как следует потрудится над ними, получит в награду доказательство одной хорошо известной теоремы теории чисел, принадлежащей Ферма.

Упражнение 33. (a) Покажите, что если порядок элемента $a$ группы $G$ равен $n$, то $H = \{I, a, a^2, \ldots, a^{n-1}\}$ — циклическая подгруппа группы $G$.

(b) Какое соотношение связывает между собой порядок произвольного элемента конечной группы и порядок самой группы?

Упражнение 34. Рассмотрим группу «остатков» порядка $p - 1$ (стр. 37) с элементами $1, 2, \ldots, p - 1$ ($p$ — простое число) и бинарной операцией умножения по модулю $p$. Для любых двух чисел $x$ и $y$ из рассматриваемого множества найдется такое чи-

сло $r$, что $xy$ и $r$ дают одинаковый остаток при делении на $p$, так что $xy \equiv r \pmod{p}$. Ясно, что каждый элемент этой конечной группы «остатков» имеет конечный порядок. Пусть $g$ — некоторый элемент порядка $n$.

(a) Покажите, что число $g^n - 1$ кратно числу $p$, т. е. что

$$g^n - 1 \equiv 0 \pmod{p}.$$

(b) Используя теорему Лагранжа, покажите, что $g^{p-1} - 1$ есть число, кратное числу $p$, или

$$g^{p-1} - 1 \equiv 0 \pmod{p}$$

(см. упр. 33).

Упражнение 35. Пусть число $a$ кратно простому числу $p$, т. е. $a \equiv 0 \pmod{p}$. Тогда оба числа $a^p$ и $a^p - a$ являются кратными числа $p$ и, значит, $a^p \equiv (a^p - a) \pmod{p} \equiv 0 \pmod{p}$. Докажите, что и в том случае, когда целое положительное число $a$ *не* является кратным числа $p$, т. е. $a \not\equiv 0 \pmod{p}$, $a^p - a$ есть число, кратное $p$. [*Указание.* Мы должны доказать, что $a^p \equiv a \pmod{p}$, или $a(a^{p-1} - 1) \equiv 0 \pmod{p}$. Для доказательства этого последнего соотношения нужно использовать результат упражнения 34.]

При решении этого упражнения доказана следующая теорема Ферма: *если $p$ — простое число и $a$ — любое целое положительное число, то $a^p - a$ кратно числу $p$.*

Упражнение 36. Пусть $a$ и $b$ — элементы группы $G$. Покажите, что

(a) порядок элемента $ab$ равен порядку элемента $ba$;

(b) если $ab = ba$, то порядок элемента $ab$ является делителем произведения порядков элементов $a$ и $b$;

(c) если $ab = ba$, а порядки $m$ и $n$ элементов $a$ и $b$ соответственно — взаимно простые числа, то порядком элемента $ab$ является число $mn$ (числа $m$ и $n$ называются *взаимно простыми*, если единственный их общий делитель есть 1).

ГЛАВА 9

# ОТОБРАЖЕНИЯ

Понятие группы тесно связано с понятием отображения или, вернее, множества отображений. Мы сейчас введем это понятие (являющееся основным для многих разделов современной математики), начав с рассмотрения некоторых простых примеров.

Слово «отображение» обычно означает «наглядное описание чего-нибудь». Смысл, в котором это слово употребляется в математике, довольно близок к тому значению, в котором оно используется в повседневной жизни. Это случается сравнительно редко — чаще всего математическое значение термина весьма далеко от его обыденного смысла. (Ср. термины «группа», «поле», «кольцо».)

Математическое понятие отображения возникло путем естественного абстрагирования из обычного понятия плана[1]), например «плана города». В идеальном случае план — это такое изображение некоторого объекта (города) на листе бумаги, что для каждой точки этого объекта (города) имеется одна и только одна точка на бумаге в качестве ее копии. В математике понятие отображения во всех его вариантах основывается на понятии соответствия между элементами исходного объекта и элементами его образа.

Мы начнем изучение отображения с рассмотрения простого случая, когда отображается множество с конечным числом элементов. Пусть задано множество $X = \{a, b, c\}$, состоящее из трех элементов, и множество $Y = \{r, s, t\}$, также состоящее из трех элементов.

---

[1]) В английском языке «отображение» («mapping») образовано от слова «план» («map»). — *Прим. перев.*

Мы можем различными путями объединить элементы этих двух множеств в пары; например,

$$\begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix}.$$

Здесь соответствующие элементы расположены один под другим, каждому верхнему элементу *ставится в соответствие* расположенный под ним элемент. Это *соответствие* и есть пример *отображения* одного множества на другое ($X$ на $Y$). Вообще отображение множества $X$ в множество $Y$ *определяется* следующим образом: каждому элементу множества $X$ ставится в соответствие *в точности один* элемент множества $Y$.

Рассмотренное выше отображение множества $X$ на множество $Y$ можно различными способами записать с помощью двух строк, заключенных в круглые скобки:

$$\begin{pmatrix} a & b & c \\ r & s & t \end{pmatrix}, \text{ или } \begin{pmatrix} a & c & b \\ r & t & s \end{pmatrix}, \text{ или } \begin{pmatrix} b & c & a \\ s & t & r \end{pmatrix}.$$

Это все записи *одного и того же* отображения множества $X$ на множество $Y$, так как каждому элементу множества $X$ всякий раз ставится в соответствие *один и тот же* элемент множества $Y$: $a$ всегда отображается в $r$, $b$ — в $s$ и $c$ — в $t$.

Имеются, однако, и другие отображения множества $X$ на $Y$, существенно отличающиеся от приведенного выше; например,

$$\begin{pmatrix} a & b & c \\ s & r & t \end{pmatrix}.$$

Это отображение отлично от предыдущего, так как, хотя элемент $c$ по-прежнему отображается в элемент $t$ множества $Y$, элемент $a$ отображается теперь в элемент $s$, а не в $r$, как это было в предыдущем случае.

С понятием отображения одного множества в другое связаны самые разнообразные термины и обозначения. Некоторые из них нам будут необходимы, и

мы их сейчас введем, надеясь, что читатель усвоит их постепенно в процессе чтения этой главы.

Мы продемонстрировали один из возможных способов записи отображения — с помощью двух строк, заключенных в скобки. В книге будут употребляться и другие способы записи отображений. Если читатель вспомнит наши первоначальные рассуждения о бинарной операции в группе, то он убедится, что *групповую бинарную операцию можно рассматривать как отображение.* Действительно, каждой упорядоченной паре элементов $r$ и $s$ группы ставится в соответствие единственный элемент $t$ группы, такой, что

$$(r, s) \to t.$$

Таким образом, множество упорядоченных пар элементов группы *отображается* на группу. Таблица умножения группы полностью описывает это отображение. Первые элементы всех пар $(r, s)$ записываются в столбце слева, вторые элементы — в строке сверху, а *образ* пары $(r, s)$ при отображении записывается в соответствующем месте таблицы.

Для отображения множества $X$ в множество $Y$ употребляется запись $X \to Y$. Стрелки используются и для обозначения соответствия между отдельными элементами; так, в нашем первом примере $a \to r$, $b \to s$, $c \to t$. Элемент $r$ множества $Y$, сопоставляемый элементу $a$ при отображении множества $X$, называется *образом* элемента $a$, элемент $s$ — образом элемента $b$ и $t$ — образом элемента $c$. Множество $X$ называется *областью определения* отображения, а совокупность всех элементов множества $Y$, являющихся образами элементов из множества $X$, называется *областью значений* отображения или *образом* множества $X$.

В этой книге мы будем в основном иметь дело со специальным классом отображений $X \to Y$, при которых каждый элемент множества $Y$ является образом по крайней мере одного элемента множества $X$, иначе говоря, когда *образ множества X совпадает с множеством Y*. Про такие отображения мы будем говорить, что они отображают множество $X$ *на* множество $Y$.

Оба рассмотренных выше отображения являются отображениями такого типа. Возьмем теперь отображение

$$N: \begin{pmatrix} a & b & c \\ s & r & s \end{pmatrix}$$

множества $X$ в множество $Y$. Это действительно отображение, так как каждому элементу множества $X$ ставится в соответствие точно один элемент множества $Y$. Однако множество $X$ при этом отображается *не* на все множество $Y$, так как элемент $t$ из $Y$ *не* является образом никакого элемента из множества $X$.

Отображение множества $X$ в множество $Y$ часто обозначается каким-нибудь символом, например $f$, тогда мы пишем

$$f: \quad X \to Y.$$

В этом случае $f(a) = r$ означает, что $a \to r$, т. е. что образом элемента $a$ является элемент $r$. Аналогично, образами элементов $b$ и $c$ являются элементы $f(b) = s$ и $f(c) = t$ соответственно.

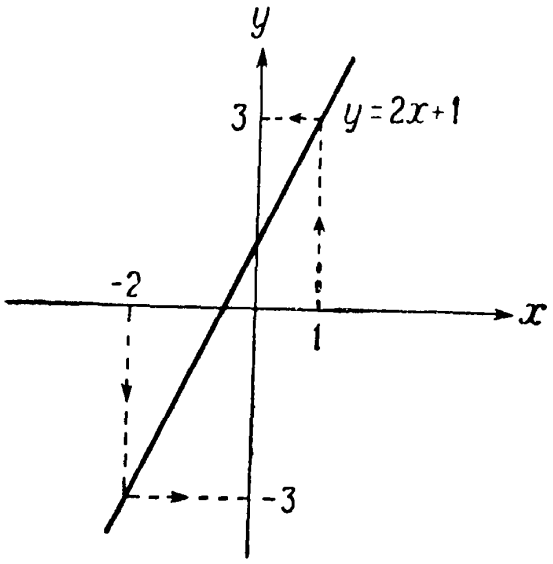



Рис. 9.1.

Понятие отображения одного множества в другое неявно используется всякий раз, когда мы строим график уравнения с двумя неизвестными. Рассмотрим, например, уравнение

$$y = 2x + 1$$

и его график (рис. 9.1). Уравнение описывает отображение оси $x$ *на* ось $y$, так как ось абсцисс является его областью определения, а вся ось ординат — его областью значений. Рассматриваемое отображение можно записать в виде

$$f: \quad x \to y, \quad \text{или} \quad f(x) = y.$$

Эта запись означает, что образом элемента $x$ является элемент $y$, где $y = 2x + 1$, или $f(x) = 2x + 1$.

Каждой точке оси $x$ уравнение $y = 2x + 1$ ставит в соответствие *в точности одну* точку оси $y$. Таким образом, каждому действительному числу ставится в соответствие в точности одно действительное число. Например, число $x = 1$ переходит в число $2 \cdot 1 + 1 = 3$.

Наряду с отображениями одного множества на другое можно рассматривать отображения множества на себя. Рассмотрим множество $X = \{a, b, c\}$. Одним из его отображений на себя является отображение

$$\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}.$$

Оно ставит в соответствие каждому элементу множества $X$ в точности один элемент этого же множества,

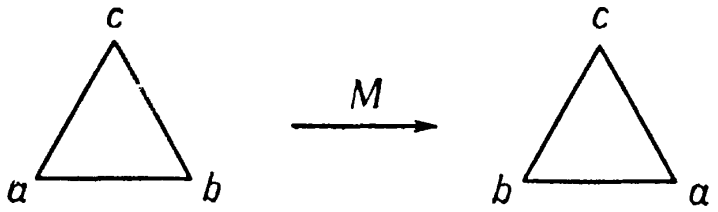



Рис. 9.2.

и область определения этого отображения совпадает с его областью значений. Обозначим данное отображение буквой $M$.

Предположим теперь, что $a$, $b$, $c$ — вершины равностороннего треугольника. Отображение $M$ можно интерпретировать как опрокидывание этого треугольника относительно высоты, проходящей через вершину $c$ (рис. 9.2). Мы покажем, что два таких последовательных опрокидывания можно рассмотреть как «последовательное выполнение» двух отображений $M$ и представить такую суперпозицию отображений как одно отображение.

Спросим себя сначала: что означает «последовательное выполнение» двух отображений:

$$M^2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = ?$$

Напомним, что одно и то же отображение можно записать с помощью двух строк, заключенных в круг-

лые скобки, разными способами. Например, $M$ можно представить в виде

$$\begin{pmatrix} b & a & c \\ a & b & c \end{pmatrix}.$$

Заметим, что верхняя строка при такой записи совпадает с нижней строкой при первоначальной записи отображения $M$. Поставленный выше вопрос можно теперь переписать так:

$$M^2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} b & a & c \\ a & b & c \end{pmatrix} = ?$$

Первый сомножитель показывает, что $a \to b$, а второй — что $b \to a$. В конечном счете получаем $a \to a$,

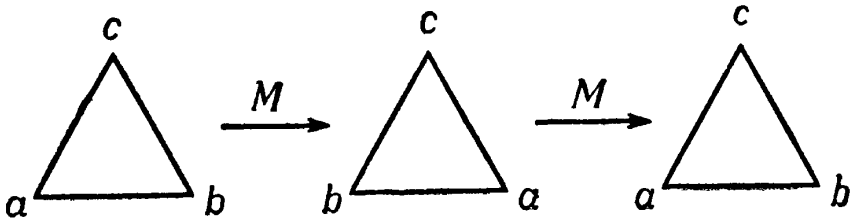



Рис. 9.3.

т. е. элемент $a$ переходит в себя. Аналогично $b \to a$, затем $a \to b$ и в результате $b \to b$. Наконец, $c \to c$, затем $c \to c$ и в результате $c \to c$. Итак, мы можем написать

$$M^2 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = I$$

и сделать вывод, что в результате последовательного выполнения двух отображений $M$ получается отображение, которое каждому элементу ставит в соответствие сам этот элемент. Отображение, обладающее таким свойством, называется *тождественным отображением* и обозначается через $I$.

Возвращаясь к геометрической интерпретации отображения $M$, видим, что $I$ соответствует двум последовательным опрокидываниям треугольника относительно высоты, проходящей через вершину $c$, в результате которых треугольник возвращается в свое исходное положение (рис. 9.3).

Уравнение $y = x$ или $f(x) = x$ дает другой пример тождественного отображения. Из графика этого уравнения (рис. 9.4) видно, что каждое число отображается само в себя.

**Отображения как элементы группы.** Отображение $M$ можно рассматривать как элемент множества отображений. Более того, мы видели, что существует тождественное отображение, и мы покажем далее, что суперпозиция двух отображений снова является отображением. Все это наводит на мысль, что *отображения могут быть элементами группы.* И действительно, будет установлено, что некоторые множества отображений удовлетворяют групповым аксиомам. При этом *мы ограничимся рассмотрением отображений множества на себя.*

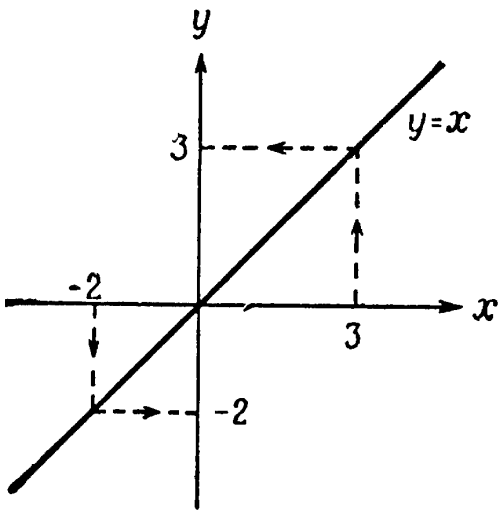


Рис. 9.4.

Для доказательства того, что множество отображений образует группу, нам придется поступить, как всегда, — проверить выполнение групповых аксиом. Мы занимались такого рода проверкой много раз, и общая процедура нам хорошо знакома. Однако наш опыт обращения с отображениями крайне ограничен, и они по-прежнему представляются нам какими-то странными образованиями, которые могут — и весьма сложным способом — переставлять элементы множеств. Поэтому будем проводить проверку очень тщательно, уделяя особое внимание некоторым тонким вопросам. В результате детального исследования мы установим, какие именно множества отображений множества на себя образуют группу. Вообще говоря, далеко не всякое отображение может служить элементом группы. Мы исследуем, насколько совместимы свойства отображения с групповыми аксиомами, и выясним, каким условиям должно удовлетворять отображение, являющееся элементом группы.

Сначала покажем, что последовательное выполнение, или суперпозиция, двух отображений является бинарной операцией на множестве отображений данного множества $S$ на себя.

(1) *Бинарная операция.* Нужно показать, что если $M_1$ и $M_2$ — два отображения множества $S$ *на* себя, то их произведение также является таким отображением.

Представим $M_1$ и $M_2$ схематически в виде

$$M_1 = \begin{pmatrix} a & \dots \\ b & \dots \end{pmatrix}, \qquad M_2 = \begin{pmatrix} \dots & b & \dots \\ \dots & c & \dots \end{pmatrix},$$

где $a$, $b$, $c$, ... — элементы данного множества $S$. Первое отображение $M_1$ ставит в соответствие элементу $a$ некоторый элемент $b$, т. е. $a \to b$. Отображение $M_2$ ставит в соответствие элементу $b$ элемент $c$, т. е. $b \to c$.

Таким образом, при последовательном выполнении отображений $M_1$ и $M_2$ элемент $a$ переходит в элемент $c$, т. е. $a \to c$, и, следовательно, $M_1M_2$ — отображение множества $S$. Предоставляем читателю самостоятельно доказать, что $M_1M_2$ — *отображение на* все множество $S$, т. е. что если $y$ — произвольный элемент множества $S$, то найдется элемент $x$, который переходит при отображении $M_1M_2$ в элемент $y$.

(2) *Ассоциативность.* На первый взгляд может показаться, что бинарная операция — *последовательное выполнение* отображений — несомненно ассоциативна. Однако если учесть, что элементы исходного множества при каждом отображении меняются местами, то этот факт перестает быть столь уж очевидным. Остановимся подробно на проверке этого требования.

Мы должны показать, что для любых трех отображений $M_1$, $M_2$ и $M_3$ множества $S$ на себя справедливо соотношение

$$(M_1M_2)\,M_3 = M_1\,(M_2M_3).$$

Если $x$ — произвольный элемент множества $S$, то $M_1$ переводит $x$ в некоторый элемент $y$. Так как каждое из отображений $M_2$ и $M_3$ ставит в соответствие

каждому элементу множества $S$ в точности один элемент этого же множества, то найдутся такие элементы $z$ и $w$ множества $S$, что

$$M_1\colon\ x \to y, \quad M_2\colon\ y \to z, \quad M_3\colon\ z \to w.$$

Таким образом, при отображении $(M_1M_2)M_3$ осуществляются последовательные переходы: $x \to z$ и $z \to w$, в результате которых $x \to w$. При отображении $M_1(M_2M_3)$ сначала элемент $x$ переходит в $y$, затем $y$ переходит в $w$ и в результате $x$ также переходит в $w$. Следовательно, образом элемента $x$ при обоих отображениях $(M_1M_2)M_3$ и $M_1(M_2M_3)$ является один и тот же элемент $w$. Это и доказывает ассоциативность.

(3) *Единица.* При тождественном отображении каждый элемент рассматриваемого множества соответствует сам себе, т. е.

$$I = \begin{pmatrix} a & b & c & \dots \\ a & b & c & \dots \end{pmatrix}.$$

Ясно, что это отображение является единичным элементом относительно бинарной операции суперпозиции отображений: $MI = IM = M$.

(4) *Обратные элементы*[1]). Рассмотрим отображение

$$M = \begin{pmatrix} u & v & w \\ r & s & t \end{pmatrix};$$

обратное к нему отображение, обозначаемое через $M^{-1}$, должно переводить элемент из области значений отображения $M$ в тот элемент области определения, которому он был сопоставлен при отображении $M$. Иначе говоря, при отображении $M^{-1}$ каждый образ переводится обратно в тот элемент, из которого он получился при отображении $M$. Тогда

$$M^{-1} = \begin{pmatrix} r & s & w \\ u & v & t \end{pmatrix}.$$

---

[1]) В этом пункте фактически рассматриваются произвольные отображения множеств, а не только отображения множества на себя. — *Прим. ред.*

(Заметим, что в записи отображения $M^{-1}$ участвуют те же строки, что и в записи отображения $M$, их лишь нужно поменять местами.) Тогда

$$MM^{-1}=\begin{pmatrix} u & v & w \\ r & s & t \end{pmatrix}\begin{pmatrix} r & s & t \\ u & v & w \end{pmatrix}=\begin{pmatrix} u & v & w \\ u & v & w \end{pmatrix}=I,$$

и, аналогично, $M^{-1}M = I$, т. е. отображение $M^{-1}$ является обратным к $M$.

Рассмотрим, например, отображение

$$N=\begin{pmatrix} u & v & w \\ r & s & r \end{pmatrix}.$$

Допустим, что это отображение имеет обратное, скажем $X$. Тогда для выполнения равенств $XN = NX = I$ необходимо, чтобы $X$ переводило соответственно $r \to u$, $s \to v$ и $r \to w$. Но это уже *не* отображение, так как по определению отображение ставит в соответствие каждому элементу области определения *в точности один* элемент области значений, в то время как $X$ переводит элемент $r$ в *два* элемента $u$ и $w$. Поэтому отображение $N$ не имеет обратного.

Какое различие между отображениями $M$ и $N$ приводит к тому, что $M$ имеет обратное отображение, а $N$ — нет? При отображении $M$ различные элементы области определения переходят в различные элементы области значений, а при отображении $N$ элементам $u$ и $w$ сопоставляется один и тот же элемент $r$. *Отображение имеет обратное в том и только том случае, когда оно различные элементы переводит в различные элементы*, т. е. каждый элемент из его области значений соответствует только одному элементу области определения. Отображение, обладающее таким свойством, *называется взаимно однозначным*[1]).

---

[1]) Отображение *на* себя *конечного* множества элементов будет, очевидно, взаимно однозначным. Однако для *бесконечных* множеств это уже неверно. Рассмотрим, например, отображение отрезка [0, 2] оси $x$, определяемое формулой $x' = f(x) = 2(x-1)^2$. Ясно, что оно является отображением *на* себя, однако каждому $x'$, $0 < x' \leqslant 2$, соответствуют в точности *два* значения $x$, поэтому обратное отображение определить нельзя. — *Прим. ред.*

Мы показали, что *множество всех взаимно однозначных отображений множества на себя образует группу относительно операции суперпозиции, или последовательного выполнения отображений.* В следующих главах мы познакомимся с такими группами конкретно, когда займемся исследованием *групп подстановок* и *симметрических групп.*

*Дополнительные замечания об обратных отображениях.* Рассмотрим отображение $M$: $x \to y$, определенное формулой

$$y = 2x + 1, \quad \text{или} \quad f(x) = 2x + 1.$$

График отображения $y=2x+1$ изображен на рис. 9.1 (стр. 125). Будет ли это отображение взаимно однозначным? Предположим, что $x_1$ и $x_2$ — различные числа. Различны ли также их образы $f(x_1) = y_1$ и $f(x_2) = y_2$? Числа $x_1$ и $x_2$ различны, когда их разность не равна нулю. Так как

$$y_1 - y_2 = (2x_1 + 1) - (2x_2 + 1) = 2(x_1 - x_2),$$

т. е.

$$y_1 - y_2 = 2(x_1 - x_2),$$

то правая часть равенства отлична от нуля ($x_1$ и $x_2$ по предположению различны); следовательно, и левая часть отлична от нуля и $y_1 \neq y_2$.

Отображение $M^{-1}$, таким образом, существует. Покажем, что оно задается формулой

$$M^{-1}\colon\ x = \frac{y-1}{2}.$$

Для проверки этого утверждения возьмем сначала образ $y$ числа $x$ при отображении $M$ ($y=2x+1$), а затем найдем образ числа $y$ при отображении $M^{-1}$. Мы получим

$$MM^{-1}\colon\ \frac{(2x+1)-1}{2} = x,$$

так что отображение $MM^{-1}$ переводит каждый элемент в себя и, следовательно, $MM^{-1} = I$. Точно так же

$M^{-1}M$ отображает $y$ в $y$, поскольку

$$2\frac{y-1}{2}+1=y,$$

и, таким образом, $M^{-1}M=I$.

Рассмотрим теперь отображение $N$: $x\to y$, задаваемое формулой

$$y=x^2, \quad \text{или} \quad f(x)=x^2,$$

график которого показан на рис. 9.5. Взаимно однозначно ли это отображение? Пусть $x_1$ и $x_2$ — различ-

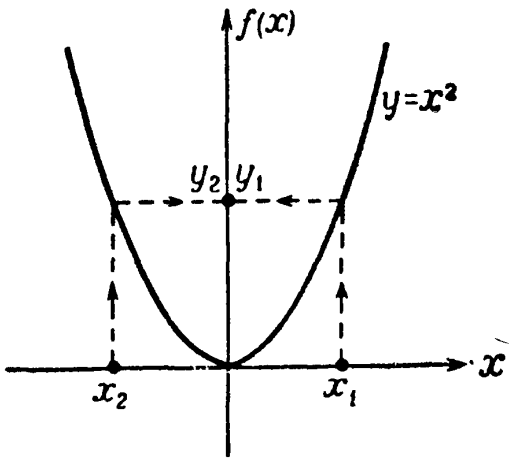



Рис. 9.5.

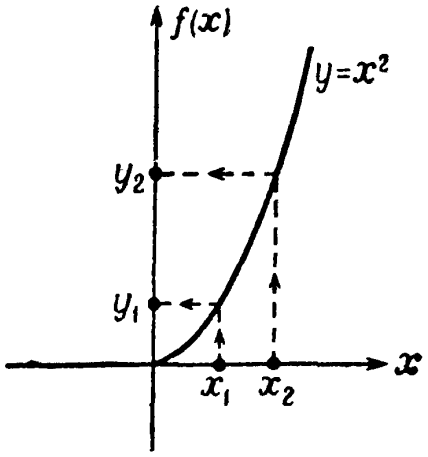



Рис. 9.6.

ные числа, т. е. $x_1-x_2\neq 0$. Следует ли отсюда, что $y_1-y_2=f(x_1)-f(x_2)\neq 0$? Разность образов равна

$$y_1-y_2=x_1^2-x_2^2=(x_1-x_2)(x_1+x_2).$$

По предположению $x_1-x_2\neq 0$, однако если $x_1+x_2=0$, то $y_1-y_2=0$. Поэтому даже если $x_1$ и $x_2$ различны, $y_1$ и $y_2$ не обязаны быть различными. Действительно, если $x_1=-x_2$, причем $x_1\neq 0$, то $y_1=y_2$. Таким образом, отображение $N$ не взаимно однозначно и поэтому не имеет обратного. Однако если из области определения отображения $N$ исключить всю отрицательную полуось оси $x$ (или всю положительную полуось), то полученное при этом отображение $\hat{N}$, определенное формулой

$$y=x^2, \quad x\geqslant 0,$$

взаимно однозначно и имеет обратное (рис. 9.6). В области определения отображения $\hat{N}$ равенство

$x_1 = -x_2$ выполняется только для $x_1 = x_2 = 0$, так что различные элементы переходят в различные. Отображение $\hat{N}$ — это взаимно однозначное отображение множества всех неотрицательных действительных чисел на себя. Обратным для него является отображение

$$\hat{N}^{-1}: \quad x = \sqrt{y}, \quad y \geqslant 0.$$

Чтобы проверить равенства $\hat{N}\hat{N}^{-1} = \hat{N}^{-1}\hat{N} = I$, заметим, что отображение $\hat{N}\hat{N}^{-1}$ можно задать формулой

$$F(x) = \sqrt{x^2} = x, \quad x \geqslant 0,$$

а $\hat{N}^{-1}\hat{N}$ — формулой

$$G(y) = (\sqrt{y})^2 = y, \quad y \geqslant 0.$$

**Гомоморфизм.** Перейдем теперь к рассмотрению отображений специального типа, играющих в теории групп большую роль. Нас будут интересовать отображения, называемые *гомоморфизмами*, и их частный вид — *изоморфизмы*. Понятия, связанные с этими отображениями, важны для изучения свойств не только групп, но и других алгебраических систем. Слова «гомоморфизм» и «изоморфизм» однокоренные. Корень «морф» (что по-гречески означает «форма») указывает на их связь со *структурой*.

Прежде чем дать строгое определение, рассмотрим пример гомоморфного отображения аддитивной группы $N$ целых чисел на аддитивную группу $E$ *четных* чисел (стр. 111). Это отображение $M$ ставит в соответствие каждому элементу $n$ группы $N$ элемент $2n$, принадлежащий $E$,

$$M = \begin{pmatrix} \ldots, & -2, & -1, & 0, & 1, & 2, & \ldots \\ \ldots, & -4, & -2, & 0, & 2, & 4, & \ldots \end{pmatrix}.$$

Заметим, что любые два элемента $n_1$ и $n_2$ группы $N$ при этом переходят в элементы $2n_1$ и $2n_2$ соответственно, а их сумма $n_1 + n_2$ — в элемент $2(n_1 + n_2)$, т. е. *образ* $2(n_1 + n_2)$ *суммы* элементов $n_1$ и $n_2$, равный $2n_1 + 2n_2$, есть *сумма образов* $2n_1$ и $2n_2$ этих эле-

ментов. Советуем читателю запомнить это отображение $M$ как конкретный пример гомоморфизма одной группы на другую.

Пусть теперь даны две группы $G$ и $H$ и отображение группы $G$ на группу $H$. Это означает, что каждый элемент группы $H$ является образом некоторого элемента группы $G$. Обозначим образы элементов $a$ и $b$ группы $G$ через $f(a)$ и $f(b)$ соответственно. Тогда $f(a)$ и $f(b)$ — элементы группы $H$. Так как $G$ и $H$ — группы, то произведения $a \cdot b$ и $f(a) \cdot f(b)$ принадлежат группам $G$ и $H$ соответственно.

Характеристическое свойство гомоморфного отображения, или гомоморфизма, группы $G$ на группу $H$ заключается в том, что для любых двух элементов $a$ и $b$ группы $G$ их произведение $a \cdot b$ переходит в элемент $f(a) \cdot f(b)$ группы $H$, т. е. *образ произведения двух элементов равен произведению их образов:*

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

В рассмотренном выше примере гомоморфизма группы $N$ на группу $E$ (групповой операцией в обеих группах было сложение) выполняется равенство

$$f(n_1 + n_2) = f(n_1) + f(n_2).$$

Нужно ясно представлять себе, что, вообще говоря, каждая из групп $G$ и $H$ имеет свою собственную единицу, бинарную операцию и т. д. Поэтому

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

является сокращенной записью следующего утверждения. Пусть символ $\otimes$ обозначает бинарную операцию в группе $G$, символ $\circledast$ — бинарную операцию в группе $H$, а $f$ — гомоморфное отображение группы $G$ в группу $H$; тогда для любых элементов $a$ и $b$ группы $G$

$$f(a \otimes b) = f(a) \circledast f(b).$$

В дальнейшем мы не будем пользоваться этой сложной формой записи, за исключением случаев, когда отказ от нее затрудняет понимание, и будем, как правило, писать $f(ab) = f(a)f(b)$. В то время как при

произвольном отображении устанавливается соответствие между отдельно взятыми элементами двух множеств, при гомоморфном отображении принимаются во внимание также бинарные операции в обеих группах и устанавливается *соответствие как между отдельными элементами, так и между произведениями элементов.*

Чтобы получить еще один пример гомоморфизма, рассмотрим следующее отображение циклической группы $C_4$ (с образующей $a$) на циклическую группу $C_2$ (с образующей $b$):

$$f: \begin{pmatrix} I & a & a^2 & a^3 \\ I^* & b & I^* & b \end{pmatrix}.$$

Отметим, что единицу группы $C_2$ мы обозначили через $I^*$, чтобы отличить ее от единицы группы $C_4$. Ранее мы уже обращали внимание на то, что и бинарные операции в двух связанных гомоморфизмом группах различны. Мы надеемся, *что в дальнейшем читатель будет помнить об этих различиях, даже если это никак не отражается в обозначениях.*

Пользуясь таблицей умножения группы $C_4$, можно проверить, что $f$ переводит каждое произведение элементов группы $C_4$ в произведение образов этих элементов в группе $C_2$, так что

$$f(rs) = f(r)\,f(s),$$

где $r$, $s$ — любые два элемента группы $C_4$. В таблице умножения группы $C_4$ (табл. 9.1) указаны все произведения элементов группы и (прямо под ними) их образы в группе $C_2$. Отметим, что таблица образов всех произведений элементов группы $C_4$ представляет собой *четырежды повторенную* таблицу умножения группы $C_2$.

Гомоморфное отображение обнаруживает сходство структур групп $C_4$ и $C_2$. На самом деле именно благодаря наличию этого сходства и существует такое отображение. Если мы попытаемся построить гомоморфизм, например группы $C_3$ на группу $C_2$, то столкнемся с непреодолимыми трудностями, причина кото-

рых заключается в отсутствии необходимого для существования гомоморфизма сходства структур этих групп.

*Таблица 9.1*

| | $I$ | $a$ | $a^2$ | $a^3$ |
|---|---|---|---|---|
| $I$ | $I$<br>$f(I)=I$ | $a$<br>$f(a)=b$ | $a^2$<br>$f(a^2)=I$ | $a^3$<br>$f(a^3)=b$ |
| $a$ | $a$<br>$f(a)=b$ | $a^2$<br>$f(a^2)=I$ | $a^3$<br>$f(a^3)=b$ | $I$<br>$f(I)=I$ |
| $a^2$ | $a^2$<br>$f(a^2)=I$ | $a^3$<br>$f(a^3)=b$ | $I$<br>$f(I)=I$ | $a$<br>$f(a)=b$ |
| $a^3$ | $a^3$<br>$f(a^3)=b$ | $I$<br>$f(I)=I$ | $a$<br>$f(a)=b$ | $a^2$<br>$f(a^2)=I$ |

Упражнение 37. Докажите, что если отображение $f$ группы $G$ на группу $H$ не переводит единичный элемент группы $G$ в единичный элемент группы $H$, то оно *не* гомоморфно, или, напротив, если $f$ — гомоморфное отображение группы $G$ на группу $H$, то $f(I)=I$.

Упражнение 38. Пусть $f$ — гомоморфизм группы $G$ на группу $H$. Покажите, что если $x^{-1}$ — обратный к $x$ элемент, то

$$f(x^{-1})=[f(x)]^{-1},$$

т. е. при гомоморфизме образ обратного элемента есть элемент, обратный к образу.

Упражнение 39. Пусть группа $G$ гомоморфно отображается (с помощью гомоморфизма $f$) на группу $H$, и пусть $f(x)=f(y)$ для некоторых двух элементов $x$ и $y$ группы $G$. Покажите, что

$$f(xy^{-1})=f(x^{-1}y)=I.$$

Упражнение 40. Пусть $f$ — гомоморфизм одной группы на другую. Докажите, что

(a) если $f(x) = I$ и $f(y) = I$, то $f(xy) = I$;

(b) если $f(xy) = I$, то $f(yx) = I$.

**Изоморфизм.** Рассмотренное выше гомоморфное отображение группы $C_4$ на группу $C_2$ не является взаимно однозначным; два различных элемента $a$ и $a^3$ группы $C_4$ переходят при нем в один и тот же элемент $b$ группы $C_2$. (Отображение одной конечной группы на другую может быть взаимно однозначным лишь в том случае, когда эти группы имеют одинаковый порядок.) Взаимно однозначное гомоморфное отображение одной группы на другую называется *изоморфным отображением*, или *изоморфизмом*. Итак, изоморфизм групп — это отображение одной группы на другую, удовлетворяющее двум условиям:

1) $f(ab) = f(a)f(b)$ для всех элементов $a$ и $b$ (гомоморфизм);

2) $f(a) = f(b)$ в том и только том случае, когда $a = b$ (взаимная однозначность).

Рассмотрим два примера таких отображений. В одном из них участвуют конечные группы, а в другом — бесконечные. Читателю следует обратить внимание на следующий факт: изоморфизм одной группы на другую означает, что они имеют одинаковую алгебраическую структуру. Именно по этой причине и существует изоморфизм одной группы на другую.

Пусть элементами группы $H$ служат корни уравнения $x^4 - 1 = 0$,

$$H = \{1, i, -1, -i\}, \quad \text{где} \quad i = \sqrt{-1}.$$

Групповая операция — обычное умножение. Рассмотрим циклическую группу $C_4$ таких вращений квадрата в его плоскости, в результате которых он совмещается с собой,

$$C_4 = \{I, a, a^2, a^3\}.$$

Обозначим через $f$: $C_4 \to H$ такое отображение группы $C_4$ на $H$:

$$\begin{pmatrix} I & a & a^2 & a^3 \\ 1 & i & -1 & -i \end{pmatrix}.$$

Очевидно, что $f$ — взаимно однозначное отображение. Но будет ли оно гомоморфным? Чтобы ответить на этот вопрос, исследуем таблицу умножения группы $C_4$ (табл. 9.2) и сравним каждое произведение $r$ с его образом $f(r)$ (записанным под ним):

*Таблица 9.2*

| | $I$ | $a$ | $a^2$ | $a^3$ |
|---|---|---|---|---|
| $I$ | $I$<br>1 | $a$<br>$i$ | $a^2$<br>$-1$ | $a^3$<br>$-i$ |
| $a$ | $a$<br>$i$ | $a^2$<br>$-1$ | $a^3$<br>$-i$ | $I$<br>1 |
| $a^2$ | $a^2$<br>$-1$ | $a^3$<br>$-i$ | $I$<br>1 | $a$<br>$i$ |
| $a^3$ | $a^3$<br>$-i$ | $I$<br>1 | $a$<br>$i$ | $a^2$<br>$-1$ |

Читатель легко проверит (учитывая равенство $i^2 = -1$), что образы $f(r)$ элементов группы $C_4$ образуют таблицу умножения группы $H$. Таким образом,

$$f(rs) = f(r)\,f(s),$$

и потому отображение $f$ не только взаимно однозначно, но и гомоморфно. Значит, $f$ — изоморфизм. В таких случаях мы будем говорить, что *группы $C_4$ и $H$ изоморфны*. Две группы изоморфны, если существует изоморфизм одной группы на другую. С точки зрения этого определения изоморфизм есть как свойство двух групп, так и свойство связывающего их отображения. Именно это свойство мы и имели в виду, когда говорили, что группы имеют одинаковую структуру.

Графы двух изоморфных групп изображены на рис. 9.7. Ясно, что эти графы *совпадают* с точностью до *обозначений* при вершинах и образующих.

В качестве второго примера изоморфных групп рассмотрим множество $P$ положительных действительных чисел и множество $L$ их логарифмов. (Не важно, по какому основанию рассматриваются логарифмы, но для определенности будем считать, что они десятичные.) Прежде всего отметим, что каждое из

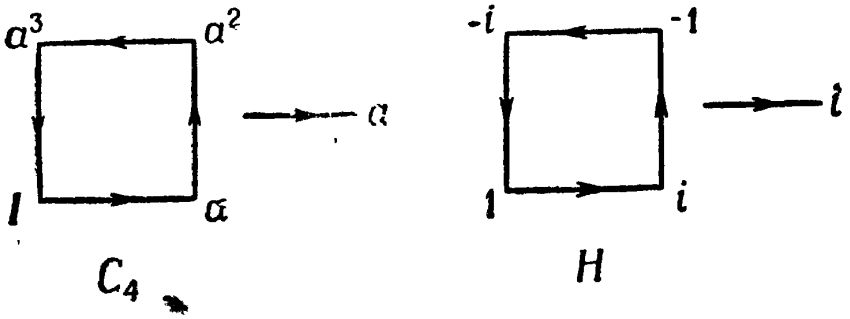



Рис. 9.7.

этих множеств является группой относительно бинарной операции, указанной в следующей таблице:

| | Группа $P$ | Группа $L$ |
|---|---|---|
| Элементы: | *Положительные числа* | *Логарифмы положительных чисел (все действительные числа)* |
| Бинарная операция: | *Обычное умножение ($x>0$ и $y>0$ влечет за собой $xy>0$)* | *Обычное сложение* [$\log x + \log y = \log (xy)$] |
| Единица: | 1 | 0 |
| Обратный: | Обратное число | Противоположное число |

Докажем, что эти группы изоморфны и что отображение $f: P \to L$, определенное формулой

$$f(x) = \log x,$$

есть изоморфизм. Каждый элемент множества $L$ при указанном отображении $f$ является образом некоторого элемента $x$ из $P$. Итак, областью определения этого отображения служит множество всех положительных чисел, а областью значений — множество всех действительных чисел (рис. 9.8). Остается проверить, что

(1) $f(xy) = f(x)f(y)$ для любых $x$ и $y$ из $P$;
(2) отображение взаимно однозначно.

Здесь нужно быть осторожным, чтобы не спутать операции в группах $P$ и $L$. Пусть $\otimes$ — бинарная операция группы $P$, а $\circledast$ — бинарная операция группы $L$.

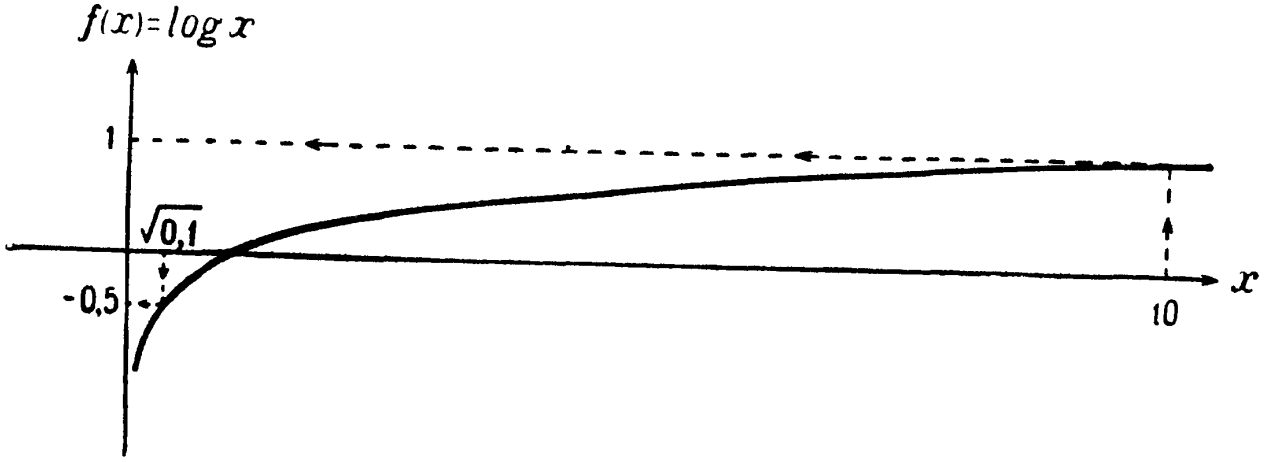



Рис. 9.8.

Тогда для любых двух элементов $x$, $y$ группы $P$

$x \otimes y = xy$ (*умножение* положительных действительных чисел);

а для их образов $f(x)$, $f(y)$ в группе $L$

$f(x) \circledast f(y) = \log x + \log y$ (*сложение* действительных чисел).

Таким образом, для выполнения условия (1) (определяющего свойства гомоморфизма) нужно, чтобы для любых элементов $x$ и $y$ группы $P$ имело место соотношение

$$f(x \otimes y) = f(x) \circledast f(y), \quad \text{или} \quad \log(xy) = \log x + \log y.$$

Но последнее равенство выражает известное свойство логарифмов. Поэтому рассматриваемое отображение есть *гомоморфизм* группы всех положительных чисел на группу всех действительных чисел.

Чтобы убедиться в его *взаимной однозначности*, посмотрим на график функции $f(x) = \log x$. Достаточно проверить, что любые два различных элемента переходят в два различных элемента. Предположим, что $f(x) = f(y)$, т. е. что $\log x = \log y$. Тогда

$$\log x - \log y = 0, \quad \text{или} \quad \log \frac{x}{y} = 0.$$

Отсюда следует, что $\frac{x}{y} = 1$ и, значит, $x = y$. Таким образом, отображение $f$ взаимно однозначно и, следовательно, является изоморфизмом.

**Абстрактные группы.** Будем называть две изоморфные группы *абстрактно равными* и считать абстрактно равные группы одной и той же *абстрактной группой.* Именно благодаря этому приобретают полную определенность, например, такие термины, как «группа диэдра порядка 6» или «циклическая группа порядка 6». Утверждение, что две изоморфные группы абстрактно равны, не означает, что такие группы совершенно одинаковы; из него лишь следует, что они обладают одинаковыми групповыми структурными свойствами. Из упражнения 41 будет видно, что группа может быть изоморфна своей *собственной* подгруппе. Группа и одна из ее собственных подгрупп — это, конечно, *не одно и то же*, однако их групповая структура может быть одинаковой.

Можно показать, что существует лишь конечное число «абстрактно различных» групп порядка $n$. С точностью до обозначения элементов для множества, состоящего из $n$ различных символов, существует лишь конечное число таблиц умножения, имеющих $n$ клеток. Отметим, что группа диэдра порядка 6 и циклическая группа порядка 6 *не* изоморфны (и, следовательно, абстрактно различны), так как вторая из этих групп коммутативна, а первая — нет. Можно показать, что других абстрактных групп порядка 6 не существует. Аналогично, если $p$ — простое число, то существует только одна абстрактная группа порядка $p$, и это, конечно, циклическая группа $C_p$.

На основании этих примеров не следует делать вывода, что легко перечислить все абстрактно различные группы данного порядка. Известно, что существует 267 абстрактных групп порядка 64, но пока еще никто не подсчитал число абстрактных групп порядка 256.

Отождествление изоморфных групп и образование понятия абстрактной группы аналогично образованию понятия числа путем абстрагирования от его конкрет-

ных интерпретаций. Число *пять* — это некая абстракция, которая возникает из рассмотрения конкретных множеств, состоящих из пяти элементов; например, пять пальцев, пять рублей, пять морей, пять гласных букв. Точно так же можно рассматривать конкретные представления абстрактной группы: существует лишь *одна* абстрактная циклическая группа четвертого порядка, но есть много ее конкретных интерпретаций.

Понятие изоморфных, или абстрактно равных, групп является очень важным: иногда мы можем существенно упростить доказательство теоремы, используя вместо некоторой группы ей изоморфную. Так как *изоморфные группы имеют одну и ту же групповую структуру*, теорема распространяется на все группы, изоморфные той, которая была использована в доказательстве.

Упражнение 41. Может ли группа быть изоморфна собственной подгруппе? Пусть $G$ — аддитивная группа целых чисел (стр. 25). Пусть $H$ — ее (собственная) подгруппа, состоящая из всех четных чисел. Покажите, что группу $G$ можно изоморфно отобразить на группу $H$, т. е. существует отображение $f$ группы $G$ на группу $H$, такое, что

$$f(x+y)=f(x)+f(y)$$

и

$f(x)=f(y)$ тогда и только тогда, когда $x=y$.

Упражнение 42. Распространите результат упражнения 41 на абстрактную группу $C_\infty$ (стр. 66). Пусть $G$ — бесконечная циклическая группа, порожденная элементом $r$, и $H$ — ее (собственная) подгруппа, порожденная элементом $r^n$, $n>1$. Покажите, что группу $G$ можно изоморфно отобразить на группу $H$.

Упражнение 43. Пусть $G$ — бесконечная группа, порожденная элементом $r$, и пусть $H$ — циклическая группа второго порядка с элементами $I$, $b$, где $b^2=I$. Покажите, что существует гомоморфизм группы $G$ на группу $H$, а изоморфизма не существует.

Упражнение 44. Пусть $G$ — группа и $r$ — некоторый ее фиксированный элемент. Если $x$ — любой элемент группы $G$, то и $r^{-1}xr$ — элемент этой группы. Определим отображение $f$: $G \to G$ формулой

$$f\colon\ x \to r^{-1}xr, \quad \text{или} \quad f(x) = r^{-1}xr.$$

Докажите, что $f$ — изоморфизм группы на себя.

Упражнение 45. Пусть $G$ — группа и $f$ — отображение, ставящее в соответствие каждому элементу группы его квадрат. Таким образом, $f$: $x \to x^2$, или $f(x) = x^2$. Будет ли это отображение изоморфизмом? Может ли $f$ быть гомоморфизмом, и если да, то для каких групп?

ГЛАВА 10

# ГРУППЫ ПОДСТАНОВОК

Многие работы по теории групп посвящены исследованию класса групп, называемых группами *подстановок* (или группами *перестановок*). Группы подстановок особенно интересны тем, что с их помощью можно получить конкретные представления всех конечных групп. В этой главе мы увидим, что *любая конечная группа изоморфна некоторой группе подстановок.*

Мы приводили много примеров отображений, записанных в виде двух строк, заключенных в скобки, где элементы из области определения стояли в верхней строке, а элементы из области значений — в нижней. Было показано также, что множество взаимно однозначных отображений множества из $n$ элементов на себя составляет *группу отображений.* Такие отображения называют *подстановками*, а группы, элементами которых являются подстановки, — *группами подстановок.*

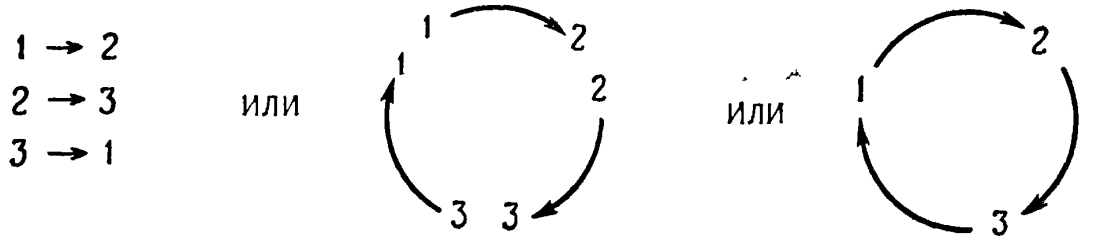
Пусть множество состоит из трех элементов, расположенных в произвольном, но фиксированном порядке: $a_1$, $a_2$, $a_3$. В таких случаях часто бывает удобно обращать внимание лишь на нижние индексы и считать, что мы имеем дело с последовательностью 1, 2, 3; таким образом, например, третий элемент $a_3$ обозначается просто как 3.

Пусть теперь $M$ — некоторое взаимно однозначное отображение этого множества на себя:

$$M: \begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix}, \quad \text{или} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \text{или} \quad \begin{array}{l} 1 \to 2, \\ 2 \to 3, \\ 3 \to 1. \end{array}$$

Будем рассматривать это отображение $M$ как *подстановку* элементов упорядоченного множества (вместо 1 «подставляется» 2, вместо 2 — 3, вместо 3 — 1) или как *перестановку* последовательности 1, 2, 3, в результате которой получается последовательность 2, 3, 1. Именно по этой причине мы называем группу отображений конечного множества в себя *группой подстановок* (или группой перестановок).

*Разложение подстановок в произведение циклов.* Отображение, или подстановка $M$, устанавливает соответствия




Эта *циклическая* конфигурация наводит на мысль записать $M$ в виде одной строки, заключенной в скобки:

$$M = (1\ 2\ 3),$$

и такая запись будет означать, что $M$ отображает каждый символ в ближайший к нему справа, а последний — в первый. Подстановку $M$ можно записать в виде цикла тремя способами:

$$(1\ 2\ 3),\quad (2\ 3\ 1),\quad (3\ 1\ 2),$$

так как несущественно, какой элемент указанного цикла мы поставим первым.

Пусть задано следующее отображение $N$ множества из четырех элементов $a_1$, $a_2$, $a_3$, $a_4$:

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

Можно ли представить это отображение в виде цикла? Так как 4 отображается в 4, то $N$ можно представить как

$$(1\ 2\ 3),$$

если условиться, что любой элемент, не появляющийся в цикле, переходит в себя. Аналогично,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2\ 4),$$

так как отображение, записанное в левой части, полностью описывается двучленным циклом (2 4), если эту запись понимать так: $2 \to 4$, $4 \to 2$, $1 \to 1$ и $3 \to 3$.

Можно ли записать с помощью циклов произвольное отображение конечного множества в себя? Например, как записать отображение

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

в котором в противоположность предыдущему отображению $N$ множество соответствий не «выстраивается» в один цикл? Начнем с символа 1 и запишем справа от него его образ 2:

$$(1\ \ 2\ \ .$$

Чтобы продолжить цикл далее, надо посмотреть, во что переходит символ 2. Его образом будет 4, и мы пишем

$$(1\ 2\ 4\ .$$

Если мы попытаемся продолжить цикл дальше, то увидим, что отображение $A$ переводит 4 в 1, и окончательно имеем

$$(1\ 2\ 4).$$

Но этот цикл *не* есть запись отображения $A$, так как соответствующее ему отображение не переводит 3 в 5, а 5 в 3. Эти переходы осуществляются циклом (3 5), который каждый из остальных символов переводит в себя. Итак, ясно, что если выполняется сначала отображение

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

а затем отображение

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

то произведение этих отображений (их суперпозиция) есть отображение $A$, т. е.

$$(1\ 2\ 4)\cdot(3\ 5)=\begin{pmatrix}1&2&3&4&5\\2&4&3&1&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5\\1&2&5&4&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}.$$

Отметим, что поскольку эти два цикла не содержат общих символов и не оказывают друг на друга влияния, то безразлично, в каком порядке мы производим соответствующие отображения; следовательно,

$$(1\ 2\ 4)(3\ 5)=(3\ 5)(1\ 2\ 4).$$

Чтобы получить представление отображения $A$ с помощью циклов, мы воспользовались способом, который можно применить к отображению любого конечного множества на себя. Отсюда следует, что *каждую подстановку конечного множества можно записать как произведение циклов, не содержащих общих символов.*

Рассмотрим теперь отображения

$$(1\ 2)(2\ 3)\quad\text{и}\quad(2\ 3)(1\ 2)$$

и выясним, будут ли перестановочны циклы (1 2) и (2 3) с общим символом 2. Произведение (1 2) и (2 3) дает:

$1\to 2$, затем $2\to 3$ и окончательно $1\to 3$,

$3\to 3$, затем $3\to 2$ и окончательно $3\to 2$,

$2\to 1$, затем $1\to 1$ и окончательно $2\to 1$.

Таким образом,

$$(1\ 2)(2\ 3)=(1\ 3\ 2).$$

С другой стороны, (2 3) (1 2) дает:

$1\to 1$, затем $1\to 2$ и окончательно $1\to 2$,

$2\to 3$, затем $3\to 3$ и окончательно $2\to 3$,

$3\to 2$, затем $2\to 1$ и окончательно $3\to 1$.

Таким образом,

$$(2\ 3)(1\ 2) = (1\ 2\ 3),$$

т. е. циклы (1 2) и (2 3) *не* коммутируют. Циклы, не содержащие общих символов, перестановочны между собой, а содержащие общие символы могут и не быть перестановочны.

*Конечная группа изоморфна группе подстановок.* Мы уже подготовили фундамент для одной из основных теорем о представлении конечных групп. В гл. 9 указывалось, что каждую конкретную группу можно рассматривать как одно из многих возможных представлений некоторой абстрактной группы, которая изоморфна каждому из этих представлений. В сформулированной ниже теореме утверждается, что для каждой конечной абстрактной группы существует ее конкретное представление в виде некоторой группы подстановок. Напомним, что подстановка на $n$ символах — это взаимно однозначное отображение множества из $n$ элементов на себя [1]).

Теорема 5. *Пусть задана конечная группа порядка $n$. Тогда существует группа подстановок на $n$ элементах, изоморфная данной группе.*

Доказательство этой теоремы можно найти в любой книге, посвященной теории конечных групп. Поэтому нам кажется, что читателю будет полезнее проследить ход доказательства в применении к какой-либо конкретной группе (используемый здесь способ рассуждения может быть обобщен до формального доказательства теоремы).

Найдем представление в виде группы подстановок для циклической группы $C_4$ четвертого порядка. Составим прежде всего таблицу умножения этой группы, причем элементы $I$, $a$, $a^2$, $a^3$ будем обозначать также символами $g_1$, $g_2$, $g_3$, $g_4$ соответственно.

---

[1]) Подстановку на $n$ символах называют подстановкой *степени $n$*, а группу всех таких подстановок — группой *степени $n$*. — *Прим. ред.*

*Таблица 10.1*

| | $I$ | $a$ | $a^2$ | $a^3$ |
|---|---|---|---|---|
| | $g_1$ | $g_2$ | $g_3$ | $g_4$ |
| $I$ | $I$ | $a$ | $a^2$ | $a^3$ |
| $g_1$ | $g_1$ | $g_2$ | $g_3$ | $g_4$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $I$ |
| $g_2$ | $g_2$ | $g_3$ | $g_4$ | $g_1$ |
| $a^2$ | $a^2$ | $a^3$ | $I$ | $a$ |
| $g_3$ | $g_3$ | $g_4$ | $g_1$ | $g_2$ |
| $a^3$ | $a^3$ | $I$ | $a$ | $a^2$ |
| $g_4$ | $g_4$ | $g_1$ | $g_2$ | $g_3$ |

$$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}=m_1$$

$$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=m_2$$

$$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}=m_3$$

$$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}=m_4$$

Каждая строка табл. 10.1 — это перестановка верхней строки (см. теорему 1 на стр. 53); например, последовательность $g_2$, $g_3$, $g_4$, $g_1$ (или просто 2, 3, 4, 1) во второй строке есть перестановка последовательности 1, 2, 3, 4 из первой строки. Четыре подстановки (или взаимно однозначных отображения), соответствующие перестановкам в строках, записаны справа от таблицы. Их можно представить с помощью циклов:

$$m_1=(1)(2)(3)(4)=I, \quad m_3=(1\ 3)(2\ 4),$$
$$m_2=(1\ 2\ 3\ 4), \qquad m_4=(1\ 4\ 3\ 2).$$

(Чтобы записать $m_1=I$ в виде циклов, нам пришлось ввести циклы, содержащие один символ.)

Упражнение 46. Проверьте непосредственно, что

(a) $m_2^2=m_3$, (b) $m_3^2=I$, (c) $m_2^3=m_4$, (d) $m_2m_4=I$

и что отображения $m_1$, $m_2$, $m_3$, $m_4$ образуют группу $M$.

Чтобы убедиться в том, что группа $M$, состоящая из подстановок $m_1$, $m_2$, $m_3$, $m_4$, изоморфна группе $C_4$,

рассмотрим такие движения квадрата, вершины которого перенумерованы цифрами 1, 2, 3, 4, в результате которых вершины перемещаются в соответствии с подстановками $m_1$, $m_2$, $m_3$, $m_4$ (рис. 10.1). Ясно, что $m_1$ — единица группы подстановок $M$. Сопоставим ей единичный элемент $I$ группы $C_4$. Подстановка $m_2$ эквивалентна повороту против часовой стрелки на 90° [1]). Сопоставим ей образующую $a$ группы $C_4$.

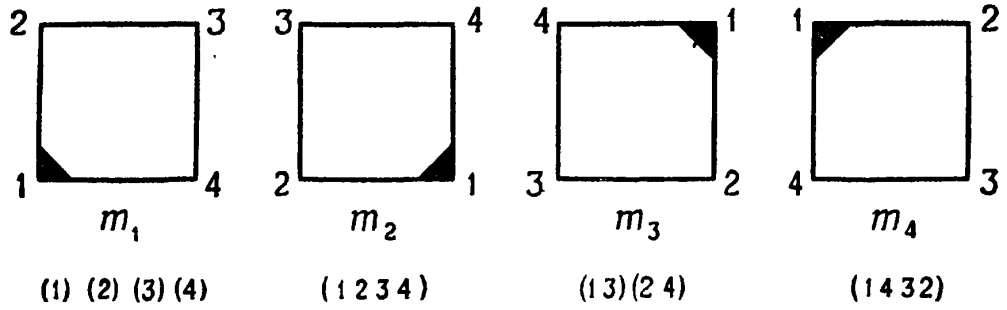



Рис. 10.1.

Упражнение 47. Отобразите оставшиеся элементы $m_3$ и $m_4$ группы $M$ на элементы группы $C_4$ таким образом, чтобы группа $M$ отображалась на группу $C_4$ изоморфно.

Возникает естественный вопрос: *почему* отображения, выписанные в табл. 10.1, образуют группу, изоморфную исходной? Вот вкратце основные соображения по этому поводу. Четыре отображения $m_j$ ($j = 1, 2, 3, 4$) можно описать так:

$$m_j = \begin{pmatrix} g_1 & g_2 & g_3 & g_4 \\ g_j g_1 & g_j g_2 & g_j g_3 & g_j g_4 \end{pmatrix},$$

т. е. $m_j$ — это отображение

$$g_i \to g_j g_i \qquad (i = 1, 2, 3, 4).$$

[1]) Чтобы убедиться, что подстановка $m_2 = (1\,2\,3\,4)$ соответствует повороту на 90° *против* часовой стрелки, вспомним наше первоначальное обсуждение группы самосовмещений (стр. 26—34). Можно считать, что повернутая фигура наложена на фигуру, находящуюся в исходном положении (рис. 3.2); запись $a \to b$ означает, что вершина $a$ в результате движения замещается вершиной $b$ (стр. 28). Таким образом, $m_2 = (1\,2\,3\,4)$ означает, что $1 \to 2$ (вершина 1 замещается вершиной 2), $2 \to 3$ (вершина 2 замещается вершиной 3) и т. д. В результате квадрат оказывается повернутым на 90° против часовой стрелки.

Отображение $m_j m_k$ есть последовательное выполнение отображений $m_j$ и $m_k$, т. е. при $m_j m_k$

$$g_i \to g_j g_i, \quad \text{а затем} \quad g_i \to g_k g_i.$$

Таким образом, при отображении $m_j m_k$

$$g_i \to g_j (g_k g_i) = (g_j g_k)\, g_i.$$

Следовательно, существует взаимно однозначное соответствие между произведениями $m_j m_k$ в группе подстановок и произведениями $g_j g_k$ в группе $C_4$. (Ср. с теоремой 1 на стр. 53.)

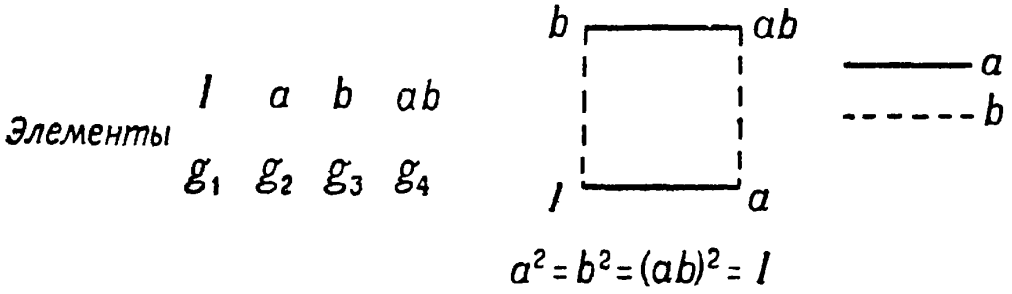



Рис. 10.2

Теперь найдем представление *четверной группы* $D_2$ в виде группы подстановок (рис. 10.2 и табл. 10.2).

*Таблица 10.2*

| | $I$ | $a$ | $b$ | $ab$ | |
|---|---|---|---|---|---|
| | $g_1$ | $g_2$ | $g_3$ | $g_4$ | |
| $I$ | $I$ | $a$ | $b$ | $ab$ | $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = m_1$ |
| $g_1$ | $g_1$ | $g_2$ | $g_3$ | $g_4$ | |
| $a$ | $a$ | $I$ | $ab$ | $b$ | $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = m_2$ |
| $g_2$ | $g_2$ | $g_1$ | $g_4$ | $g_3$ | |
| $b$ | $b$ | $ab$ | $I$ | $a$ | $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} = m_3$ |
| $g_3$ | $g_3$ | $g_4$ | $g_1$ | $g_2$ | |
| $ab$ | $ab$ | $b$ | $a$ | $I$ | $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix} = m_4$ |
| $g_4$ | $g_4$ | $g_3$ | $g_2$ | $g_1$ | |

Элементы группы подстановок $M$ записаны в виде двух строк, заключенных в скобки. Их можно следующим образом выразить как произведения циклов:

$$m_1 = (1)(2)(3)(4) = I, \quad m_2 = (1\ 2)(3\ 4).$$
$$m_3 = (1\ 3)(2\ 4), \quad m_4 = (1\ 4)(2\ 3).$$

Упражнение 48. (a) Проверьте, что в группе $M$ выполняются равенства $m_2^2 = m_3^2 = (m_2 m_3)^2 = I$.

(b) Запишите с помощью двух строк, заключенных в скобки, изоморфизм группы подстановок $M$ на четверную группу с элементами $I$, $a$, $b$, $ab$ и определяющими соотношениями $a^2 = b^2 = (ab)^2 = I$.

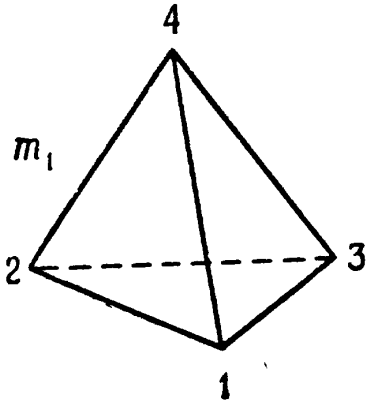
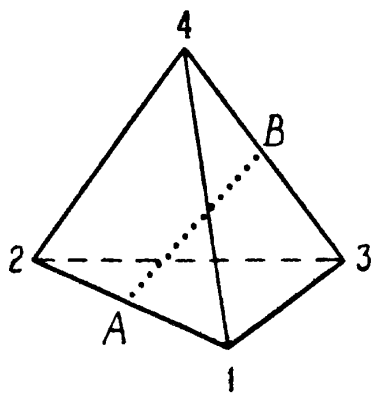
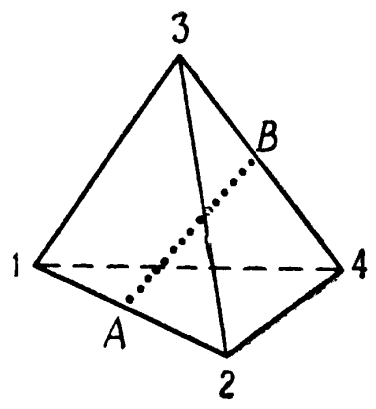



Рис. 10.3.




$m_1 = I$




$m_2 = (1\,2)(3\,4)$

Рис. 10.4.

Как и в предыдущем примере группы $C_4$, представление четверной группы с помощью подстановок подсказывает конкретную интерпретацию, основанную на перемещениях четырех объектов. На этот раз объекты будут помещены в четыре вершины правильного тетраэдра (рис. 10.3). Тождественная подстановка $m_1$ оставляет все вершины в первоначальном положении. Чтобы представить подстановку $m_2 = (1\ 2)(3\ 4)$, нужно поменять местами объекты в вершинах 1 и 2, 3 и 4 (рис. 10.4). Правильный тетраэдр можно перевести из начального положения в положение, соответствующее результату подстановки $m_2$, вращением на 180° вокруг оси $AB$, изображенной на рис. 10.4 Ось $AB$ проходит через середины двух «противоположных» ребер 1—2 и 3—4. Мы будем называть ее *медианой* тетраэдра.

Аналогично, отображения $m_3$ и $m_4$ можно интерпретировать как вращение на 180° вокруг медиан $CD$ и $EF$ соответственно (рис. 10.5).

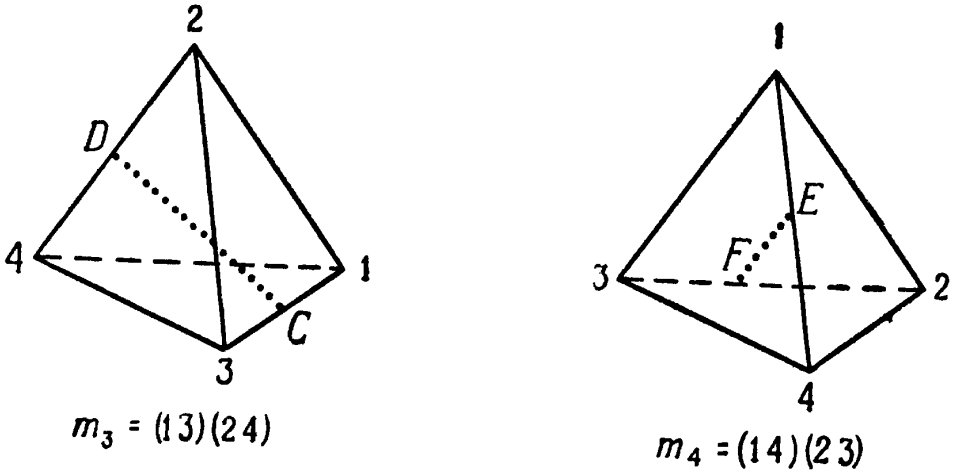



Рис. 10.5.

Таким образом, одним из представлений четверной группы является некоторое множество движений правильного тетраэдра, в результате которых он совмещается со своим первоначальным положением, а именно вращений на 180° вокруг медиан. Можно показать, что три эти медианы пересекаются в одной точке и попарно перпендикулярны. Поэтому можно считать, что четверная группа состоит из вращений взаимно перпендикулярных осей, в результате которых оси совмещаются со своим исходным положением.

В следующем разделе мы рассмотрим совокупность всех самосовмещений правильного тетраэдра — *группу тетраэдра* — и увидим, что *группа тетраэдра содержит четверную группу в качестве своей подгруппы.*

Упражнение 49. (a) Постройте группу подстановок на шести объектах, изоморфную группе диэдра $D_3$ порядка 6.

(b) Запишите каждый из элементов этой группы подстановок с помощью циклов.

Упражнение 50. Пусть задано шесть элементов: $I$, $a = (1\ 2\ 3)$, $b = (1\ 3\ 2)$, $c = (1\ 2)$, $d = (1\ 3)$, $e = (2\ 3)$. Покажите, что они образуют группу диэдра $D_3$ порядка 6. [*Замечание*: здесь элементы группы представлены с помощью подстановок на *трех* сим-

волах, в то время как в предыдущем упражнении для этой цели использовались подстановки на *шести* символах.]

**Группа тетраэдра.** Значительный интерес представляют группы, связанные с самосовмещениями пяти правильных многогранников: тетраэдра, куба (гексаэдра), октаэдра, додекаэдра и икосаэдра. Мы не можем подробно останавливаться на каждой из этих групп и ограничимся рассмотрением лишь группы тетраэдра.

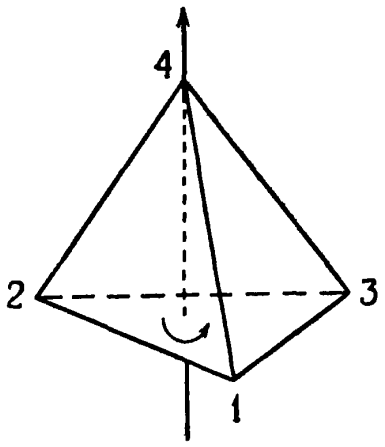


Рис. 10.6.

Следует помнить, что в качестве групповой бинарной операции здесь, как и во всех группах движений, рассматривается суперпозиция, или «последовательное выполнение». (Советуем читателю для наглядности использовать какую-нибудь модель тетраэдра.)

Прежде всего подсчитаем, сколько различных элементов содержит группа самосовмещений правильного тетраэдра, а затем выделим некоторые основные движения, которые порождают всю группу. Для этого мы обобщим метод, который ранее использовался нами для изучения группы самосовмещений равностороннего треугольника (группы диэдра $D_3$; см. стр. 42).

Выберем за ось вращения перпендикуляр, опущенный из вершины 4 на плоскость треугольника с вершинами 1, 2 и 3, и зададим на ней направление, как показано на рис. 10.6. Мы рассматриваем стрелку на оси как конец правостороннего винта и обозначаем через $r$ вращение на 120° в направлении ввинчивания винта. При вращении вокруг этой оси верхняя вершина 4 остается на месте и можно получить три различных положения тетраэдра, отмеченные на рис. 10.7 буквами $I$, $r$, $r^2$. Заметим, что изображенные на рис. 10.7 вращения исчерпывают все движения тетраэдра, при которых он совмещается сам с собой, а вершина 4 остается на месте. Аналогичная ситуация возникает и при рассмотрении других вершин, и

потому мы имеем всего $4 \cdot 2 = 8$ нетождественных самосовмещений тетраэдра, при которых какая-либо одна вершина остается неподвижной. Легко видеть также, что единственными самосовмещениями тетра-

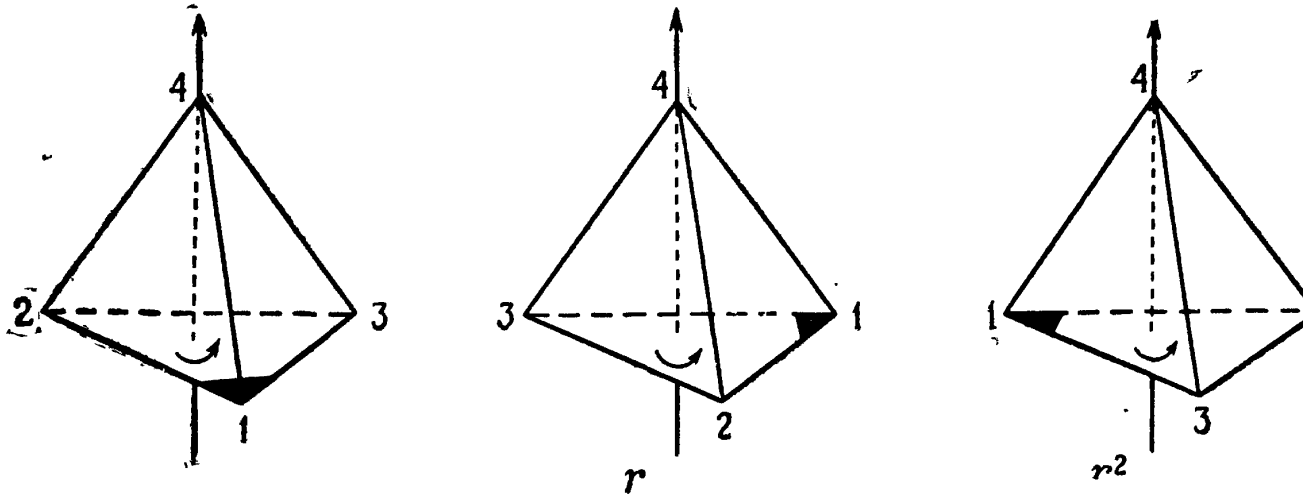



Рис. 10.7.

эдра, при которых ни одна из вершин не остается на месте, являются вращения на 180° вокруг трех его медиан. Таким образом, существует всего двенадцать самосовмещений правильного тетраэдра. *Группа тетраэдра имеет порядок* 12.

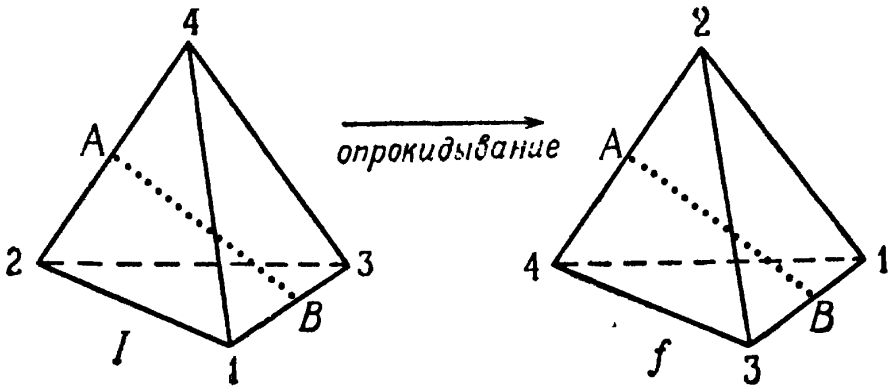



Рис. 10.8.

Обозначим опрокидывание (вращение на 180°) относительно медианы $AB$ через $f$. В результате этого движения тетраэдр переходит в новое положение, изображенное на рис. 10.8. (Заметим, что $f$ переставляет вершины каждой из пар 2, 4 и 1, 3.) На рис. 10.9 (соответственно на рис. 10.10) изображено положение, в которое переходит тетраэдр в результате последовательного выполнения движений $r$ и $f$ (соответственно $f$ и $r$).

Читателю следует проверить, что все двенадцать самосовмещений тетраэдра являются комбинациями движений $r$ и $f$, т. е. *$r$ и $f$ порождают группу тетраэдра*. Отметим, в частности, что опрокидывание относительно каждой из трех медиан можно представить

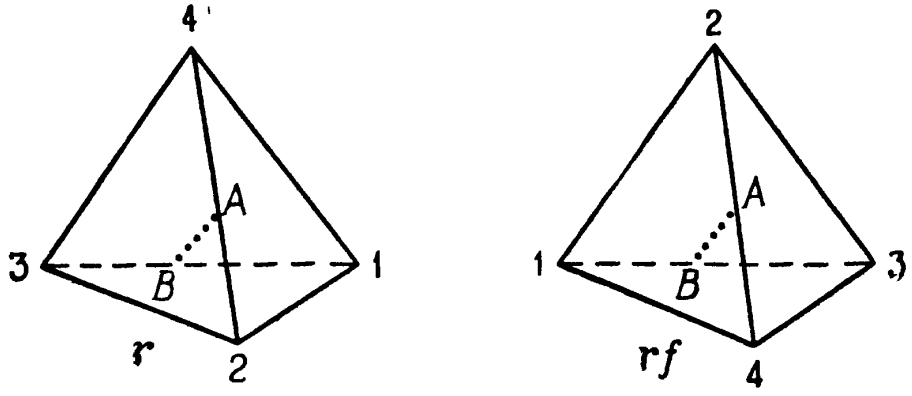



Рис. 10.9.

в виде слова от $r$ и $f$. Но эти движения, как мы уже видели, дают конкретное представление четверной группы (стр. 153). Следовательно, четверная группа является подгруппой группы тетраэдра.

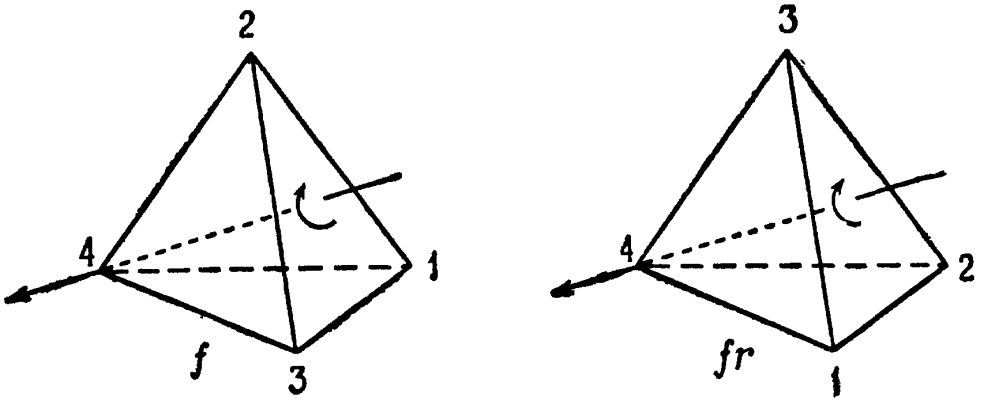



Рис. 10.10.

Образующие элементы $r$ и $f$ можно представлять себе как отображения множества, состоящего из четырех вершин, на себя:

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1\ 2\ 3) = (1\ 2)(1\ 3),$$

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\ 3)(2\ 4).$$

Отметим, что как $r$, так и $f$ являются *произведениями двух циклов, содержащих по два символа каждый.*

Мы не в состоянии еще полностью оценить значение этого факта, которое прояснится в дальнейшем (стр. 193) при обсуждении *симметрической* и *знакопеременной групп*. Пока отметим только, что группу тетраэдра часто обозначают через $A_4$, чтобы указать на совпадение ее со знакопеременной [1]) группой от четырех символов.

*Граф группы тетраэдра* $A_4$. Построение графа группы $A_4$ будет проводиться аналогично построению графа группы диэдра (стр. 76).

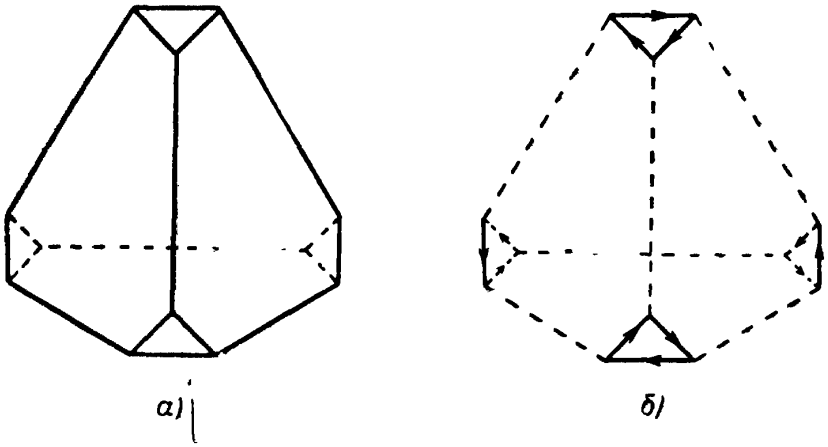



Рис. 10.11.

Рассмотрим усеченный тетраэдр, изображенный на рис. 10.11, *а*). Треугольник при каждой вершине соответствует вращению порядка 3. На рис. 10.11, *б*) мы снабдили стороны треугольников стрелками, чтобы напомнить о вращении вокруг фиксированной вершины тетраэдра. Когда мы увидим, как из этого представления самосовмещений получается граф, станет ясно, почему мы выбрали именно такие направления, которые показаны на рисунке. Отрезок, соединяющий два треугольника, можно рассматривать как представление опрокидывания относительно медианы (порядок этого движения равен 2). Напоминаем, что образующие порядка 2 изображались на графе группы как один отрезок без стрелки; поэтому мы не ставим стрелок и на соответствующих ребрах тетраэдра, изображенного на рис. 10.11, *б*).

[1]) По-английски знакопеременная группа — «alternative group», откуда и возникло обозначение $A$. — *Прим. перев.*

Заметим, что грани усеченного тетраэдра — это треугольники и шестиугольники. Чтобы перейти к двумерному представлению, сплющим наш тетраэдр так, чтобы в середине оказался треугольник или шестиугольник (рис. 10.12). В этих плоских представлениях каждый направленный отрезок, соответствующий вращению $r$ на 120°, изображается непрерывной линией, а каждый отрезок, соответствующий опрокидыванию $f$ порядка 2, — пунктирной линией. Две сети, изображенные на рис. 10.12, топологически эквивалентны.

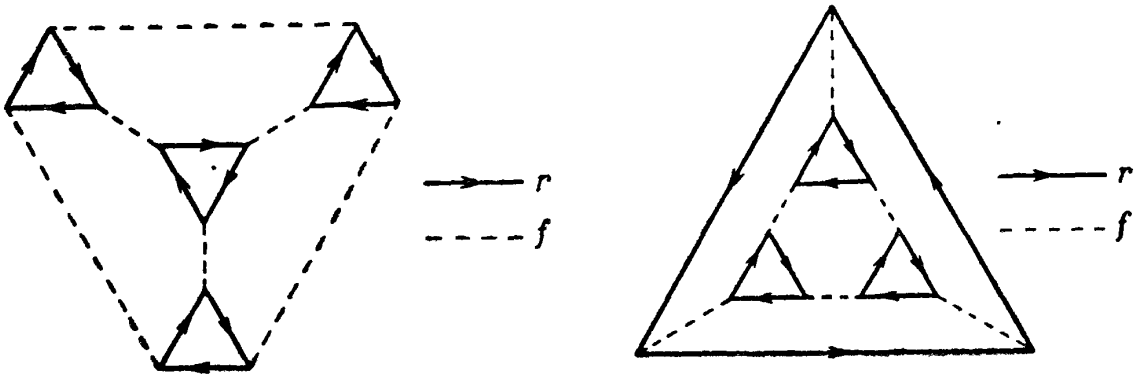



Рис. 10.12.

Мы утверждаем, что эти сети являются графами группы тетраэдра $A_4$. Очень важно, чтобы читатель отдавал себе отчет в том, что построение модели, представляющей самосовмещения, не обязательно приводит к графу группы. В каждом конкретном случае следует проверять, что полученная сеть удовлетворяет всем требованиям, которым, как мы установили раньше, должен удовлетворять граф группы.

*Определяющие соотношения для группы тетраэдра* $A_4$. В гл. 7 мы подробно рассмотрели группу диэдра $D_3$. Аналогичные соображения показывают, что *группа* $A_4$ *полностью определяется следующими данными:*

(1) $A_4$ *порождается двумя образующими, обозначаемыми через* $r$ *и* $f$;

(2) *эти образующие удовлетворяют определяющим соотношениям*

$$r^3 = I, \quad f^2 = I, \quad rfrfrf = I \quad [\text{или } (rf)^3 = I].$$

Упражнение 51. Пользуясь графом группы $A_4$, убедитесь, что $rfr^2 \cdot r^2fr = f$. Докажите то же самое, используя соотношения $r^3 = f^2 = (rf)^3 = I$.

На этом мы заканчиваем рассмотрение самосовмещений правильного тетраэдра. Краткие замечания по поводу групп, связанных с кубом и октаэдром, приведены на стр. 188, в приложении будут рассмотрены некоторые существенные особенности группы икосаэдра (и группы додекаэдра).

ГЛАВА 11

# НОРМАЛЬНЫЕ ПОДГРУППЫ

Мы займемся теперь гомоморфными отображениями группы, обращая особое внимание на то, как действует отображение на *подгруппах* группы.

В развитии и применении теории групп особую роль играли некоторые подгруппы специального вида. В 1830 г. Галуа [1]), занимаясь исследованием корней алгебраических уравнений, выявил значение этих особых подгрупп, так называемых *нормальных* [2]) (или *самосопряженных*, или *инвариантных*) подгрупп. Он показал, что каждому алгебраическому уравнению соответствует группа конечного порядка, а природа корней уравнения зависит от того, каковы *нормальные подгруппы* этой группы, т. е. в основе изучения свойств решений соответствующего алгебраического уравнения лежит рассмотрение нормальных подгрупп.

Исследуем нормальные подгруппы с двух точек зрения: (1) с точки зрения гомоморфных отображений, (2) с точки зрения разбиения группы на смежные классы по нормальной подгруппе. Как мы увидим, оба эти подхода соответствуют различным аспектам одного и того же основного структурного

---

[1]) Эварист Галуа (1811—1832) был одним из первых, кто предложил такой подход к математике, при котором центр тяжести переносится на общие теоремы об абстрактных структурах. Благодаря такому подходу он установил условия разрешимости в радикалах произвольных алгебраических уравнений. При этом им было введено понятие *поля* и найдено соответствие между полями и группами, сохранившее значение до настоящего времени (оно известно теперь под названием «теория Галуа»). Галуа был убит на дуэли в возрасте 21 года.

[2]) Нормальные подгруппы часто называют «нормальными делителями». — *Прим. перев.*

свойства. Первый подход опирается на выявление ряда соотношений между элементами группы путем «вычислений», опирающихся на групповые аксиомы. Мы уже проводили подобные вычисления, когда, например, решали групповые уравнения и получали определяющие соотношения группы.

**Нормальные подгруппы и гомоморфные отображения.** Начнем исследование нормальных подгрупп с рассмотрения некоторых групповых гомоморфизмов.

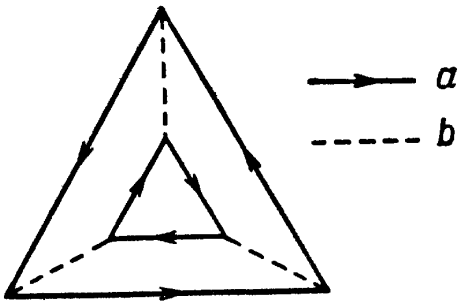



Рис. 11.1.
Группа диэдра $D_3$ с элементами $I$, $a$, $a^2$, $b$, $ba$, $ba^2$ и определяющими соотношениями $a^3 = b^2 = (ba)^2 = I$.

Мы потребуем, чтобы эти гомоморфизмы отображали некоторые специальные подгруппы в единицу группы-образа, и посмотрим, к каким результатам приведут эти условия.

Конкретно, рассмотрим группу диэдра $D_3$ порядка 6 (рис. 11.1). Эта группа имеет подгруппу $H = \{I, b\}$. Предположим, что $f$ — гомоморфное отображение группы $D_3$ на группу $G$, такое, что *все элементы подгруппы H переходят в I группы G*, т. е.

$$f(I) = I \quad \text{и} \quad f(b) = I.$$

Посмотрим, во что при гомоморфизме $f$ переходят элементы, *не* принадлежащие подгруппе $H$. Мы утверждаем, что

$$f(a) = I.$$

Действительно,

$$a = Ia = (ba)^2 a = babaa, \quad \text{или} \quad a = (ba)(ba^2).$$

Так как $f$ — гомоморфизм, то для любых элементов $r$ и $s$ этой группы

$$f(rs) = f(r) f(s);$$

следовательно,

$$f(a) = f(ba \cdot ba^2) = f(ba)\,f(ba^2) =$$
$$= f(b)\,f(a)\,f(b)\,f(a^2) = f(a)\,f(a^2) \text{ [так как } f(b) = I] =$$
$$= f(a^3) = f(I) = I,$$

как и утверждалось. Поэтому

$$f(a^2) = f(a)\,f(a) = I,$$
$$f(ba) = f(b)\,f(a) = f(a) = I,$$
$$f(ba^2) = f(b)\,f(a^2) = f(a^2) = I,$$

так что каждый элемент группы $D_3$ отображается в $I$. Это доказывает, что *любой гомоморфизм группы* $D_3$, *который переводит подгруппу* $H$ *в* $I$, *отображает в* $I$ *всю группу* $D_3$.

Рассмотрим теперь гомоморфизм группы $D_3$ в группу $G$, который переводит в $I$ некоторую другую подгруппу, скажем подгруппу $K = \{I, a, a^2\}$. Из соотношений

$$f(I) = f(a) = f(a^2) = I$$

следует, что

$$f(ba) = f(b)\,f(a) = f(b),$$
$$f(ba^2) = f(b)\,f(a^2) = f(b),$$

и этот гомоморфизм можно представить в виде

$$\begin{pmatrix} I & a & a^2 & b & ba & ba^2 \\ I & I & I & c & c & c \end{pmatrix},$$

где $c = f(b)$. Так как

$$c^2 = f(b)\,f(b) = f(b^2) = f(I) = I,$$

то множество, состоящее из элементов $I$ и $c$, является *циклической группой второго порядка* [1]). Таким образом, *гомоморфное отображение группы* $D_3$, *которое*

[1]) Мы неявно предполагаем, что $c = f(b) \neq I$. Конечно, существует (тривиальное) отображение $f$, такое, что $f(b) = I$, но равенство $f(b) = I$ не является *непременным* следствием равенства $f(a) = I$.

*переводит подгруппу $K$ в $I$, не обязательно отображает в $I$ всю группу $D_3$; оно может отображать группу $D_3$ на циклическую группу второго порядка.*

Эти результаты показывают, что между подгруппами $K$ и $H$ в $D_3$ имеется существенное различие. В дальнейшем мы увидим, что подгруппа $K$ действительно обладает некоторой особенностью, которую можно охарактеризовать как «неизменяемость» (инвариантность) некоторого связанного с ней объекта, в то время как соответствующий объект подгруппы $H$ будет «изменяемым»; в связи с этим подгруппу $K$ называют *нормальной*, или *инвариантной*. Изучить существенные свойства нормальных подгрупп нам поможет рассмотрение *смежных классов* по таким подгруппам.

В гл. 8 мы уже имели дело со смежными классами по подгруппе и выписали все левые и правые смежные классы группы диэдра $D_3$ порядка 6 по подгруппе $H$. Было отмечено, что классы $aH$ и $Ha$ *не* совпадают (как множества) (стр. 117); левый смежный класс $aH$ — это множество

$$\{aI,\ ab\} = \{a,\ ba^2\},$$

а правый смежный класс $Ha$ — это множество

$$\{Ia,\ ba\} = \{a,\ ba\}.$$

Что можно сказать о левых и правых смежных классах группы $D_3$ по подгруппе $K$ порядка 3? Вот они:

| Левые смежные классы | Правые смежные классы |
|---|---|
| $K = \{I,\ a,\ a^2\},$ | $K = \{I,\ a,\ a^2\},$ |
| $bK = \{b,\ ba,\ ba^2\};$ | $Kb = \{b,\ ab,\ a^2b\} = \{b,\ ba^2,\ ba\}.$ |

Левые и правые смежные классы по подгруппе $K$ совпадают, т. е. $bK = Kb$.

Гомоморфное отображение $f$ группы $D_3$ на циклическую группу порядка 2 действует следующим образом:

$$\text{смежный класс } K \to I,$$

$$\text{смежный класс } bK = \text{смежный класс } Kb \to f(b).$$

На рис. 11.2 значком ○ отмечены те элементы группы диэдра $D_3$, которые принадлежат смежному классу $K$, а значком □ — те элементы, которые принадлежат смежному классу $bK$. На рис. 11.3 одинаковыми

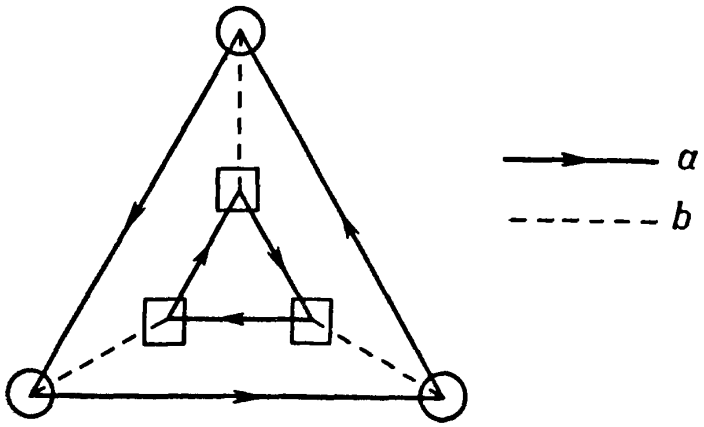



Рис. 11.2.

значками обозначены элементы, принадлежащие одному и тому же левому или правому смежному классу группы $D_3$ по подгруппе $H$.

Из этого примера видно, что представление группы $D_3$ в виде объединения смежных классов по $K$

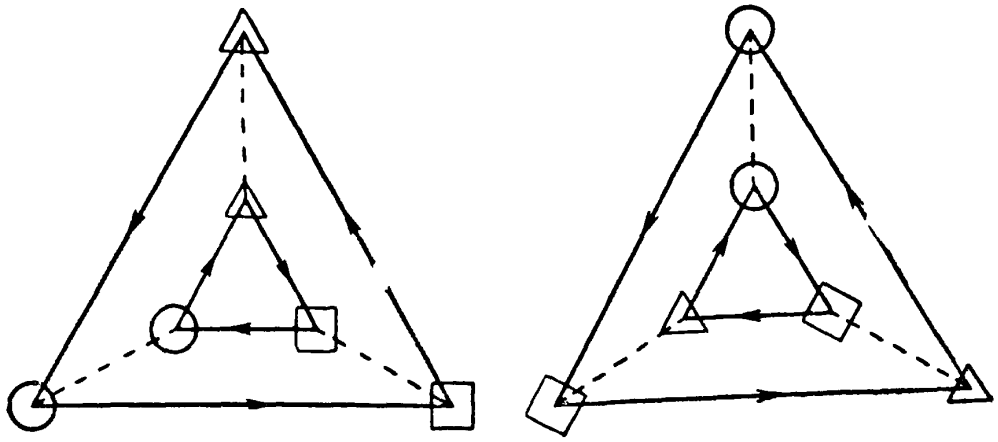


Рис. 11.3.

На левом рисунке, отвечающем левым смежным классам, символом ○ обозначены элементы из $H$, символом □ — элементы из $aH$ и символом △ — элементы из $a^2H$.
На правом рисунке, отвечающем правым смежным классам, символом ○ обозначены элементы из $H$, символом □ — элементы из $Ha$ и символом △ — элементы из $Ha^2$.

остается неизменным, иначе, *инвариантным*, вне зависимости от того, представляется ли группа в виде объединения левых или правых смежных классов.

Вообще подгруппа $K$ группы $G$ называется *нормальной*, или *инвариантной*, если каждый *левый смежный класс* $aK$ *группы* $G$ *по* $K$ *совпадает с соответствующим правым классом* $Ka$. Отметим, в частности,

что подгруппа, состоящая из одного элемента $I$, нормальна, поскольку для каждого элемента $g$ группы $G$ классы $gI$ и $Ig$ совпадают (каждый из них состоит из единственного элемента $g$). Вся группа $G$ также является своей нормальной подгруппой, поскольку любой левый смежный класс $gG$ и любой правый смежный класс $Gg$ совпадает со всей группой $G$.

В следующей теореме устанавливается связь между нормальными подгруппами и гомоморфными отображениями.

Теорема 6. *Пусть $f$ — гомоморфное отображение группы $G$ на группу $H$; тогда множество $K$ всех таких элементов $x$ группы $G$, что $f(x) = I$ (где $I$ — единица группы $H$), является нормальной подгруппой группы $G$.*

Доказательство. Убедимся сначала, что $K$ является подгруппой группы $G$. Для этого проверим выполнение двух указанных на стр. 107 условий, которым должна удовлетворять подгруппа. Затем докажем, что подгруппа $K$ нормальна.

(1) *Замкнутость.* Нужно показать, что если $x_1$ и $x_2$ — два произвольных элемента из $K$, то $x_1x_2$ также принадлежит $K$. Для этого покажем, что если $f(x_1) = I$ и $f(x_2) = I$, то $f(x_1x_2) = I$. Поскольку $f$ — гомоморфизм,

$$f(x_1x_2) = f(x_1)f(x_2) = I \cdot I = I.$$

Тем самым доказана замкнутость множества $K$.

(2) *Обратимость.* Покажем, что если элемент $x$ принадлежит множеству $K$, то его обратный $x^{-1}$ также принадлежит $K$, т. е. если $f(x) = I$, то и $f(x^{-1}) = I$. Так как $f$ — гомоморфизм, то $f(I) = I$ (см. упр. 37, стр. 137) и

$$f(x^{-1}) = I \cdot f(x^{-1}) = f(x)f(x^{-1}) = f(xx^{-1}) = f(I) = I.$$

Таким образом, для $K$ выполняется свойство обратимости.

Теперь докажем, что $K$ является нормальной подгруппой группы $G$. Для этого мы должны показать, что $yK = Ky$ *для любого элемента $y$ группы $G$.* (На-

помним, что *определение* нормальной подгруппы содержит лишь требование совпадения левых и правых смежных классов по этой подгруппе.)

Пусть $x_1$ — произвольный, но фиксированный элемент подгруппы $K$. Тогда $x_1y$ является элементом смежного класса

$$Ky = \{x_1y,\ x_2y,\ x_3y,\ \ldots\}.$$

Мы хотим показать, что элемент $x_1y$ принадлежит смежному классу

$$yK = \{yx_1,\ yx_2,\ yx_3,\ \ldots\};$$

для этого решим относительно $z$ уравнение

$$yz = x_1y$$

и покажем, что $z$ *является элементом подгруппы* $K$. Элемент

$$z = y^{-1}x_1y$$

является решением этого уравнения, и остается лишь показать, что $f(z) = I$. Но

$$\begin{aligned} f(z) = f(y^{-1}x_1y) = &\quad \text{(поскольку } f \text{ — гомоморфизм)} \\ = f(y^{-1})f(x_1)f(y) = &\quad \text{(поскольку } x_1 \text{ принадлежит } K\text{)} \\ = f(y^{-1})f(y) = &\quad \text{(поскольку } f \text{ — гомоморфизм)} \\ = f(I) = I. & \end{aligned}$$

Таким образом, $z$ принадлежит подгруппе $K$. Так как $x_1y$ — произвольный элемент смежного класса $Ky$, то мы доказали, что *каждый элемент из смежного класса* $Ky$ *принадлежит смежному классу* $yK$.

Аналогично, если $yx_1$ — произвольный элемент смежного класса $yK$, то мы можем показать, что $yx_1$ принадлежит смежному классу $Ky$. Для этого нужно лишь решить относительно $z$ уравнение $zy = yx_1$, а затем проверить, что $z = yx_1y^{-1}$ является элементом подгруппы $K$. Отсюда будет следовать, что *каждый элемент смежного класса* $yK$ *принадлежит* $Ky$. Таким образом, $yK = Ky$.

*Подгруппы абелевой группы нормальны.* Пусть $K$ — нормальная подгруппа группы $G$. Внешний вид соотношения $yK = Ky$ наводит на мысль о том, что речь идет о некоторой разновидности коммутативности. Интересующее нас свойство можно сформулировать следующим образом: для произвольного элемента $y$ группы $G$ и любого элемента $x_1$ подгруппы $K$ можно найти элемент $x_2$ из $K$, такой, что

$$yx_2 = x_1y, \quad \text{или} \quad x_2 = y^{-1}x_1y \quad \text{и} \quad x_1 = yx_2y^{-1}.$$

Из этого свойства вытекает, что *каждая подгруппа абелевой, или коммутативной, группы нормальна*; действительно, в абелевой группе для любых двух ее элементов $y$ и $x_1$

$$yx_1 = x_1y$$

и, таким образом, $yK = Ky$.

Упражнение 52. Докажите, что если порядок группы $G$ равен $2n$, где $n$ — целое число, и $H$ — подгруппа порядка $n$ группы $G$, то $H$ — ее нормальная подгруппа.

Упражнение 53. Пусть группа $G$ состоит из элементов $g_1, g_2, g_3, \ldots$ . Пусть, далее, $x$ обозначает любой из этих элементов; рассмотрим множество

$$S = \{xg_1x^{-1}, xg_2x^{-1}, xg_3x^{-1}, \ldots\}.$$

Докажите, что множество $S$ содержит все элементы группы $G$. (Элемент $xg_1x^{-1}$ называется *сопряженным* к элементу $g_1$ с помощью элемента $x$.)

Упражнение 54. Пусть $x$ и $y$ — любые два элемента некоторой группы, такие, что $x = yxy^{-1}$. Каким из известных нам ранее свойств обладает такая пара элементов? (Элемент $x$ называется *самосопряженным* с помощью $y$.)

Упражнение 55. Пусть $K$ — нормальная подгруппа группы $G$, причем $K$ состоит из элементов $k_1$, $k_2$, $k_3$, .... Пусть, далее, $g$ — произвольный элемент группы $G$. Рассмотрим множество $S = \{gk_1g^{-1}, gk_2g^{-1}, gk_3g^{-1}, \ldots\}$. Докажите, что множества $S$ и $K$ совпа-

дают. (Выражая это свойство, мы будем говорить, что нормальная подгруппа *самосопряжена.*)

*Обращение теоремы* 6 (*факторгруппа*). Когда математик завершает доказательство некоторой теоремы, он автоматически задает себе новый вопрос: верно ли обратное утверждение? Ответ на этот вопрос для теоремы 6 содержит неожиданный дополнительный результат — своего рода «премию» — в процессе доказательства возникает новый тип групп, называемых *факторгруппами.* Сформулируем теорему, обратную к теореме 6 (которая и в самом деле оказывается справедливой).

Теорема 7. *Пусть задана нормальная подгруппа $K$ группы $G$. Тогда существуют группа $H$ и гомоморфное отображение $f$ группы $G$ на группу $H$, такие, что все элементы группы $K$, и только они, переходят при $f$ в единицу группы $H$.*

В следующем разделе мы *построим* пример группы, связанной с группами $G$ и $K$ так, как это описано в теореме 7, и тем самым убедимся, что группа $H$ «существует». Такую группу называют *факторгруппой* группы $G$ по подгруппе $K$ и обозначают через $G/K$. Мы увидим, что элементами группы $G/K$ являются *множества* элементов, а именно *смежные классы* группы $G$ по подгруппе $K$.

Отметим, что эта теорема позволяет установить, может ли элемент $x$ принадлежать хотя бы одной нормальной подгруппе, не совпадающей со всей группой. Нужно лишь выяснить, какие следствия вытекают из предположения о существовании гомоморфизма $f$, при котором $f(x) = I$. Если любое отображение $f$, удовлетворяющее условию $f(x) = I$, переводит в $I$ *все* элементы группы, то $x$ не является элементом никакой собственной нормальной подгруппы.

**Факторгруппа.** Эварист Галуа первым показал, что *смежные классы группы $G$ по ее нормальной подгруппе $K$ образуют группу.* Эту группу мы назвали факторгруппой $G/K$. В ходе ее изучения нам придется приспособиться к новому для нас факту, а именно что

элементами данной группы являются множества элементов другой группы.

Прежде чем мы сможем на каком-либо примере проверить замечательный результат Галуа, необходимо определить на множестве смежных классов группы $G$ по нормальной подгруппе $K$ бинарную операцию. Определим *произведение двух смежных классов* $R$ и $S$ (в таком *порядке*) как *множество* всех произведений вида $rs$ (в таком *порядке*), где $r$ — элемент множества $R$, а $s$ — элемент множества $S$. Таким образом, произведение $R \cdot S$ двух смежных классов есть *множество*, состоящее из всех произведений элементов группы, первые сомножители которых принадлежат смежному классу $R$ и вторые — смежному классу $S$ (это множество легко найти по таблице умножения). Читателю следует доказать, что если $R$ и $S$ — смежные классы группы $G$ по ее *нормальной* подгруппе $K$, то $R \cdot S$ также будет смежным классом группы $G$ по подгруппе $K$, т. е. взятие произведения является бинарной операцией на множестве смежных классов группы $G$ по подгруппе $K$.

Поясним это определение, используя ранее найденные смежные классы группы диэдра $D_3$ по нормальной подгруппе $K$, циклической группе порядка 3 (стр. 164):

$$K = \{I,\ a,\ a^2\} \quad \text{и} \quad bK = \{b,\ ba,\ ba^2\}.$$

Образуем, согласно нашему определению, произведение $K \cdot K$. В результате мы получим множество элементов, которые составляют таблицу умножения 11.1. Это *множество* совпадает, очевидно, с $K$; таким образом, $K \cdot K = K$. Множество элементов, из которых состоит произведение $K \cdot bK$, составляет таблицу умножения 11.2. Читателю следует проверить, используя в качестве удобной формы таблицы умножения граф группы $D_3$, что это множество, состоящее из девяти произведений, совпадает со смежным классом $bK$, т. е. $K \cdot bK = bK$. Аналогично можно проверить, что $bK \cdot K = bK$ и $bK \cdot bK = K$. Таким образом, произ-

ведение любых двух смежных классов — снова смежный класс, а $K$ — единичный элемент.

*Таблица 11.1*

$K \cdot K$

| | $I$ | $a$ | $a^2$ |
|---|---|---|---|
| $I$ | $I$ | $a$ | $a^2$ |
| $a$ | $a$ | $a^2$ | $I$ |
| $a^2$ | $a^2$ | $I$ | $a$ |

*Таблица 11.2*

$K \cdot bK$

| | $b$ | $ba$ | $ba^2$ |
|---|---|---|---|
| $I$ | $b$ | $ba$ | $ba^2$ |
| $a$ | $ab$ | $aba$ | $aba^2$ |
| $a^2$ | $a^2b$ | $a^2ba$ | $a^2ba^2$ |

Таблица умножения 11.3 для *смежных классов* $K$ и $bK$ суммирует полученные результаты. Она показывает, что эти смежные классы образуют циклическую группу порядка 2 и что смежный класс $K$ является ее единицей. Эта группа $D_3/K$ смежных классов

*Таблица 11.3*

| | $K$ | $bK$ |
|---|---|---|
| $K$ | $K$ | $bK$ |
| $bK$ | $bK$ | $K$ |

называется *факторгруппой* группы $D_3$ по нормальной подгруппе $K$. Читателю следует проверить, что отображение $D_3 \to D_3/K$, определенное формулой

$$x \to xK,$$

есть гомоморфное отображение группы $D_3$ на группу $D_3/K$. (Покажите, что $xy \to xyK = xK \cdot yK$.)

Название «факторгруппа» и обозначение $D_3/K$ объясняются аналогией между разложением группы в объединение смежных классов

$$D_3 = K \cup bK$$

и факторизацией чисел, т. е. их разложением в произведение двух сомножителей [1]), так что мы «как бы» имеем

$$D_3 = (I + b)K = IK + bK = K + bK.$$

Вообще если группа $L$ представлена как объединение

$$L = J \cup rJ \cup sJ \cup \ldots \cup vJ$$

смежных классов по нормальной подгруппе $J$, то эти классы образуют факторгруппу [2]), обозначаемую через $L/J$. Эта факторгруппа однозначно определяется двумя группами: $L$ и $J$.

Упражнение 56. Образуйте произведение двух *подгрупп* $R$ и $S$ группы $G$ так же, как это делается для смежных классов. Покажите, что

(a) *множество* $R \cdot S$ является подгруппой тогда и только тогда, когда $R \cdot S = S \cdot R$;

(b) если одна из подгрупп $R$ или $S$ нормальна, то $R \cdot S = S \cdot R$ является подгруппой.

*Групповые соотношения и факторгруппы.* Выразим некоторые из полученных результатов о нормальных подгруппах, гомоморфных отображениях и факторгруппах с помощью групповых соотношений и графов групп.

На рис. 11.4 изображен граф группы диэдра $D_3$. Факторгруппа $D_3/K$ содержит всего два элемента

$$K = \{I, a, a^2\} \quad \text{и} \quad bK = \{b, ba, ba^2\},$$

в то время как группа $D_3$ содержит шесть элементов, представленных в виде вершин ее графа. Если мы

---

[1]) Этой же аналогией объясняется другое название нормальной подгруппы — «нормальный делитель». — *Прим. ред.*

[2]) Легко проверить, что для факторгруппы выполняются все групповые аксиомы. Действительно, 1) замкнутость относительно бинарной операции умножения смежных классов уже была показана (стр. 170); 2) ассоциативность сразу следует из ассоциативности умножения в $L$; 3) единицей является сама нормальная подгруппа $J$; 4) обратный к $rJ$ смежный класс есть $r^{-1}J$. — *Прим. ред.*

к определяющим соотношениям группы $D_3$ присоединим соотношение

$$a = I,$$

элементы в смежных классах $K$ и $bK$ примут вид

$$\{I,\ a = I,\ a^2 = I\} \quad \text{и} \quad \{b,\ bI = b,\ bI = b\},$$

т. е. мы добились не только того, что все элементы подгруппы $K$ превратились в элемент $I$, но и того, что все элементы смежного класса $bK$ превратились в элемент $b$. Иными словами, дополнительное соотношение

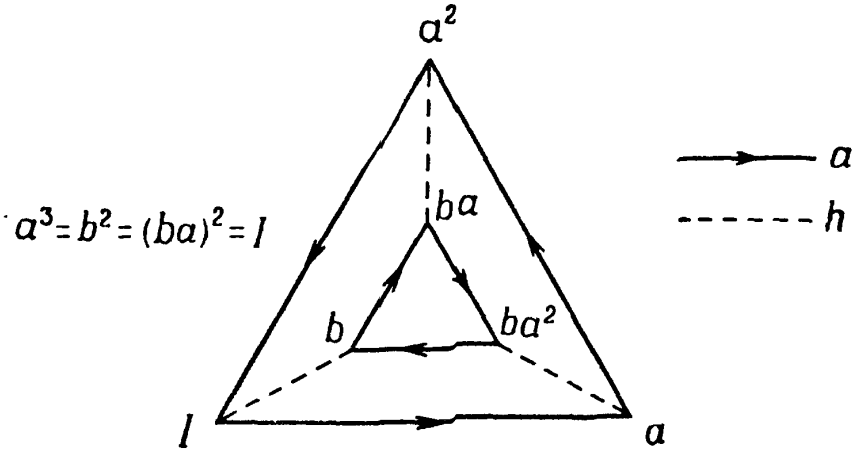



Рис. 11.4.

$a = I$ склеивает все элементы подгруппы $K$ в единственный элемент $I$, а все элементы смежного класса $bK$ — в единственный элемент $b$. Так как $b^2 = I$, то добавление соотношения $a = I$ приводит нас к циклической группе порядка 2, т. е. группе, изоморфной группе $D_3/K$. Таким образом, ввести дополнительное соотношение $a = I$ — это все равно, что гомоморфно отобразить группу $D_3$ на $D_3/K$ так, чтобы в единицу факторгруппы перешли в точности элементы подгруппы $K$.

Можно считать, что введение соотношения $a = I$ приводит к такой деформации графа, при которой вершины, соответствующие элементам подгруппы $K$, сливаются с вершиной, соответствующей элементу $I$. Такой процесс можно представлять себе как «стягивание» в точку образующей $a$, и это легче всего сделать, если сначала придать графу трехмерную форму, а затем «стянуть» все $a$-отрезки в точку.

Постепенная деформация изображена (слева направо) на рис. 11.5. Видно, что присоединение соотношения $a = I$ (т. е. обращение подгруппы $K$ в единицу группы $D_3/K$) превращает граф в *утроенный граф циклической группы порядка* 2, у которого одна вер-

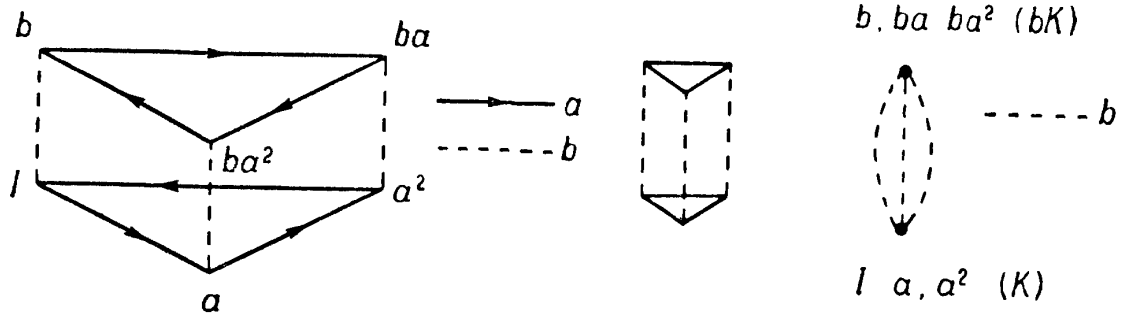



Рис. 11.5.

шина соответствует смежному классу $K$, а другая — смежному классу $bK$. Итак, с помощью деформации графа группы $D_3$ мы приходим к *графическому представлению факторгруппы* $D_3/K$, изображенному на рис. 11.6.

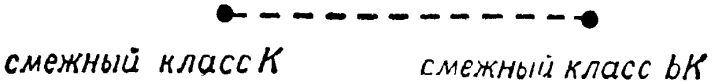



Рис. 11.6.

Посмотрим, в какой мере эти результаты справедливы для бесконечных групп. Рассмотрим аддитивную циклическую группу $N$ всех целых чисел и возьмем в качестве ее нормальной подгруппы множество $E$ всех четных чисел. Представим группу $N$ в виде объединения смежных классов по нормальной подгруппе $E$, т. е.

$$N = E \cup aE, \text{ где } a \text{ не принадлежит } E;$$

см. стр. 118. (Можно не сомневаться, что $E$ — нормальная подгруппа группы $N$, поскольку каждая подгруппа абелевой, или коммутативной, группы нормальна.) Смежный класс $aE$ совпадает с множеством $O$ всех нечетных чисел и, следовательно,

$$N = E \cup O.$$

Образуют ли смежные классы $E$ и $O$ группу? Нам нужно убедиться в том, что каждое из произведений

$$E \cdot E, \quad E \cdot O, \quad O \cdot E, \quad O \cdot O$$

есть либо смежный класс $E$, либо смежный класс $O$ и что выполняются аксиомы группы. Вспомним, что бинарная операция группы $N$ — это *сложение*. Тогда

$E \cdot E = E$, так как $E \cdot E$ есть множество всех *сумм* двух четных чисел;

$E \cdot O = O$, так как $E \cdot O$ есть множество всех *сумм* четного и нечетного чисел;

$O \cdot E = O$, так как $O \cdot E$ есть множество всех *сумм* нечетного и четного чисел;

$O \cdot O = E$, так как $O \cdot O$ есть множество всех *сумм* двух нечетных чисел.

Таблица 11.4 — это таблица умножения для смежных классов $E$ и $O$. Таким образом, у факторгруппы $N/E$ такая же таблица умножения, как у циклической группы порядка 2 ($E$ играет роль единицы). В гл. 8 мы видели, что бесконечная циклическая группа не имеет конечных *подгрупп*; теперь мы видим, что конечная группа может быть ее *факторгруппой*.

*Таблица 11.4*

| | $E$ | $O$ |
|---|---|---|
| $E$ | $E$ | $O$ |
| $O$ | $O$ | $E$ |

Построим теперь факторгруппу $N/E$ с помощью графа группы $N$ (рис. 11.7), следуя схеме, использованной в предыдущем примере, и найдем дополнительно соотношение, эквивалентное обращению нормальной подгруппы $E$ в единицу.

Если обозначить через $a$ образующую группы и ввести соотношение

$$a^2 = I,$$

то

$$a^{-2} = I, \quad a^4 = I, \quad a^{-4} = I, \quad a^6 = I \text{ и т. д.}$$

Присоединенное соотношение отображает *четные* степени элемента $a$ в $I$; другими словами, подгруппа $E$ *аддитивной* циклической группы $N$ отображается в $I$. Определенная этим *расширенным* множеством соотношений группа (факторгруппа $N/E$) есть в точности циклическая группа порядка 2. (Мы говорили о соотношении, присоединенном к «исходному» множеству

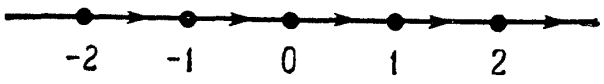



Рис. 11.7.
В группе нет соотношений.

соотношений, лишь для того, чтобы сохранить схему рассуждений предыдущего примера (группа $D_3$). Но в нашем случае «исходное» множество соотношений «пусто» — группа $C_\infty$ *свободна*; см. стр. 81.)

Какое действие на граф группы $N$ оказывает переход всех элементов подгруппы $E$ в элемент $I$? Чтобы

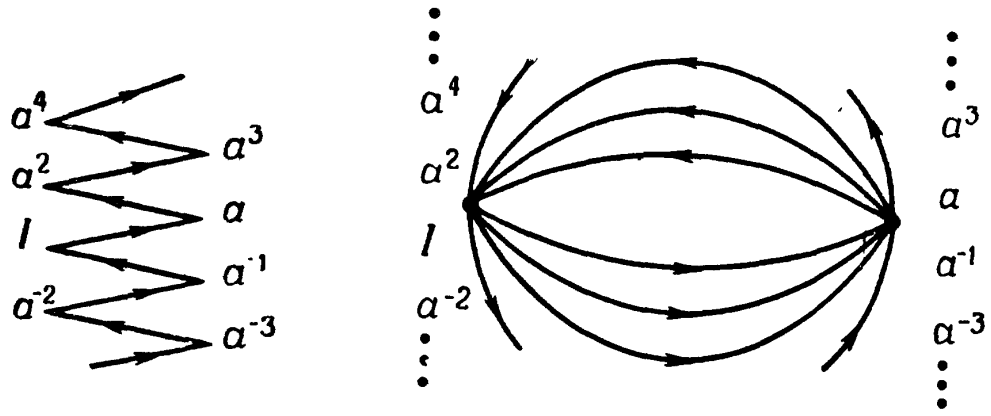



Рис. 11.8.

ответить на этот вопрос, придадим графу удобную форму и затем склеим вершины, соответствующие элементам подгруппы $E$, с вершиной, соответствующей вершине $I$. Остальные вершины, соответствующие элементам класса смежности $O$, также склеиваются в одну точку (рис. 11.8). При этом граф группы $N$ превращается в бесконечно много раз повторенный граф циклической группы порядка 2, одна из вершин которого соответствует смежному классу $E$, а другая —

смежному классу $O$. На рис. 11.9 изображен граф факторгруппы $N/E$.

Если вместо соотношения $a^2 = I$ мы присоединим соотношение $a^3 = I$, то в $I$ будет обращаться подгруппа $T$ всех чисел, кратных 3. Граф, приведенный к

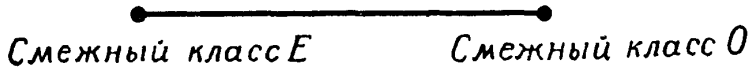



Рис. 11.9.

удобному нам виду, и граф, полученный после склеивания вершин, соответствующих элементам подгруппы $T$, с вершиной, соответствующей элементу $I$, изображены на рис. 11.10. Полученный граф есть граф факторгруппы $N/T$.

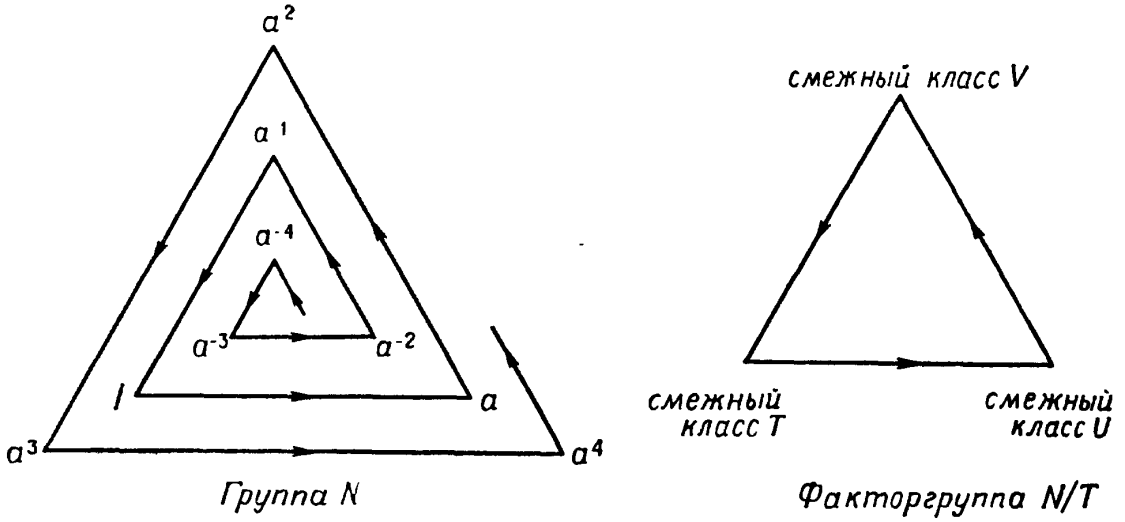



Рис. 11.10.

$T$ — подгруппа, состоящая из всех чисел, кратных 3; $U$ — смежный класс $aT$, где $a$ имеет вид $3n+1$; $V$ — смежный класс $bT$, где $b$ имеет вид $3n+2$.

Изучение групп $D_3$ и $N$ приводит нас к такому способу построения факторгрупп:

(1) Рассмотрим группу $G$ с заданными образующими и определяющими соотношениями.

(2) Введем новое соотношение, т. е. приравняем элементу $I$ некоторое слово от образующих группы $G$.

(3) Из этого нового соотношения следует, что становятся равными $I$ еще и некоторые другие элементы группы $G$. Множество всех элементов $g$ группы $G$, для которых равенство $g = I$ является следствием

добавленного соотношения и групповых аксиом, образует нормальную подгруппу $K$ группы $G$.

(4) Соотношения из п. (1) и (2) в совокупности определяют факторгруппу $G/K$.

Это некоторая разновидность определения факторгруппы с помощью гомоморфного отображения, так как условия п. (2) и (3) вместе эквивалентны заданию гомоморфного отображения группы $G$ на факторгруппу $G/K$, при котором в $I$ отображаются в точности все элементы нормальной подгруппы $K$.

Мы можем следующим образом обобщить этот способ:

(1) Рассмотрим группу $G$ с заданными образующими и $n$ определяющими соотношениями

$$R_1 = I, \quad R_2 = I, \ \ldots, \ R_n = I.$$

(2) Введем $s$ дополнительных соотношений

$$R_{n+1} = I, \quad R_{n+2} = I, \ \ldots, \ R_{n+s} = I,$$

приравнивая к $I$ слова от образующих группы $G$.

(3) Множество всех элементов $g$ группы $G$, для которых равенство $g = I$ является следствием добавленных соотношений и групповых аксиом, образует нормальную подгруппу $K$ группы $G$.

(4) Все $n + s$ соотношений $R_1 = I$, $R_2 = I$, ... ..., $R_{n+s} = I$ определяют факторгруппу $G/K$.

Мы не будем приводить полного доказательства этих утверждений и ограничимся лишь тем, что укажем, как присоединение новых соотношений определяет нормальную подгруппу $K$ группы $G$. Рассмотрим сначала элементы $g$ группы $G$, для которых равенство $g = I$ является следствием некоторого присоединенного соотношения, скажем $R_{n+1} = I$. Так как $R_{n+1}$ — слово от образующих группы $G$, то $R_{n+1}$ соответствует некоторому элементу $x$ группы $G$. Согласно нашему новому соотношению, $x = I$; следовательно, $x^{-1} = I$, $yxy^{-1} = I$ и $yx^{-1}y^{-1} = I$, где $y$ — произвольный элемент группы $G$. Таким образом,

$$J = \{y_1 x y_1^{-1}, \ y_1 x^{-1} y_1^{-1}, \ y_2 x y_2^{-1}, \ y_2 x^{-1} y_2^{-1}, \ \ldots\}$$

есть множество элементов $g$, для которых соотношение $g = I$ является прямым следствием соотношения $R_{n+1} = I$. Ясно, что произведение любых двух элементов множества $J$ снова равно $I$, произведение любых двух таких произведений также равно $I$ и т. д., т. е. если $K$ — множество элементов группы $G$, *порожденное* элементами из множества $J$, то каждый элемент из $K$ равен $I$, и это равенство есть следствие соотношения $R_{n+1} = I$ [1]). Мы предоставляем читателю самостоятельно убедиться, что $K$ — подгруппа группы $G$.

Будет ли $K$ *нормальной* подгруппой? Подгруппа $K$ нормальна тогда и только тогда, когда

$$yK = Ky \quad \text{или} \quad yKy^{-1} = K,$$

где $y$ — произвольный элемент группы $G$. Покажем, что если $k_1$ — некоторое конкретное слово из $K$, то $yk_1y^{-1}$ снова принадлежит $K$. Наш метод применим к любому элементу из $K$ и основан на том факте, что любой элемент из $K$ является словом от элементов множества $J$. Пусть мы выбрали слово

$$k_1 = (y_1xy_1^{-1})(y_2xy_2^{-1})(y_3xy_3^{-1}).$$

Тогда

$$yk_1y^{-1} = y(y_1xy_1^{-1})(y^{-1}y)(y_2xy_2^{-1})(y^{-1}y)(y_3xy_3^{-1})y^{-1},$$

так как $y^{-1}y = I$. Поскольку $(yy_1)^{-1} = y_1^{-1}y^{-1}$, мы имеем

$$\begin{aligned} yk_1y^{-1} &= (yy_1)\,x\,(yy_1)^{-1}\,(yy_2)\,x\,(yy_2)^{-1}\,(yy_3)\,x\,(yy_3)^{-1} = \\ &= (\text{слово от элементов из } J) = \\ &= (\text{элемент подгруппы } K). \end{aligned}$$

Процедура, примененная нами для доказательства того, что $yk_1y^{-1}$ принадлежит $K$, применима к любому элементу $yky^{-1}$, где $k$ — элемент из $K$, и, значит, *каждый элемент множества* $yKy^{-1}$ *принадлежит подгруппе* $K$. Кроме того, этот метод применим к любому элементу $y$ группы $G$; в частности, если $k$ — произвольный элемент подгруппы $K$, то $y^{-1}k(y^{-1})^{-1}$ принадлежит

[1]) Ср. с множеством $K$, описанным на стр. 86.

$K$. Таким образом, для любого элемента $k$ подгруппы $K$ существует элемент $\hat{k}$ в $K$, такой, что

$$\hat{k} = y^{-1}k\,(y^{-1})^{-1} = y^{-1}ky,$$

или

$$k = y\hat{k}y^{-1}.$$

Это показывает, что *каждый элемент подгруппы* $K$ *принадлежит множеству* $yKy^{-1}$. Следовательно, $K = yKy^{-1}$ и $K$ — нормальная подгруппа группы $G$.

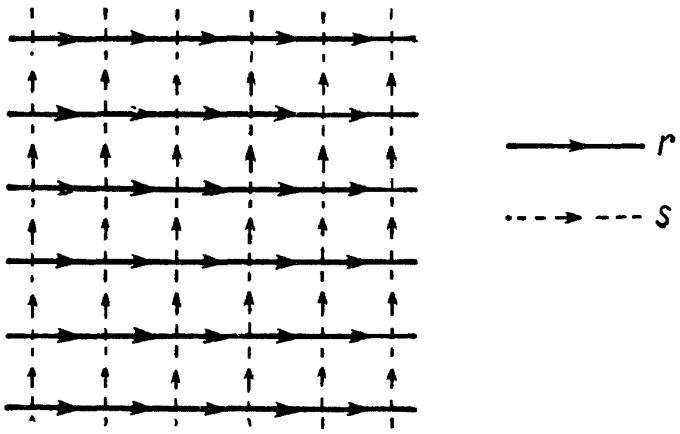



Рис. 11.11.

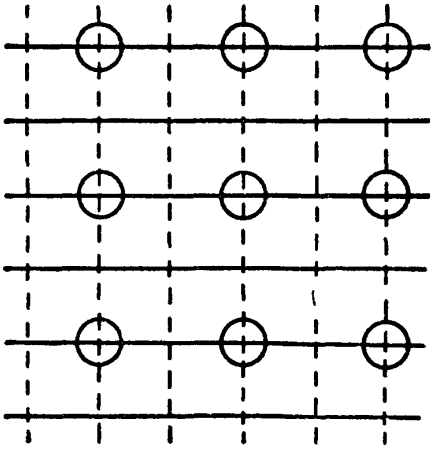


Рис. 11.12.

Чтобы проиллюстрировать наши общие рассуждения об определении факторгруппы с помощью дополнительных определяющих соотношений, рассмотрим такой пример:

(1) В качестве группы $G$ возьмем группу «городских улиц» (стр. 102) с образующими $r$ и $s$ и определяющим соотношением $rsr^{-1}s^{-1} = I$ (рис. 11.11).

(2) Присоединим соотношения $r^2 = I$, $s^2 = I$.

(3) Множество таких элементов $g$ группы $G$, для которых равенство $g = I$ является следствием этих новых соотношений и групповых аксиом, порождается элементами $r^2$ и $s^2$ и равно множеству всех элементов вида $r^{2m}s^{2n}$, где $m$ и $n$ принимают значения 0, $\pm 1$, $\pm 2$, ... (т. е. множеству всех слов, в которые образующие $r$ и $s$ входят с *четными* степенями). Эти элементы образуют нормальную подгруппу $K$. На графе рис. 11.12 соответствующие вершины отмечены кружками. (Мы опустили стрелки, поскольку они несущественны при изучении распределения элементов по смежным классам.)

(4) Факторгруппа $G/K$ определяется расширенным множеством соотношений

$$r^2 = I, \quad s^2 = I, \quad rsr^{-1}s^{-1} = I.$$

Первые два соотношения дают равенства $r = r^{-1}$, $s = s^{-1}$, а последнее можно переписать в виде $rsrs = (rs)^2 = I$. Читатель без труда узнает в них определяющие соотношения *четверной* группы (стр. 96).

Графически распределение элементов по смежным классам факторгруппы $G/K$ показано на рис. 11.13.

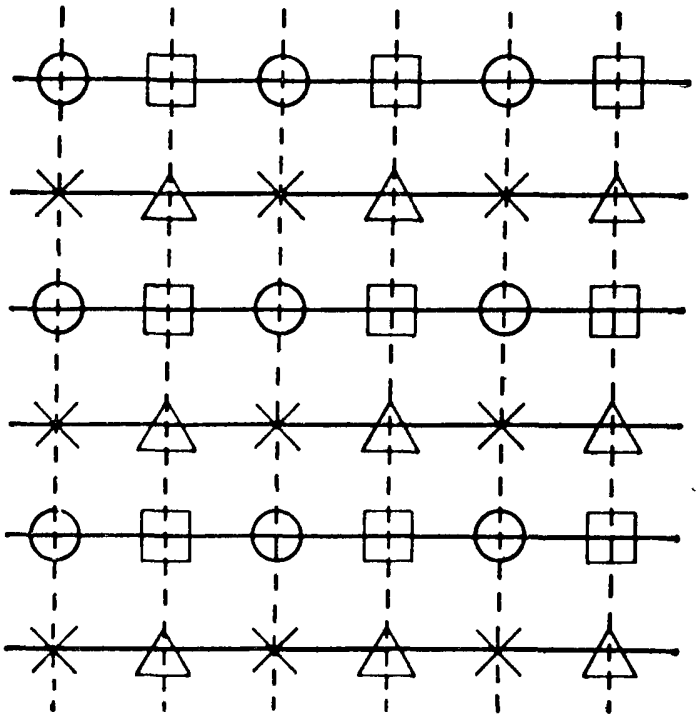


Рис. 11.13.

Символом ○ обозначены элементы из $K$ (вида $r^{2m}s^{2n}$); символом □ — элементы из $rK$ (вида $r^{2m+1}s^{2n}$); символом × — элементы из $sK$ (вида $r^{2m}s^{2n+1}$); символом △ — элементы из $rsK$ (вида $r^{2m+1}s^{2n+1}$).

Упражнение 57. Пусть $G$ — некоторая группа и $G/K$ — ее факторгруппа. Что можно сказать о коммутативности следующих групп?

(a) $G/K$, если $G$ коммутативна.
(b) $G/K$, если $G$ некоммутативна.
(c) $G$, если $G/K$ коммутативна.
(d) $G$, если $G/K$ некоммутативна.

Упражнение 58. Пусть группа $G$ с образующими $x$ и $y$ определена соотношением $x^2y^{-3} = I$. Покажите, что $G$ некоммутативна. [*Указание*: используйте результаты предыдущего упражнения, подобрав подходящую некоммутативную группу, изоморфную некоторой факторгруппе $G/K$.]

ГЛАВА 12

# ГРУППА КВАТЕРНИОНОВ

*Каждая* подгруппа коммутативной группы нормальна. Существуют ли неабелевы группы, у которых *все* подгруппы нормальны? Существуют ли такие неабелевы группы, ни одна собственная подгруппа которых не является нормальной? Группы обоих указанных типов действительно существуют. Наименьшая неабелева группа, *все* подгруппы которой нормальны, — это так называемая *группа кватернионов*, открытая Гамильтоном [1]). Она имеет порядок 8. Наименьшая неабелева группа без собственных нормальных подгрупп — это *группа икосаэдра* порядка 60.

Группа икосаэдра хорошо известна в математике благодаря той роли, которую она сыграла в исследованиях Галуа о разрешимости уравнения пятой степени общего вида. Галуа показал, что свойства решений любого алгебраического уравнения зависят от группы подстановок, связанной с этим уравнением, и что разрешимость уравнения в сущности определяется наличием или отсутствием нормальных подгрупп и свойствами факторгрупп по этим подгруппам. Для уравнений пятой степени общего вида, например, решающим оказывается то обстоятельство, что группа икосаэдра не имеет собственных нормальных подгрупп. Эту группу мы рассмотрим в приложении.

Основные свойства группы кватернионов $Q$ порядка 8 были описаны в 40-х годах прошлого века Гамильтоном. Сделав ряд важнейших открытий в области оптики и динамики, он обратился к математи-

---

[1]) Уильям Роуэн Гамильтон (1805—1865).

ческим исследованиям. Гамильтон изучал вопрос о возможности обобщения комплексных чисел (т. е. чисел вида $a + ib$, где $i = \sqrt{-1}$), надеясь получить с помощью этих обобщенных комплексных чисел такое же удобное описание вращений в трехмерном пространстве, какое достигается с помощью обычных комплексных чисел для вращений в плоскости. Гамильтон показал, что для этого необходимо ввести две дополнительные «единицы», $j$ и $k$. В то время как обычные комплексные числа строятся с помощью двух «единиц», 1 и $i$, обобщенные *гиперкомплексные* числа Гамильтона строятся с помощью *четырех* «единиц», 1, $i$, $j$, $k$; отсюда и их название «кватернионы». Кватернион $q$ есть линейная комбинация четырех единиц, т. е. комбинация вида

$$q = \alpha + i\beta + j\gamma + k\delta,$$

где $\alpha$, $\beta$, $\gamma$, $\delta$ — действительные числа. Эти *гипер*комплексные числа и в самом деле представляют вращения в трехмерном пространстве (а также и в четырехмерном пространстве).

По определению они удовлетворяют следующим основным соотношениям:

$$i^2 = j^2 = k^2 = ijk = -1;$$

отсюда можно вывести, что

$$ij = k, \quad jk = i, \quad ki = j$$

и

$$ji = -k, \quad kj = -i, \quad ik = -j.$$

Таким образом, не все кватернионные единицы и, следовательно, не все кватернионы перестановочны. Это и не удивительно в свете того факта, что вращения в трехмерном пространстве, вообще говоря, не коммутируют между собой.

*Группа кватернионов* $Q$ состоит из восьми элементов:

$$1, \quad -1, \quad i, \quad -i, \quad j, \quad -j, \quad k, \quad -k$$

(четырех кватернионных «единиц» и четырех противоположных им элементов).

Для удобства положим

$$i = a, \quad j = b, \quad 1 = I;$$

тогда $ab = ij = k$ и группа $Q$ определяется соотношениями

$$a^2 = b^2 = (ab)^2.$$

Перепишем все восемь ее элементов:

$$I,\ a,\ b,\ ab,\ ba,\ a^2,\ a^3,\ b^3.$$

Нетрудно построить граф группы кватернионов, если заметить, что

$$a^4 = b^4 = (ab)^4 = I.$$

Выписанные соотношения можно вывести из основных соотношений этой группы. (Относительно подробностей см. решение упр. 21.) Соотношения $a^4 = b^4 = I$

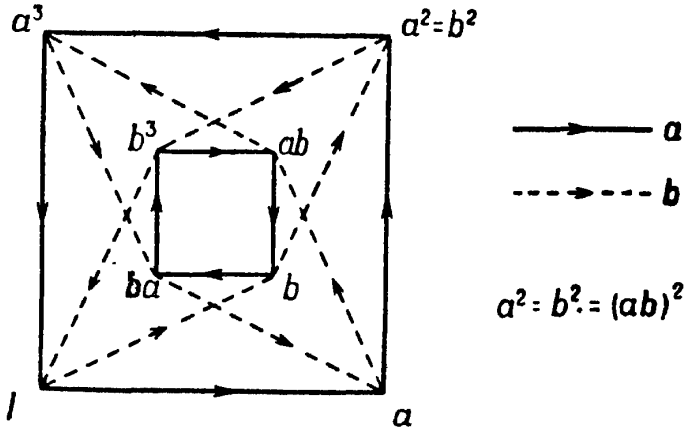



Рис. 12.1.

сразу наводят на мысль, что искомый граф состоит из двух связанных между собой четырехугольников. Граф группы кватернионов $Q$ представлен на рис. 12.1. Следует помнить, что это лишь проекция на плоскость его трехмерного изображения. На самом деле $b$-отрезки проходят один над другим, *не пересекаясь* (но изобразить это на плоском рисунке в принципе невозможно).

Из теоремы Лагранжа следует, что любая собственная подгруппа группы $Q$ имеет порядок 2 или 4. Единственная абстрактная группа (стр. 142) порядка 2 — это циклическая группа $C_2$, а единственными

абстрактными группами порядка 4, как нетрудно показать [1]), являются циклическая группа $C_4$ и четверная группа. Мы уже определили порядки всех элементов группы $Q$, и теперь это поможет нам найти все ее подгруппы. Используя граф группы как компактную запись таблицы умножения, выясняем, что $a^2$ — единственный элемент группы $Q$, порядок которого равен 2; элемент $I$, конечно, имеет порядок 1, а остальные шесть элементов — порядок 4. Таким образом, группа $Q$ содержит одну подгруппу, изоморфную циклической подгруппе $C_2$, и три подгруппы, изоморфные группе $C_4$ (порожденные элементами $a$, $b$, $ab$ соответственно).

Остается еще выяснить, есть ли у группы $Q$ подгруппы, изоморфные четверной группе. Ответ на этот вопрос отрицательный, поскольку мы знаем, что четверная группа содержит три различных элемента порядка 2 (стр. 96).

Мы утверждаем, что *все подгруппы некоммутативной группы $Q$ нормальны.* Рассмотрим прежде всего единственную подгруппу порядка 2:

$$H = \{I, a^2\}.$$

Будет ли она нормальной подгруппой? Да. Чтобы доказать это, построим гомоморфное отображение группы $Q$ на группу $Q^*$, при котором $H$ отображается в единицу группы $Q^*$. Как и в примерах гл. 11, *мы добавим соотношение, эквивалентное обращению в $I$ всех элементов подгруппы $H$ (и только их).* В данном случае это должно быть соотношение $a^2 = I$. Расширенное множество соотношений

$$I = a^2 = b^2 = (ab)^2 \qquad (1)$$

[1]) Действительно, пусть $I$, $a$, $b$, $c$ — элементы группы $G$ порядка 4. Если среди них найдется элемент, скажем $a$, порядка 4, то группа $G$ — циклическая группа $C_4 = \{a, a^2, a^3, a^4 = I\}$. Если же нет, то по теореме Лагранжа порядок подгруппы $H = \{I, x, x^{-1}, x^2, x^{-2}, \ldots\}$, порожденной каждым из элементов группы, равен 2, т. е. имеем $a^2 = b^2 = c^2 = I$, $a = a^{-1}$, $b = b^{-1}$, $c = c^{-1}$. Из аксиом группы тогда следует, что $ab \neq I, a, b$; следовательно, $ab = c$ и, аналогично, $ba = c$. Итак, $ab = ba$, и в группе $G$ выполнены все соотношения, определяющие четверную группу. Так как других соотношений нет, то $G$ совпадает с четверной группой. — *Прим. ред.*

определяет факторгруппу $Q^*$. Подгруппа $H$ будет нормальной подгруппой группы $Q$ в том и только том случае, когда $Q^*$ есть группа порядка 4, т. е. в том и только том случае, когда элементы группы $Q^*$ есть смежные классы группы $Q$ по подгруппе $H$ порядка 2. Но в определяющих соотношениях (1) группы $Q^*$ мы сразу узнаем определяющие соотношения *четверной группы*, и поэтому подгруппа $H$ группы $Q$ нормальна. Все циклические подгруппы порядка 4 также нормальны, поскольку порядок группы $Q$ равен $2 \cdot 4$ (см. упр. 52, стр. 168). Таким образом, все подгруппы [1]) неабелевой группы $Q$ являются нормальными.

Любая неабелева группа, все подгруппы которой нормальны, называется *гамильтоновой группой*. Группа кватернионов $Q$ — это гамильтонова группа наименьшего возможного порядка (а именно порядка 8). Можно показать, что любая конечная гамильтонова группа получается из группы кватернионов и абелевых групп с помощью конструкции, называемой прямым произведением групп.

---

[1]) Из приведенных рассуждений не следует делать вывода, что если $H$ — нормальная подгруппа группы $G$, то любая другая, изоморфная ей подгруппа группы $G$ также нормальна. Группа $S_4$, о которой пойдет речь в гл. 13, имеет четыре подгруппы, изоморфные четверной группе, но *лишь одна из них* является нормальной подгруппой группы $S_4$.

ГЛАВА 13

# СИММЕТРИЧЕСКИЕ И ЗНАКОПЕРЕМЕННЫЕ ГРУППЫ

В этой главе мы более подробно изучим группу всех отображений заданного конечного множества на себя. Такая группа называется *симметрической* группой. Если исходное множество содержит $n$ элементов, то соответствующая симметрическая группа обозначается через $S_n$.


Рис. 13.1.

Предположим, что задано множество из двух элементов. Каковы все те отображения, или подстановки, которые составляют группу $S_2$? В ней всего лишь два элемента — отображения

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

Геометрически их можно представлять себе как совмещения прямолинейного отрезка; см. рис. 13.1. Эта группа самосовмещений является циклической группой $C_2$, т. е. группа $S_2$ изоморфна группе $C_2$.

Рассмотрим теперь группу $S_3$. Когда мы отображаем на себя множество $\{a_1, a_2, a_3\}$, нам предоставляются *три* возможности для выбора образа элемента $a_1$ — это $a_1$, $a_2$ или $a_3$. Как бы мы ни поступили, образом элемента $a_2$ должен быть один из *двух* оставшихся элементов. (Имеется лишь два элемента, которые могут стать образом элемента $a_2$, поскольку

отображение должно быть взаимно однозначным.) И наконец, образ элемента $a_3$ определяется уже однозначно. Итак, существует $3 \cdot 2 \cdot 1 = 6$ различных отображений множества, состоящего из трех элементов, на себя. Вот они:

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

Эти отображения геометрически можно представлять как самосовмещения равностороннего треугольника

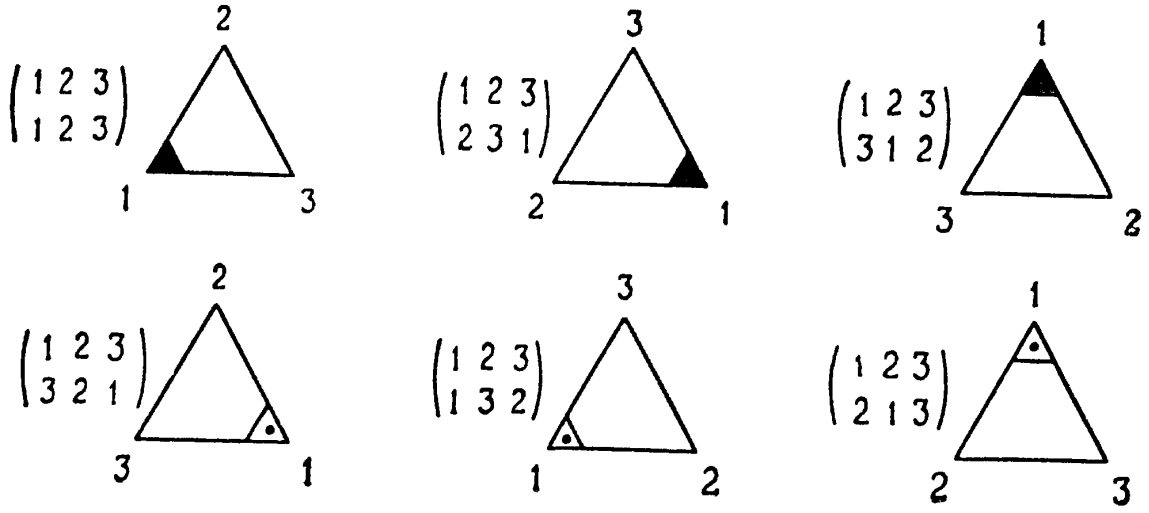



Рис. 13.2.

(см. рис. 13.2). Мы узнаем в этой группе группу диэдра $D_3$. Таким образом, группа $S_3$ изоморфна группе $D_3$.

Сформулируем без доказательства или каких-либо пояснений некоторые утверждения относительно группы $S_4$.

(1) Множество всех самосовмещений куба является группой, изоморфной группе $S_4$.

(2) Множество всех самосовмещений правильного октаэдра является группой, изоморфной группе $S_4$.

(3) Тот факт, что группы самосовмещений этих двух многогранников (стр. 155) изоморфны одной и той же группе $S_4$, связан с тем, что куб и правильный

октаэдр являются *двойственными* фигурами [1]). (Еще одна пара двойственных многогранников указана в приложении.)

В общем случае, когда отображается на себя множество $\{a_1, a_2, \ldots, a_n\}$, образ элемента $a_1$ можно выбрать $n$ способами, образ элемента $a_2$ можно выбрать $n-1$ способами и т. д. В конце концов для выбора образа элемента $a_n$ остается единственная возможность, так как остальные $n-1$ элементов уже «заняты» образами элементов $a_1, a_2, \ldots, a_{n-1}$. Следовательно, симметрическая группа $S_n$ состоит из $n(n-1)(n-2)\ldots 3\cdot 2\cdot 1$ различных отображений, или подстановок. Если использовать обозначение

$$n(n-1)(n-2)\ldots 3\cdot 2\cdot 1 = n!,$$

где $n!$ читается как «$n$ факториал», то можно сказать, что порядок группы $S_n$ равен $n!$.

**Симметрические многочлены.** Существует связь между симметрическими группами и симметрическими многочленами. В качестве примера симметрического многочлена от двух переменных рассмотрим

$$d_2 = (x_1 - x_2)^2.$$

Значение $d_2$ зависит от значений $x_1$ и $x_2$. Однако значение $d_2$ не изменится, если мы поменяем между собой $x_1$ и $x_2$. Такая операция на самом деле означает, что мы отображаем множество $\{x_1, x_2\}$ на себя так, что $x_1 \to x_2$ и $x_2 \to x_1$, а затем каждый элемент в записи многочлена $d_2$ заменяем его образом. Так как

---

[1]) Шесть граней куба являются квадратами, и центры этих квадратов составляют вершины правильного октаэдра, т. е. геометрической фигуры с восемью гранями (одинаковыми равносторонними треугольниками) и шестью вершинами. Обратно, центры восьми граней правильного октаэдра составляют вершины куба. Эти многогранники называют *двойственными*; любое самосовмещение одного из них является самосовмещением другого. Тетраэдр двойствен самому себе (см. стр. 135—142 книги О. Оре «Графы и их применение», «Мир», М., 1965).

существует всего два отображения множества $\{x_1, x_2\}$ на себя,

$$\begin{pmatrix} x_1 & x_2 \\ x_1 & x_2 \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix},$$

то *значение многочлена $d_2$ не меняется при замене элементов на их образы при любом отображении из симметрической группы $S_2$.*

Примером симметрического многочлена от трех переменных служит

$$d_3 = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2.$$

Легко показать, что значение многочлена $d_3$ не меняется при замене элементов $x_1$, $x_2$, $x_3$ их образами при любом отображении из группы $S_3$.

В общем случае симметрический многочлен от $n$ переменных — это многочлен, значение которого не меняется при замене $n$ переменных их образами при любом отображении (или подстановке) из симметрической группы $S_n$.

*Транспозиции.* Когда мы выражаем элементы симметрической группы с помощью циклов специального вида — так называемых *транспозиций*, — то отчетливо проявляются некоторые интересные особенности ее структуры. В гл. 10 мы показали, что любое отображение конечного множества на себя можно записать в виде произведения циклов от непересекающихся множеств символов, например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} = (1\ 2\ 4)(3\ 5).$$

В цикл (1 2 4) входят три символа, а в цикл (3 5) — только два. Цикл, в который входят лишь два различных символа, называется *транспозицией.* Мы покажем, что любой цикл можно представить в виде произведения транспозиций. Так как каждое отображение из симметрической группы есть произведение циклов, то *любой элемент симметрической группы можно представить в виде произведения* (последовательное выполнение) *транспозиций.*

В качестве иллюстрации этого утверждения проверим, что $(1\ 2\ 4) = (1\ 2)(1\ 4)$. Для этого проследим, как отображаются символы 1, 2, 4:

| $(1\ 2)$ | | $(1\ 4)$ | | $(1\ 2)(1\ 4)$ |
|---|---|---|---|---|
| $1 \to 2$, | затем | $2 \to 2$, | окончательно | $1 \to 2$, |
| $2 \to 1$, | затем | $1 \to 4$, | окончательно | $2 \to 4$, |
| $4 \to 4$, | затем | $4 \to 1$, | окончательно | $4 \to 1$. |

Таким образом, подстановка $(1\ 2)(1\ 4)$ действует следующим образом: $1 \to 2$, $2 \to 4$, $4 \to 1$, т. е. как цикл $(1\ 2\ 4)$, что и утверждалось.

Любой цикл из трех различных символов можно представить в виде произведения двух транспозиций:

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

Аналогично, цикл из четырех символов можно представить с помощью трех транспозиций:

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

Вообще, цикл из $n$ символов представляется в виде последовательности $n - 1$ транспозиций:

$$(a_1\ a_2 \ldots a_n) = (a_1\ a_2)(a_1\ a_3) \ldots (a_1\ a_n).$$

Упражнение 59. Покажите, что если подстановка на множестве из $n$ символов представима в виде произведения $r$ циклов, в которые входят все $n$ символов, но ни один из символов не входит в два цикла, то ее можно представить как последовательность $n - r$ транспозиций.

Заметим, что представление отображения или подстановки в виде произведения транспозиций *не* единственно. Например, отображение

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

можно представить так:

$(1\ 2\ 3) = (1\ 2)(1\ 3)$ или

$(2\ 3\ 1) = (2\ 3)(2\ 1)$ или $(3\ 1\ 2) = (3\ 1)(3\ 2)$.

Но мы видим, что в каждом из этих представлений *число* транспозиций одно и то же, и можно было бы высказать предположение, что каждая подстановка характеризуется этим *числом* транспозиций. Однако простой пример показывает, что это не так:

$$(1\ 2)(1\ 3)(2\ 3) = (1\ 3).$$

В действительности существует бесконечно много способов такого представления — чтобы убедиться в этом, достаточно принять во внимание тождества

$$(a\ b)(a\ b) = I \quad \text{и} \quad (a\ b) = (c\ a)(c\ b)(c\ a).$$

Покажем теперь, что либо каждое представление заданной подстановки в виде произведения транспозиций содержит *четное* число транспозиций, либо каждое такое представление содержит *нечетное* число транспозиций. Рассмотрим многочлен

$$g_3 = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

от трех переменных $x_1$, $x_2$, $x_3$. (Мы ограничимся рассмотрением случая трех переменных, но наши рассуждения без труда переносятся и на случай $n$ переменных.) Посмотрим, как устроен многочлен $g_3$: он представляет собой произведение всех разностей $x_j - x_k$, где $j < k$. Ясно, что любое *четное* число транспозиций переменных оставляет многочлен $g_3$ без изменения, в то время как *нечетное* число таких транспозиций переводит его в многочлен $-g_3$. Рассмотрим теперь любую подстановку трех переменных $x_1$, $x_2$, $x_3$ или, что равносильно, любую подстановку трех индексов 1, 2, 3. Каждая такая подстановка есть элемент группы $S_3$, и ее можно записать в виде последовательности транспозиций. Если некоторая подстановка $p$ не изменяет многочлена $g_3$, то любое ее представление в виде произведения транспозиций должно содержать *четное* число транспозиций. Если же $p$ преобразует многочлен $g_3$ в $-g_3$, то любое представление ее с помощью транспозиций будет содержать нечетное число транспозиций. Отсюда мы заключаем, что одна и та же подстановка не может быть одновре-

менно записана в виде произведения четного и нечетного числа транспозиций.

*Подстановка* называется *четной*, если число транспозиций в любом из ее представлений четно; в противном случае она называется *нечетной*. Тождественную подстановку (единицу группы) будем считать четной, так как в нее не входит ни одна транспозиция. Четность или нечетность данной подстановки не зависит от ее конкретного представления с помощью транспозиций.

Упражнение 60. Покажите, что любая подстановка на множестве из $n$ символов может быть представлена в виде произведения, в которое могут входить лишь транспозиции $(a_1\ a_2)$, $(a_1\ a_3)$, ..., $(a_1\ a_n)$. Выведите отсюда, что эти $n-1$ транспозиций можно взять в качестве множества образующих группы $S_n$. [*Указание*: используйте следующее тождество: $(ab) = (ca)(cb)(ca)$.]

**Знакопеременные группы.** Множество $A_n$ всех четных подстановок на множестве из $n$ символов представляет особенный интерес. Ясно, что это *подмножество* симметрической группы $S_n$. Мы утверждаем, что $A_n$ является *подгруппой* группы $S_n$. Чтобы доказать это, проверим, что $A_n$ удовлетворяет двум условиям, характеризующим подгруппу.

(1) *Замкнутость*. Если $p_1$ и $p_2$ — подстановки из $A_n$, представимые в виде произведений $n_1$ и $n_2$ транспозиций соответственно, то их произведение $p_1p_2$ можно записать с помощью $n_1 + n_2$ транспозиций. Если $n_1$ и $n_2$ — четные числа, то и $n_1 + n_2$ четно, откуда можно заключить, что подстановка $p_1p_2$ четная и, следовательно, эта подстановка принадлежит $A_n$.

(2) *Обратимость*. Подстановка $p$ имеет обратную $p^{-1}$ (в группе $S_n$); $pp^{-1} = I$ можно представить только с помощью четного числа транспозиций, поскольку $I$ — четная подстановка. Значит, если $p$ — четная подстановка, то $p^{-1}$ также должна быть четной, т. е. у каждого элемента из группы $A_n$ есть обратный в $A_n$.

Подгруппа $A_n$ группы $S_n$ называется *знакопеременной группой.* Причины такого названия станут ясными в скором времени, когда мы обратимся к знакопеременным многочленам.

Порядок группы $S_n$ равен $n!$ (см. стр. 189). Мы утверждаем, что *порядок группы* $A_n$ *равен* $\frac{1}{2}n!$, *т. е.* $S_n$ *содержит* $\frac{1}{2}n!$ *четных подстановок и* $\frac{1}{2}n!$ *нечетных.*

Доказательство. Пусть $a$ — транспозиция из симметрической группы $S_n$ $(n>1)$, скажем $a=(1\ 2)=$ $=(1\ 2)\,(3)\,(4)\ \ldots\ (n)$. Умножим каждый элемент группы $S_n$ слева на $a=(1\ 2)$. В результате мы снова получим множество всех элементов из $S$ и ни один из них не повторяется дважды. (Это доказано в теореме 1, стр. 53.) Но произведение любой четной подстановки из $S_n$ и элемента (1 2) является нечетной подстановкой, а произведение нечетной подстановки и элемента (1 2) является четной подстановкой. Множество нечетных подстановок и множество четных при этом умножении взаимно однозначно отображаются одно на другое. Это возможно лишь при том условии, что количество четных и нечетных подстановок одинаково. Следовательно, порядок группы $A_n$ равен $\frac{1}{2}n!$, как и утверждалось.

В упр. 52 было доказано, что если $G$ — группа порядка $2n$ и $H$ — ее подгруппа порядка $n$, то последняя будет *нормальной* подгруппой группы $G$. Так как порядок группы $A_n$ равен $\frac{1}{2}n!$, а порядок группы $S$ равен $n!$, то *знакопеременная группа* $A_n$ *является нормальной подгруппой симметрической группы* $S_n$. Мы уже отмечали, что симметрические группы и нормальные подгруппы играют важную роль в теории Галуа о разрешимости алгебраических уравнений. Теоремы о строении знакопеременных групп — одна из основных составных частей этой теории.

*Геометрическая реализация группы* $A_3$. Симметрическая группа $S_3$ изоморфна группе диэдра $D_3$; см. стр. 188. Поэтому $S_3$ можно представлять геометрически как симметрии или самосовмещения равносто-

роннего треугольника; $A_3$ — подгруппа порядка $\frac{1}{2}\cdot 3! = 3$, которая содержит все четные подстановки группы $S_3$. Положения треугольника, изображенные на рис. 13.3 в верхнем ряду, соответствуют четным подстановкам, т. е. произведениям четного числа транспозиций вершин треугольника. Читатель может каждую транспозицию вершин представлять себе как опрокидывание треугольника относительно некоторой подходящей высоты. Положения треугольника, изображенные в верхней части рисунка, являются результатом четного числа опрокидываний, а положения в нижней части — результатом нечетного числа опрокидываний.

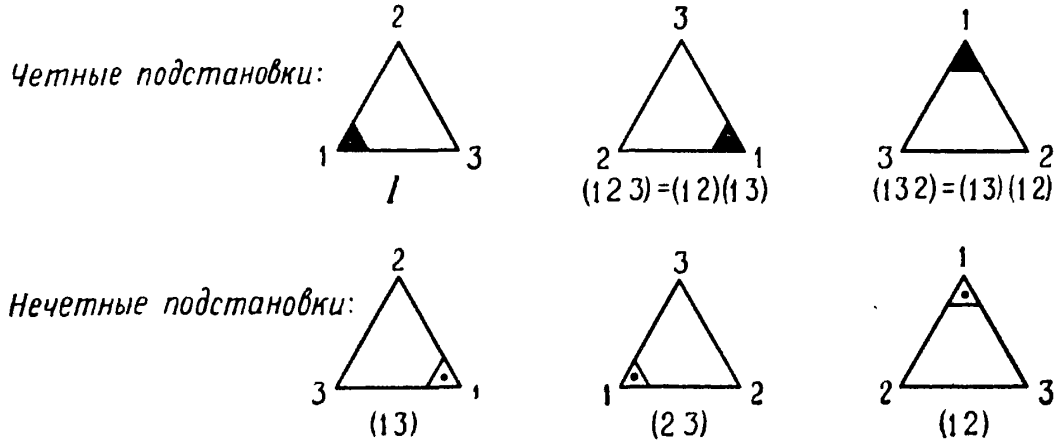



Рис. 13.3.

*Знакопеременные многочлены.* Существует тесная связь между знакопеременными группами и знакопеременными многочленами. В предыдущих рассуждениях о нечетных и четных подстановках мы ввели знакопеременный многочлен $g_3$. В качестве примера знакопеременного многочлена от двух переменных рассмотрим многочлен

$$g_2 = x_1 - x_2.$$

Если мы переставляем $x_1$ и $x_2$ *нечетное* число раз, то многочлен $g_2$ преобразуется в $-g_2$; если же $x_1$ и $x_2$ меняются местами *четное* число раз, то многочлен $g_2$ не меняется.

Совокупность всех подстановок на множестве из двух переменных $x_1$ и $x_2$ является симметрической группой $S_2$, и мы можем следующим образом перефор-

мулировать наше утверждение относительно многочлена $g_2 = x_1 - x_2$: *многочлен $g_2$ инвариантен относительно подстановок из знакопеременной группы $A_2$ и преобразуется в многочлен $-g_2$ под действием нечетных подстановок из группы $S_2$.*

Этот результат можно обобщить на случай знакопеременного многочлена $g_n$ от $n$ переменных, где

$$\begin{aligned} g_n = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4) \ldots (x_1 - x_n) \times \\ \times (x_2 - x_3)(x_2 - x_4) \ldots (x_2 - x_n) \times \\ \times (x_3 - x_4) \ldots (x_3 - x_n) \times \\ \ldots\ldots\ldots\ldots \\ \times (x_{n-1} - x_n). \end{aligned}$$

*Многочлен $g_n$ инвариантен относительно подстановок из знакопеременной группы $A_n$ и преобразуется в многочлен $-g_n$ под действием нечетных подстановок из группы $S_n$.*

Мы закончим этот раздел, посвященный знакопеременным группам, кратким обсуждением интересных свойств группы $A_4$, группы тетраэдра (см. стр. 155). В основном нас будет интересовать утверждение, обратное к теореме Лагранжа. На стр. 120 мы поставили такой вопрос: если порядок группы $G$ равен $g$, а $h$ — делитель числа $g$, то обязательно ли группа $G$ имеет подгруппу порядка $h$? Группу $A_4$ можно использовать для доказательства того факта, что это обращение *не* верно. Эта группа имеет порядок 12, но в ней нет подгрупп порядка 6. Таким образом, *утверждение, обратное к теореме Лагранжа, не верно.*

Однако некоторое достаточное условие для того, чтобы группа $G$ порядка $g$ имела подгруппу порядка $h$, где $h$ — делитель числа $g$, указывается в следующей теореме Силова [1]).

*Пусть $G$ — группа порядка $g$ и $h$ — делитель числа $g$; если $h = p^n$, где $p$ — простое число, а $n$ — положительное целое число, то $G$ содержит подгруппу порядка $h$.*

---

[1]) Л. Силов, норвежский математик, опубликовал эту теорему в 1872 г. Для частного случая $n = 1$ теорема была еще раньше доказана Коши.

Порядок группы $A_4$ равен 12; простыми делителями числа 12 являются 2 и 3. По теореме Силова мы можем лишь утверждать, что группа $A_4$ содержит подгруппы порядка 2, $2^2 = 4$ и 3, но ничего не можем сказать о подгруппе порядка 6.

Мы наметим основные шаги доказательства того факта, что группа $A_4$ не содержит подгруппы порядка 6. Читателю предлагается воспроизвести недостающие детали.

(1) Все элементы группы $A_4$ (кроме элемента $I$) имеют порядок 2 или 3. [*Указание*: рассмотрите представление каждого элемента с помощью *циклов*; см. упр. 62.]

(2) Ни один из элементов порядка 3 не принадлежит нормальной подгруппе. [*Указание*: покажите, что любой гомоморфизм, который отображает элемент порядка 3 группы $A_4$ в $I$, обязательно отображает в $I$ всю группу $A_4$.]

(3) Множество элементов порядка 2 из группы $A_4$ составляет *четверную группу* (порядка 4).

(4) Так как любая собственная нормальная подгруппа группы $A_4$ содержит только элементы порядка 2, то максимальный возможный порядок такой нормальной подгруппы равен *четырем*.

(5) *Группа $A_4$ не имеет подгрупп порядка* 6.

Упражнение 61. Докажите утверждение из п. (5), т. е. докажите, что группа $A_4$ не имеет подгрупп порядка 6. (Разумеется, можно использовать результаты предыдущих четырех пунктов.)

Упражнение 62. Рассмотрите подстановки на множестве символов $a$, $b$, $c$, $d$. Докажите, что (a) если $x = (a\,b\,c)$, то $x^3 = I$; (b) если $x = (a\,b)(c\,d)$, то $x^2 = I$. [Это упражнение связано с утверждением из п. (1); см. выше.]

В вопросах разрешимости алгебраических уравнений важную роль играет группа $A_5$, знакопеременная группа на пяти символах. Это группа икосаэдра, наименьшая неабелева группа, не содержащая собственных нормальных подгрупп. Некоторые сведения о группе $A_5$ и ее графе читатель найдет в приложении.

ГЛАВА 14

# ГРУППЫ ПУТЕЙ

**Пути в пространстве.** В этой главе мы рассмотрим *группы путей.* Мы хотим показать, что определение группы с помощью образующих и соотношений совершенно естественно возникает и при изучении некоторых топологических вопросов. Изложение понятий, связанных с группами путей, будет существенно опираться на пространственную интуицию читателя[1]).

Мы будем рассматривать замкнутые пути, которые начинаются и кончаются в фиксированной точке $P$ (*начальной*, или *базисной* точке) пространства. Термину «путь» мы отдаем предпочтение перед термином «кривая», подчеркивая тем самым, что на пути задано определенное направление. Это согласуется с нашими прежними рассмотрениями путей вдоль направленных отрезков графа группы. Форма пути для нас не существенна. Напротив, мы даже заинтересованы в допустимых изменениях его формы. Назовем два пути $a_1$ и $a_2$, исходящие из точки $P$, *равными* и будем говорить, что это «один и тот же путь», если путь $a_1$ можно при помощи непрерывной деформации превратить в путь $a_2$. Мы уже называли такие пути топологически эквивалентными (см. стр. 72). Они называются также *гомотопными.*

С первого взгляда может показаться, что все замкнутые пути равны, или гомотопны. Если взять точку $P$ в «пустом» пространстве, то любой замкнутый путь, исходящий из точки $P$, можно непрерывным образом (не допуская разрывов) стянуть в эту точку.

---

[1]) См. по этому поводу статью В. Г. Болтянского и В. А. Ефремовича «Очерк основных идей топологии» в сб. «Математическое просвещение», вып. 2—4, 6, 1959. — *Прим. перев.*

Если же в пространстве содержится «препятствие», то положение меняется. Предположим, например, что нам «запрещено» выходить за пределы некоторой плоскости и что в этой плоскости задан круг, через который не может проходить никакой путь. Тогда любой путь $a_1$, который не обходит этот круг, можно непрерывным образом стянуть в точку $P$. Но путь $a_2$, огибающий этот круг, нельзя ни стянуть в точку $P$, не «разрывая» пути и не проходя при этом через «запретную» область, ни деформировать в путь $a_1$ (см. рис. 14.1).

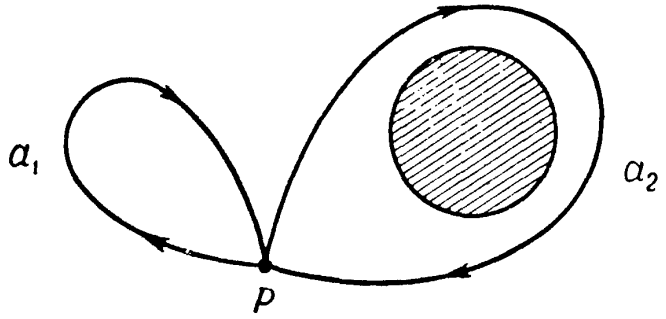



Рис. 14.1.

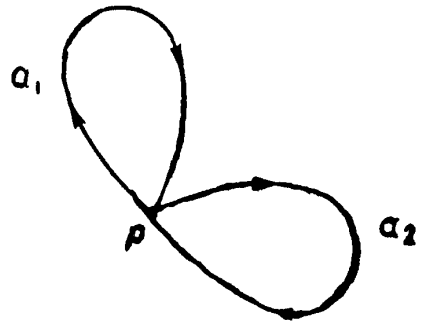



Рис. 14.2.

*Бинарная операция на путях в пространстве.* Рассмотрим теперь замкнутые пути в трехмерном пространстве и определим бинарную операцию для любых двух замкнутых путей $a_1$ и $a_2$, исходящих из точки $P$ (см. рис. 14.2), следующим образом:

(a) оторвем конечную точку пути $a_1$ от точки $P$ (рис. 14.3, *а*));

(b) оторвем начальную точку пути $a_2$ от точки $P$ (рис. 14.3, *б*));

(c) соединим конечную точку пути $a_1$ с начальной точкой пути $a_2$; в результате мы получим замкнутый путь (рис. 14.3, *в*)).

Назовем путь $b$ *произведением* путей $a_1$ и $a_2$ и будем писать $a_1a_2 = b$. Легко проверить, что эта операция ассоциативна.

Мы хотим построить группу, элементами которой являются множества или *классы* гомотопных путей, так что нам нужно определить бинарную операцию на *классах* путей. (Два замкнутых пути принадлежат *одному и тому же* классу, если их можно непрерывно деформировать один в другой.) Изучая классы путей,

мы будем использовать по одному элементу от класса в качестве *представителя* всего класса. (Аналогичные ситуации встречались нам и раньше, например на стр. 29 мы использовали одно вращение в качестве представителя целого класса $A$ вращений, а на стр. 86 — одно слово в качестве представителя целого класса эквивалентных слов.) Поэтому мы определим *произведение* двух классов гомотопных путей

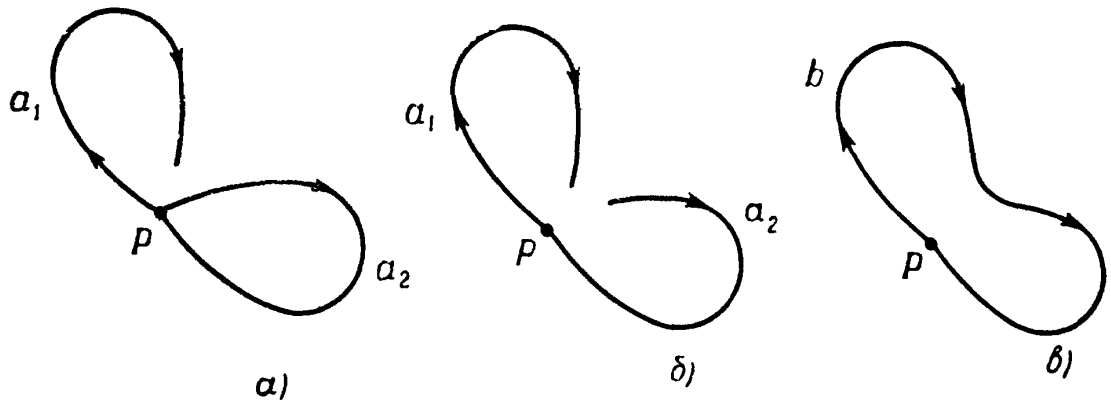



Рис. 14.3.

следующим образом: если $a_1$ — путь из первого класса, $a_2$ — путь из второго класса, а $b = a_1a_2$ — их произведение, то класс всех путей, гомотопных пути $b = a_1a_2$, будет произведением этих двух классов.

Следует проверить, что это определение корректно, т. е. что произведение двух классов не зависит от выбора путей-представителей в каждом из сомножителей. Пусть $a_1$ и $a_2$ — два пути и $b = a_1a_2$. Предположим, что $a_1^*$ — произвольный путь из того же класса, что и $a_1$ ($a_1^*$ можно непрерывной деформацией перевести в $a_1$), и $a_2^*$ — произвольный путь из того же класса, что и $a_2$. Интуиция подсказывает нам, что путь-произведение $b^* = a_1^*a_2^*$ гомотопен пути $b = a_1a_2$. Таким образом, произведение двух классов не зависит от того, какие конкретные пути $a_1$ и $a_2$ выбраны в качестве представителей этих классов.

Введем теперь в пространство некоторое «препятствие»: пути могут проходить через все точки трехмерного пространства, кроме точек, принадлежащих некоторой замкнутой кривой $A$. (Для определенности будем считать, что $A$ — окружность.) Чтобы наши

дальнейшие рассуждения были более понятными, советуем читателю представлять себе кривую $A$ как некую непреодолимую преграду. Множество точек трехмерного пространства, которое останется, если выкинуть точки, принадлежащие кривой $A$, называется *многообразием*. Рассмотрим замкнутые пути в многообразии, которые начинаются и кончаются в точке $P$, и определим их гомотопические классы. Мы изучаем пути, проходящие только через точки нашего многообразия, а $A$ рассматриваем как непреодолимую преграду. Тогда возникают по меньшей мере две существенно различные ситуации, которым соответствуют пути $a_1$ и $a_2$ на рис. 14.4 (разрыв на линии $A$

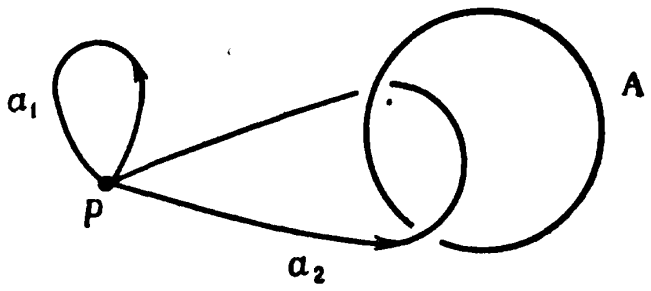



Рис. 14.4.

показывает, что путь $a_2$ проходит *над* $A$, а разрыв на пути $a_2$ — что он проходит *под* кривой $A$):

(1) путь $a_1$ *можно* стянуть в точку $P$ с помощью непрерывной деформации;

(2) путь $a_2$ *нельзя* непрерывно деформировать в точку $P$, не проходя через непреодолимую преграду.

Таким образом, существует по крайней мере два гомотопических класса замкнутых путей, исходящих из точки $P$: один класс состоит из всех путей, которые можно непрерывно деформировать в $P$ (он обозначается через $[I]$), а второй состоит из всех путей, которые можно непрерывно деформировать в путь $a_2$, но нельзя стянуть в $P$ (он обозначается через $[a]$). Пути из класса $[a]$ один раз зацепляют кривую $A$.

Мы использовали символ $[a]$ для обозначения совокупности всех путей, гомотопных пути $a_2$, т. е. всех путей, *один* раз зацепляющих окружность $A$, как показано на рис. 14.4. Произвольный путь из этого

множества, или класса, можно взять в качестве *представителя* всего этого класса. Мы будем употреблять для него символ $a$ (выбирать какой-либо специальный путь нет необходимости). Вообще, если $p$ — любой путь, то $[p]$ обозначает класс путей, гомотопных пути $p$.

*Обратный путь.* Покажем, что для любого класса $[b]$ гомотопных путей многообразия существует класс $[b]^{-1}$, обратный к $[b]$, такой, что произведение любого пути из $[b]$ и любого пути из $[b]^{-1}$ принадлежит классу $[I]$. Иными словами, $[I]$ оказывается единицей группы,

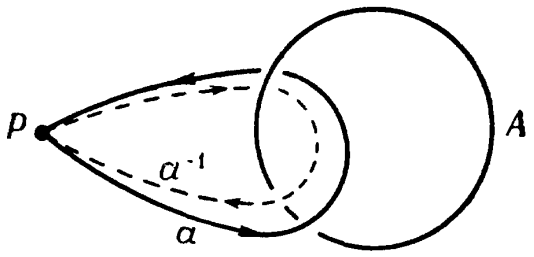



Рис. 14.5.

элементами которой являются классы гомотопных путей.

Опишем сначала путь, обратный к каждому отдельному пути, а затем покажем, что для любого пути, гомотопного данному, обратный путь лежит в том же самом классе, что и обратный к исходному пути. Если $b$ — произвольный путь, исходящий из точки $P$, то через $b^{-1}$ обозначим путь, полученный из пути $b$ лишь переменой направления. Покажем, что пути $bb^{-1}$ и $b^{-1}b$ принадлежат классу $[I]$ для любого пути $b$.

Рассмотрим, например, путь $a$ на рис. 14.5. Мы изобразили обратный к нему путь пунктирной линией. (На самом деле пунктирная и сплошная линии совпадают, на них лишь заданы противоположные направления; мы разделили их лишь для наглядности.) Образуем описанным ранее способом произведения $aa^{-1}$ и $a^{-1}a$. Получающиеся при этом пути изображены на рис. 14.6, *а*) и 14.6, *б*). (Здесь снова каждый из этих путей отличается лишь направлением, и для наглядности мы разделили их.) Нетрудно заметить, что вне зависимости от того, как данный путь $p$ расположен по отношению к окружности, пути $pp^{-1}$ и $p^{-1}p$

можно стянуть в точку. Ясно также, что любой сомножитель в произведении $pp^{-1}$ (или $p^{-1}p$) можно заменить некоторым эквивалентным ему путем, т. е. если путь $b$ гомотопен пути $p$, а $c$ гомотопен $p^{-1}$, то путь $bc$ можно стянуть в точку и он принадлежит классу

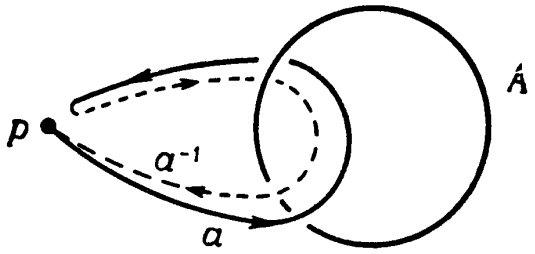



Рис. 14.6, *а*)

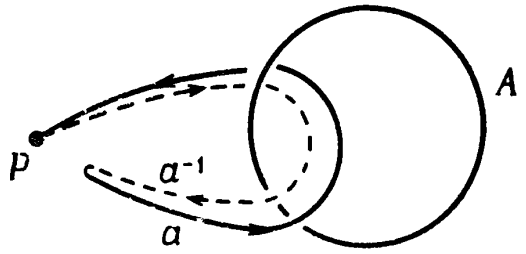



Рис. 14.6, *б*)

$[l]$. Таким образом, класс, обратный к классу гомотопных путей $[p]$, — это совокупность всех путей, гомотопных пути $p^{-1}$. Тогда произведение (в том виде, как оно было определено выше) любого класса и обратного к нему равно классу $[l]$. Читателю предоставляется проверить, что $[l]$ — единица, т. е. что $[l][b] = [b][l] = [b]$, где $[b]$—произвольный класс гомотопных путей.

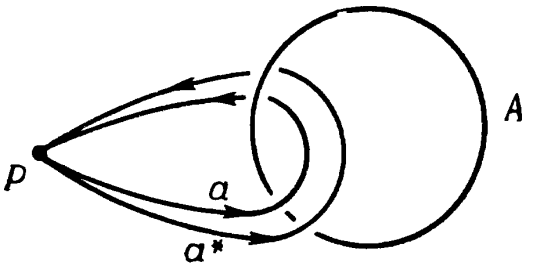



Рис. 14.7.

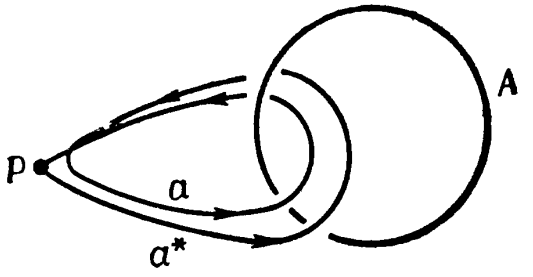



Рис. 14.8.

Рассмотрим теперь класс путей, представляемый элементом $aa$, или $a^2$. Так как произведение классов $[a]\cdot[a]$ не зависит от выбора того или иного представителя, мы образуем произведение двух разных путей из класса $[a]$; эти пути на рис. 14.7 помечены символами $a$ и $a^*$. Напоминаем, что произведение $a^*a$ получается соединением конечной точки пути $a^*$ с начальной точкой пути $a$; см. рис. 14.8. Заметим теперь, что путь $a^*a$ проходит над и под окружностью $A$ следующим образом (в направлении, указанном стрелками): он начинается в точке $P$, проходит *над* дугой

окружности $A$, затем *под* ней, затем снова *над* и снова *под* и возвращается в точку $P$. Таким образом, путь $a*a$, или путь $a^2$, дважды зацепляет окружность $A$. Его можно деформировать в путь, показанный на рис. 14.9, и, конечно, нельзя деформировать ни в путь класса $[l]$, ни в путь класса $[a]$. Путь $a^2$ принадлежит новому классу, который мы обозначим через $[a^2]$ или $[a]^2$. Представителем обратного к нему

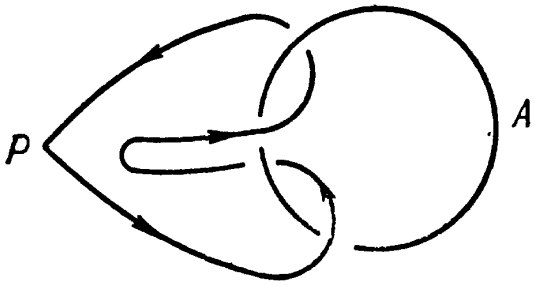



Рис. 14.9.

класса $[a^{-2}] = [a]^{-2}$ будет путь, который делает *двойную* петлю вокруг дуги окружности $A$ в направлении, противоположном направлению пути $a^2$. Другими словами, после выхода из точки $P$ путь $a^{-2}$ проходит сначала *под* $A$, затем *над* $A$, затем снова *под* и снова *над*, а потом возвращается в точку $P$.

Обозначим через $[a]^3$ класс путей, гомотопных произведению пути из $[a]^2$ и пути из $[a]$. Легко видеть, что путь из класса $[a]^3$ делает *тройную* петлю (трижды зацепляет $A$) вокруг дуги окружности $A$, а $[a]^{-3}$ — класс путей, которые *трижды* обходят вокруг дуги окружности $A$, но в противоположном направлении. Аналогичным образом можно построить классы $[a]^4$, $[a]^{-4}$, $[a]^5$, $[a]^{-5}$ и т. д.

Множество всех гомотопических классов путей в нашем многообразии образует группу.

*Элементы группы.* Классы замкнутых путей, которые можно непрерывно деформировать один в другой. Эти пути лежат в многообразии, определенном окружностью $A$; все они начинаются и кончаются в точке $P$.

*Ассоциативная бинарная операция.* Объединение в один путь двух путей-представителей посредством

соединения конечной точки первого с начальной точкой второго.

*Единица.* Класс $[I]$ замкнутых путей, которые можно непрерывно стянуть в точку $P$.

*Обратные элементы.* Каждому классу путей соответствует единственный обратный класс, такой, что произведение любой пары представителей этих классов принадлежит классу $[I]$.

Элементы этой группы — классы

$$\ldots, [a]^{-3}, [a]^{-2}, [a]^{-1}, [I], [a], [a]^2, [a]^3, \ldots.$$

Ясно, что наша группа порождается классом $[a]$ и изоморфна бесконечной циклической группе $C_\infty$.

*Многообразие, определенное двумя окружностями.* Рассмотрим теперь многообразие, которое получается

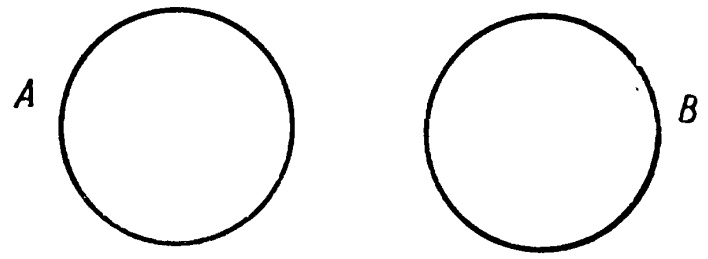



Рис. 14.10.

из трехмерного пространства выкидыванием двух непересекающихся и несцепленных окружностей; см. рис. 14.10. Оно состоит из всех точек трехмерного пространства, за исключением точек этих окружностей $A$ и $B$. Как и прежде, нас интересуют замкнутые пути в этом многообразии, начинающиеся и кончающиеся в фиксированной точке $P$ многообразия. Замкнутые пути, зацепляющие лишь одну из этих окружностей,—это пути уже рассмотренного нами типа. Обозначим классы таких путей, связанных с окружностью $A$, через $[a]$, $[a]^2$ и т. д, а связанных с окружностью $B$ — через $[b]$, $[b]^2$ и т. д. К новому типу приводят пути, зацепляющие обе окружности. Построим пути $ab$ и $ba$ и выясним, можно ли один из этих путей непрерывно деформировать в другой. Решить этот вопрос — все равно, что выяснить, будет ли группа

путей, связанная с нашим новым многообразием, коммутативной.

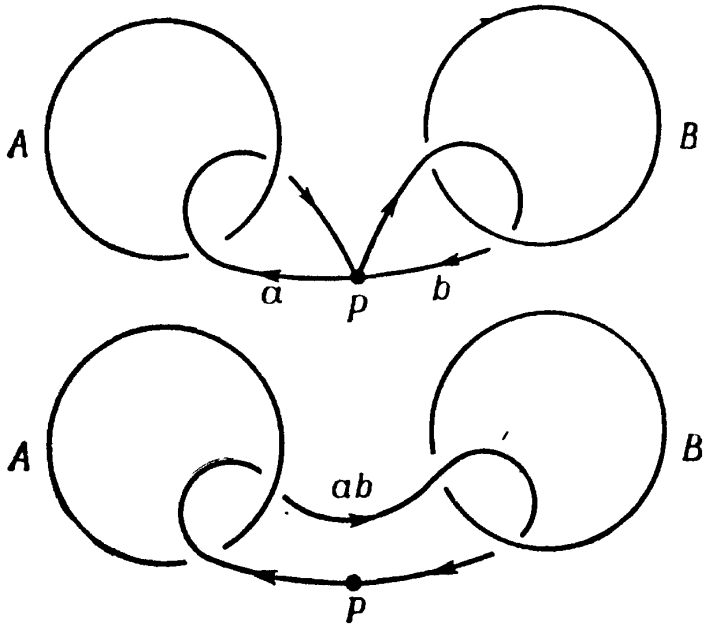



Рис. 14.11.

Чтобы найти путь $ab$, соединим конечную точку пути $a$ из класса $[a]$ с начальной точкой пути $b$ из класса $[b]$; см. рис. 14.11. Выпишем последователь-

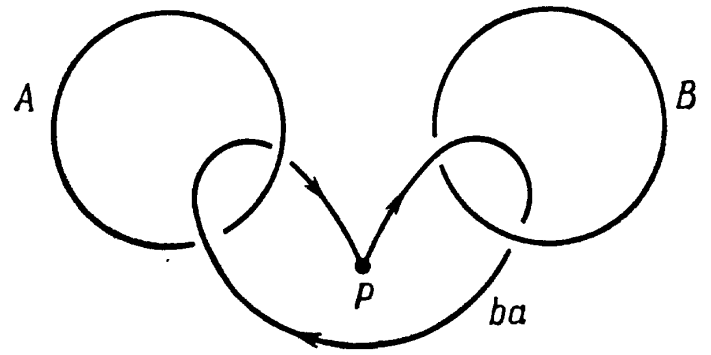



Рис. 14.12.

ность прохождения этих путей под и над соответствующими окружностями:

$$\underbrace{\text{над } A,\ \text{под } A}_{a} \qquad \underbrace{\text{над } B,\ \text{под } B}_{b}$$

Аналогично образуем путь $ba$; см. рис. 14.12. Распространим понятие *обратного* пути на наше новое многообразие. Назовем путь, который проходит по пути $ba$, но в направлении, противоположном его стрелкам, обратным к пути $ba$ и обозначим его через $(ba)^{-1}$. Мы

предоставляем читателю убедиться, что оба пути

$$(ba)(ba)^{-1} \quad \text{и} \quad (ba)^{-1}(ba)$$

можно стянуть в точку $P$, т. е. что оба они принадлежат классу $[I]$. Читатель может также проверить, используя рис. 14.13, что

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

Вернемся теперь к вопросу о коммутативности: равны ли пути $ab$ и $ba$, т. е. можно ли путь $ab$ не-

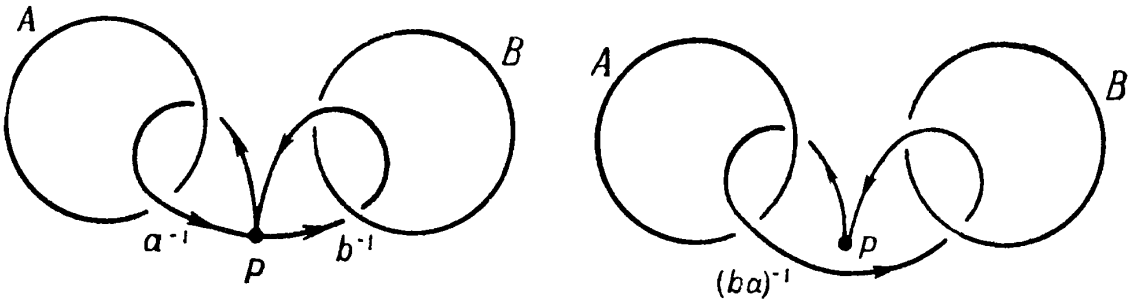



Рис. 14.13.

прерывно деформировать в путь $ba$? Используя то, что мы знаем об обратных путях, сформулируем этот вопрос так: выполняется ли в нашем многообразии соотношение

$$(ab)(ba)^{-1} = I, \quad \text{или} \quad aba^{-1}b^{-1} = I?$$

Чтобы ответить на этот вопрос, изучим путь $aba^{-1}b^{-1}$, изображенный на рис. 14.14. Он получается

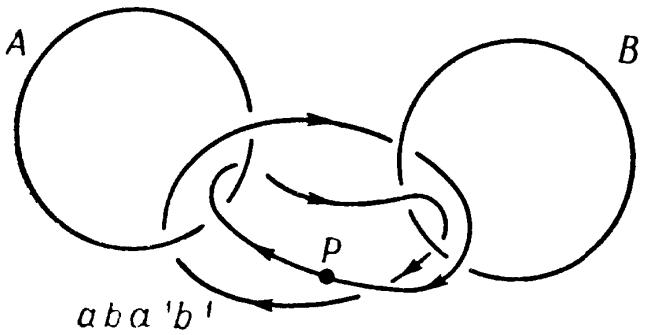



Рис. 14.14.

соединением конечной точки пути $ab$ с начальной точкой пути $a^{-1}b^{-1} = (ba)^{-1}$. Этот путь можно деформировать в путь, изображенный на рис. 14.15. (Здесь мы полагаемся на геометрическую интуицию читателя;

к тому же можно взять модель, сделанную из двух колец и куска бечевки, и убедиться в том, что это действительно так.) Путь такого типа, изображенный на рис. 14.14, называется *зацепленным* в многообразии, определенном двумя несцепленными окружностями $A$ и $B$. Таким образом, мы убедились, что путь

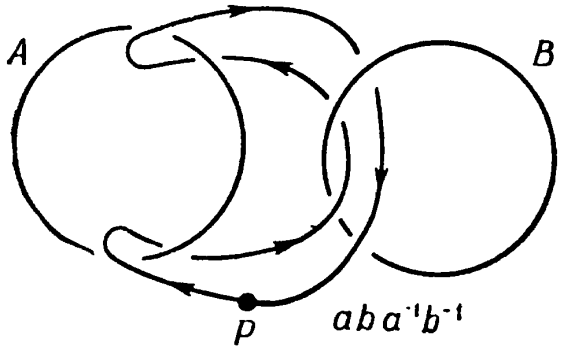



Рис. 14.15.

$aba^{-1}b^{-1}$ нельзя стянуть к точке $P$, и тем самым установили, что ассоциированная с нашим многообразием группа путей некоммутативна.

*Новое многообразие с двумя сцепленными окружностями.* Рассмотрим многообразие, определенное двумя сцепленными окружностями $A$ и $B$; см.

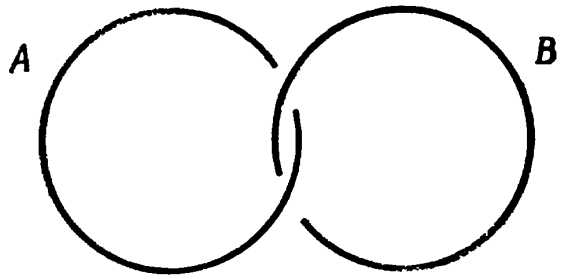



Рис. 14.16.

рис. 14.16. Теперь мы уже не можем стянуть одну из них в точку, не затронув другую. Как и раньше, наши классы состоят из путей в многообразии всех точек трехмерного пространства, за исключением точек, лежащих на окружностях $A$ и $B$. Снова мы рассматриваем лишь замкнутые пути, начинающиеся и кончающиеся в фиксированной точке $P$ этого многообразия.

Построим пути $ab$ и $ba$, чтобы выяснить, будет ли в этом новом многообразии выполняться равенство $ab = ba$. Тем же способом, что и раньше, строим путь

$aba^{-1}b^{-1}$. Заметим, что он проходит в нашем новом «сцепленном» многообразии через *те же точки*, через которые проходил соответствующий путь в прежнем «несцепленном» многообразии (ср. рис. 14.15 и 14.17). Мы утверждаем, что путь $aba^{-1}b^{-1}$ можно непрерывной деформацией стянуть в точку $P$, т. е. что путь $aba^{-1}b^{-1}$ принадлежит классу $[I]$.

Легче всего убедиться в этом, обратившись к модели. Если надеть петлю из бечевки на два сцепленных кольца так, как это показано на рис. 14.17 (петля

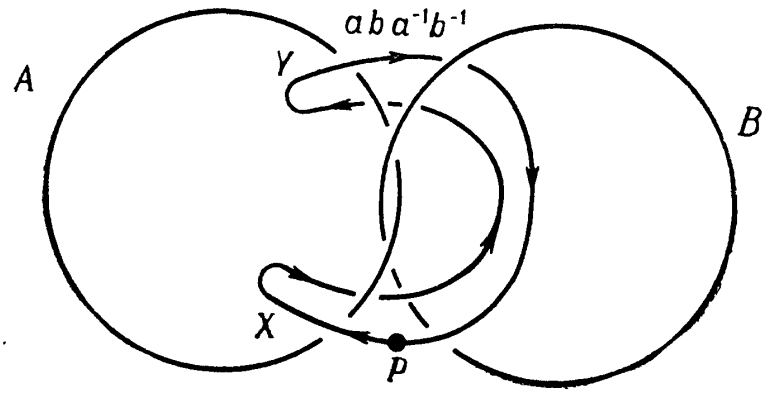



Рис. 14.17.

тогда изобразит путь $aba^{-1}b^{-1}$), то можно освободить бечевку от колец, не разрывая бечевки и не ломая колец. Чтобы убедиться в этом, подвинем петлю $X$ вдоль окружности $A$ в направлении против часовой стрелки к петле $Y$, проходя сначала *над* окружностью $B$, а затем *под* ней. Когда петля $X$ подойдет к $Y$, мы увидим, что *путь не зацепляет окружности* $B$. Относительно окружности $A$ путь расположен так: он начинается в точке $P$, проходит над $A$, под $A$, под $A$ и над $A$. Такая последовательность показывает, что *путь не зацепляет окружность* $A$. Таким образом, путь $aba^{-1}b^{-1}$ принадлежит классу $[I]$ и $[ab] = [a][b] = [b][a] = [ba]$.

Группа путей, соответствующая нашему многообразию, определенному двумя сцепленными окружностями, имеет две образующие — пути $a$ и $b$ (точнее, *классы* путей $[a]$ и $[b]$). Эти образующие удовлетворяют соотношению $aba^{-1}b^{-1} = I$. С такой группой мы уже встречались — это группа $C^2_\infty$, группа «городских улиц» (см. стр. 102).

*Зацепленные пути в многообразии.* Мы видели, что путь $aba^{-1}b^{-1}$ в многообразии, определенном двумя несцепленными окружностями, *зацеплен*, но тот же путь, рассматриваемый как путь в многообразии, определенном двумя сцепленными окружностями, *не зацеплен.* Таким образом, будет ли данный путь зацеплен, зависит не только от пути, но и от многообразия, в котором он расположен [1]).

[1]) Рисунки 14.15 и 14.17 позволяют продемонстрировать такой фокус. Возьмите два кольца, которые можно замыкать и размыкать, и наденьте на них кусок бечевки так, как это показано на рис. 14.15. Связав концы, вы получите замкнутую петлю. Петля в этот момент зацеплена вокруг обоих колец. Затем разомкните одно кольцо, скажем $B$, и сцепите его с кольцом $A$ так, чтобы получилась конфигурация, изображенная на рис. 14.17. В этом новом многообразии петля не зацеплена, и ее можно снять с колец, ко всеобщему изумлению.

ГЛАВА 15

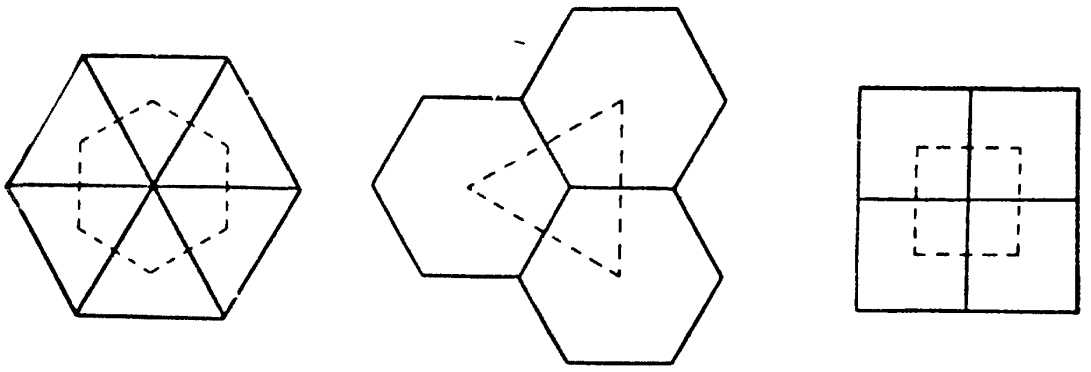
# ГРУППЫ И ОРНАМЕНТЫ

Как мы видели, изучение групп приводит по существу к рассмотрению некоторых основных структур и соотношений между ними. Поэтому неудивительно, что с конкретными реализациями групп так часто приходится сталкиваться в декоративном искусстве. Фактически покрывающий всю плоскость узор, составленный из повторяющихся частей, каждая из которых воспроизводит один и тот же основной рисунок, соответствует некоторой группе. Узоры (орнаменты) такого типа часто используют для обоев, тканей, в архитектурных украшениях и т. п. Таким образом, в повседневной жизни мы, можно сказать, постоянно окружены группами. Чрезвычайно полно такие группы представлены в архитектуре дворца Альгамбра в Гренаде. Мавританские зодчие, строившие его в тринадцатом веке, использовали в декоративном убранстве дворца узоры, соответствующие всем возможным «группам орнаментов» (распространимых на всю плоскость).

Отметим, к сведению читателей, что всего существует двадцать четыре группы орнаментов; графы семи из них представляют собой периодически повторяющийся рисунок, заполняющий лишь бесконечную полосу в плоскости, графы остальных семнадцати заполняют всю плоскость.

Эти группы иногда называют плоскими кристаллографическими группами, так как расположение атомов на гранях кристаллических пород (в кристаллах кварца, например) представляет собой какую-либо из повторяющихся конфигураций «орнаментного» типа.

В этой главе мы ограничимся рассмотрением орнаментов, связанных с графами, которые заполняют всю плоскость. Одним из способов построения таких орнаментов является «замощение» плоскости равными правильными многоугольниками. Можно показать, что существует лишь три возможности такого рода, показанные на рис. 15.1 (см. упр. 63). Отметим, что две первые конфигурации двойственны друг другу в том



*Треугольники* *Шестиугольники* *Квадраты*

Рис. 15.1.

смысле, что точки, служащие центрами многоугольников, из которых состоит один орнамент, являются вершинами многоугольников второго орнамента; третья конфигурация двойственна сама себе.

Упражнение 63. Предположим, что плоскость «замощена» правильными $n$-угольниками так, что два соседних многоугольника имеют в точности одно общее ребро. Покажите, что $n$ может принимать лишь значения 3, 4 и 6.

Нас интересуют не столько сами исходные конфигурации, по которым строится орнамент, сколько соответствующие им группы. Как мы увидим, те или иные орнаменты связаны со структурой некоторых групп движений; элементы такой группы перемещают *фундаментальную область* (исходную конфигурацию) так, чтобы получалось полное покрытие плоскости, подобно тому как пол покрывается плитками одинаковой *основной* формы. Пусть наша фундаментальная область — это квадрат $S$. Рассмотрим два основных его движения:

$r$ — сдвиг квадрата $S$ вправо на длину его стороны (рис. 15.2);

$s$ — сдвиг квадрата $S$ вверх на длину его стороны (рис. 15.3).

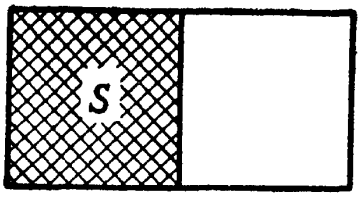



Рис. 15.2.
Положение области $S$ в результате движения $r$.

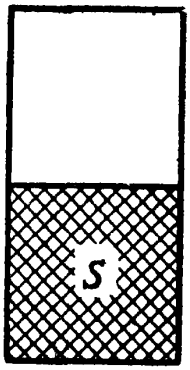
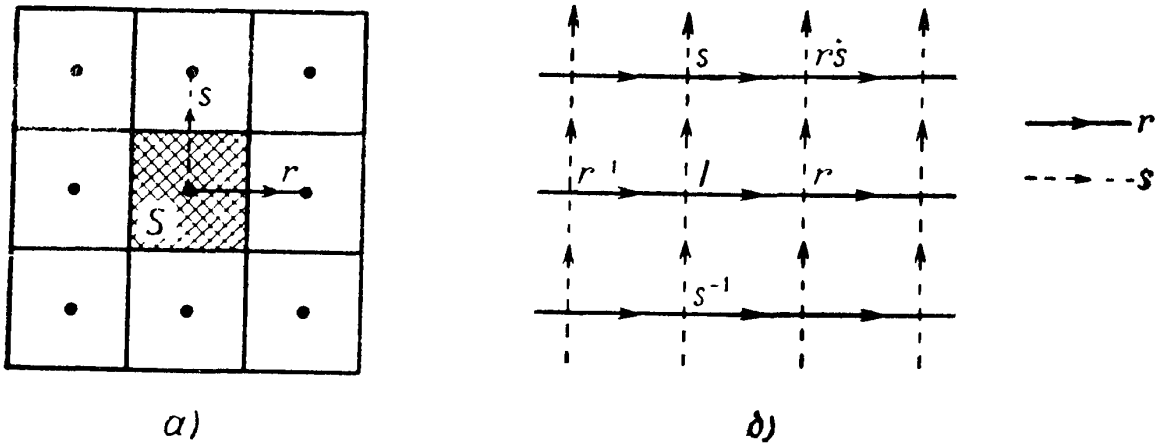



Рис. 15.3.
Положение области $S$ в результате движения $s$.

Можно покрыть плоскость областями, равными $S$, используя все возможные произведения двух порождающих движений. [*Замечание.* Наше «произведение» — это результат применения операции последовательного выполнения. Так как у нас есть всего одна




*а)* *б)*

Рис. 15.4.
*а)* Фундаментальная область $S$ и ее сдвиги с помощью $r$ и $s$.
*б)* Граф группы с образующими $r$ и $s$ и определяющим соотношением $rsr^{-1}s^{-1} = 1$.

фундаментальная область, а мы хотим заполнить всю плоскость, то мы представляем себе, что $S$ оставляет свой «отпечаток» на каждом из мест, в которое она попадает.] На рис. 15.4, *а*) показана часть плоскости, покрытая квадратами с помощью образующих движений $r$ и $s$. На рисунке отмечены образы центра

основной области. Отметим, что эти точки-образы соответствуют вершинам графа группы таких движений фундаментальной области, при которых ее образы покрывают всю плоскость. Читатель легко распознает в этой группе группу «городских улиц» $C_\infty^2$ (см. стр. 102).

Мы должны четко представлять себе различие между двумя рисунками. На рис. 15.4, *а*) изображена картина заполнения плоскости дубликатами фундаментальной области $S$, в то время как рисунок 15.4, *б*) изображает *граф группы движений*, а именно таких сдвигов области $S$, в результате которых создается

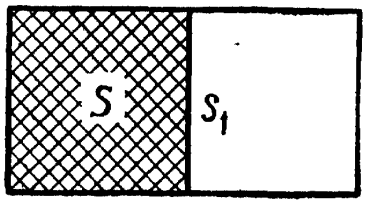



Рис. 15.5.
Положение области $S$ в результате движения $a$.

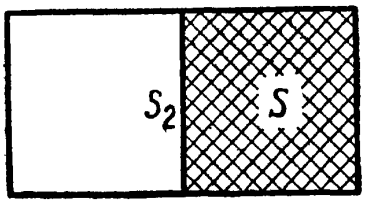



Рис. 15.6.
Положение области $S$ в результате движения $b$.

эта картина «шахматной доски». Причиной сходства этих двух изображений является отношение двойственности между ними (одно получается из другого следующим образом: каждому многоугольнику нужно поставить в соответствие его центр и соединить полученные точки отрезками; вспомните куб и октаэдр; стр. 189).

Мы можем заполнить образами нашей области бесконечную «шахматную доску» также с помощью движений, отличных от сдвигов. Это означает, что *различные группы могут быть связаны с одним и тем же покрытием плоскости квадратами.* Например, пусть $a$ — опрокидывание области $S$ относительно ее стороны $s_1$; см. рис. 15.5. Тогда движение $aa = a^2$ возвращает квадрат $S$ в исходное положение, т. е. $a^2 = I$. Аналогично, если $b$ обозначает опрокидывание области $S$ вокруг стороны $s_2$ (см. рис. 15.6), то $b^2 = I$. Результат последовательного выполнения движений $a$ и $b$ (в различном порядке) показан на рис. 15.7.

Конечно, $a$ и $b$ не перестановочны между собой. Предположим теперь, что мы ввели в рассмотрение третье основное движение $c$: *сдвиг* квадрата $S$ вверх на длину его стороны. С помощью трех движений $a$, $b$ и $c$ получается *в точности та же картина* замощения пло-

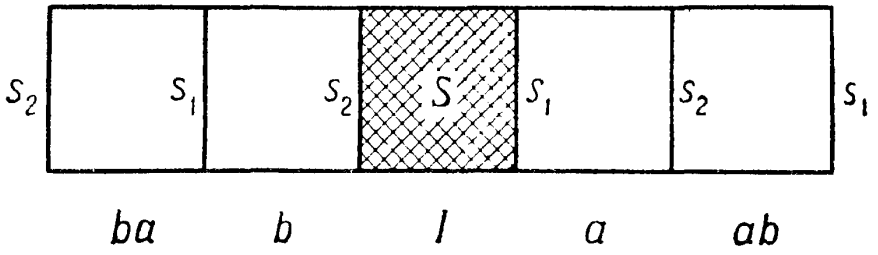



Рис. 15.7.

скости («шахматная доска»), что и с помощью двух сдвигов $r$ и $s$, но *соответствующие группы различны.* Граф группы, порожденной движениями $a$, $b$ и $c$, показан на рис. 15.8.

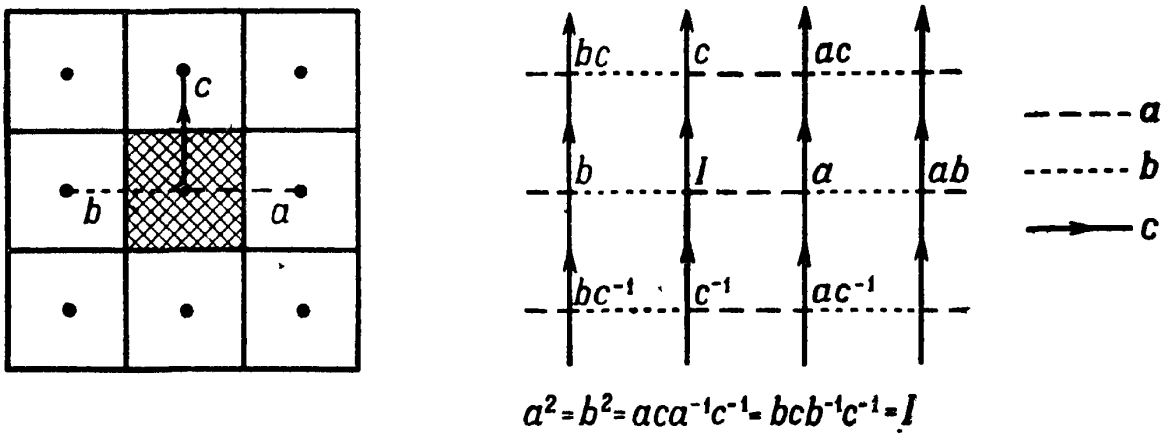



Рис. 15.8.

Выберем теперь другую фундаментальную область — равнобедренный прямоугольный треугольник, а за образующие движения примем:

$r$ — вращение на 90° (против часовой стрелки) вокруг вершины прямого угла (см. рис. 15.9);

$s$ — вращение на 180° вокруг середины гипотенузы (рис. 15.10). Ясно, что порядок элемента $r$ равен четырем, а $s$ — двум.

Движения $r$ и $s$ фундаментального равнобедренного прямоугольного треугольника задают некоторое покрытие плоскости. Получающаяся при этом кар-

тина и граф соответствующей группы движений изображены на рис. 15.11. Заметим, что этот последний граф дает новый план замощения плоскости — многоугольниками двух типов, а не одного. Здесь в каждой вершине сходятся квадрат и два восьмиугольника.

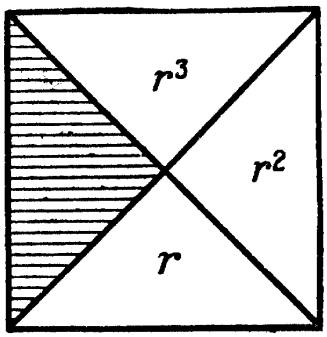



Рис. 15.9.

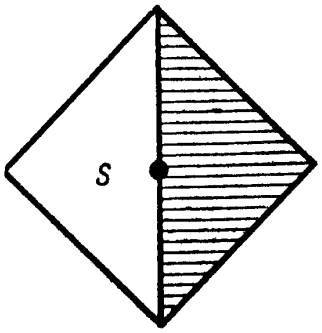



Рис. 15.10.

Как же в общем случае получаются орнаменты? Они получаются из графов групп движений, осуществляющих полное покрытие плоскости некоторой фундаментальной областью. Орнамент, определённый

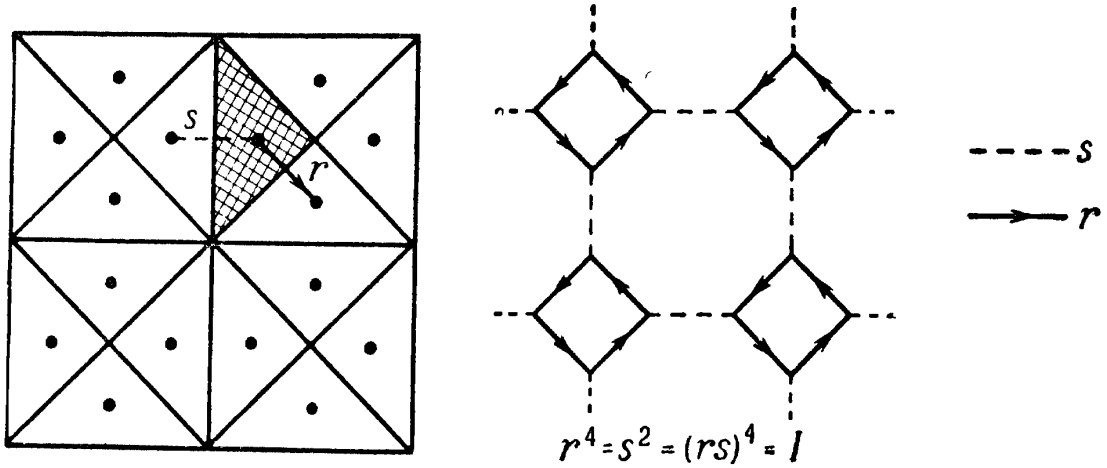



Рис. 15.11.

графом, изображенным на рис. 15.11, показан на рис. 15.12.

Приведем еще один пример орнамента, заполняющего всю плоскость, в образовании которого принимают участие геометрические фигуры нескольких типов. Возьмем в качестве фундаментальной области ромб, один из углов которого равен 60°, а в качестве образующих — два движения:

$r$ — вращение на 120° (против часовой стрелки) вокруг вершины одного из углов в 120°;

$s$ — вращение на 120° (против часовой стрелки) вокруг вершины другого угла в 120°.

Заметим, что $r^3 = s^3 = I$; см. рис. 15.13.

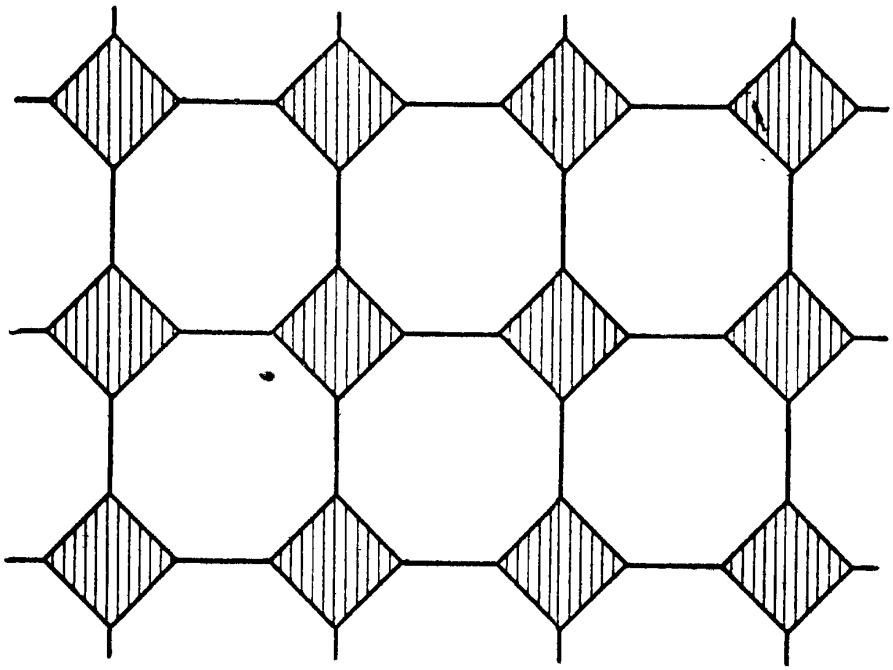


Рис. 15.12.
Один из семнадцати различных орнаментов.

На рис. 15.14 изображены покрытие плоскости ромбами и граф группы движений, порожденной элементами $r$ и $s$.

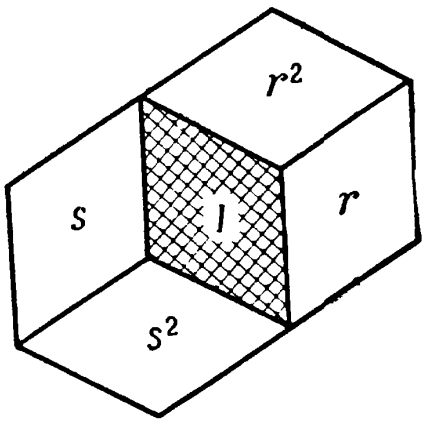



Рис. 15.13.

Упражнение 64. Найдите множество определяющих соотношений для этой группы с образующими $r$ и $s$.

Граф на рис. 15.14 показывает, что наша схема орнамента в каждой вершине имеет два различных треугольника (один — состоящий из $r$-отрезков и другой — из $s$-отрезков) и два шестиугольника.

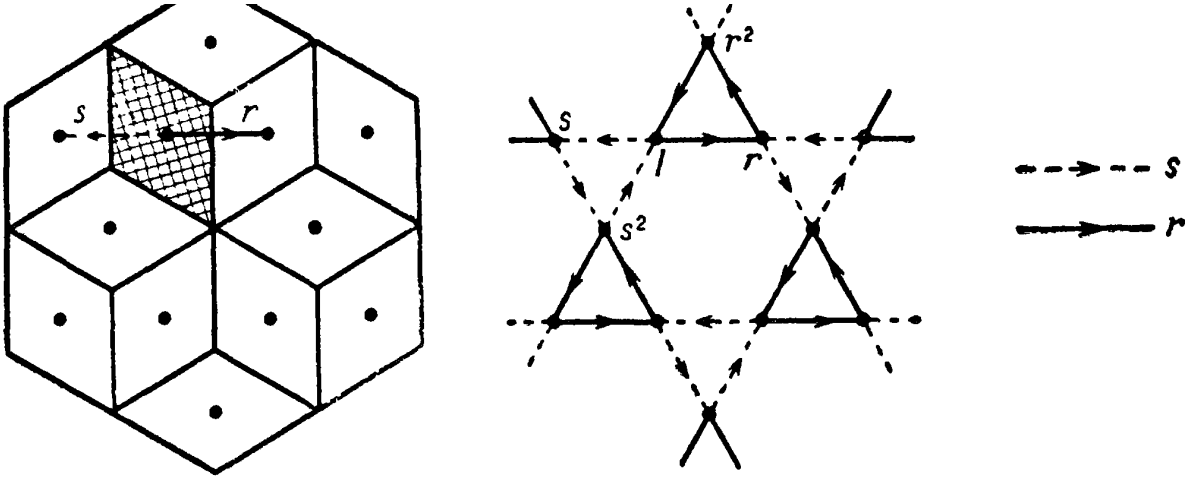



Рис. 15.14.

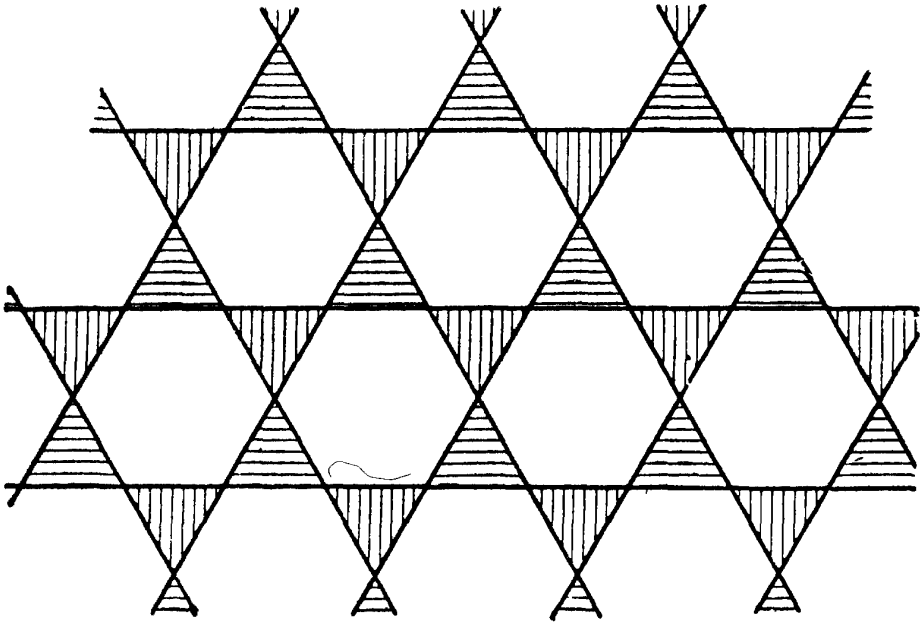


Рис. 15.15.

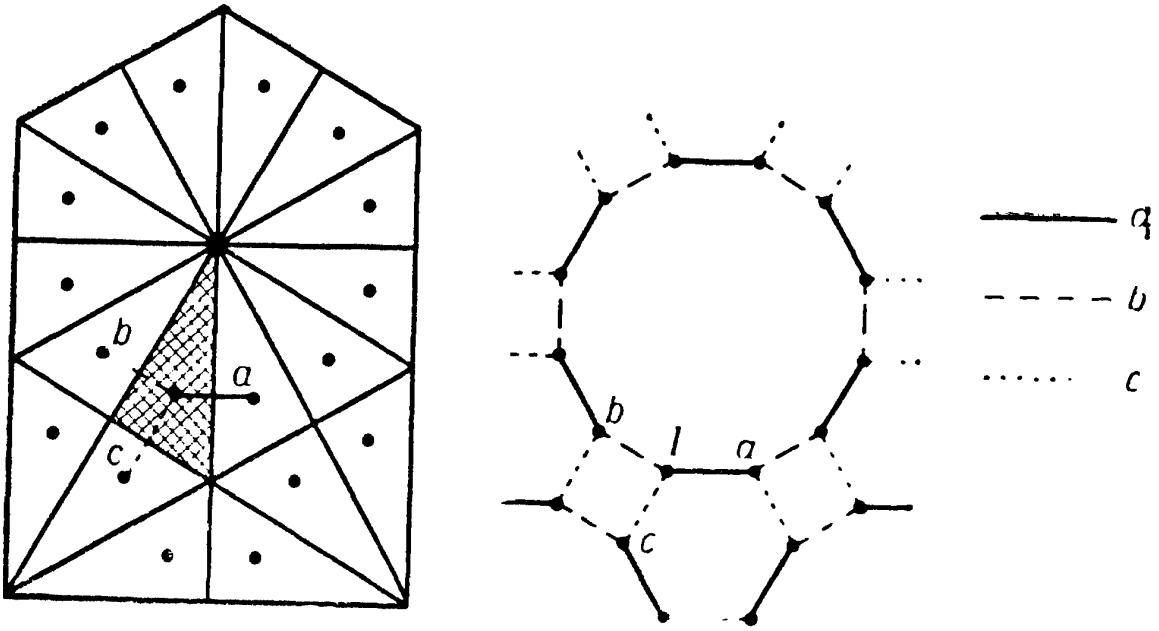



Рис. 15.16.

Рис. 15.15 на несколько большей площади изображает соответствующий орнамент.

В заключение рассмотрим пример такой кристаллографической группы, что в каждой вершине ее графа сходятся многоугольники трех типов. В качестве фундаментальной области здесь взят треугольник

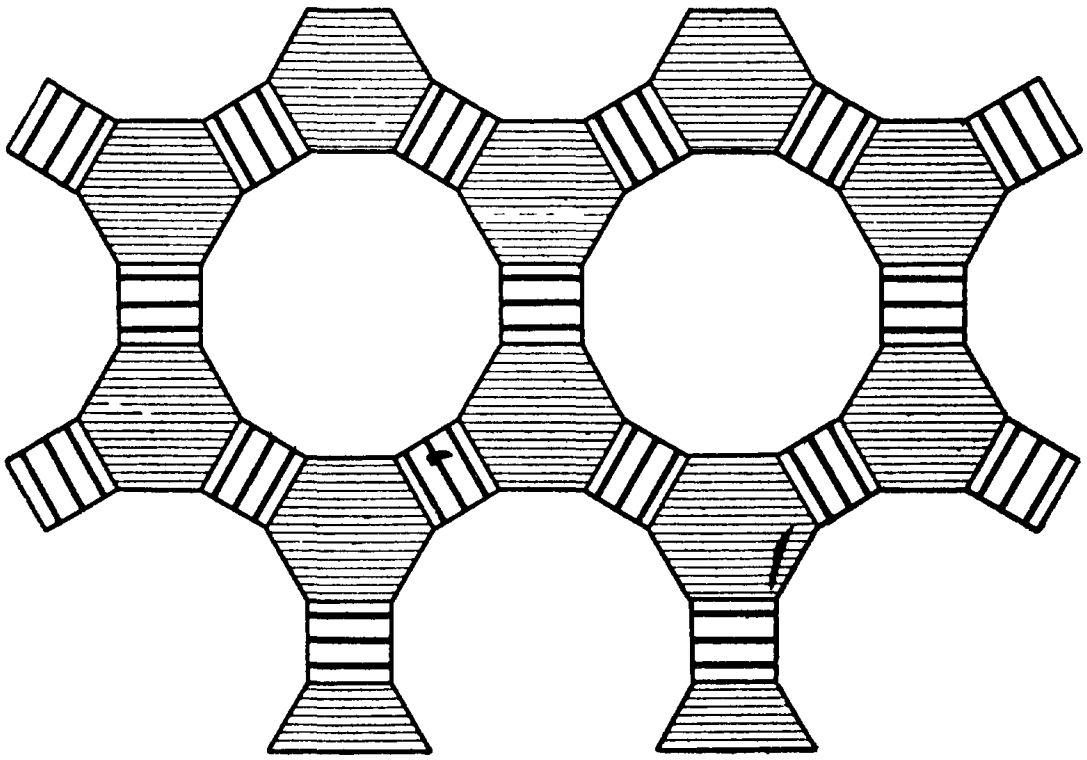


Рис. 15.17.

с углами 30°, 60° и 90°, а в качестве образующих движений — опрокидывания относительно каждой из трех сторон треугольника. Рис. 15.16 показывает, что граф этой группы заполняет всю плоскость, причем в каждой его вершине сходятся квадрат, шестиугольник и двенадцатиугольник. Орнамент, соответствующий этому графу, представлен на рис. 15.17.

Упражнение 65. Найдите множество определяющих соотношений для этой группы с образующими $a$, $b$ и $c$.

ПРИЛОЖЕНИЕ

# ГРУППА ДОДЕКАЭДРА И ИКОСАЭДРА: ЗНАКОПЕРЕМЕННАЯ ГРУППА $A_5$ ПОРЯДКА 60

Структура группы, связанной с додекаэдром и икосаэдром, существенно отличается от структуры всех групп, которые мы изучали до сих пор. Галуа, исследуя разрешимость алгебраических уравнений, обнаружил, что хотя у группы движений правильного икосаэдра много собственных подгрупп, *но ни одна из них не является нормальной подгруппой.* Группа, не имеющая собственных нормальных подгрупп, называется *простой.*

Группы самосовмещений додекаэдра и икосаэдра изоморфны друг другу, поскольку эти фигуры *двойственны* (стр. 189) — «центры» двенадцати правильных пятиугольников, составляющих грани додекаэдра, являются вершинами икосаэдра, а «центры» двенадцати равносторонних треугольников, образующих грани икосаэдра, являются вершинами додекаэдра. Группы самосовмещений обеих фигур «совпадают».

Определим теперь число элементов в группе икосаэдра. Для этого зафиксируем положение одной из вершин икосаэдра; вращение на 72° против часовой стрелки (имеющее порядок 5) порождает все самосовмещения, которые оставляют на месте указанную вершину; см. рис. 16.1. Поскольку в это положение может быть переведена любая из двенадцати вершин, то *порядок группы икосаэдра равен* 60 [1]).

Порядок группы $A_5$ равен $\frac{1}{2} \cdot 5! = 60$ (см. стр. 194), и мы утверждаем, что группа икосаэдра изоморфна

---

[1]) Это следует из того, что все движения, переводящие некоторую вершину $c$ в вершину $a$, образуют смежный класс по подгруппе, состоящей из движений, оставляющих $a$ на месте. — *Прим. ред.*

группе $A_5$. В справедливости этого утверждения читатель сможет убедиться, следуя тому методу доказательства, который кратко изложен в оставшейся части приложения.

Мы введем в рассмотрение множество, состоящее из пяти геометрических объектов и обладающее тем свойством, что любое самосовмещение икосаэдра вызывает *четную* подстановку на этом множестве. У икосаэдра 30 ребер и 15 *медиан*, т. е. отрезков, соединяющих вершины противоположных ребер. В правильном икосаэдре эти пятнадцать медиан разбиваются на пять множеств, каждое состоящее из трех взаимно перпендикулярных медиан, т. е. на пять *ортогональных триад*. Самосовмещения икосаэдра вызывают четные подстановки на множестве этих пяти триад; действительно, каждое самосовмещение принадлежит к одному из следующих трех типов:

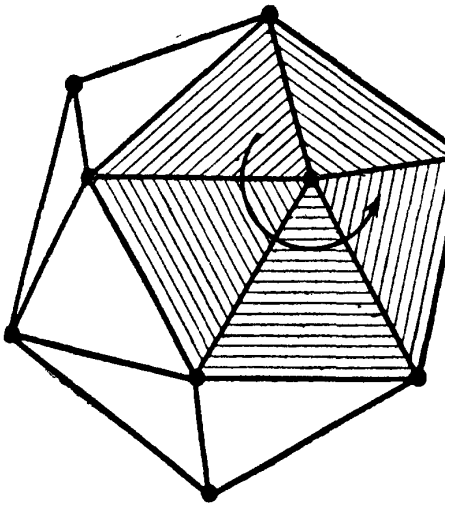


Рис. 16.1.

| *Самосовмещения* | *Четные подстановки* |
|---|---|
| (1) Вращение вокруг диагонали, соединяющей противоположные вершины | Циклическая перестановка пяти триад, т. е. $(abcde) = (ab)(ac)(ad)(ae)$ |
| (2) Вращение вокруг отрезка, соединяющего центры двух противоположных граней | Циклическая перестановка трех из пяти триад, т. е. $(abc) = (ab)(ac)$ (каждая из остальных двух переходит в себя) |
| (3) Вращение вокруг медианы | Перестановка двух пар триад, т. е. $(ab)(cd)$ |

Всего существует 24 движения типа (1) (каждое из них имеет *порядок* 5), 20 движений типа (2) (каждое *порядка* 3) и 15 движений типа (3) (*порядка* 2).

Чтобы найти граф группы икосаэдра, прежде всего представим эти самосовмещения графически подобно тому, как мы поступали в случае тетраэдра (см. стр. 155). Начнем с того, что изобразим усеченный

икосаэдр, т. е. икосаэдр, у которого каждая вершина заменена пятиугольником, соответствующим вращению $r$ порядка 5. Линии, соединяющие вершины этих двенадцати пятиугольников, соответствуют опрокидываниям порядка 2, замещающим вершины, лежащие на оси, вокруг которой происходят вращения.

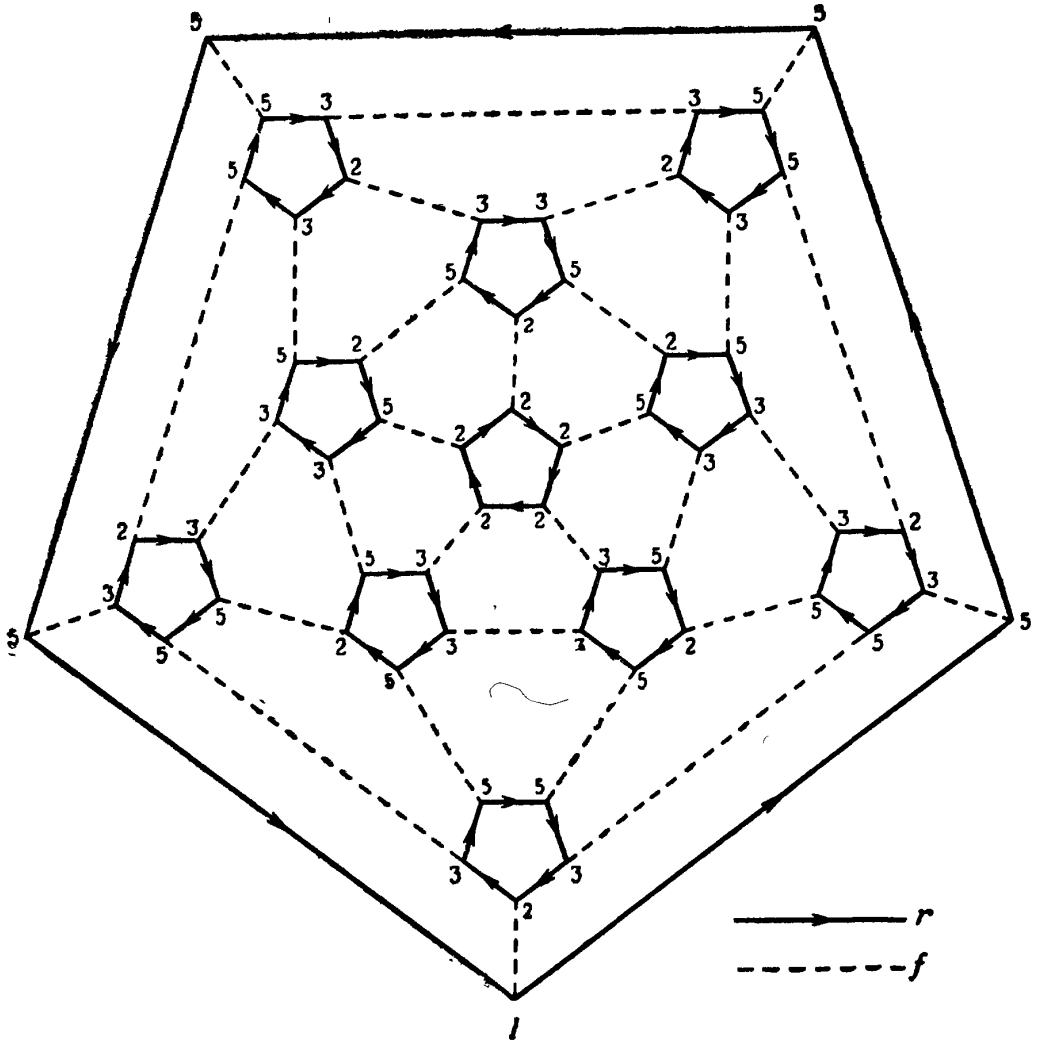



Рис. 16.2.

Чтобы превратить эту конфигурацию в плоскую сеть, мы поместим внутри одного из пятиугольников все остальные и придем, наконец, к сети, изображенной на рис. 16.2.

Мы предлагаем читателю изучить внутреннюю структуру этой группы; здесь окажет помощь граф группы, играющий роль компактной таблицы умножения. Чтобы навести читателя на некоторые соображения по поводу этой структуры, мы поставили при каждой вершине графа цифру, указывающую порядок соответствующего элемента группы. (Элемент $I$ выбран произвольным образом.) С помощью этого гра-

фа группы $A_5$ можно показать, что группа икосаэдра порождается двумя элементами $r$ и $f$ и определяется тремя соотношениями

$$r^5 = I, \quad f^2 = I, \quad (rf)^3 = I.$$

Исходя из такого задания группы, можно установить, что $A_5$ — *простая* группа. Для этого прежде всего нужно доказать, что если $g$ — произвольный гомоморфизм группы $A_5$, то как соотношение $g(r) = I$, так и соотношение $g(f) = I$ влекут за собой равенство $g(a) = 0$ для всех элементов $a$ из группы $A_5$; затем нужно убедиться в том, что если $g(x) = I$ для некоторого элемента $x$ группы $A_5$, то либо $g(r) = I$, либо $g(f) = I$.

**Упр. 1.** (a) Нет. (b) Да. (c) Нет. (d) Да.

**Упр. 2.** Вращение $b \otimes c$ — это вращение по часовой стрелке на 450°. Оно переводит квадрат в то же положение, что и вращение по часовой стрелке на 90°; таким образом, $b \otimes c = a$. Вращение $a \otimes c$ представляет собой вращение на 360°; оно возвращает квадрат в исходное положение.

**Упр. 3.** 0 является единицей, так как $x + 0 = 0 + x = x$ для любого действительного числа $x$.

**Упр. 4.** Мы сразу же видим, что обратным к 1 является элемент 1; действительно,

$$1 \cdot 1 \equiv 1 \pmod{p}.$$

Пусть $x \not\equiv 1$ — одно из чисел 2, 3, 4, ..., $p - 1$; рассмотрим $p$ целых чисел $x$, $x^2$, $x^3$, ..., $x^p$. Так как числа $x$ и $p$ не имеют общих делителей (взаимно просты), ни одно из этих $p$ чисел не делится на $p$; следовательно, остатки от деления этих чисел на $p$ находятся среди $p - 1$ чисел 1, 2, ..., $p - 1$, и хотя бы два из них, скажем $x^r$ и $x^s$, дают один и тот же остаток. Для определенности пусть $0 < r < s \leqslant p$. Тогда

$$x^s - x^r = x^r (x^{s-r} - 1) \equiv 0 \pmod{p},$$

где $x^r \not\equiv 0 \pmod{p}$, $x^s \not\equiv 0 \pmod{p}$ и $x^s - x^r > 0$. Поскольку $x^r (x^{s-r} - 1) \equiv 0 \pmod{p}$ и $x^r \not\equiv 0 \pmod{p}$, то

$$x^{s-r} - 1 \equiv 0 \pmod{p}.$$

(Здесь мы используем тот факт, что $ab$ сравнимо с нулем по модулю простого числа $p$ тогда и только тогда, когда или $a \equiv 0 \pmod{p}$, или $b \equiv 0 \pmod{p}$; читателю следует проверить это утверждение и сформулировать его иначе, используя понятие кратных числа $p$.)

Пусть теперь $y$ — остаток от деления числа $x^{s-r-1}$ на $p$. Тогда

$$x^{s-r-1} \equiv y \pmod{p},$$

и если мы умножим обе части этого сравнения на $x$, то получим

$$x^{s-r} \equiv xy \pmod{p}.$$

[Следует проверить, что если $a \equiv b \pmod p$, то $xa \equiv xb \pmod p$.] С другой стороны, мы показали, что $x^{s-r} - 1 \equiv 0 \pmod p$, откуда следует, что

$$x^{s-r} \equiv 1 \pmod p.$$

Поэтому $xy \equiv 1 \pmod p$.

**Упр. 5.** (a) Умножая слева на элемент $a^{-1}$, получаем равенство $bx = a^{-1}c$. Затем умножаем слева на $b^{-1}$ и получаем $x = b^{-1}a^{-1}c$. (b) $x = a^{-1}cb^{-1}$. (c) $x = cb^{-1}a^{-1}$. (d) Умножим обе части первого соотношения справа на $x$; тогда $ax = bx^3 = bI = b$, или $ax = b$; следовательно, $x = a^{-1}b$. (e) $I = x^4 = ax$, значит, $x = a^{-1}$. (f) Умножаем слева на $x$ и получаем $I = xabc$. Повторным умножением справа на соответствующие элементы мы последовательно получаем

$$c^{-1} = xab, \quad c^{-1}b^{-1} = xa, \quad x = c^{-1}b^{-1}a^{-1}.$$

**Упр. 6.** Из основных свойств таблицы умножения и групповых аксиом получаем:

(a) $vw = I$, или $w^{-1} = v$; $uw = s$, или $u = sw^{-1} = sv$; $vz = r$, или $z = v^{-1}r$; таким образом, $x = uz = (sv)(v^{-1}r) = sr$.

(b) $uw = I$, или $u^{-1} = w$; $uz = r$, или $z = u^{-1}r = wr$; $vw = s$, или $v = sw^{-1}$; таким образом, $x = vz = (sw^{-1})(wr) = sr$.

(c) $uz = I$, или $u^{-1} = z$; $uw = s$, или $w = u^{-1}s = zs$; $vz = r$, или $v = rz^{-1}$; таким образом, $x = vw = (rz^{-1})(zs) = rs$.

| | $w$ | $z$ |
|---|---|---|
| $u$ | $s$ | $x$ |
| $v$ | $I$ | $r$ |

(a)

| | $w$ | $z$ |
|---|---|---|
| $u$ | $I$ | $r$ |
| $v$ | $s$ | $x$ |

(b)

| | $w$ | $z$ |
|---|---|---|
| $u$ | $s$ | $I$ |
| $v$ | $x$ | $r$ |

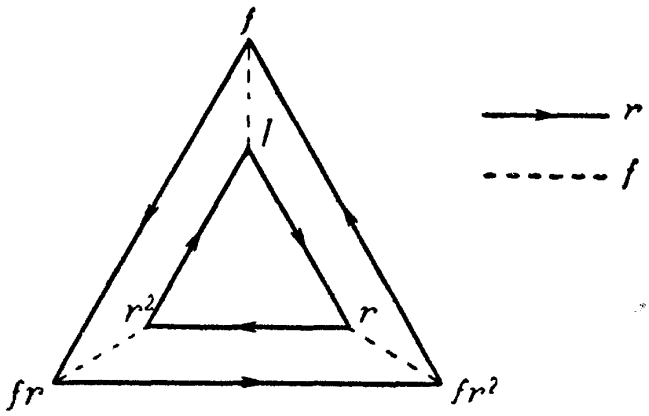
(c)

**Упр. 7.**

| | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

**Упр. 8.** (a) Циклическая группа. (b) Циклическая группа. (c) Не является группой, так как не содержит единицы аддитивной группы, а именно нуля. (d) Циклическая группа.

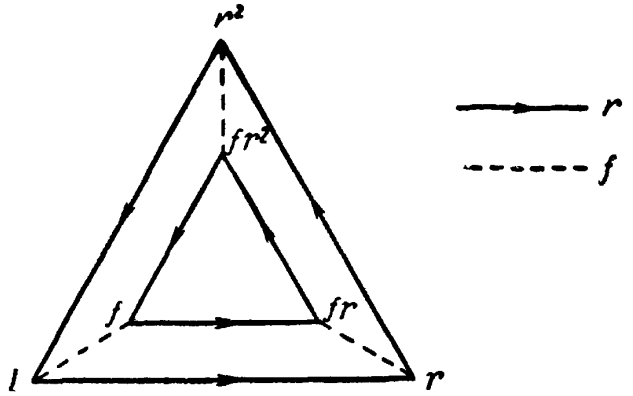
**Упр. 9.**




**Упр. 10.**

| | $I$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
|---|---|---|---|---|---|---|
| $I$ | $I$ | $r$ | $r^2$ | $f$ | $fr$ | $fr^2$ |
| $r$ | $r$ | $r^2$ | $I$ | $fr$ | $fr^2$ | $f$ |
| $r^2$ | $r^2$ | $I$ | $r$ | $fr^2$ | $f$ | $fr$ |
| $f$ | $f$ | $fr$ | $fr^2$ | $I$ | $r$ | $r^2$ |
| $fr$ | $fr$ | $fr^2$ | $f$ | $r$ | $r^2$ | $I$ |
| $fr^2$ | $fr^2$ | $f$ | $fr$ | $r^2$ | $I$ | $r$ |

Таблица умножения показывает, что мы имеем дело с группой. (Например, каждый элемент $a$ имеет единственный обратный, т. е. такой элемент $a^{-1}$, что $aa^{-1} = a^{-1}a = I$.) Отметим, что группа коммутативна.




**Упр. 11.** Слово $rsr$ соответствует следующим путям (за начальные точки берутся последовательно $A$, $B$, $C$):

из $A$ в $B$ в $C$ в $A$ — *замкнутый;*

из $B$ в $C$ в $B$ в $C$ — *незамкнутый;*

из $C$ в $A$ в $A$ в $B$ — *незамкнутый.*

**Упр. 12.** Как следствие соотношения $frfr^{-2} = I$ получаем

$$r^2 = Ir^2 = (frfr^{-2})\, r^2 = frf.$$

Отсюда вытекает, что $fr^2f = f(frf)f$, или, поскольку $f^2 = I$, что $fr^2f = r$; значит,

$$r^2 = (fr^2f)\,(fr^2f) = fr^4f.$$

Следовательно, $fr^4f = frf$, откуда вытекает, что $r^4 = r$ и $r^3 = I$. Наконец,

$$I = r^3 = r\,(r^2) = r\,(frf),$$

что дает оставшееся соотношение из множества $A$.

**Упр. 13.** (a) Мы можем записать

$$(y^3)^2 = (xyx^{-1})\,(xyx^{-1}) = xy\,(x^{-1}x)\,yx^{-1} = xy^2x^{-1},$$
$$(y^3)^3 = (xy^2x^{-1})\,(xyx^{-1}) = xy^3x^{-1}.$$

Заменяя $y^3$ в правой части второго уравнения на $xyx^{-1}$, получим

$$x\,(xyx^{-1})\,x^{-1} = y^9, \quad \text{или} \quad x^2yx^{-2} = y^9.$$

Так как соотношение $x^2 = I$ влечет за собой равенство $x^{-2} = I$, то мы можем отсюда заключить, что $y = y^9$, или $y^8 = I$, как и утверждалось. (Порядок элемента $y$ *не превосходит* 8.)

(b) Имеем $y^{2n} = (y^n)^2 = (xyx^{-1})\,(xyx^{-1}) = xy^2x^{-1}$. Аналогично, $y^{3n} = (y^n)^3 = xy^3x^{-1}$. Продолжая таким же образом, приходим к соотношениям

$$(y^n)^n = y^{n^2} = xy^nx^{-1} = x\,(xyx^{-1})\,x^{-1} = x^2yx^{-2} = y \ (\text{так как } x^2 = I).$$

Следовательно, $y^{n^2} = y$ и $y^{n^2-1} = I$. (Таким образом, порядок элемента $y$ *не превосходит* $n^2 - 1$.)

**Упр. 14.** (a) Используем тот же метод, что и в упр. 13. Имеем

$$(uvu^{-1})\,(uvu^{-1}) = (v^4)^2, \quad \text{или} \quad uv^2u^{-1} = (v^4)^2.$$

Продолжая таким же образом, получаем последовательно $uv^3u^{-1} = (v^4)^3$ и $uv^4u^{-1} = (v^4)^4$. Заменяя $v^4$ на $uvu^{-1}$, приходим к равенству $u(uvu^{-1})u^{-1} = v^{16}$, или $u^2vu^{-2} = v^{16}$. Так как мы знаем, что $u^3 = I$, но ничего не знаем относительно $u^2$, то мы должны продолжать такое последовательное умножение, пока в левой части не появится $u^3$. Таким образом,

$$(u^2vu^{-2})\,(u^2vu^{-2}) = (v^{16})^2, \quad \text{или} \quad u^2v^2u^{-2} = (v^{16})^2.$$

Далее, мы последовательно получаем $u^2v^3u^{-2} = (v^{16})^3$ и $u^2v^4u^{-2} = (v^{16})^4$. Отсюда

$$u^2\,(uvu^{-1})\,u^{-2} = (v^{16})^4, \quad \text{или} \quad u^3vu^{-3} = v^{64}.$$

Из того что $u^3 = I$, мы можем теперь заключить, что $v = v^{64}$, или $v^{63} = I$. Таким образом, порядок элемента $v$ не превосходит 63.

(b) Поступаем, как и раньше;

$$v^{2k} = (v^k)^2 = (uvu^{-1})(uvu^{-1}) = uv^2u^{-1};$$
$$v^{k^2} = (v^k)^k = uv^ku^{-1} = u(uvu^{-1})u^{-1} = u^2vu^{-2}.$$

Тогда

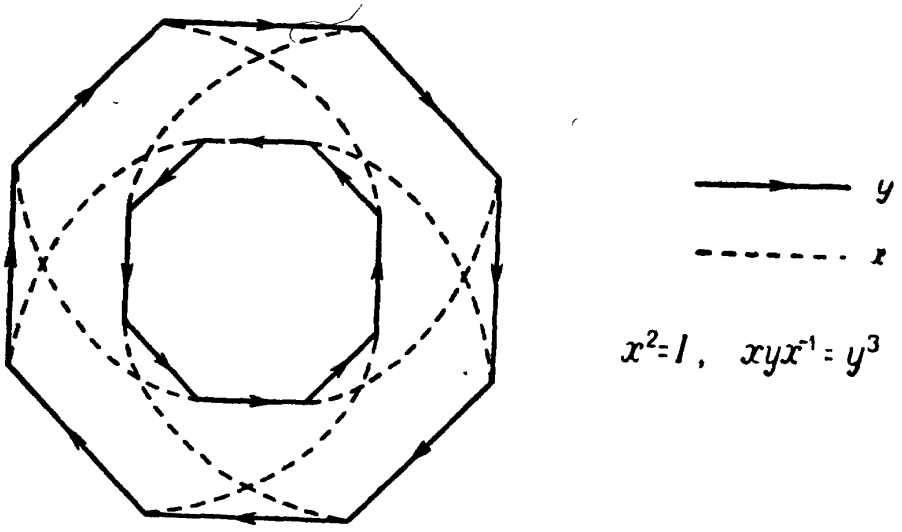
$$(v^{k^2})^k = (u^2vu^{-2})^k = u^2v^ku^{-2} = u^2(uvu^{-1})u^{-2} = u^3vu^{-3},$$

т. е. $v^{k^3} = u^3vu^{-3}$. Продолжая таким же образом, приходим к равенствам

$$v^{k^m} = u^mvu^{-m} = v \quad (\text{так как } u^m = I),$$

т. е. $v^{k^m-1} = I$; порядок элемента $v$ не превосходит $k^m - 1$. [*Замечание:* упражнения 13 и 14 иллюстрируют соотношение, справедливое в любой группе: $(uvu^{-1})^n = uv^nu^{-1}$.]

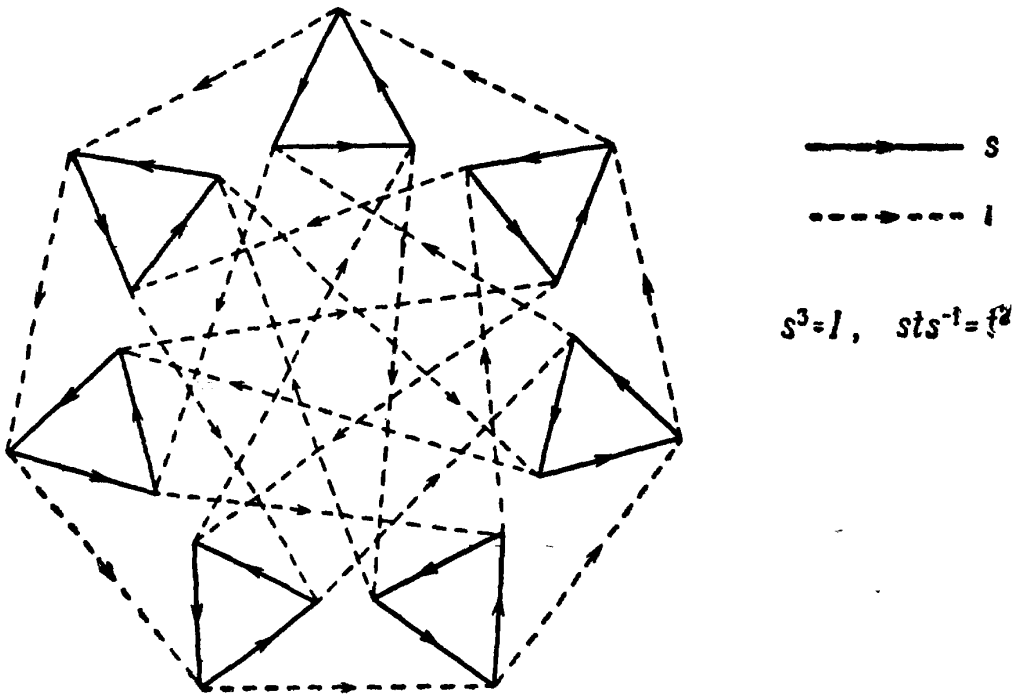
**Упр. 15.** Из упр. 13 мы знаем, что $y$ — элемент конечного порядка и $y^8 = I$. Это подсказывает выбор восьмиугольника в качестве основной фигуры графа. Метод решения становится теперь очевидным, и мы в конце концов приходим к следующему графу:




**Упр. 16.** Из упр. 14 мы знаем, что порядок элемента $t$ не превосходит $k^n - 1$. Пусть $r$ — порядок $t$. (Мы предполагаем, что $r > 1$, так как в противном случае приходится иметь дело с особым случаем $t = I$.) Из того что $t^r = I$, получаем равенство $t^{-1} = t^{r-1}$. Аналогично, соотношение $s^n = I$ влечет за собой $s^{-1} = s^{n-1}$. (Здесь мы снова предполагаем, что $n > 1$, чтобы исключить тривиальный случай $s = I$.) Следовательно, в любом слове $W$ можно заменить $s^{-1}$ на $s^{n-1}$ и $t^{-1}$ на $t^{r-1}$ и, значит, любое слово, определяющее элемент нашей группы, может быть выражено через положительные степени элементов $s$ и $t$. Теперь можно умножить заданное соотношение $sts^{-1} = t^k$ справа на $s$ и получить соотношение $st = t^ks$. Таким образом, в любом слове мы можем последовательность символов $st$ заменить на $t^ks$. Если повторять эту процедуру в данном слове, содержащем последова-

тельность символов $st$, то в конце концов мы придем к слову, в котором все степени элемента $t$ стоят слева от степеней элемента $s$. Таким образом, любой элемент в нашей группе можно записать как слово вида $t^x s^y$. Кроме того, для значения $x$ существует лишь $r$ возможностей (так как $t^r = I$), а для $y$ — лишь $n$ возможностей; следовательно, в группе не более чем $rn$ различных элементов. Так как $r \leqslant k^n - 1$, то порядок нашей группы не превосходит $(k^n - 1)n$.

**Упр. 17.** Из решения упр. 14 следует, что $t^7 = I$. Но так как 7 — простое число, то порядок элемента $t$ равен 7 [1]). Результат упр. 16 позволяет заключить, что порядок нашей группы равен 21. Граф нашей группы можно строить, основываясь на трех семиугольниках или на семи треугольниках (соответствующих соотношениям $s^3 = I$ и $t^7 = I$). Здесь изображен граф нашей группы порядка 21, основанный на семи треугольниках:




**Упр. 18.** Мы можем использовать граф группы $C_2 \times C_3$ (рис. 7.6), чтобы вычислить следующие степени элемента $g = fr$:

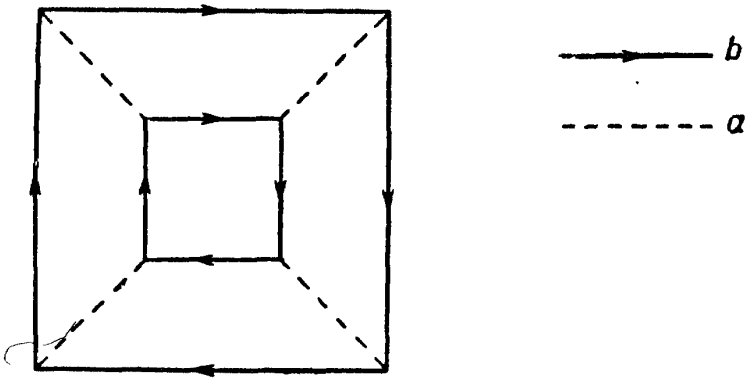
$$g = fr; \qquad g^4 = (fr)^4 = (r^2)^2 = r;$$
$$g^2 = (fr)^2 = r^2; \qquad g^5 = (fr)^5 = (fr)\,r = fr^2;$$
$$g^3 = gg^2 = (fr)\,r^2 = f; \qquad g^6 = (g^3)^2 = f^2 = I.$$

Таким образом, $g$ порождает циклическую группу $C_6$.

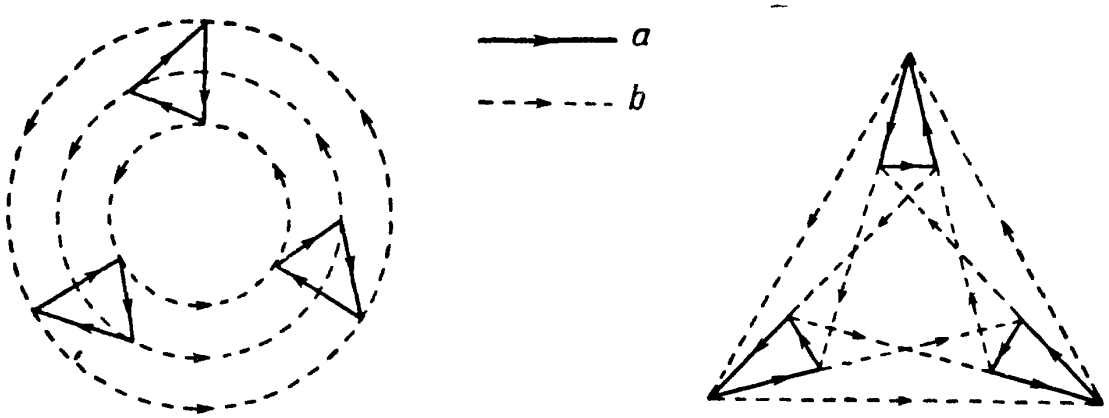
---

[1]) Действительно, если $t^a = I$, то $a$ делится на порядок $d$ элемента $t$. Если бы это было не так, то, поделив $a$ на $d$, мы получили бы $a = dq + r$, где $0 < r < d$. Но тогда бы мы имели $t^r = t^{a-dq} = t^a (t^d)^{-q} = I$, что противоречит определению порядка элемента. В частности, в нашем случае 7 должно делиться на порядок элемента $t$, т. е. $d$ действительно равен 7. — *Прим. ред.*

**Упр. 19.** (a) Группа $C_2 \times C_4$ получается из группы $C_2$ (с образующей $a$ и определяющим соотношением $a^2 = I$) и группы $C_4$ (с образующей $b$ и определяющим соотношением $b^4 = I$). По определению прямого произведения групп $a$ и $b$ должны коммутировать, т. е. $ab = ba$, или $aba^{-1}b^{-1} = I$. Таким образом, группа $C_2 \times C_4$ имеет образующие $a$ и $b$, связанные соотношениями $a^2 = b^4 = aba^{-1}b^{-1} = I$. Этим соотношениям соответствует граф коммутативной группы порядка 8:




(b) Группа $C_3 \times C_3$ получается из группы, порожденной элементом $a$, удовлетворяющим соотношению $a^3 = I$, и группы, порожденной элементом $b$, удовлетворяющим соотношению $b^3 = I$. Так как $a$ и $b$ в группе $C_3 \times C_3$ коммутируют, то $aba^{-1}b^{-1} = I$. Таким образом, группа $C_3 \times C_3$ порождается элементами $a$ и $b$, удовлетворяющими соотношениям $a^3 = b^3 = aba^{-1}b^{-1} = I$. Для этой группы порядка 9 мы имеем два таких графа:




(Будут ли они топологически эквивалентны?)

**Упр. 20.** $C_2$: $a^2 = I$. $D_3$: $r^3 = f^2 = (rf)^2 = I$. Так как элемент $a$ перестановочен в группе $C_2 \times D_3$ и с $r$ и с $f$, то $ara^{-1}r^{-1} = I$ и $afa^{-1}f^{-1} = I$. Если в группе $C_2 \times D_3$ существуют такие элементы $x$ и $y$, что $x^6 = y^2 = (xy)^2 = I$ (определяющие соотношения группы $D_6$), то $D_6$ содержится в $C_2 \times D_3$. Поскольку равенство $ar = ra$ влечет за собой $(ar)^2 = a^2r^2 = r^2$ и порядок элемента $r^2$ равен 3, то порядок элемента $ar = x$ равен 6. Обозначим через $y$ элемент $f$. Выясним, будет ли $(xy)^2 = (arf)^2 = I$. Имеем

$$(arf)^2 = a^2 (rf)^2 = I \cdot I = I.$$

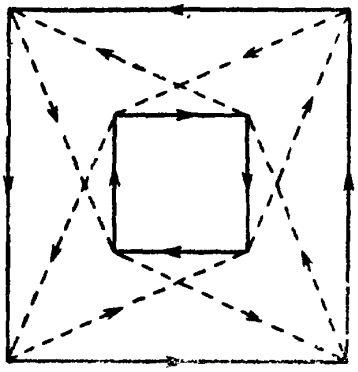
Таким образом, элементы $x = ar$ и $y = f$ удовлетворяют определяющим соотношениям группы $D_6$, и последняя содержится в группе $C_2 \times D_3$.

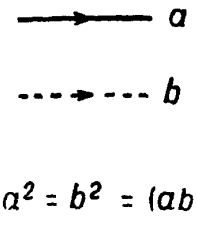
Для доказательства того, что $D_6 = C_2 \times D_3$, надо только показать следующее: группа $C_2 \times D_3$ содержит столько же элементов, сколько группа $D_6$ (а именно 12). Так как $a$ перестановочен с $r$ и с $f$, то любое слово от этих трех образующих эквивалентно слову, которое получается из него перемещением всех степеней элемента $a$ влево, в то время как степени элементов $r$ и $f$ остаются в прежнем порядке; например, $farfr^2a^2f = a^3frfr^2f$. Таким образом, число элементов в группе $C_2 \times D_3$ равно произведению числа элементов в группе $C_2$ (2) на число элементов в группе $D_3$ (6).

**Упр. 21.** Из того что $a^2 = b^2$, мы заключаем, что $a = a^{-1}b^2$, $a = b^2a^{-1}$ и $ab^{-1} = a^{-1}b$. Из того что $a^2 = abab$, мы заключаем, что $a = bab$ и $ab^{-1} = ba$. Таким образом, $a^{-1}b = ba$. Следовательно,

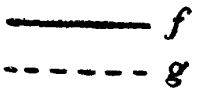
$$(ab)^2 = abab = (a^{-1}b^2)\, b\, (b^2a^{-1})\, b = a^{-1}b^5\, (a^{-1}b) =$$
$$= a^{-1}b^5\, (ba) = a^{-1}\, (a^6)\, a = a^6$$

(так как $a^2 = b^2$), и потому $a^2 = (ab)^2 = a^6$. Отсюда следует, что $a^4 = I$ и $b^4 = I$. Таким образом, наш граф содержит связанные четырехугольники, соответствующие соотношениям $a^4 = b^4 = I$. Это граф некоммутативной группы порядка 8, так называемой группы кватернионов, которую мы подробно рассматриваем в гл. 12:






**Упр. 22.**




(a) $D_\infty$

(b) Пусть $g$ обозначает элемент $rf$. Мы можем написать $f^2 = g^2 = I$, $r = gf^{-1} = gf$ и $r^{-1} = fg$. Таким образом, любое слово от $r$ и $f$ можно выразить через $f$ и $g$. Обратно, если $f^2 = g^2 = I$, то $f^2 = (rf)^2 = I$, и в любом слове от $f$ и $g$ мы можем заменить $g$ на $rf$ и прийти к слову только от $r$ и $f$.

**Упр. 23.** *Единица*: если $a$ принадлежит $H$, то $aa^{-1} = I$ принадлежит $H$,

*Обратимость:* если $b$ принадлежит $H$, то $Ib^{-1} = b^{-1}$ также принадлежит $H$.

*Замкнутость:* если $a$ и $b$ — элементы множества $H$, то $b^{-1}$ также принадлежит $H$, а потому и $a(b^{-1})^{-1} = ab$ принадлежит $H$.

**Упр. 24.** (a) *Замкнутость:* $I(ba) = (ba)I = ba$, $(ba)^2 = I$.
*Обратимость:* $(ba)^{-1} = ba$, так как $(ba)^2 = I$.
(b) $I$, $a$, $a^2$ (они образуют циклическую группу $C_3$).
(c) Подгрупп порядка 4 нет. Такая подгруппа должна была бы содержать самое меньшее по одному элементу из следующих двух множеств: $\{a, a^2\}$ и $\{b, ba, ba^2\}$. Но любая пара, в которую входит один элемент из первого множества и один элемент из второго множества, порождает всю группу.

**Упр. 25.** Элементы группы $C_5$: $a$, $a^2$, $a^3$, $a^4$, $a^5 = I$. Порядок элемента $a$ равен 5, а порядок любого элемента $a^k \neq I$ группы $C_5$ *не превосходит* 5, так как при $k = 2$, 3 и 4 $(a^k)^5 = (a^5)^k = I$. Если допустить, что порядок элемента $a^k$ $(1 < k < 5)$ равен $n < 5$, то мы придем к противоречию: $(a^k)^n = a^{kn} = I$, где $kn$ не кратно 5. Таким образом, порядок каждого элемента группы $C_5$ (кроме $I$) равен 5. Отсюда следует, что любая подгруппа группы $C_5$, в которую входит $x \neq I$, содержит пять различных элементов и не может быть собственной подгруппой.

**Упр. 26.** (a) *Замкнутость:* $3m + 3n = 3(m + n)$.
*Обратимость:* $3m + (-3m) = 0$.
(b) *Замкнутость:* $jn + kn = (j + k)n$.
*Обратимость:* $kn + (-kn) = 0$.

**Упр. 27.** Обозначим через $R \cap S$ множество общих элементов групп $R$ и $S$.

*Замкнутость:* Пусть $t_1$ и $t_2$ принадлежат $R \cap S$. Это означает, что $t_1$ и $t_2$ являются элементами как $R$, так и $S$. Поскольку $R$ и $S$ — группы, элемент $t_1t_2$ принадлежит как $R$, так и $S$, а потому и $R \cap S$.

*Обратимость:* Если $t$ принадлежит $R \cap S$, то $t$ и, следовательно, $t^{-1}$ являются элементами как группы $R$, так и группы $S$. Таким образом, $t^{-1}$ принадлежит $R \cap S$.

**Упр. 28.** (a) Сложение является ассоциативной бинарной операцией на нашем множестве, поскольку $(a + ib) + (x + iy) = (a + x) + i(b + y)$, и если $a$, $b$, $x$, $y$ — целые, то $a + x$ и $b + y$ — также целые числа.
*Единица:* $(a + ib) + 0 = a + ib = 0 + (a + ib)$.
*Обратные:* $(a + ib) + (-a - ib) = 0$.
(b) *Замкнутость:* $(r + is) + (x + iy) = (r + x) + i(s + y)$, числа $r + x$ и $s + y$ оба четны, если четны $r$, $s$, $x$, $y$.
*Обратимость:* $(r + is) + (-r - is) = 0$.

**Упр. 29.** Предположим, что смежные классы $rH$ и $sH$ имеют хотя бы один общий элемент, скажем $rh_1 = sh_2$. Тогда $s^{-1}r = h_2h_1^{-1}$ является элементом группы $H$ и $s^{-1}rh = h_2h_1^{-1}h$ пробегает множество всех элементов подгруппы $H$, когда $h$ последова-

тельно пробегает это множество. Следовательно, из очевидного равенства $s(s^{-1}rh) = s(h_2h_1^{-1}h)$, или $rh = s(h_2h_1^{-1}h)$, вытекает, что $rH = sH$. Таким образом, если два смежных класса имеют хотя бы один общий элемент, то они совпадают.

**Упр. 30.** (a) Пусть $rJ$ — смежный класс, $rJ = \{rj_1, rj_2, \ldots\}$. Пусть $c = rj_k$ (т. е. $c$ принадлежит смежному классу $rJ$). Тогда смежный класс $cJ$ можно записать так: $cJ = (rj_k)J = \{r(j_kj_1), r(j_kj_2), \ldots\}$. Но $j_kj_1, j_kj_2, \ldots$ — это все элементы подгруппы $J$, только в другом порядке. Таким образом, $cJ = rJ$, как и утверждалось.

(b) Если $r^{-1}c$ принадлежит $J$, то мы можем записать, что $r^{-1}c = j_k$, где $j_k$ — некоторый элемент группы $J$. Умножая это равенство слева на $r$, получаем $c = rj_k$, а это показывает, что $c$ принадлежит смежному классу $rJ$. Таким образом, смежные классы $cJ$ и $rJ$ совпадают.

Предположим теперь, что смежные классы $cJ$ и $rJ$ совпадают. Тогда произвольный элемент $cj_k$ из $cJ$ равен некоторому элементу $rj_n$ из $rJ$, т. е. $cj_k = rj_n$, где $j_k$ и $j_n$ — элементы подгруппы $J$. Умножая это равенство слева на $r^{-1}$ и справа на $j_k^{-1}$, мы получаем, что $r^{-1}cj_k = j_n$, $r^{-1}c = j_nj_k^{-1}$. Так как $j_k$ и $j_n$ принадлежат подгруппе $J$, то ей принадлежат и $j_k^{-1}$ и $j_nj_k^{-1} = r^{-1}c$.

**Упр. 31.** Доказательство может быть основано на такой идее: показать, что если $xJ$ и $yJ$ — два различных левых смежных класса группы $L$, то $Jx^{-1}$ и $Jy^{-1}$ — два различных правых смежных класса. Или в противоположной формулировке: если $Jx^{-1}$ и $Jy^{-1}$ совпадают, то $xJ$ и $yJ$ тоже совпадают. Чтобы убедиться в этом, предположим, что некоторый элемент из смежного класса $Jx^{-1}$ равен некоторому элементу из $Jy^{-1}$, скажем $j_1x^{-1} = j_2y^{-1}$. Тогда $x^{-1} = j_1^{-1}j_2y^{-1}$ и $x = yj_2^{-1}j_1 = y(j_2^{-1}j_1)$ является элементом смежного класса $yJ$. Таким образом, если совпадают смежные классы $Jx^{-1}$ и $Jy^{-1}$, то левые смежные классы $xJ$ и $yJ$ имеют общий элемент $x$ и, следовательно, также совпадают, так как никакие два различных смежных класса не имеют общих элементов. Поэтому и соответствующие правые смежные классы различны.

**Упр. 32.** Левые смежные классы:

$$K = \{I, a, a^2\} \quad \text{и} \quad bK = \{b, ba, ba^2\}.$$

Правые смежные классы:

$$K = \{I, a, a^2\} \quad \text{и} \quad Kb = \{b, ab, a^2b\}.$$

Так как $(ba)^2 = baba = I$, то $ba = a^{-1}b^{-1} = a^2b$. Аналогично $ab = ba^2$. Таким образом, левые и правые смежные классы совпадают.

**Упр. 33.** (a) *Замкнутость.* Для любых двух элементов из $H$ справедливо равенство $a^ja^k = a^{j+k}$. Так как $j + k = nq + r$, где

$q$ и $r$ — целые числа, такие, что $0 \leqslant r < n$, то $a^{j+k} = (a^n)^q a^r = a^r$ является элементом из $H$.

*Обратимость.* Если элемент $a^j$ принадлежит $H$, то $a^{n-j}$ также принадлежит $H$ и $a^j a^{n-j} = a^n = I$.

(b) Если $g$ — порядок группы $G$, а $n$ — порядок некоторого элемента этой группы, то по теореме Лагранжа и по п. (a) $g$ кратно $n$. Иными словами, порядок элемента конечной группы является делителем порядка группы.

**Упр. 34.** (a) Так как $g$ — элемент порядка $n$ и 1 есть единичный элемент группы «остатков», то $g^n \equiv 1 \pmod p$, или $g^n - 1 \equiv 0 \pmod p$.

(b) Так как $n$ — порядок элемента $g$, то число $p - 1$ должно быть кратно $n$ (см. упр. 33b), скажем $p - 1 = kn$. Тогда поскольку $g^n \equiv 1 \pmod p$, то обязательно $(g^n)^k \equiv 1 \pmod p$, т. е. $g^{p-1} - 1 \equiv 0 \pmod p$, или $g^{p-1} - 1$ кратно $p$.

**Упр. 35.** Так как $a$ не кратно $p$, то $a \not\equiv 0 \pmod p$; следовательно, $a \equiv r \pmod p$, где $r$ — одно из чисел 1, 2, ..., $p - 1$, и, значит, $a - r \equiv 0 \pmod p$. Рассмотрим теперь

$$a^{p-1} - r^{p-1} = (a - r)(a^{p-2} + a^{p-3}r + \ldots + r^{p-2}).$$

Так как $a - r \equiv 0 \pmod p$, то $a^{p-1} - r^{p-1} \equiv 0 \pmod p$ (по модулю простого числа $ab \equiv 0$ тогда и только тогда, когда или $a \equiv 0$, или $b \equiv 0$), т. е.

$$(a^{p-1} - 1) - (r^{p-1} - 1) \equiv 0 \pmod p.$$

Из упр. 34b мы знаем, что $r^{p-1} - 1 \equiv 0 \pmod p$. Таким образом, мы приходим к выводу, что $a^{p-1} - 1 \equiv 0 \pmod p$. Следовательно, $a^p - a = a(a^{p-1} - 1) \equiv 0 \pmod p$. Это доказывает теорему Ферма.

**Упр. 36.** (a) Пусть $x$ — порядок элемента $ab$, а $y$ — порядок элемента $ba$. Можно записать $(ab)^x = a(ba)^{x-1}b = I$. Тогда, умножив это равенство слева на $a^{-1}$ и справа на $b^{-1}$, получим $(ba)^{x-1} = a^{-1}b^{-1} = (ba)^{-1}$. С другой стороны, $(ba)^{x-1} = (ba)^x (ba)^{-1}$; отсюда следует, что $(ba)^x = I$. Так как $y$ есть порядок элемента $ba$, то $x = ky$, где $k$ — положительное целое число [1]). Применив то же рассуждение к $(ba)^y$, приходим к выводу, что $y = lx$, где $l$ — положительное целое число. Следовательно, $x = y$.

(b) Пусть $m$ — порядок элемента $a$, а $n$ — порядок элемента $b$. Мы должны показать, что $(ab)^{mn} = I$, поскольку из этого будет следовать, что $mn$ кратно порядку элемента $ab$. Так как $ab = ba$, то мы можем менять $a$ и $b$ местами в любом произведении вида $(ab)^k$. Таким образом, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n \cdot (b^n)^m = I \cdot I = I$.

(c) Предположим, что порядок элемента $ab$ равен $r$. Из п. (b) мы знаем, что $r$ является делителем числа $mn$ и, следовательно, должно иметь вид $m_1 n_1$, где $m_1$ — делитель $m$, а $n_1$ — делитель $n$

---

[1]) См. примечание на стр. 229. — *Прим. перев.*

(допускается, что $m_1 = 1$ или $m_1 = m$, а также что $n_1 = 1$ или $n_1 = n$). Тогда

$$I = (ab)^r = (ab)^{r\,(m/m_1)} = (ab)^{m\,(r/m_1)} = (ab)^{mn_1} = a^{mn_1} \cdot b^{mn_1} = b^{mn_1},$$

поскольку $a^m = I$. Из равенства $b^{mn_1} = I$ следует, что $mn_1$ кратно $n$, скажем $mn_1 = kn$. Тогда $m = k(n/n_1)$, т. е. все простые делители числа $m$ должны находиться среди простых делителей чисел $k$ и $n/n_1$. Но поскольку $m$ и $n$ взаимно просты, то $m$ и $n/n_1$ взаимно просты. Следовательно, простые делители числа $m$ в точности совпадают с простыми делителями числа $k$, а $n/n_1 = 1$ или $n = n_1$. Аналогично, используя соотношения $I = (ab)^{r(n/n_1)} = a^{m_1 n}$, мы убеждаемся, что $m = m_1$. Таким образом, $r = m_1 n_1 = mn$, как и утверждалось.

**Упр. 37.** Мы доказываем противоположное утверждение. Если отображение $f$ гомоморфно, то $f(I) = I$. Для любого элемента $r$ группы $G$ имеем $f(r) = f(Ir) = f(I)f(r)$. Умножая справа на $[f(r)]^{-1}$, получаем, что $I = f(I)$ в группе $H$.

**Упр. 38.** Имеем $I = f(I) = f(xx^{-1}) = f(x)f(x^{-1})$, или $I = f(x)f(x^{-1})$. Умножая слева на $[f(x)]^{-1}$, получаем, что $[f(x)]^{-1} = f(x^{-1})$.

**Упр. 39.** $f(xy^{-1}) = f(x)\,f(y^{-1}) =$

$= f(x)\,[f(y)]^{-1}$ (в силу упр. 38) $=$

$= f(y)\,[f(y)]^{-1}$ (так как $f(x) = f(y)$) $=$

$= I.$

Аналогично $f(x^{-1}y) = I$.

**Упр. 40.** (a) $f(xy) = f(x)f(y) = I \cdot I = I$.

(b) По предположению $f(xy) = f(x)f(y) = I$. Тогда $f(y) = [f(x)]^{-1}$ и, таким образом, $f(yx) = f(y)f(x) = [f(x)]^{-1}f(x) = I$.

**Упр. 41.** Мы покажем, что отображение $f$, которое сопоставляет каждому целому числу $n$ из $G$ число $2n$, обладает всеми нужными свойствами. При этом отображении $f(n) = 2n$, или $n \to 2n$,

$$f(m + n) = 2(m + n) = 2m + 2n = f(m) + f(n).$$

Кроме того, $f(m) = f(n)$ означает, что $2m = 2n$, а это последнее равенство выполняется тогда и только тогда, когда $m = n$. (Может ли существовать изоморфизм *конечной* группы на ее собственную подгруппу?)

**Упр. 42.** Любой элемент группы $G$ можно представить в виде $r^k$, $k = 0, \pm 1, \pm 2, \ldots$, а любой элемент из $H$ — в виде $r^{kn}$, $k = 0, \pm 1, \pm 2, \ldots$. Определим отображение $f$ формулой $f(x) = x^n$, или $x \to x^n$, где $x$ — произвольный элемент группы $G$,

# ОГЛАВЛЕНИЕ